UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/361,748	07/28/2023	ÚLFAR ERLINGSSON	FORT-055521	4323

182115 7590 10/22/2024

Lacework, Inc.
c/o Kennedy Lenart Spraggins LLP
797 Sam Bass Road #2559
ROUND ROCK, TX 78681

EXAMINER	
BOUTAH, ALINA A	

ART UNIT	PAPER NUMBER
2442	

NOTIFICATION DATE	DELIVERY MODE
10/22/2024	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

april.piepenburg@jwhdlaw.com
eofficeaction@appcoll.com
mike.desanctis@jwhdlaw.com

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00001

APPLICATION NO.	ISSUE DATE	PATENT NO.
18/361,748	22-Oct-2024	12126695

Lacework, Inc.
c/o Kennedy Lenart Spraggins LLP
797 Sam Bass Road #2559
ROUND ROCK, TX 78681

EGRANT NOTIFICATION

Your electronic patent grant (eGrant) is now available, which can be accessed via Patent Center at https://patentcenter.uspto.gov

The electronic patent grant is the official patent grant under 35 U.S.C. 153. For more information, please visit https://www.uspto.gov/electronicgrants

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00002

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/361,748	10/22/2024	12126695	L0041B1CIP2C1	4323

182115 7590 10/02/2024

Lacework, Inc.
c/o Kennedy Lenart Spraggins LLP
797 Sam Bass Road #2559
ROUND ROCK, TX 78681

ISSUE NOTIFICATION

The projected patent number and issue date are specified above. The patent will issue electronically. The electronically issued patent is the official patent grant pursuant to 35 U.S.C. § 153. The patent may be accessed on or after the issue date through Patent Center at https://patentcenter.uspto.gov/. The patent will be available in both the public and the private sides of Patent Center. Further assistance in electronically accessing the patent, or about Patent Center, is available by calling the Patent Electronic Business Center at 1-888-217-9197.

The USPTO is implementing electronic patent issuance with a transition period, during which period the USPTO will mail a ceremonial paper copy of the electronic patent grant to the correspondence address of record. Additional copies of the patent (i.e., certified and presentation copies) may be ordered for a fee from the USPTO's Certified Copy Center at https://certifiedcopycenter.uspto.gov/index.html. The Certified Copy Center may be reached at (800)972-6382.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Center (https://patentcenter.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Patents Stakeholder Experience (OPSE), Stakeholder Support Division (SSD) at (571)-272-4200.

INVENTOR(s) (Please see PATENT CENTER site https://patentcenter.uspto.gov for additional inventors):

ÚLFAR ERLINGSSON, PALO ALTO, CA;
YIJOU CHEN, CUPERTINO, CA;

APPLICANT(s) (Please see PATENT CENTER site https://patentcenter.uspto.gov for additional applicants):

LACEWORK, INC., MOUNTAIN VIEW, CA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00004

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	89	20220376970	A1	2022-11-24	Chawathe et al.	
Change(s) applied to document. /A.C./ 7/18/2024	90	20220382611	A1	~~2023-01-03~~ 12/2022	Kapish et al.	
	91	20220394082	A1	2022-12-08	Keren et al.	
	92	20220414072	A1	2022-12-29	Tandon et al.	
	93	20220414105	A1	2022-12-29	Umay et al.	
	94	20230025252	A1	2023-01-26	Erickson et al.	
	95	20230039566	A1	2023-02-09	Ghag et al.	
	96	20230052827	A1	2023-02-16	Araujo et al.	
	97	20230088960	A1	2023-03-23	Popelka et al.	
	98	20230096930	A1	2023-03-30	Dasdan	
	99	20230101773	A1	2023-03-30	Katahanas et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

Change(s) applied to document /A.C./ 7/18/2024	78	20220058193	A1	~~2023-09-12~~ 02/2022	Smith Shawn et al.	
	79	20220067186	A1	2022-03-03	Thakur et al.	
	80	20220086179	A1	~~2023-05-09~~ 03/2022	Levin et al.	
	81	20220092481	A1	2022-03-24	Neithalath et al.	
	82	20220121741	A1	~~2023-09-05~~ 04/2022	Araujo et al.	
	83	20220124108	A1	2022-04-21	Gamble et al.	
	84	20220129803	A1	2022-04-28	Bikumala et al.	
	85	20220191226	A1	2022-06-16	Chan et al.	
	86	20220327119	A1	2022-10-13	Gasper et al.	
	87	20220350789	A1	~~2023-05-02~~ 11/2022	Yang et al.	
	88	20220374800	A1	~~2023-09-26~~ 11/2022	Adinarayan et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

Change(s) applied to document, /A.C./ 7/18/2024	34	20170102961	A1	~~2020-01-14~~ 04/2017	Hilemon et al.	
	35	20170118099	A1	2017-04-27	HUANG	
	36	20170142140	A1	2017-05-18	Muddu et al.	
	37	20170148197	A1	2017-05-25	Winternitz et al.	
	38	20170155570	A1	2017-06-01	Maheshwari et al.	
	39	20170155672	A1	2017-06-01	Muthukrishnan et al.	
	40	20170223036	A1	2017-08-03	Muddu et al.	
	41	20170346683	A1	~~2018-05-29~~ 11/2017	Li et al.	
	42	20180004835	A1	2018-01-04	Piechowicz et al.	
	43	20180004859	A1	~~2020-08-30~~ 01/2018	Piechowicz et al.	
	44	20180007145	A1	~~2018-10-29~~ 01/2018	Piechowicz et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

Change(s) applied to document, /A.C./ 7/18/2024

	23	20140125672	A1	~~2015-07-07~~ 05/2014	Winternitz et al.	
	24	20140279779	A1	~~2017-08-13~~ 09/2014	Zou et al.	
	25	20150310649	A1	~~2017-03-21~~ 10/2015	Winternitz et al.	
	26	20160120070	A1	2016-04-28	Myrah et al.	
	27	20160357521	A1	~~2019-07-02~~ 12/2016	Zhang et al.	
	28	20170063888	A1	2017-03-02	Muddu et al.	
	29	20170063903	A1	2017-03-02	Muddu et al.	
	30	20170063905	A1	2017-03-02	Muddu et al.	
	31	20170063909	A1	2017-03-02	Muddu et al.	
	32	20170063911	A1	2017-03-02	Muddu et al.	
	33	20170070594	A1	~~2019-11-26~~ 03/2017	Oetting et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

Change(s) applied to document, /A.C./ 7/18/2024

	12	20090063857	A1	~~2010-04-27~~ 03/2009	Bade et al.	
	13	20090307651	A1	2009-12-10	Senthil et al.	
	14	20090327328	A1	~~2015-08-18~~ 12/2009	Woodall et al.	
	15	20100042823	A1	~~2011-08-09~~ 02/2010	Arndt et al.	
	16	20110119100	A1	2011-05-19	Ruhl et al.	
	17	20110154287	A1	2011-06-23	Mukkamala et al.	
	18	20120143898	A1	2012-06-07	Bruno et al.	
	19	20120159333	A1	2012-06-21	Mital et al.	
	20	20130024412	A1	2013-01-24	Gong et al.	
	21	20130151453	A1	2013-06-13	Bhanot et al.	
	22	20140067750	A1	~~2015-05-26~~ 03/2014	Ranganathan et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

Change(s) applied to document, /A.C./ 7/18/2024	1	20040225929	A1	~~2007-01-23~~ 11/2004	Agha et al.	
	2	20050246521	A1	~~2009-01-27~~ 11/2005	Bade et al.	
	3	20060025987	A1	2006-02-02	Baisley et al.	
	4	20060026419	A1	~~2009-01-13~~ 02/2006	Arndt et al.	
	5	20060109271	A1	~~2007-08-19~~ 05/2006	Lomask	
	6	20070214111	A1	~~2017-08-08~~ 09/2007	Jin et al.	
	7	20070282916	A1	2007-12-06	Albahari et al.	
	8	20080109730	A1	2008-05-08	Coffman et al.	
	9	20080147707	A1	~~2012-04-17~~ 06/2008	Jin et al.	
	10	20090006843	A1	~~2011-12-27~~ 01/2009	Bade et al.	
	11	20090007010	A1	2009-01-01	Kriss et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	147	20180034840	A1	2018-02-01	Marquardt et al.	
	148	20180039688	A1	2018-02-08	Ahn et al.	
	149	20180063178	A1	2018-03-01	Jadhav et al.	
	150	20180067981	A1	2018-03-08	Ahuja et al.	
	151	20180069885	A1	2018-03-08	Patterson et al.	
Change(s) applied to document, /A.C./ 7/18/2024	152	20180084069	A1	2018-03-22	~~Be'ery et al.~~ Be'ery et al.	
	153	20180096047	A1	2018-04-05	Childress et al.	
	154	20180097793	A1	2018-04-05	Agarwal et al.	
	155	20180103052	A1	2018-04-12	Choudhury et al.	
	156	20180115578	A1	2018-04-26	Subbarayan et al.	
	157	20180123864	A1	2018-05-03	Tucker et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via the USPTO patent electronic filing system.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

182115 7590 06/12/2024

Lacework, Inc.
c/o Kennedy Lenart Spraggins LLP
797 Sam Bass Road #2559
ROUND ROCK, TX 78681

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via the USPTO patent electronic filing system or by facsimile to (571) 273-2885, on the date below.

April Piepenburg	(Typed or printed name)
/April Piepenburg/	(Signature)
9/11/24	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/361,748	07/28/2023	ÚLFAR ERLINGSSON	L0041B1CIP2C1	4323

TITLE OF INVENTION: Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1200	$0.00	$0.00	$1200	09/12/2024

EXAMINER	ART UNIT	CLASS-SUBCLASS
BOUTAH, ALINA A	2442	709-224000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Jaffery Watson Hamilton & DeSanctis LLP
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Fortinet, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Sunnyvale, CA

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☒ Issue Fee ☐ Publication Fee (if required)

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

☒ Electronic Payment via the USPTO patent electronic filing system ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 60-6522

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

☐ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Michael A. DeSanctis/ Date 9/11/24

Typed or printed name Michael A. DeSanctis Registration No. 39,957

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00012

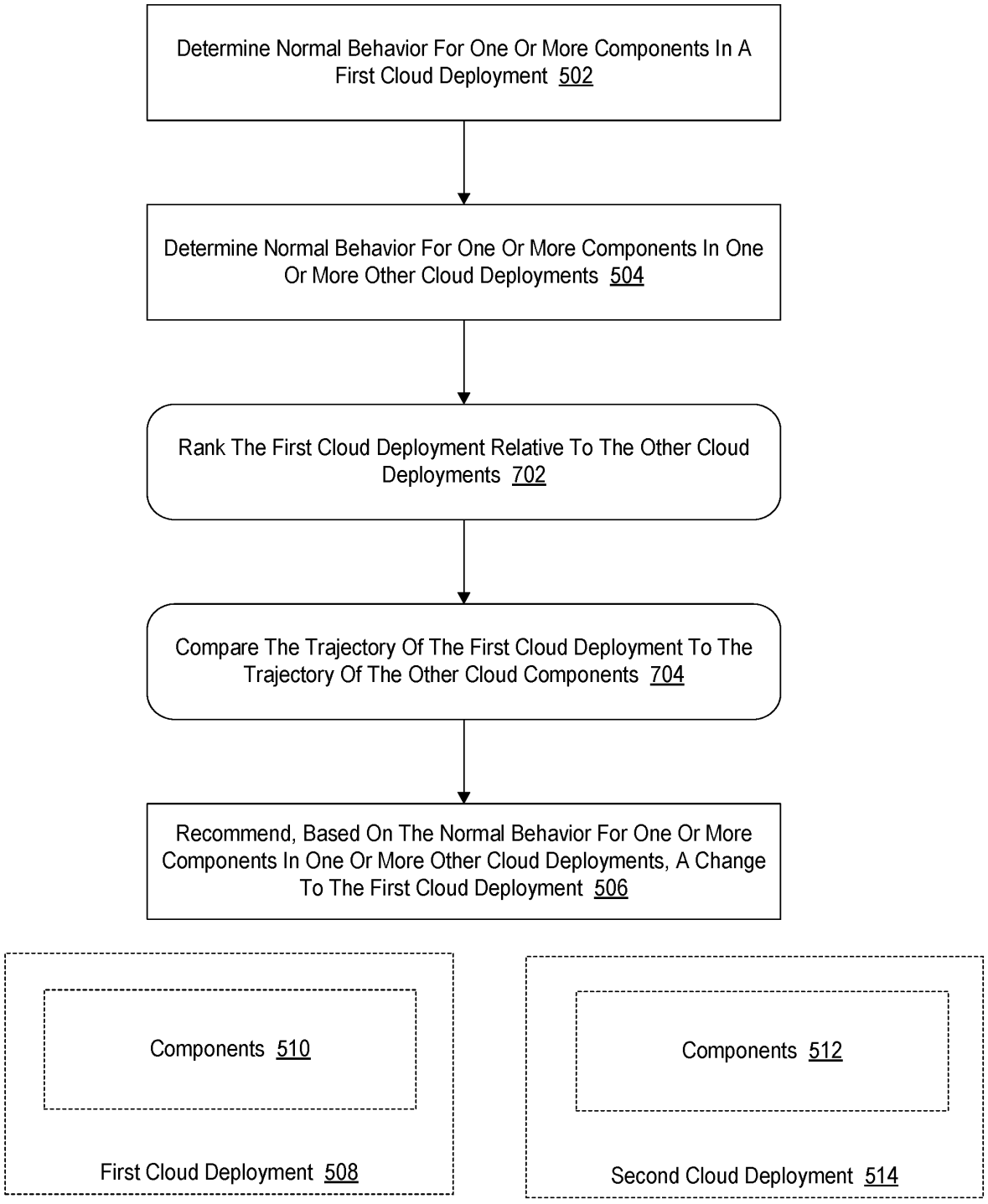

Determine Normal Behavior For One Or More Components In A First Cloud Deployment 502
Determine Normal Behavior For One Or More Components In One Or More Other Cloud Deployments 504
Rank The First Cloud Deployment Relative To The Other Cloud Deployments 702
Compare The Trajectory Of The First Cloud Deployment To The Trajectory Of The Other Cloud Components 704
Recommend, Based On The Normal Behavior For One Or More Components In One Or More Other Cloud Deployments, A Change To The First Cloud Deployment 506
Components 510
First Cloud Deployment 508
Components 512
Second Cloud Deployment 514

Fig. 5 7

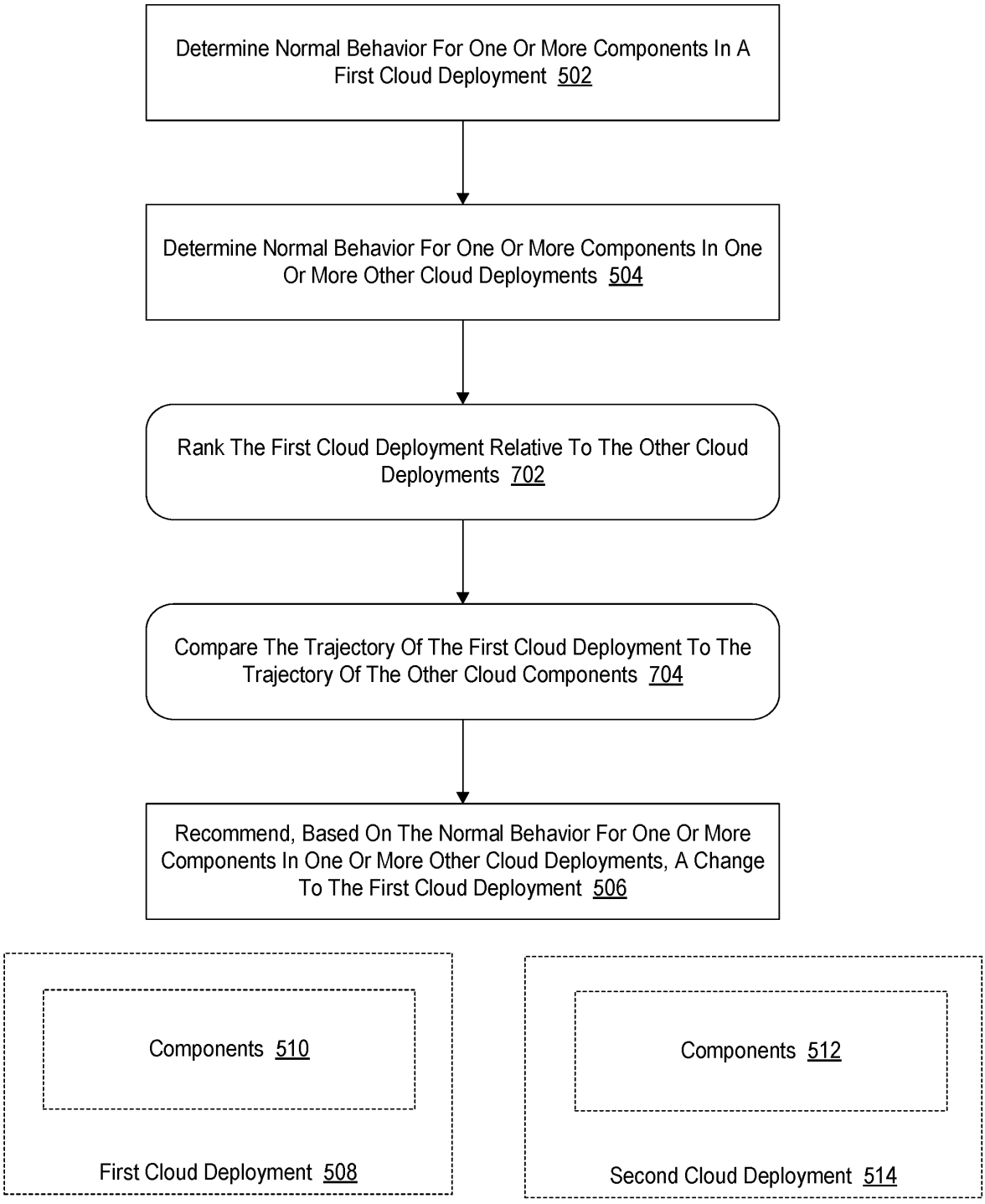

Determine Normal Behavior For One Or More Components In A First Cloud Deployment 502
Determine Normal Behavior For One Or More Components In One Or More Other Cloud Deployments 504
Rank The First Cloud Deployment Relative To The Other Cloud Deployments 702
Compare The Trajectory Of The First Cloud Deployment To The Trajectory Of The Other Cloud Components 704
Recommend, Based On The Normal Behavior For One Or More Components In One Or More Other Cloud Deployments, A Change To The First Cloud Deployment 506
Components 510
First Cloud Deployment 508
Components 512
Second Cloud Deployment 514

Fig. 7

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/361,748	**09/11/2024 12:39:14 PM Z ET**	**L0041B1CIP2C1**

Title of Invention

Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4323	FILED BY	April Piepenburg
PATENT CENTER #	67129902	FILING DATE	07/28/2023
CUSTOMER #	182115	FIRST NAMED INVENTOR	ÚLFAR ERLINGSSON
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Michael DeSanctis

Documents

TOTAL DOCUMENTS: 4

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
FORT-055521 ISSUE FEE.pdf	1	Issue Fee Payment (PTO-85B)	183 KB
FORT-055521 Response to CAP.pdf	4	Applicant Response to Pre-Exam Formalities Notice	26 KB
FORT-055521 Annotated_Sheet.pdf	1	Drawings-only black and white line drawings	495 KB
FORT-055521 Replacement_Sheet.pdf	1	Drawings-only black and white line drawings	502 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)

FORT-055521 ISSUE FEE.pdf	4DD4A84AA1920B193BF30829079DE3A2E368465C51C65893D B09CB5428CE6A01BCF4306D0824623467612BBC1083E9C3DA 4D84CF843652D5CEC6F30A9F6F1495
FORT-055521 Response to CAP.pdf	C460A936F80AA7484C1B4D658CAB25A401833EBB863CD5360 D4293BCB83ACFA6A0D0771BAF679AE5D5B056A603B05F2B6 C0E6A4452D10A3683269C9509AFD3D3
FORT-055521 Annotated_Sheet.pdf	C93B1D4D93A3590C28C2A946EAA68E0D2BD887B95568CE66 DD1E1221375DBC25BA6D8CB7101CF28A7A1D288555EB8699 6F2BC1FF5E4C91A3109220690B5B0AAB
FORT-055521 Replacement_Sheet.pdf	6A7A8E2A4C2D1166372E709CF2AA2DC6F8A1FD91FB9019ED 866DE75F607A113543B19994CAD14439E6F599FF1E28B8BFC 0DF84C0BCDEABD82377ACCD8A0D2711

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Erlingsson	Examiner: Boutah, Alina A.
Appl. No.:	18/361,748	Group Art Unit: 2442
Filed:	July 28, 2023	Docket No.: FORT-055521 (24256)
Title:	Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments	

RESPONSE TO NOTICE TO FILE CORRECTED APPLICATION PAPERS

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir or Madam:

In response to the Notice to File Corrected Application Papers mailed July 18, 2024 in the above identified patent application, the Applicant respectfully requests the Examiner to enter the following amendment and to consider the following remarks:

Amendments to the Drawings begin on page 2 of this paper.

Remarks begin on page 3 of this paper.

AMENDMENT

Amendments to the Drawings

The attached sheet of formal drawings replaces the previously submitted drawing for the second figure inadvertently mislabeled as FIG. 5 (which should have been labeled as FIG. 7). No new subject matter has been added by the submission of this replacement sheet of formal drawings.

Attachment: Replacement Sheet (1 page) and Annotated Sheet (1 page)

REMARKS

This communication is being submitted in response to the Notice to File Corrected Application Papers mailed July 18, 2024. A replacement sheet (and an annotated sheet illustrating the proposed changes) to the second figure marked as FIG. 5 is submitted herewith. It is believed that this Response is fully responsive to the Notice and corrects the items identified therein. No new matter is believed to have been introduced hereby.

Request for Approval to Amend Drawings Under 37 C.F.R. §1.121(d)

In the figures as originally filed, two figures were inadvertently numbered as FIG. 5. The second of these should have been numbered FIG. 7. The undersigned proposes renumbering the second FIG. 5 as FIG. 7 to conform the drawing to the specification.

Accordingly, the undersigned has included herewith a marked up original of the second FIG. 5 reflecting the proposed changes in the form of an "Annotated Sheet." No new matter has been added. The Examiner's approval is respectfully requested for the proposed changes to the second FIG. 5 to FIG. 7

CONCLUSION

If the Examiner believes that there are any unresolved issues in the application, it is requested that the Examiner telephone the undersigned at (833) 596-4529 x706 to expeditiously resolve such issues.

Respectfully submitted,

/Michael A. DeSanctis/

Date 9/11/24 By _____
Michael A. DeSanctis
Reg. No. 39,957

Jaffery Watson Hamilton & DeSanctis LLP
7501 Village Square, Suite 206
Castle Pines, CO 80108

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/361,748	**09/11/2024 12:39:14 PM Z ET**	**L0041B1CIP2C1**

Title of Invention

Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4323	FILED BY	April Piepenburg
PATENT CENTER #	67129902	AUTHORIZED BY	Michael DeSanctis
CUSTOMER #	182115	FILING DATE	07/28/2023
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	ÚLFAR ERLINGSSON

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 7716	**E20249AC39565460**	**Michael DeSanctis**

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
1501	UTILITY ISSUE FEE	1200.00	1	1200.00
			TOTAL AMOUNT:	**$1,200.00**

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

DocCode - SCORE

Placeholder Sheet for Supplemental Content

Application Number: 18361748 Document Date: 09/11/2024

The presence of this form indicates that the following document type was received in electronic format on the date identified above. This document is stored separately from the typical case contents which are stored in image format.

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded and no paper documents or physical media exist.

- Drawing

At the time of document entry (noted above):

- USPTO employees may access this supplemental content via Docket Application Viewer (DAV) or Supplemental Content Viewer (SCV).
- External customers may access this supplemental content via Patent Center.

Form Revision Date: March 1, 2024

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/361,748	07/28/2023	ÚLFAR ERLINGSSON	L0041B1CIP2C1	4323

182115 7590 07/18/2024

Lacework, Inc.
c/o Kennedy Lenart Spraggins LLP
797 Sam Bass Road #2559
ROUND ROCK, TX 78681

EXAMINER	
BOUTAH, ALINA A	

ART UNIT	PAPER NUMBER
2442	

NOTIFICATION DATE	DELIVERY MODE
07/18/2024	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

eofficeaction@appcoll.com
kate@klspatents.com
office@klspatents.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Application No. : 18361748
Applicant : Erlingsson
Filing Date : 07/28/2023
Date Mailed : 07/18/2024

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Notice of Allowance Mailed

This application has been accorded an Allowance Date and is being prepared for issuance. The application, however, is incomplete for the reasons below.

Applicant is given two (2) months from the mail date of this Notice within which to respond. This time period for reply is extendable under 37 CFR 1.136(a) for only TWO additional MONTHS.

The informalities requiring correction are indicated in the attachment(s). If the informality pertains to the abstract, specification (including claims) or drawings, the informality must be corrected with an amendment in compliance with 37 CFR 1.121 (or, if the application is a reissue application, 37 CFR 1.173). Such an amendment may be filed after payment of the issue fee if limited to correction of informalities noted herein. See Waiver of 37 CFR 1.312 for Documents Required by the Office of Patent Publication, 1280 Off. Gaz. Patent Office 918 (March 23, 2004). In addition, if the informality is not corrected until after payment of the issue fee, for purposes of 35 U.S.C. 154(b)(1)(iv), "all outstanding requirements" will be considered to have been satisfied when the informality has been corrected. A failure to respond within the above-identified time period will result in the application being ABANDONED.

See attachment(s).

A copy of this notice MUST be returned with the reply. Please address response to "Mail Stop Issue Fee, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450".

/Kevin Danemark/
Publication Branch
Office of Data Management
(571) 272-4200

Application No. 18361748 **Drawings filed: 07/28/2023**

IDENTIFICATION OF DRAWING DEFICIENCIES

- [ ] There is a hole or the image thereof within the illustration. FIG(s)
- [ ] The illustration is penetrated or traversed by a solid or broken line that is not intended to be part of the drawing, such as a dark line caused by a flaw in the copying process. FIG(s)
- [ ] An ink stamp or the image thereof obscures part of the illustration. FIG(s)
- [ ] The drawing is marred by black smudges, obliterations, or fax/copier marks (for example, speckles or dots in a substantial portion of the drawing). FIG(s)
- [X] Figure numbers are duplicated or missing. FIG(s) 5, 7
- [ ] Drawing sheet or figure is missing. FIG(s)
- [ ] Numbers, letters, or reference characters in the drawing have been crossed out or are illegibly handwritten. FIG(s)
- [ ] The character of the lines, numbers, and letters is poor. FIG(s)
- [ ] The drawing's background shows that the original drawing was made on graph paper or other paper with a pattern or decoration. FIG(s)
- [ ] The FIG. number label is placed in a location that causes the drawing to be read upside down. FIG(s)
- [ ] Data, a reference number, or part of the drawing is truncated or missing, or a lead line has no reference number. FIG(s)
- [ ] The drawing and/or the FIG. label contain(s) foreign language. FIG(s)
- [ ] This utility application contains a photograph of a view that is capable of being illustrated as a line drawing. FIG(s)
- [ ] A petition under 37 CFR 1.84(a)(2) to accept color drawings has been granted, but the brief description of the drawings in the specification does not contain (or has not been amended to contain) the paragraph required by 37 CFR 1.84(a)(2)(iii).
- [ ] This reissue application contains added and/or amended drawings that are not labeled as “New” or “Amended” or “Canceled” as required by 37 CFR 1.173(b)(3). FIG(s)
- [ ] This Design reissue application contains a drawing that is labeled as “Canceled” but is not surrounded by brackets, or a drawing that is surrounded by brackets but is not labeled as “Canceled.” See 37 CFR 1.173(b)(3). FIG(s)
- [ ] OTHER:
- [ ] COMMENTS:

Application No. 18361748

IDENTIFICATION OF SPECIFICATION/DRAWING INCONSISTENCIES

[X] On Page 3 of the specification there is a brief description of FIG. 7, but the drawings filed 07/28/2023 do not include a drawing with that designation. Applicant must respond either by supplying the omitted drawing or by amending the specification to remove all references to that drawing.

[ ] The drawings filed include FIG. , but the specification's brief description of the drawings does not describe a drawing with that designation. Applicant must respond either by amending the specification to add a brief description of that drawing or by correcting the drawings to remove the drawing in question.

[ ] In the utility application, drawings are present in the application and are referred to in the detailed description of the invention, but the specification does not contain a brief description of the several views as required by 37 CFR 1.74 and 37 CFR 1.77(b)(9).

[ ] The design application does not contain a description of the figure or figures of the drawing as required by 37 CFR 1.153(a) and 37 CFR 1.154(b)(4).

[ ] In the plant application, the specification does not contain a brief description of the drawing as required by 37 CFR 1.163(c)(8).

[ ] Page of the specification refers to FIG. , but no drawing with that designation is described in the brief description of the drawings and no drawing with that designation is present in the application. Applicant must respond either by amending the specification to remove all references to that drawing, or by supplying that drawing and amending the specification to add a brief description of it.

[ ] In the reissue application, FIG. , is labeled as "New" but is not described in the reissue specification's brief description of the drawings. Applicant must respond by amending the reissue specification's brief description of the drawings to add a brief description of the new drawing.

[ ] OTHER:

[ ] COMMENTS:

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

182115 7590 06/12/2024

Lacework, Inc.
c/o Kennedy Lenart Spraggins LLP
797 Sam Bass Road #2559
ROUND ROCK, TX 78681

EXAMINER
BOUTAH, ALINA A

ART UNIT	PAPER NUMBER
2442	

DATE MAILED: 06/12/2024

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/361,748	07/28/2023	ÚLFAR ERLINGSSON	L0041B1CIP2C1	4323

TITLE OF INVENTION: Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1200	$0.00	$0.00	$1200	09/12/2024

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via the USPTO patent electronic filing system.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

182115 7590 06/12/2024

Lacework, Inc.
c/o Kennedy Lenart Spraggins LLP
797 Sam Bass Road #2559
ROUND ROCK, TX 78681

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via the USPTO patent electronic filing system or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/361,748	07/28/2023	ÚLFAR ERLINGSSON	L0041B1CIP2C1	4323

TITLE OF INVENTION: Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1200	$0.00	$0.00	$1200	09/12/2024

EXAMINER	ART UNIT	CLASS-SUBCLASS
BOUTAH, ALINA A	2442	709-224000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1_____
2_____
3_____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑Issue Fee ❑Publication Fee (if required)

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via the USPTO patent electronic filing system ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29
NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

❑ Applicant asserting small entity status. See 37 CFR 1.27
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

❑ Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00029

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
18/361,748	07/28/2023	ÚLFAR ERLINGSSON	L0041B1CIP2C1	4323

182115 7590 06/12/2024

Lacework, Inc.
c/o Kennedy Lenart Spraggins LLP
797 Sam Bass Road #2559
ROUND ROCK, TX 78681

EXAMINER	
BOUTAH, ALINA A	

ART UNIT	PAPER NUMBER
2442	

DATE MAILED: 06/12/2024

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00030

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. The United States Patent and Trademark Office (USPTO) collects the information in this record under authority of 35 U.S.C. 2. The USPTO's system of records is used to manage all applicant and owner information including name, citizenship, residence, post office address, and other information with respect to inventors and their legal representatives pertaining to the applicant's/ owner's activities in connection with the invention for which a patent is sought or has been granted. The applicable Privacy Act System of Records Notice for the information collected in this form is COMMERCE/PAT-TM-7 Patent Application Files, available in the Federal Register at 78 FR 19243 (March 29, 2013).
https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf

Routine uses of the information in this record may include disclosure to:

1) law enforcement, in the event that the system of records indicates a violation or potential violation of law;
2) a federal, state, local, or international agency, in response to its request;
3) a contractor of the USPTO having need for the information in order to perform a contract;
4) the Department of Justice for determination of whether the Freedom of Information Act (FOIA) requires disclosure of the record;
5) a Member of Congress submitting a request involving an individual to whom the record pertains, when the individual has requested the Member's assistance with respect to the subject matter of the record;
6) a court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel in the course of settlement negotiations;
7) the Administrator, General Services Administration (GSA), or their designee, during an inspection of records conducted by GSA under authority of 44 U.S.C. 2904 and 2906, in accordance with the GSA regulations and any other relevant (i.e., GSA or Commerce) directive, where such disclosure shall not be used to make determinations about individuals;
8) another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c));
9) the Office of Personnel Management (OPM) for personnel research purposes; and
10) the Office of Management and Budget (OMB) for legislative coordination and clearance.

If you do not furnish the information requested on this form, the USPTO may not be able to process and/or examine your submission, which may result in termination of proceedings, abandonment of the application, and/or expiration of the patent.

Notice of Allowability	Application No. 18/361,748	Applicant(s) ERLINGSSON et al.	
	Examiner ALINA N BOUTAH	Art Unit 2442	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to 7/28/23.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 1-20 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some* c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☑ Notice of References Cited (PTO-892)
2. ☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☑ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☑ Examiner's Amendment/Comment
6. ☐ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/ALINA A BOUTAH/
Primary Examiner, Art Unit 2442

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00032

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Information Disclosure Statement

The IDS filed 7/31/2023, 12/07/2023, and 5/29/2024 have been considered.

Allowable Subject Matter

Claims 1-20 are allowed.

The closest prior art of record, Kirti et a al. (US 20170251013), teaches a security management system that discovers use of applications within a computing environment to manage access to applications for minimizing security threats. The system analyzes user activity across multiple clouds using machine learning to perform threat detection to provide recommendations concerning appropriate responses to the threats.

Similarly, Wolf et al. (US 2020/0259852), teaches receiving activity data, generating predictive model to detect deviations across platforms and facilitating remedial action to address the deviations.

Another prior art of record, Thampy (US 20190068627), teaches a cloud security system that learns patterns of user behavior and uses the patterns to detect anomalous behavior in a network.

However, in combination with every limitation in the claim, none of the prior art of record teaches identifying additional cloud deployments to utilize for cross-customer

learning, receiving information describing security threat, and setting used to combat the threat, and identifying configurations used to adopt the first cloud deployment.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ALINA N BOUTAH whose telephone number is (571)272-3908. The examiner can normally be reached M-F 7:00 AM - 3:00 PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Trost can be reached on 571-272-7872. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ALINA BOUTAH
Primary Examiner
Art Unit 2442

/ALINA A BOUTAH/
Primary Examiner, Art Unit 2442

Examiner-Initiated Interview Summary	**Application No.** 18/361,748	**Applicant(s)** ERLINGSSON et al.		
	Examiner ALINA N BOUTAH	**Art Unit** 2442	**AIA (First Inventor to File) Status** Yes	**Page** 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	**Title**	**Type**
ALINA N BOUTAH	Primary Examiner	Telephonic
JASON FLETCHER	Attorney of Record	

Date of Interview: 29 May 2024

Issues Discussed:

Non-statutory Double Patenting

Examiner requested a terminal disclaimer be filed to overcome any potential double patenting rejection over US Patent No. 11,785,104. Applicant agreed and a TD was filed accordingly.

/ALINA A BOUTAH/ Primary Examiner, Art Unit 2442	

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

Notice of References Cited	Application/Control No. 18/361,748	Applicant(s)/Patent Under Reexamination ERLINGSSON et al.	
	Examiner ALINA N BOUTAH	Art Unit 2442	Page 1 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Name	CPC Classification	US Classification
*	A	US-20220417273-A1	2022-12-29	Levin; Roy	H04L63/20	1/1
*	B	US-20220198322-A1	2022-06-23	Kuperman; Leonid	G06N20/00	1/1
*	C	US-20220092668-A1	2022-03-24	Lu; Cindy Han	G06N5/04	1/1
*	D	US-20210182248-A1	2021-06-17	JAYANTHI; Swaroop	G06F9/45558	1/1
*	E	US-20200336503-A1	2020-10-22	Xu; Brian H.	G06F11/076	1/1
*	F	US-20200259852-A1	2020-08-13	Wolff; Matt	H04L67/10	1/1
*	G	US-20200233961-A1	2020-07-23	Wolfin; Nadav	G06F11/3495	1/1
*	H	US-20200218579-A1	2020-07-09	D M; Vikas	G06F16/24578	1/1
*	I	US-20190123973-A1	2019-04-25	Jeuk; Sebastian	G06N20/00	1/1
*	J	US-20190068627-A1	2019-02-28	Thampy; Sajjit	H04L63/1425	1/1
*	K	US-20180124189-A1	2018-05-03	Edgington; Jeff	H04L41/5096	1/1
*	L	US-20170251013-A1	2017-08-31	Kirti; Ganesh	H04L63/1441	1/1
*	M	US-20160080204-A1	2016-03-17	MISHRA; Rajnish	H04L41/0853	709/220

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in YYYY-MM-DD format are publication dates. Classifications may be US or foreign.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00037

Notice of References Cited	Application/Control No. 18/361,748	Applicant(s)/Patent Under Reexamination ERLINGSSON et al.	
	Examiner ALINA N BOUTAH	Art Unit 2442	Page 2 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Name	CPC Classification	US Classification
*	A	US-20150319185-A1	2015-11-05	Kirti; Ganesh	H04L63/1416	726/23
*	B	US-20150302440-A1	2015-10-22	Monden; Jason Peter	G06Q30/0206	705/7.35
*	C	US-20150172321-A1	2015-06-18	Kirti; Ganesh	H04L63/1416	726/1
*	D	US-20140229607-A1	2014-08-14	Jung; Gueyoung	H04L43/08	709/224
*	E	US-11080392-B2	2021-08-03	Bennett; Juan Carlos	G06F21/566	1/1
*	F	US-10951648-B2	2021-03-16	Doron; Ehud	H04L63/1458	1/1
*	G	US-10009358-B1	2018-06-26	Xie; Yinglian	G06F21/552	1/1
*	H	US-20230306118-A1	2023-09-28	Rawat; Ambrish	G06F21/552	1/1
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in YYYY-MM-DD format are publication dates. Classifications may be US or foreign.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00038

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/361,748	ERLINGSSON et al.
	Examiner	**Art Unit**
	ALINA N BOUTAH	2442

CPC						
Symbol					**Type**	**Version**
H04L	/	67	/	535	F	2022-05-01
G06F	/	16	/	9024	I	2019-01-01
G06F	/	21	/	57	I	2013-01-01
H04L	/	63	/	10	I	2013-01-01
H04L	/	67	/	306	I	2013-01-01
G06F	/	16	/	9537	I	2019-01-01
G06F	/	9	/	455	I	2013-01-01
G06F	/	9	/	545	I	2013-01-01
G06F	/	16	/	9535	I	2019-01-01
G06F	/	16	/	9038	I	2019-01-01
G06F	/	16	/	2456	A	2019-01-01
H04L	/	41	/	08	A	2013-01-01

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	20	
/ALINA A BOUTAH/ Primary Examiner, Art Unit 2442	31 May 2024	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	12

U.S. Patent and Trademark Office — Part of Paper No.: 20240220

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00039

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/361,748	ERLINGSSON et al.
	Examiner	**Art Unit**
	ALINA N BOUTAH	2442

INTERNATIONAL CLASSIFICATION				
CLAIMED				
H04L	/	41	/	08
H04L	/	67	/	50

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	20	
/ALINA A BOUTAH/ Primary Examiner, Art Unit 2442	31 May 2024	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	12

U.S. Patent and Trademark Office — Part of Paper No.: 20240220

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00040

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/361,748	ERLINGSSON et al.
	Examiner	**Art Unit**
	ALINA N BOUTAH	2442

☑ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/ALINA A BOUTAH/ Primary Examiner, Art Unit 2442	31 May 2024	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	12

U.S. Patent and Trademark Office — Part of Paper No.: 20240220

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00041

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/361,748	ERLINGSSON et al.
	Examiner	Art Unit
	ALINA N BOUTAH	2442

CPC - Searched*		
Symbol	**Date**	**Examiner**
H04L67/535,306	05/28/2024	ANB
G06F9/455,545	05/28/2024	ANB
G06F16/9024,9038,9535,9537,2456	05/28/2024	ANB
G06F21/57	05/28/2024	ANB
H04L43/06	05/28/2024	ANB
H04L63/10,1425,1441,20,1416	05/28/2024	ANB
H04L41/08	05/28/2024	ANB

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00042

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/361,748	ERLINGSSON et al.
	Examiner	Art Unit
	ALINA N BOUTAH	2442

Search Notes		
Search Notes	**Date**	**Examiner**
inventor and assignee search	02/20/2024	ANB
Global dossier	02/20/2024	ANB
PE2E SEARCH	02/20/2024	ANB
STIC	05/30/2024	ANB
IEEE	05/31/2024	ANB
ACM	05/31/2024	ANB
IP.com	05/31/2024	ANB
SAFARI	05/31/2024	ANB
Google Patents	05/31/2024	ANB
Google scholar	05/31/2024	ANB
Google	05/31/2024	ANB
updated PE2E SEARCH	05/31/2024	ANB

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
H04L	67/535,306	05/31/2024	ANB
G06F	9/455,545	05/31/2024	ANB
G06F	16/9024,9038,9535,9537,2456	05/31/2024	ANB
G06F	21/57	05/31/2024	ANB
H04L	63/10,1425,1441,20,1416	05/31/2024	ANB
H04L	41/08	05/31/2024	ANB

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00043

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	18/361,748	ERLINGSSON et al.
	Examiner	**Art Unit**
	ALINA N BOUTAH	2442

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☑ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	05/31/2024								
	1	=								
	2	=								
	3	=								
	4	=								
	5	=								
	6	=								
	7	=								
	8	=								
	9	=								
	10	=								
	11	=								
	12	=								
	13	=								
	14	=								
	15	=								
	16	=								
	17	=								
	18	=								
	19	=								
	20	=								

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00044

IEEE.org IEEE Xplore IEEE SA IEEE Spectrum More Sites Donate Cart Create Account Personal Sign In

Browse My Settings Help Access provided by: United States Patent and Trademark Office Sign Out

Access provided by: United States Patent and Trademark Office Sign Out

All ADVANCED SEARCH

Search within results Download PDFs Items Per Page Export Alert Set Search Alerts Search History

Showing 1-25 of 248 results for cloud deploy* learn* threat* ×

Conferences (169) Journals (55) Magazines (12) Books (11)

Early Access Articles (1)

Filter Alert Set Search Alerts Sort Relevance Sort

Search

Documents Images(Beta)

Show

All Results

Subscribed Content

Open Access Only

Year

Range Single Year

2009 2024

Clear Apply

Author

Affiliation

Sign In to Save Your Search

Get notified when new research is published matching your search criteria.

* Email Address

* Password

Sign In

Forgot Password? | Create Account

Network Security with Network Intrusion Detection System using Machine Learning Deployed in a Cloud Infrastructure

C. Kaushik; T. Ram; C Ritvik; T. Lakshman

2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC)

Year: 2022 | Conference Paper | Publisher: IEEE

Cited by: Papers (5)

Abstract HTML

Network Security with Network Intrusion Detection System using Machine Learning Deployed in a Cloud Infrastructure

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising purposes. Privacy Policy

Accept

Deny

Conference Location

Publication Topics

Sushila Kumari; Kamna Solanki; Sandeep Dalal; Amita Dhankhar
2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)
Year: 2022 | Conference Paper | Publisher: IEEE

Abstract HTML

Analysis Of Cloud Computing Security Threats and Countermeasures

Sushila Kumari; Kamna Solanki; Sandeep Dalal; Amita Dhankhar
2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)
Year: 2022 | Conference Paper | Publisher: IEEE

Machine Learning Approach for Cloud Computing Security
Garima; Suhail Javed Quraishi
2022 3rd International Conference on Intelligent Engineering and Management (ICIEM)
Year: 2022 | Conference Paper | Publisher: IEEE
Cited by: Papers (2)

Abstract HTML

Machine Learning Approach for Cloud Computing Security

Garima; Suhail Javed Quraishi
2022 3rd International Conference on Intelligent Engineering and Management (ICIEM)
Year: 2022 | Conference Paper | Publisher: IEEE

Detecting SQL Injection Attacks in Cloud SaaS using Machine Learning
Dharitri Tripathy; Rudrarajsinh Gohil; Talal Halabi
2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)
Year: 2020 | Conference Paper | Publisher: IEEE
Cited by: Papers (18)

Abstract HTML

Detecting SQL Injection Attacks in Cloud SaaS using Machine Learning

Dharitri Tripathy; Rudrarajsinh Gohil; Talal Halabi
2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)
Year: 2020 | Conference Paper | Publisher: IEEE

Detection of Various Security Threats in IoT and Cloud Computing using Machine Learning
T Antony Joseph; N. Jayapandian
2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)
Year: 2022 | Conference Paper | Publisher: IEEE
Cited by: Papers (4)

Abstract HTML

Detection of Various Security Threats in IoT and Cloud Computing using Machine Learning

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising purposes. Privacy Policy

Wangyan Feng; Wenfeng Yan; Shuning Wu; Ningwei Liu
2017 IEEE International Conference on Intelligence and Security Informatics (ISI)
Year: 2017 | Conference Paper | Publisher: IEEE
Cited by: Papers (8)

Abstract HTML

Wavelet transform and unsupervised machine learning to detect insider threat on cloud file-sharing

Wangyan Feng; Wenfeng Yan; Shuning Wu; Ningwei Liu
2017 IEEE International Conference on Intelligence and Security Informatics (ISI)
Year: 2017 | Conference Paper | Publisher: IEEE

Multi-Agent Deep Reinforcement Learning Framework for Renewable Energy-Aware Workflow Scheduling on Distributed Cloud Data Centers
Amanda Jayanetti; Saman Halgamuge; Rajkumar Buyya
IEEE Transactions on Parallel and Distributed Systems
Year: 2024 | Volume: 35, Issue: 4 | Journal Article | Publisher: IEEE

Abstract HTML

Multi-Agent Deep Reinforcement Learning Framework for Renewable Energy-Aware Workflow Scheduling on Distributed Cloud Data Centers

Amanda Jayanetti; Saman Halgamuge; Rajkumar Buyya
IEEE Transactions on Parallel and Distributed Systems
Year: 2024 | Volume: 35, Issue: 4 | Journal Article | Publisher: IEEE

A Network Attack Blocking Scheme based on Threat Intelligence
Kun Li; Rui Wang; Haiwei Li; Yan Hao
2021 6th International Conference on Intelligent Computing and Signal Processing (ICSP)
Year: 2021 | Conference Paper | Publisher: IEEE

Abstract HTML

A Network Attack Blocking Scheme based on Threat Intelligence

Kun Li; Rui Wang; Haiwei Li; Yan Hao
2021 6th International Conference on Intelligent Computing and Signal Processing (ICSP)
Year: 2021 | Conference Paper | Publisher: IEEE

Traffic Classification with Machine Learning for Enhancing Cloud Security
Md. Sagar Hossen; Tohari Ahmad; Muhammad Aidiel Rachman Putra
2023 Intelligent Methods, Systems, and Applications (IMSA)
Year: 2023 | Conference Paper | Publisher: IEEE
Cited by: Papers (2)

Abstract HTML

Traffic Classification with Machine Learning for Enhancing Cloud Security

Md. Sagar Hossen; Tohari Ahmad; Muhammad Aidiel Rachman Putra
2023 Intelligent Methods, Systems, and Applications (IMSA)
Year: 2023 | Conference Paper | Publisher: IEEE

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising purposes. Privacy Policy

Enhancing Cloud Security: A Comprehensive Review of Machine Learning Approaches

Wassim Safi; Sameh Ghwanmeh; Mahmoud Mahfuri; Waleed T. Al-Sit
2024 2nd International Conference on Cyber Resilience (ICCR)
Year: 2024 | Conference Paper | Publisher: IEEE

Real-Time Physical Threat Detection on Edge Data Using Online Learning

Utsab Khakurel; Danda B. Rawat
IEEE Consumer Electronics Magazine
Year: 2024 | Volume: 13, Issue: 1 | Magazine Article | Publisher: IEEE

Abstract HTML

Real-Time Physical Threat Detection on Edge Data Using Online Learning

Utsab Khakurel; Danda B. Rawat
IEEE Consumer Electronics Magazine
Year: 2024 | Volume: 13, Issue: 1 | Magazine Article | Publisher: IEEE

A Framework to Identify Allergen and Nutrient Content in Fruits and Packaged Food using Deep Learning and OCR

B Rohini; Divya Madhuri Pavuluri; LS Naresh Kumar; V Soorya; J Aravinth
2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)
Year: 2021 | Conference Paper | Publisher: IEEE
Cited by: Papers (4)

Abstract HTML

A Framework to Identify Allergen and Nutrient Content in Fruits and Packaged Food using Deep Learning and OCR

B Rohini; Divya Madhuri Pavuluri; LS Naresh Kumar; V Soorya; J Aravinth
2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)
Year: 2021 | Volume: 1 | Conference Paper | Publisher: IEEE

Multi-Class Threat Detection Using Neural Network and Machine Learning Approaches in Kubernetes Environments

Abdelrahman Aly; Mahmoud Fayez; Mirvat Al-Qutt; Ahmed M. Hamad
2024 6th International Conference on Computing and Informatics (ICCI)
Year: 2024 | Conference Paper | Publisher: IEEE

Abstract HTML

Multi-Class Threat Detection Using Neural Network and Machine Learning Approaches in Kubernetes Environments

Abdelrahman Aly; Mahmoud Fayez; Mirvat Al-Qutt; Ahmed M. Hamad
2024 6th International Conference on Computing and Informatics (ICCI)
Year: 2024 | Conference Paper | Publisher: IEEE

An Automatic Malaria Disease Diagnosis Framework Integrating Blockchain-Enabled Cloud–Edge Computing and Deep Learning

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising purposes. Privacy Policy

An Automatic Malaria Disease Diagnosis Framework Integrating Blockchain-Enabled Cloud–Edge Computing and Deep Learning

Sirui Chen; Shengjie Zhao; Chenxi Huang
IEEE Internet of Things Journal
Year: 2023 | Volume: 10, Issue: 24 | Journal Article | Publisher: IEEE

Toward Evaluation of Deployment Architecture of ML-Based Cyber-Physical Systems
Lucas Gisselaire; Florian Carlo; Quentin Guerre-berthelot; Bastien Zigmann; Lydie du Bousquet; Masahide Nakamura
2019 34th IEEE/ACM International Conference on Automated Software Engineering Workshop (ASEW)
Year: 2019 | Conference Paper | Publisher: IEEE
Cited by: Papers (4)

Abstract HTML

Toward Evaluation of Deployment Architecture of ML-Based Cyber-Physical Systems

Lucas Gisselaire; Florian Carlo; Quentin Guerre-berthelot; Bastien Zigmann; Lydie du Bousquet; Masahide Nakamura
2019 34th IEEE/ACM International Conference on Automated Software Engineering Workshop (ASEW)
Year: 2019 | Conference Paper | Publisher: IEEE

Auto-ML Cyber Security Data Analysis Using Google, Azure and IBM Cloud Platforms
Emmanuel Opara; Hayden Wimmer; Carl M. Rebman
2022 International Conference on Electrical, Computer and Energy Technologies (ICECET)
Year: 2022 | Conference Paper | Publisher: IEEE
Cited by: Papers (8)

Abstract HTML

Auto-ML Cyber Security Data Analysis Using Google, Azure and IBM Cloud Platforms

Emmanuel Opara; Hayden Wimmer; Carl M. Rebman
2022 International Conference on Electrical, Computer and Energy Technologies (ICECET)
Year: 2022 | Conference Paper | Publisher: IEEE

Efficient and Privacy-Preserving Federated QoS Prediction for Cloud Services
Yilei Zhang; Peiyun Zhang; Yonglong Luo; Jun Luo
2020 IEEE International Conference on Web Services (ICWS)
Year: 2020 | Conference Paper | Publisher: IEEE
Cited by: Papers (10)

Abstract HTML

Efficient and Privacy-Preserving Federated QoS Prediction for Cloud Services

Yilei Zhang; Peiyun Zhang; Yonglong Luo; Jun Luo
2020 IEEE International Conference on Web Services (ICWS)
Year: 2020 | Conference Paper | Publisher: IEEE

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising purposes. Privacy Policy

Efficient approaches for intrusion detection in cloud environment

Preeti Mishra; Emmanuel S. Pilli; Vijay Varadharajan; Udaya Tupakula
2016 International Conference on Computing, Communication and Automation (ICCCA)
Year: 2016 | Conference Paper | Publisher: IEEE

Toward cloud-based mixed reality e- learning system
Hassanin M. Al-Barhamtoshy; Abdullah. Al-Ghamdi
2017 International Conference on Informatics, Health & Technology (ICIHT)
Year: 2017 | Conference Paper | Publisher: IEEE
Cited by: Papers (3)

Abstract HTML

Toward cloud-based mixed reality e- learning system

Hassanin M. Al-Barhamtoshy; Abdullah. Al-Ghamdi
2017 International Conference on Informatics, Health & Technology (ICIHT)
Year: 2017 | Conference Paper | Publisher: IEEE

A Streaming Intrusion Monitoring and Classification System for IaaS Cloud
Jason Nikolai; Yong Wang
2016 IEEE 9th International Conference on Cloud Computing (CLOUD)
Year: 2016 | Conference Paper | Publisher: IEEE
Cited by: Papers (2)

Abstract HTML

A Streaming Intrusion Monitoring and Classification System for IaaS Cloud

Jason Nikolai; Yong Wang
2016 IEEE 9th International Conference on Cloud Computing (CLOUD)
Year: 2016 | Conference Paper | Publisher: IEEE

Work-in-Progress: A Physically Realizable Backdoor Attack on 3D Point Cloud Deep Learning
Chen Bian; Wei Jiang; Jinyu Zhan; Ziwei Song; Xiangyu Wen; Hong Lei
2021 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS)
Year: 2021 | Conference Paper | Publisher: IEEE

Abstract HTML

Work-in-Progress: A Physically Realizable Backdoor Attack on 3D Point Cloud Deep Learning

Chen Bian; Wei Jiang; Jinyu Zhan; Ziwei Song; Xiangyu Wen; Hong Lei
2021 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS)
Year: 2021 | Conference Paper | Publisher: IEEE

Securing Virtual Infrstructure in Cloud Computing using Big Data Analytics
Atul Kumar Gupta; Arjun Choudhary; Preeti Chauhan
2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising purposes. Privacy Policy

Securing Virtual Infrstructure in Cloud Computing using Big Data Analytics

Atul Kumar Gupta; Arjun Choudhary; Preeti Chauhan
2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)
Year: 2018 | Conference Paper | Publisher: IEEE

Federated Threat-Hunting Approach for Microservice-Based Industrial Cyber-Physical System

Mohamed Abdel-Basset; Hossam Hawash; Karam Sallam
IEEE Transactions on Industrial Informatics
Year: 2022 | Volume: 18, Issue: 3 | Journal Article | Publisher: IEEE
Cited by: Papers (23)

Abstract HTML

Federated Threat-Hunting Approach for Microservice-Based Industrial Cyber-Physical System

Mohamed Abdel-Basset; Hossam Hawash; Karam Sallam
IEEE Transactions on Industrial Informatics
Year: 2022 | Volume: 18, Issue: 3 | Journal Article | Publisher: IEEE

Deep Learning for Detecting Ransomware in Edge Computing Devices Based On Autoencoder Classifier

Gital AbdulsalamYa'u; Goteng Kuwunidi Job; Saleh Mustapha Waziri; Badamasi Jaafar; Nahuru Ado SabonGari; Ismail Zahraddeen Yakubu
2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT)
Year: 2019 | Conference Paper | Publisher: IEEE
Cited by: Papers (4)

Abstract HTML

Deep Learning for Detecting Ransomware in Edge Computing Devices Based On Autoencoder Classifier

Gital AbdulsalamYa'u; Goteng Kuwunidi Job; Saleh Mustapha Waziri; Badamasi Jaafar; Nahuru Ado SabonGari; Ismail Zahraddeen Yakubu
2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT)
Year: 2019 | Conference Paper | Publisher: IEEE

Reinforced Transformer Learning for VSI-DDoS Detection in Edge Clouds

Adil Bin Bhutto; Xuan Son Vu; Erik Elmroth; Wee Peng Tay; Monowar Bhuyan
IEEE Access
Year: 2022 | Volume: 10 | Journal Article | Publisher: IEEE
Cited by: Papers (2)



Abstract HTML

Reinforced Transformer Learning for VSI-DDoS Detection in Edge Clouds

Adil Bin Bhutto; Xuan Son Vu; Erik Elmroth; Wee Peng Tay; Monowar Bhuyan

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising purposes. Privacy Policy

Load More

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising purposes. Privacy Policy

About IEEE *Xplore* | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | IEEE Ethics Reporting | Sitemap | IEEE Privacy Policy

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2024 IEEE - All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies

IEEE Account

» Change Username/Password

» Update Address

Purchase Details

» Payment Options

» Order History

» View Purchased Documents

Profile Information

» Communications Preferences

» Profession and Education

» Technical Interests

Need Help?

» US & Canada: +1 800 678 4333

» Worldwide: +1 732 981 0060

» Contact & Support

About IEEE *Xplore* | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not for profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2024 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising purposes. Privacy Policy

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	18361748
Filing Date	2023-07-28
First Named Inventor	ÚLFAR ERLINGSSON
Art Unit	
Examiner Name	Alina Boutah
Attorney Docket Number	L0041B1CIP2C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	10033611	B1	2018-07-24	Linkous et al.	
	2	10104071	B2	2018-10-16	Gordon et al.	
	3	10115111	B2	2018-10-30	Miltonberger	
	4	10121000	B1	2018-11-06	Rivlin et al.	
	5	10122740	B1	2018-11-06	Finkelshtein et al.	
	6	10127273	B2	2018-11-13	Dickey	
	7	10142357	B1	2018-11-27	Tamersoy et al.	
	8	10149148	B2	2018-12-04	Zha et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	9	10182058	B2	2019-01-15	Xu	
	10	10205736	B2	2019-02-12	Rieke et al.	
	11	10237254	B2	2019-03-19	McDowell et al.	
	12	10237294	B1	2019-03-19	Zadeh et al.	
	13	10249266	B2	2019-04-02	Zamir	
	14	10331659	B2	2019-06-25	Ahuja et al.	
	15	10339309	B1	2019-07-02	Kling et al.	
	16	10367704	B2	2019-07-30	Giura et al.	
	17	10382303	B2	2019-08-13	Khanal et al.	
	18	10382529	B2	2019-08-13	WAN et al.	
	19	10389742	B2	2019-08-20	Reddy et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	20	10419468	B2	2019-09-17	Glatfelter et al.	
	21	10419469	B1	2019-09-17	Singh et al.	
	22	10425437	B1	2019-09-24	Bog et al.	
	23	10447526	B2	2019-10-15	Tucker et al.	
	24	10454753	B2	2019-10-22	Sasturkar et al.	
	25	10496263	B2	2019-12-03	So et al.	
	26	10496678	B1	2019-12-03	Tang	
	27	10505818	B1	2019-12-10	Yona et al.	
	28	10510007	B2	2019-12-17	Singhal et al.	
	29	10515095	B2	2019-12-24	Childress et al.	
	30	10521584	B1	2019-12-31	Mehr	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	31	10565373	B1	2020-02-18	Rao et al.	
	32	10581891	B1	2020-03-03	Kapoor et al.	
	33	10587609	B2	2020-03-10	Ebrahimi et al.	
	34	10592535	B2	2020-03-17	Ahn et al.	
	35	10594718	B1	2020-03-17	Deaguero et al.	
	36	10599718	B2	2020-03-24	Kumar et al.	
	37	10614200	B2	2020-04-07	Betz et al.	
	38	10642867	B2	2020-05-05	Palanciuc	
	39	10656979	B2	2020-05-19	Ishakian et al.	
	40	10664757	B2	2020-05-26	Lastras-Montano et al.	
	41	10685295	B1	2020-06-16	Ross et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	42	10701051	B2	2020-06-30	Ohsumi	
	43	10708082	B1	2020-07-07	Bakiaraj et al.	
	44	10735329	B2	2020-08-04	WANG et al.	
	45	10754940	B2	2020-08-25	Ohsumi	
	46	10775183	B2	2020-09-15	Ho et al.	
	47	10791131	B2	2020-09-29	Nor et al.	
	48	10797974	B2	2020-10-06	Giura et al.	
	49	10812497	B2	2020-10-20	Venkatramani et al.	
	50	10824675	B2	2020-11-03	Alonso et al.	
	51	10824813	B2	2020-11-03	Smith et al.	
	52	10885452	B1	2021-01-05	Garg	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	53	10904007	B2	2021-01-26	Kim et al.	
	54	10904270	B2	2021-01-26	Muddu et al.	
	55	10911470	B2	2021-02-02	Muddu et al.	
	56	10951648	B2	2021-03-16	DORON et al.	
	57	10986114	B1	2021-04-20	Singh et al.	
	58	11036800	B1	2021-06-15	Kayyoor et al.	
	59	11048492	B2	2021-06-29	Jain et al.	
	60	11080392	B2	2021-08-03	Bennett et al.	
	61	11153339	B1	2021-10-19	Kapoor et al.	
	62	11233821	B2	2022-01-25	Yadav et al.	
	63	11431735	B2	2022-08-30	SHUA	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	64	11489863	B1	2022-11-01	Shua et al.	
	65	11575693	B1	2023-02-07	Muddu et al.	
	66	11677772	B1	2023-06-13	Kapoor et al.	
	67	5584024	A	1996-12-10	Shwartz	
	68	5806062	A	1998-09-08	Chen et al.	
	69	6347339	B1	2002-02-12	Morris et al.	
	70	6363411	B1	2002-03-26	Dugan et al.	
	71	6434663	B1	2002-08-13	Grimsrud et al.	
	72	6938084	B2	2005-08-30	Gamache et al.	
	73	7054873	B2	2006-05-30	Nordström et al.	
	74	7310733	B1	2007-12-18	Pearson et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	75	7529801	B2	2009-05-05	Moore et al.	
	76	7562045	B2	2009-07-14	Beadle et al.	
	77	7743153	B2	2010-06-22	Hall et al.	
	78	7797548	B2	2010-09-14	Pearson et al.	
	79	7856544	B2	2010-12-21	Schenfeld et al.	
	80	7926026	B2	2011-04-12	Klein et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020059531	A1	2002-05-16	On	
	2	20020161889	A1	2002-10-31	Gamache et al.	
	3	20020184225	A1	2002-12-05	Ghukasyan	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	4	20030037136	A1	2003-02-20	Labovitz et al.	
	5	20030179227	A1	2003-09-25	Ahmad et al.	
	6	20030233361	A1	2003-12-18	Cady	
	7	20040015470	A1	2004-01-22	Smith et al.	
	8	20050060287	A1	2005-03-17	Hellman et al.	
	9	20050102284	A1	2005-05-12	Srinivasan et al.	
	10	20050102365	A1	2005-05-12	Moore et al.	
	11	20050108142	A1	2005-05-19	Beadle et al.	
	12	20050188222	A1	2005-08-25	Motsinger et al.	
	13	20050231760	A1	2005-10-20	Minato	
	14	20050246288	A1	2005-11-03	Kimura et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	15	20060036896	A1	2006-02-16	Gamache et al.	
	16	20060085437	A1	2006-04-20	Brodhun et al.	
	17	20060090095	A1	2006-04-27	Massa et al.	
	18	20060259470	A1	2006-11-16	Chandrasekharan et al.	
	19	20060288415	A1	2006-12-21	Wong	
	20	20070050497	A1	2007-03-01	Haley et al.	
	21	20070118909	A1	2007-05-24	Hertzog et al.	
	22	20070130330	A1	2007-06-07	Ridel et al.	
	23	20070162605	A1	2007-07-12	Chalasani et al.	
	24	20070162963	A1	2007-07-12	Penet et al.	
	25	20070168696	A1	2007-07-19	Ridel et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	26	20070169175	A1	2007-07-19	Hall et al.	
	27	20070225956	A1	2007-09-27	Pratt et al.	
	28	20070266425	A1	2007-11-15	Cho	
	29	20080034411	A1	2008-02-07	Aoyama	
	30	20080065879	A1	2008-03-13	Song et al.	
	31	20080072062	A1	2008-03-20	Pearson et al.	
	32	20080148180	A1	2008-06-19	Liu et al.	
	33	20080151893	A1	2008-06-26	Nordmark et al.	
	34	20080155335	A1	2008-06-26	Klein et al.	
	35	20080244718	A1	2008-10-02	Frost et al.	
	36	20080263643	A1	2008-10-23	Jaiswal et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	37	20080270451	A1	2008-10-30	Thomsen et al.	
	38	20090019160	A1	2009-01-15	Schuler	
	39	20090165109	A1	2009-06-25	Hird	
	40	20090177573	A1	2009-07-09	Beadle et al.	
	41	20090222740	A1	2009-09-03	Yuan	
	42	20090228474	A1	2009-09-10	Chiu et al.	
	43	20090271504	A1	2009-10-29	Ginter et al.	
	44	20090287720	A1	2009-11-19	Herter et al.	
	45	20100094767	A1	2010-04-15	Miltonberger	
	46	20100114931	A1	2010-05-06	Xie et al.	
	47	20100172261	A1	2010-07-08	Shinbo et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	48	20100217860	A1	2010-08-26	Naidu et al.	
	49	20100274785	A1	2010-10-28	Procopiuc et al.	
	50	20100309206	A1	2010-12-09	Xie et al.	
	51	20100329162	A1	2010-12-30	Kadous et al.	
	52	20110023098	A1	2011-01-27	Pearson et al.	
	53	20110029952	A1	2011-02-03	Harrington	
	54	20110055138	A1	2011-03-03	Khanduja et al.	
	55	20110302631	A1	2011-12-08	Sureshchandra et al.	
	56	20120005243	A1	2012-01-05	Merwe et al.	
	57	20120054732	A1	2012-03-01	Jain et al.	
	58	20120089875	A1	2012-04-12	Faust et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	59	20120102029	A1	2012-04-26	Larson et al.	
	60	20120158858	A1	2012-06-21	Gkantsidis et al.	
	61	20120173541	A1	2012-07-05	Venkataramani	
	62	20120317149	A1	2012-12-13	Jagota et al.	
	63	20120317151	A1	2012-12-13	Ruf et al.	
	64	20120323956	A1	2012-12-20	Dumitru et al.	
	65	20130067100	A1	2013-03-14	Kuzin et al.	
	66	20130081118	A1	2013-03-28	Ge	
	67	20130086667	A1	2013-04-04	Haven	
	68	20130097320	A1	2013-04-18	Ritter et al.	
	69	20130173915	A1	2013-07-04	Haulund	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	70	20130205357	A1	2013-08-08	Bahnck et al.	
	71	20130205357	A1	2013-08-08	Bahnck et al.	
	72	20130219295	A1	2013-08-22	Feldman et al.	
	73	20130269007	A1	2013-10-10	Yoshigaki et al.	
	74	20130304915	A1	2013-11-14	KAWAI	
	75	20140041005	A1	2014-02-06	HE	
	76	20140098101	A1	2014-04-10	Friedlander et al.	
	77	20140115001	A1	2014-04-24	Arroyo et al.	
	78	20140115011	A1	2014-04-24	Buerner et al.	
	79	20140181944	A1	2014-06-26	Ahmed et al.	
	80	20140208191	A1	2014-07-24	Zaric et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(**Not for submission under 37 CFR 1.99)**

Application Number	18361748
Filing Date	2023-07-28
First Named Inventor	ÚLFAR ERLINGSSON
Art Unit	
Examiner Name	Alina Boutah
Attorney Docket Number	L0041B1CIP2C1

	81	20140229607	A1	2014-08-14	Jung et al.	
	82	20140245443	A1	2014-08-28	Chakraborty	
	83	20140280068	A1	2014-09-18	DHOOPAR et al.	
	84	20140325631	A1	2014-10-30	Pearson et al.	
	85	20140359558	A1	2014-12-04	Chamberlain	
	86	20140379716	A1	2014-12-25	Branch et al.	
	87	20150058619	A1	2015-02-26	Sweet et al.	
	88	20150135312	A1	2015-05-14	Wada et al.	
	89	20150161201	A1	2015-06-11	Sadikov et al.	
	90	20150172321	A1	2015-06-18	Kirti et al.	
	91	20150188751	A1	2015-07-02	Vasseur et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	92	20150213598	A1	2015-07-30	Madabhushi et al.	
	93	20150302440	A1	2015-10-22	Monden et al.	
	94	20150319185	A1	2015-11-05	Kirti et al.	
	95	20150341379	A1	2015-11-26	Lefebvre et al.	
	96	20150356144	A1	2015-12-10	Chawla et al.	
	97	20160036837	A1	2016-02-04	Jain et al.	
	98	20160063226	A1	2016-03-03	Singh et al.	
	99	20160078365	A1	2016-03-17	Baumard	
	100	20160080204	A1	2016-03-17	MISHRA et al.	
	101	20160080404	A1	2016-03-17	KOHOUT et al.	
	102	20160110434	A1	2016-04-21	Kakaraddi et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	103	20160149937	A1	2016-05-26	KATMOR et al.	
	104	20160203411	A1	2016-07-14	Sadikov et al.	
	105	20160205125	A1	2016-07-14	Kim et al.	
	106	20160218911	A1	2016-07-28	WESSELS et al.	
	107	20160261544	A1	2016-09-08	Conover	
	108	20160330183	A1	2016-11-10	McDowell et al.	
	109	20160330206	A1	2016-11-10	Xu	
	110	20160359592	A1	2016-12-08	Kulshreshtha et al.	
	111	20160359872	A1	2016-12-08	Yadav et al.	
	112	20160373428	A1	2016-12-22	Shi	
	113	20170063830	A1	2017-03-02	Huang	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(**Not for submission under 37 CFR 1.99)**

Application Number	18361748
Filing Date	2023-07-28
First Named Inventor	ÚLFAR ERLINGSSON
Art Unit	
Examiner Name	Alina Boutah
Attorney Docket Number	L0041B1CIP2C1

	114	20170063906	A1	2017-03-02	Muddu et al.	
	115	20170063908	A1	2017-03-02	Muddu et al.	
	116	20170063910	A1	2017-03-02	Muddu et al.	
	117	20170063912	A1	2017-03-02	Muddu et al.	
	118	20170076206	A1	2017-03-16	Lastras-Montano et al.	
	119	20170085553	A1	2017-03-23	Gordon et al.	
	120	20170086069	A1	2017-03-23	Liu	
	121	20170111245	A1	2017-04-20	Ishakian et al.	
	122	20170116315	A1	2017-04-27	Xiong et al.	
	123	20170118240	A1	2017-04-27	Reddy et al.	
	124	20170134240	A1	2017-05-11	Hévizi et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(**Not for submission under 37 CFR 1.99)**

Application Number	18361748
Filing Date	2023-07-28
First Named Inventor	ÚLFAR ERLINGSSON
Art Unit	
Examiner Name	Alina Boutah
Attorney Docket Number	L0041B1CIP2C1

	125	20170147646	A1	2017-05-25	LEE et al.	
	126	20170163666	A1	2017-06-08	Venkatramani et al.	
	127	20170230183	A1	2017-08-10	Sweet et al.	
	128	20170249069	A1	2017-08-31	Zamir	
	129	20170251013	A1	2017-08-31	Kirti et al.	
	130	20170257358	A1	2017-09-07	Ebrahimi et al.	
	131	20170262521	A1	2017-09-14	Cho et al.	
	132	20170272344	A1	2017-09-21	Tang et al.	
	133	20170277553	A1	2017-09-28	Zada et al.	
	134	20170277997	A1	2017-09-28	Zong et al.	
	135	20170279827	A1	2017-09-28	Savalle et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	136	20170286190	A1	2017-10-05	Ishakian et al.	
	137	20170288974	A1	2017-10-05	Yoshihira et al.	
	138	20170330096	A1	2017-11-16	Gupta et al.	
	139	20170337262	A1	2017-11-23	Smith et al.	
	140	20170353853	A1	2017-12-07	Zha et al.	
	141	20170359361	A1	2017-12-14	Modani et al.	
	142	20170366492	A1	2017-12-21	Ho et al.	
	143	20180013650	A1	2018-01-11	Khanal et al.	
	144	20180019932	A1	2018-01-18	Giura et al.	
	145	20180020015	A1	2018-01-18	Munro et al.	
	146	20180025361	A1	2018-01-25	Llagostera et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	147	20180034840	A1	2018-02-01	Marquardt et al.	
	148	20180039688	A1	2018-02-08	Ahn et al.	
	149	20180063178	A1	2018-03-01	Jadhav et al.	
	150	20180067981	A1	2018-03-08	Ahuja et al.	
	151	20180069885	A1	2018-03-08	Patterson et al.	
	152	20180084069	A1	2018-03-22	Be'ery et al.	
	153	20180096047	A1	2018-04-05	Childress et al.	
	154	20180097793	A1	2018-04-05	Agarwal et al.	
	155	20180103052	A1	2018-04-12	Choudhury et al.	
	156	20180115578	A1	2018-04-26	Subbarayan et al.	
	157	20180123864	A1	2018-05-03	Tucker et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	158	20180124189	A1	2018-05-03	Edgington et al.	
	159	20180137858	A1	2018-05-17	Saxena et al.	
	160	20180139200	A1	2018-05-17	Gordon et al.	
	161	20180173789	A1	2018-06-21	Llagostera et al.	
	162	20180174062	A1	2018-06-21	Simo et al.	
	163	20180181750	A1	2018-06-28	Lamothe-Brassard	
	164	20180227286	A1	2018-08-09	Ohsumi	
	165	20180248901	A1	2018-08-30	Rieke	
	166	20180268078	A1	2018-09-20	Gianetto et al.	
	167	20180288063	A1	2018-10-04	Koottayi et al.	
	168	20180329958	A1	2018-11-15	Choudhury et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(**Not for submission under 37 CFR 1.99)**

Application Number	18361748
Filing Date	2023-07-28
First Named Inventor	ÚLFAR ERLINGSSON
Art Unit	
Examiner Name	Alina Boutah
Attorney Docket Number	L0041B1CIP2C1

	169	20180336353	A1	2018-11-22	Manadhata et al.	
	170	20180357422	A1	2018-12-13	Telang et al.	
	171	20180367548	A1	2018-12-20	Stokes III et al.	
	172	20190028327	A1	2019-01-24	SILVA et al.	
	173	20190042879	A1	2019-02-07	MUNOZ	
	174	20190068627	A1	2019-02-28	Thampy	
	175	20190087480	A1	2019-03-21	Palanciuc	
	176	20190109870	A1	2019-04-11	BEDHAPUDI et al.	
	177	20190123973	A1	2019-04-25	Jeuk et al.	
	178	20190132224	A1	2019-05-02	VERMA et al.	
	179	20190149553	A1	2019-05-16	Xu	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	180	20190158524	A1	2019-05-23	Zadeh et al.	
	181	20190222597	A1	2019-07-18	Crabtree et al.	
	182	20190259033	A1	2019-08-22	Reddy et al.	
	183	20190312796	A1	2019-10-10	Giura et al.	
	184	20190339965	A1	2019-11-07	Garvey et al.	
	185	20190342282	A1	2019-11-07	Carbune et al.	
	186	20190342311	A1	2019-11-07	Muddu et al.	
	187	20190349305	A1	2019-11-14	WANG et al.	
	188	20190364067	A1	2019-11-28	Yona et al.	
	189	20190378050	A1	2019-12-12	Edkin et al.	
	190	20200065857	A1	2020-02-27	Lagi et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	191	20200074341	A1	2020-03-05	He et al.	
	192	20200076685	A1	2020-03-05	Vaidya et al.	
	193	20200080856	A1	2020-03-12	Ho et al.	
	194	20200175042	A1	2020-06-04	Batruni	
	195	20200192690	A1	2020-06-18	Gupta et al.	
	196	20200218579	A1	2020-07-09	M et al.	
	197	20200228555	A1	2020-07-16	Wittenschlaeger	
	198	20200252376	A1	2020-08-06	Feng et al.	
	199	20200259852	A1	2020-08-13	Wolff et al.	
	200	20200272740	A1	2020-08-27	Obee et al.	
	201	20200274894	A1	2020-08-27	ARGOETI et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	202	20200278892	A1	2020-09-03	Nainar et al.	
	203	20200280592	A1	2020-09-03	Ithal et al.	
	204	20200285737	A1	2020-09-10	Kraus et al.	
	205	20200287927	A1	2020-09-10	Zadeh et al.	
	206	20200311644	A1	2020-10-01	WILLARD III et al.	
	207	20200403860	A1	2020-12-24	Lewis et al.	
	208	20200404008	A1	2020-12-24	Venkatramani et al.	
	209	20210182248	A1	2021-06-17	Jayanthi	
	210	20210329019	A1	2021-10-21	SHUA	
	211	20210336976	A1	2021-10-28	SHUA	
	212	20210377287	A1	2021-12-02	SHUA	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	213	20220092668	A1	2022-03-24	LU et al.	
	214	20220247769	A1	2022-08-04	Erlingsson et al.	
	215	20220342690	A1	2022-10-27	Shua	
	216	20220345480	A1	2022-10-27	Shua	
	217	20220345481	A1	2022-10-27	Shua	
	218	20220345483	A1	2022-10-27	Shua	
	219	20220350931	A1	2022-11-03	Shua	
	220	20220417273	A1	2022-12-29	Levin et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	110999250	CN	B	2021-11-05	Kirti et al.	Abstract only	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	2	114598840	CN	A	2022-06-07	Hua		☐
	3	2021052379	WO	A1	2021-03-25	Wu et al.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	AI-YASEEN et al., "Real-Time Intrusion Detection System Using Multi-Agent System", IAENG International Journal of Computer Science, volume 43, no. 1, February 2016, pp. 80-90, International Association of Engineers (IAENG), Hong Kong.	☐
	2	AKOGLU et al., "Graph-based Anomaly Detection and Description: A Survey", April 28, 2014.	☐
	3	AMIDON et al., “Program Fracture and Recombination for Efficient Automatic Code Reuse”, In 2015 IEEE High Performance Extreme Computing Conference (HPEC), September 2015, pp. 1-6, IEEE.org (online), DOI: 10.1109/HPEC.2015.7396314.	☐
	4	AMMAR et al., "Query Optimization Techniques in Graph Databases", International Journal of Database Management Systems (IIDMS), Vol. 8, No. 4, August 2016, pages 1-14 (Year: 2016).	☐
	5	BALASUBRAMANIYAN et al., "An Architecture For Intrusion Detection Using Autonomous Agents", In Proceedings 14th Annual Computer Security Applications Conference (Cat. No. 98EX217), 19 pages, June 1998, IEEE, DOI: 10.1109/CSAC.1998.738563.	☐
	6	BEUTEL et al., "User Behavior Modeling with Large-Scale Graph Analysis", Computer Science Department, Carnegie Mellon University, May 2016.	☐
	7	BUGIEL et al., "Towards Taming Privilege-Escalation Attacks on Android", In NOSS (Vol. 17, p. 19), 2012, February.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	8	CHANG et al., "Reality Bites - Progressive Querying and Result Visualization in Logical and VR Spaces", Proceedings of 1994 IEEE Symposium on Visual Languages, pp. 100-109, October 1994, IEEE, DOI: 10.1109NL.1994.363635.	☐
	9	CHESSON, "Communication And Control In A Cluster Network", ACM '74: Proceedings of the 1974 annual ACM conference - Volume 2, January 1974, pp 509-514, http://doi.org/10.1145/1408839 (Year 1974).	☐
	10	CROSBIE et al., “Defending a Computer System using Autonomous Agents”, docs.lib.purdue.edu (online), March 1995, 11 pages.	☐
	11	HAUTAMAKI et al., "Outlier Detection Using k-Nearest Neighbour Graph", Proceedings of the 17th International Conference on Pattern Recognition (ICPR 2004), Vol. 3, August 2004, IEEE, DOI: 10.1109/ICPR.2004.1334558.	☐
	12	HOOPER et al., "Medusa: a simple tool for interaction graph analysis", Bioinformatics, Vol. 21 no. 24, September 2005, pages 4432-4433, Oxford University Press (online), URL: https://academic.oup.com/bioinformatics/article/21/24/4432/179694.	☐
	13	KOUTRA et al., "Exploring and Making Sense of Large Graphs", Computer Science Department, Carnegie Mellon University, August 2015.	☐
	14	LEOPOLD et al., "A Visual Query System for the Specification and Scientific Analysis off Continual Queries", Proceedings, IEEE Symposia on Human-Centric Computing Languages and Environments (Cat. No.01TH8587), September 2001, pp. 203-211, IEEE, doi: 10.1109/HCC.2001.995260.	☐
	15	LIAO et al., "Visualizing Graph Dynamics And Similarity For Enterprise Network Security And Management", VizSec '10: Proceedings of the Seventh International Symposium on Visualization for Cyber Security, September 2010, pp. 34-45, URL: https://doi.org/10.1145/1850795.1850799.	☐
	16	LONG et al., “Automatic Input Rectification”, 2012 34th International Conference on Software Engineering (ICSE), June 2012, pp. 80-90, IEEE.org (online), DOI: 10.1109/ICSE.2012.6227204.	☐
	17	MATEESCU et al., "Join-Graph Propagation Algorithms", Journal of Artificial Intelligence Research, vol. 37, March 2010, pages 279-328, AI Access Foundation, Inc. (online), URL: https://doi.org/10.1613/jair.2842.	☐
	18	MORIANO et al., "Insider Threat Event Detection in User-System Interactions", MIST '17: Proceedings of the 2017 International Workshop on Managing Insider Security Threats, October 2017, pp 1-12, ACM Digital Library (online), URL: https://doi.Jrg/10.1145/3139923.3139928.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	19	PERKINS et al., “Automatically Patching Errors in Deployed Software”, Proceedings of the ACM SIGOPS 22nd Symposium on Operating Systems Principles, October 2009, pp 82-102, acm.org (online), URL: https://doi.org/10.1145/1629575.1629585.	☐
	20	RANSHOUS et al., "Anomaly detection in dynamic networks: a survey", WIREs Computational Statistics, volume 7, May/June 2015, pp. 223-247, Wiley Periodicals, Inc, United States.	☐
	21	RINARD, “Living In The Comfort Zone”, ACM SIGPLAN Notices, Volume 42, Issue 10, October 2007, pp. 611-622, acm.org (online), URL: https://doi.org/10.1145/1297105.1297072.	☐
	22	RINARD, “Manipulating Program Functionality to Eliminate Security Vulnerabilities”, In Moving Target Defense, January 2011, pp. 109-115. Springer, New York, NY.	☐
	23	SAMUEL et al., “Let’s Parse to Prevent Pwnage”, Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats (LEET’12), April 2012, 3 pages, acm.org (online), URL: https://www.usenix.org/conference/leet12/workshop-program/presentation/samuel.	☐
	24	SHEN et al., “Active Learning for Inference and Regeneration of Applications that Access Databases”, ACM Transactions on Programming Languages and Systems (TOPLAS), Volume 42, Issue 4, Article 18, January 2021, pp. 1-119, acm.org (online), URL: https://doi.org/10.1145/3430952.	☐
	25	TAMASSIA et al., "Graph Drawing for Security Visualization", In: Graph Drawing (GD 2008), Lecture Notes in Computer Science, vol 5417, Springer, Berlin, Heidelberg (online), URL: https://doi.org/10.1007/978-3-642-00219-9_2.	☐
	26	VAAS et al., "Detecting disguised processes using Application-Behavior Profiling", In 2017 IEEE International Symposium on Technologies for Homeland Security (HST), pp. 1-6, June 2017, IEEE, DOI: 10.1109/THS.2017.7943508.	☐
	27	VASILAKIS et al., “Supply-Chain Vulnerability Elimination via Active Learning and Regeneration”, Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, November 2021, pp. 1755-1770, acm.org (online), URL: https://doi.org/10.1145/3460120.3484736.	☐
	28	YU et al., "Recommending Join Queries Based on Path Frequency", 2015 12th Web Information System and Application Conference (WISA), September 2015, pp. 21-26, IEEE, DOI: 10.1109/WISA.2015.52.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

EXAMINER SIGNATURE			
Examiner Signature	/ALINA A BOUTAH/	Date Considered	02/20/2024

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Edward J. Lenart/	Date (YYYY-MM-DD)	2023-07-31
Name/Print	Edward J. Lenart	Registration Number	63,665

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	18361748
Filing Date	2023-07-28
First Named Inventor	ÚLFAR ERLINGSSON
Art Unit	
Examiner Name	Alina Boutah
Attorney Docket Number	L0041B1CIP2C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7962635	B2	2011-06-14	Naidu et al.	
	2	7996885	B2	2011-08-09	Jaiswal et al.	
	3	8032925	B2	2011-10-04	Cho	
	4	8037284	B2	2011-10-11	Schenfeld et al.	
	5	8037521	B2	2011-10-11	Minato	
	6	8103906	B1	2012-01-24	Alibakhsh et al.	
	7	8122122	B1	2012-02-21	Clingenpeel et al.	
	8	8151107	B2	2012-04-03	Song et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	9	8276197	B1	2012-09-25	Mangal et al.	
	10	8291233	B2	2012-10-16	Pearson et al.	
	11	8341711	B1	2012-12-25	Pennington et al.	
	12	8351456	B2	2013-01-08	Kadous et al.	
	13	8352589	B2	2013-01-08	Ridel et al.	
	14	8359584	B2	2013-01-22	Rao et al.	
	15	8443442	B2	2013-05-14	Wang et al.	
	16	8497863	B2	2013-07-30	Xie et al.	
	17	8549002	B2	2013-10-01	Herter et al.	
	18	8561157	B2	2013-10-15	Ge	
	19	8595262	B1	2013-11-26	Hayden	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	20	8607306	B1	2013-12-10	Bridge et al.	
	21	8655989	B2	2014-02-18	Ritter et al.	
	22	8671453	B2	2014-03-11	Underwood et al.	
	23	8725587	B2	2014-05-13	Beadle et al.	
	24	8826403	B2	2014-09-02	Bhaskaran et al.	
	25	8843646	B2	2014-09-23	Kuzin et al.	
	26	8862524	B2	2014-10-14	Zheng et al.	
	27	8959608	B2	2015-02-17	Ahmed et al.	
	28	9021583	B2	2015-04-28	Wittenstein et al.	
	29	9037273	B2	2015-05-19	Mikkelsen	
	30	9053306	B2	2015-06-09	Yoshigaki et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(**Not for submission under 37 CFR 1.99)**

Application Number	18361748
Filing Date	2023-07-28
First Named Inventor	ÚLFAR ERLINGSSON
Art Unit	
Examiner Name	Alina Boutah
Attorney Docket Number	L0041B1CIP2C1

	31	9225730	B1	2015-12-29	Brezinski	
	32	9231935	B1	2016-01-05	Bridge et al.	
	33	9239873	B2	2016-01-19	Branch et al.	
	34	9246897	B2	2016-01-26	HE	
	35	9323806	B2	2016-04-26	Sadikov et al.	
	36	9332020	B2	2016-05-03	Thomas et al.	
	37	9369450	B1	2016-06-14	Barak et al.	
	38	9391978	B2	2016-07-12	Burch et al.	
	39	9400882	B2	2016-07-26	Pearson et al.	
	40	9430830	B2	2016-08-30	Madabhushi et al.	
	41	9495522	B2	2016-11-15	Singh et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	42	9497224	B2	2016-11-15	Sweet et al.	
	43	9515999	B2	2016-12-06	Ylonen	
	44	9516053	B1	2016-12-06	Muddu et al.	
	45	9537851	B2	2017-01-03	Gordon et al.	
	46	9558265	B1	2017-01-31	Tacchi et al.	
	47	9569869	B2	2017-02-14	Hesse et al.	
	48	9582766	B2	2017-02-28	Sadikov et al.	
	49	9596253	B2	2017-03-14	Chauhan et al.	
	50	9596254	B1	2017-03-14	Muddu et al.	
	51	9596295	B2	2017-03-14	Banadaki et al.	
	52	9602506	B2	2017-03-21	Kang et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	53	9602526	B2	2017-03-21	Liu et al.	
	54	9639676	B2	2017-05-02	Betz et al.	
	55	9652875	B2	2017-05-16	Vassilvitskii et al.	
	56	9654503	B1	2017-05-16	Kowalyshyn	
	57	9659337	B2	2017-05-23	Lee et al.	
	58	9665660	B2	2017-05-30	Wensel	
	59	9729416	B1	2017-08-08	Khanal et al.	
	60	9734040	B2	2017-08-15	Gounares	
	61	9740744	B2	2017-08-22	Stetson et al.	
	62	9741138	B2	2017-08-22	Friedlander et al.	
	63	9749339	B2	2017-08-29	Kadambe et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	64	9753960	B1	2017-09-05	Troyanovsky	
	65	9760619	B1	2017-09-12	Lattanzi et al.	
	66	9781115	B2	2017-10-03	Heise	
	67	9787705	B1	2017-10-10	Love et al.	
	68	9805080	B2	2017-10-31	Joshi et al.	
	69	9805140	B2	2017-10-31	Chakrabarti et al.	
	70	9811790	B2	2017-11-07	Ahern et al.	
	71	9819671	B2	2017-11-14	Ji	
	72	9830435	B2	2017-11-28	Haven	
	73	9836183	B1	2017-12-05	Love et al.	
	74	9852230	B2	2017-12-26	Fleury et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	75	9853968	B2	2017-12-26	Shen et al.	
	76	9887999	B2	2018-02-06	DONG et al.	
	77	9923911	B2	2018-03-20	Vasseur et al.	
	78	9942220	B2	2018-04-10	Bajenov et al.	
	79	9946800	B2	2018-04-17	Qian et al.	
	80	9953014	B1	2018-04-24	Reshadi et al.	
	81	9954842	B2	2018-04-24	Huang	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	RE47937E1	E1	2020-04-07	Ramachandran et al.	
	2	RE47952E1	E1	2020-04-14	Ramachandran et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐
If you wish to add additional Foreign Patent Document citation information please click the Add button								Add

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐
If you wish to add additional non-patent literature document citation information please click the Add button			Add

EXAMINER SIGNATURE			
Examiner Signature	/ALINA A BOUTAH/	Date Considered	02/20/2024

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Edward J. Lenart/	Date (YYYY-MM-DD)	2023-07-31
Name/Print	Edward J. Lenart	Registration Number	63,665

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

Threat-specific security risk evaluation in the **cloud**

A Nhlabatsi, JB Hong, DS Kim... - ... on **Cloud** ..., 2016 - ieeexplore.ieee.org

... solutions to **deploy** in the **cloud** with respect to the **threat**-... **threats** posed to specific security requirements of a **cloud** client ... and efficient countermeasures against the **threats**. This would ...

☆ Save 99 Cite Cited by 34 Related articles All 6 versions

A **cloud** computing based network monitoring and **threat** detection system for critical infrastructures

Z Chen, G Yu, V Mahalingam, L Ge, J Nguyen, W Yu... - Big Data Research, 2016 - Elsevier

... **deploy** monitoring and detection tools in critical infrastructure systems to effectively discover exploitable vulnerabilities proactively to make the system secure. We will **deploy** ... the **learned** ...

☆ Save 99 Cite Cited by 120 Related articles All 6 versions

Data-driven **threat** analysis for ensuring security in **cloud** enabled systems

MKS Alwahedi, S Islam - Sensors, 2022 - mdpi.com

... **threats**. The main contribution of the paper is a novel data-driven **threat** analysis (d-TM) approach for the **cloud**... to the **cloud** service provider based on the **threat** layers in **cloud** computing...

☆ Save 99 Cite Cited by 12 Related articles All 6 versions »

Enhancing **cloud** compliance: A machine learning approach

JNA Malaiyappan, S Prakash, SV Bayani - ... International Journal of , 2024 - aijmr.com

... **cloud** compliance and security practices. This research paper explores the role of ML in improving **cloud** compliance, focusing on proactive **threat** ... can **learn** from evolving **threats** and ...

☆ Save 99 Cite Cited by 12 Related articles All 2 versions »

Cloud based E-learning, security **threats** and security measures

A Rahman, S Sarfraz, U Shoaib, G Abbas... - Indian Journal of ..., 2016 - isciences.com

... You can **deploy** the application running **Cloud** from your PC, Cell phone, tablet PCs and ... e-**learn**ing servers in remote areas, makes Enter the two inputs will lead to security **threats**. ...

☆ Save 99 Cite Cited by 16 Related articles All 2 versions »

Practical machine learning for **cloud** intrusion detection: Challenges and the way forward

PSS Kumar, A Wicker, M Swann - ... of the 10th ACM workshop on artificial ..., 2017 - dl.acm.org

... systems for the **cloud**'s backend infrastructure. We report the lessons **learned** in securing ... solutions, as the **threat** landscape differs based on the customer's **cloud** offering selection. ...

☆ Save 99 Cite Cited by 59 Related articles All 4 versions

Towards secure **cloud** orchestration for multi-**cloud** deployments

N Paladi, A Michalas, HV Dang - Proceedings of the 5th Workshop on , 2018 - dl.acm.org

... **threats** towards **cloud** orchestrators. We aim to present a generic overview of the **threat** model for **cloud** orchestration; this **threat** ... TOSCA templates to **deploy** the **cloud** infrastructure, set ...

☆ Save 99 Cite Cited by 25 Related articles All 8 versions

Machine learning models for secure data analytics: A taxonomy and **threat** model

P Gupta, S Tanwar, S Tyagi, N Kumar - Computer Communications, 2020 - Elsevier

... [18] Highlighted the cryptographic and security mechanisms to ensure SDA in **cloud** ... system that can **learn** the patterns of the existing **threats** and predict a similar **threat** based on the ...

☆ Save 99 Cite Cited by 195 Related articles All 3 versions

AI-Driven **Cloud** Security: Proactive Defense Against Evolving Cyber **Threats**

A Joseph - International Journal of Computer and Information ..., 2024 - researchgate.net

... **threats**. Machine learning's capacity to interpret and **learn** from massive datasets is very useful in terms of **cloud** ... and **deploy** resources more efficiently. Predictive analytics improves ...

☆ Save 99 Cite Related articles All 2 versions »

Feasibility of supervised machine learning for **cloud** security

D Bhamare, T Salman, M Samaka... - Science and Security ..., 2016 - ieeexplore.ieee.org

... own an infrastructure in order to **deploy** their applications. Instead, ... A detailed survey of other possible **threats** in **cloud** ... Later on we test the robustness of these **learned** models with ISOT ...

☆ Save 99 Cite Cited by 115 Related articles All 11 versions

Search Results

cloud deploy* learn* threat*

Advanced Search

431,695 *Results for:* ***All: cloud deploy* learn* threat****

Edit Search | Save Search | RSS

Searched The ACM Full-Text Collection (740,532 records)
Expand your search to The ACM Guide to Computing Literature (2,692,361 records)

RESULTS VIDEOS PERIODICALS SOFTWARE PEOPLE

Showing 1 - 20 of 431,695 Results

FILTERS | **Sort by:** Relevance

March 2017

Risk tolerance and trust issues in cloud-based E-learning

Siti Saimah Md Kassim, Mazleena Salleh, Anazida Zainal, Ab. Razak Che Husin

ICC '17: Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing
• March 2017 Article No.: 73, pp 1–11 • https://doi.org/10.1145/3018896.3018973

Moving in tandem with internet services nowadays, education institutions should leverage cloud computing which is considered as ready-made platform. One of the key performance index (KPI) for educational institutions progress in teaching and learning ...

Highlights

5 163

RESEARCH-ARTICLE
March 2017

A new approach to mitigate security threats in cloud environment

Chaimae Saadi, Habiba Chaoui

ICC '17: Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing
• March 2017 Article No.: 17, pp 1–7 • https://doi.org/10.1145/3018896.3018911

The cloud is a computing platform which provides a plenty of services such as network, storage, applications and even servers, allocated and released according to the service request using a minimal effort for managing and administrating the system. ...

Highlights

1 348

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00101

November 2017

Practical Machine Learning for Cloud Intrusion Detection: Challenges and the Way Forward

Ram Shankar Siva Kumar, Andrew Wicker, Matt Swann

AISec '17: Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security • November 2017,pp 81–90
• https://doi.org/10.1145/3128572.3140445

Operationalizing machine learning based security detections is extremely challenging, especially in a continuously evolving cloud environment. Conventional anomaly detection does not produce satisfactory results for analysts that are investigating ...

Highlights

39 879

SHORT-PAPER
November 2017

Privacy-preserving Machine Learning in Cloud

Ehsan Hesamifard, Hassan Takabi, Mehdi Ghasemi, Catherine Jones

CCSW '17: Proceedings of the 2017 on Cloud Computing Security Workshop • November 2017,pp 39–43
• https://doi.org/10.1145/3140649.3140655

Machine learning algorithms based on deep neural networks (NN) have achieved remarkable results and are being extensively used in different domains. On the other hand, with increasing growth of cloud services, several Machine Learning as a Service (...

Highlights

37 1,196

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00102

April 2018

Towards Secure Cloud Orchestration for Multi-Cloud Deployments

Nicolae Paladi, Antonis Michalas, Hai-Van Dang

CrossCloud'18: Proceedings of the 5th Workshop on CrossCloud Infrastructures & Platforms • April 2018,Article No.: 4, pp 1 – 6

• https://doi.org/10.1145/3195870.3195874

Cloud orchestration frameworks are commonly used to deploy and operate cloud infrastructure. Their role spans both vertically (deployment on infrastructure, platform, application and microservice levels) and horizontally (deployments from many distinct ...

Highlights

10 479

Upcoming Conferences

MOBISYS '24

June 3 – 7, 2024

Toranomon Hills Forum, Minato-ku, Tokyo, Japan

MOBISYS '24 Website

HPDC '24

June 3 – 7, 2024

University of Pisa, Pisa, Italy

PASC '24

June 3 – 5, 2024

ETH Zurich, Zurich, Switzerland

PASC '24 Website

August 2017

Self-healing Multi-Cloud Application Modelling

Erkuden Rios, Eider Iturbe, Maria Carmen Palacios

ARES '17: Proceedings of the 12th International Conference on Availability, Reliability and Security • August 2017,Article No.: 93, pp 1–9 • https://doi.org/10.1145/3098954.3104059

Cloud computing market forecasts and technology trends confirm that Cloud is an IT disrupting phenomena and that the number of companies with multi-cloud strategy is continuously growing. Cost optimization and increased competitiveness of companies that ...

Highlights

7 374

RESEARCH-ARTICLE

September 2023

Are You Cloud-Certified? Preparing Computing Undergraduates for Cloud Certification with Experiential Learning

Eng Lieh Ouh, Benjamin Kok Siew Gan

ICSE-SEET '23: Proceedings of the 45th International Conference on Software Engineering: Software Engineering Education and Training • May 2023,pp 46–57 • https://doi.org/10.1109/ICSE-SEET58685.2023.00011

Cloud Computing skills have been increasing in demand. Many software engineers are learning these skills and taking cloud certification examinations to be job competitive. Preparing undergraduates to be cloud-certified remains challenging as cloud ...

Highlights

0 16

May 2018

Challenges to Deploying Library Services in the Cloud: Data Issues Influencing IT, People, Costs, and Policy Challenges

Devendra Potnis, Reynard Regenstreif-Harms, Dwight Hunter

JCDL '18: Proceedings of the 18th ACM/IEEE on Joint Conference on Digital Libraries • May 2018,pp 375–376
• https://doi.org/10.1145/3197026.3203897

This poster analyzes challenges to planning, deploying, and maintaining different types of library services in the cloud. We apply grounded theory principles to analyze 75 articles authored by library administrators, librarians with IT expertise, IT ...

Highlights

0 167

RESEARCH-ARTICLE
PUBLIC ACCESS
October 2016

Lurking Malice in the Cloud: Understanding and Detecting Cloud Repository as a Malicious Service

Xiaojing Liao, Sumayah Alrwais, Kan Yuan, Luyi Xing, XiaoFeng Wang, + 2

CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security • October 2016,pp 1541–1552
• https://doi.org/10.1145/2976749.2978349

The popularity of cloud hosting services also brings in new security challenges: it has been reported that these services are increasingly utilized by miscreants for their malicious online activities. Mitigating this emerging threat, posed by such "bad ...

Highlights

7 1,394

November 2017

Prioritizing Cloud Security Controls

Mohammed M. Alani

AWICT 2017: Proceedings of the Second International Conference on Advanced Wireless Information, Data, and Communication Technologies

• November 2017,Article No.: 1, pp 1–6 • https://doi.org/10.1145/3231830.3231831

As more and more organization move to the cloud, security remains a major concern. Given the unique nature of a cloud computing system, security threats take a different form in the cloud. These unique threats require unique security measures and ...

Highlights

543

RESEARCH-ARTICLE

April 2011

Towards an efficient e-learning system based on cloud computing

E. Aljenaa, F. S. Al-Anzi, M. Alshayeji

ICCSS '11: Proceedings of the Second Kuwait Conference on e-Services and e-Systems • April 2011,Article No.: 13, pp 1–7

• https://doi.org/10.1145/2107556.2107569

The rapid development in information and Communication Technology has had a significant impact on traditional educational systems and learning. Today, E-Learning has become a widely accepted way of learning. With increasing numbers of users, a wide ...

Highlights

25 1,647

February 2022

The Future of FPGA Acceleration in Datacenters and the Cloud

Christophe Bobda, Joel Mandebi Mbongue, Paul Chow, Mohammad Ewais, + 13

ACM Transactions on Reconfigurable Technology and Systems (TRETS), Volume 15, Issue 3 • Article No.: 34, pp 1–42
• https://doi.org/10.1145/3506713

In this article, we survey existing academic and commercial efforts to provide Field-Programmable Gate Array (FPGA) acceleration in datacenters and the cloud. The goal is a critical review of existing systems and a discussion of their evolution from ...

Highlights

20 5,201

RESEARCH-ARTICLE

September 2013

Clustering on the cloud: reducing CLARA to MapReduce

Belle Iakovits, Satish Narayana Srirama

NordiCloud '13: Proceedings of the Second Nordic Symposium on Cloud Computing & Internet Technologies • September 2013,pp 64–71
• https://doi.org/10.1145/2513534.2513546

Cloud computing, with its promise of virtually limitless resources, seems to suit well in solving resource intensive problems from machine learning and data mining domains, by allowing to scale any distributed data mining or machine learning application ...

Highlights

6 312

April 2024

Is Securing an Untrusted Cloud with Cryptography Still Economically Unviable?

Kevin Klassen, Jake Skinner, Joel Coffman

UCC '23: Proceedings of the IEEE/ACM 16th International Conference on Utility and Cloud Computing
• December 2023,Article No.: 59, pp 1–6 • https://doi.org/10.1145/3603166.3632554

This paper explores the economic implications of outsourcing data and computation to a cloud provider in comparison to maintaining an on-premise data center. Our investigation is twofold: contrasting a private data center with a trusted cloud, and the ...

Highlights

0 28

RESEARCH-ARTICLE
December 2017

A Multi-layered Cloud Protection Framework

Saad Khan, Simon Parkinson, Andrew Crampton

UCC '17 Companion: Companion Proceedings of the10th International Conference on Utility and Cloud Computing
• December 2017,pp 233–238 • https://doi.org/10.1145/3147234.3148098

Cloud computing has many commercial advantages; however, companies tend to avoid trusting cloud service providers (CSPs) with their sensitive data because of the associated risks. Cloud infrastructures can be vulnerable due to a single flaw in any node ...

Highlights

1 238

March 2016

A System for Intrusion Prediction in Cloud Computing

Mohamed Abdilhamed, Kashif Kifayat, Qi Shi, William Hurst

ICC '16: Proceedings of the International Conference on Internet of Things and Cloud Computing • March 2016,Article No.: 35, pp 1–9
• https://doi.org/10.1145/2896387.2896420

Modern critical infrastructures have to process significantly large data sets. Intrusion-detection systems and unified threat management systems have the role of keeping critical infrastructures secure against cyber-attacks. However, in the world of big ...

Highlights

4 523

RESEARCH-ARTICLE
OPEN ACCESS
March 2021

A Systematic Review on Anomaly Detection for Cloud Computing Environments

Tanja Hagemann, Katerina Katsarou

AICCC '20: Proceedings of the 2020 3rd Artificial Intelligence and Cloud Computing Conference • December 2020,pp 83–96
• https://doi.org/10.1145/3442536.3442550

The detection of anomalies in data is a far-reaching field of research which also applies to the field of cloud computing in several different ways: from the detection of various types of intrusions to the detection of hardware failures, many ...

Highlights

10 5,750

May 2011

Implementing Trust in Cloud Infrastructures

Ricardo Neisse, Dominik Holling, Alexander Pretschner

CCGRID '11: Proceedings of the 2011 11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing
• May 2011,pp 524 – 533 • https://doi.org/10.1109/CCGrid.2011.35

Today's cloud computing infrastructures usually require customers who transfer data into the cloud to trust the providers of the cloud infrastructure. Not every customer is willing to grant this trust without justification. It should be possible to ...

Highlights

15 183

RESEARCH-ARTICLE
March 2017

Security in Cloud-Based Medical Image Processing: Requirements and Approaches

M. Marwan, A. Kartit, H. Ouahmane

BDCA'17: Proceedings of the 2nd International Conference on Big Data, Cloud and Applications • March 2017,Article No.: 6, pp 1–6
• https://doi.org/10.1145/3090354.3090369

Imaging technology has played a crucial role in the development of healthcare sector. In fact, analyzing medical images is an important source of valuable biological information. That is why healthcare professionals rely heavily on these digital records ...

Highlights

0 175

December 2014

A Cloud Adoption Risk Assessment Model

Erdal Cayirci, Alexandr Garaga, Anderson Santana, Yves Roudier

UCC '14: Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing • December 2014,pp 908–913 • https://doi.org/10.1109/UCC.2014.148

Cloud Adoption Risk Assessment Model is designed for cloud customers to assess the risks that they face by selecting a specific cloud service provider. It is an expert system to evaluate various background information obtained from cloud customers, ...

Highlights

2 598

Categories

Journals
Magazines
Books
Proceedings
SIGs
Conferences
Collections
People

About

About ACM Digital Library
ACM Digital Library Board
Subscription Information
Author Guidelines
Using ACM Digital Library
All Holdings within the ACM Digital Library
ACM Computing Classification System
Digital Library Accessibility

Join

Join ACM
Join SIGs
Subscribe to Publications
Institutions and Libraries

Connect

Contact
Facebook
X
LinkedIn
Feedback
Bug Report

The ACM Digital Library is published by the Association for Computing Machinery. Copyright © 2024 ACM, Inc.

Terms of Usage | Privacy Policy | Code of Ethics



Patents | cloud deploy* learn* threat*

(cloud deploy* learn* threat*);

About 34,459 results

Download | Side-by-side

Sort by: Relevance | Group by: None | Deduplicate by: Family | Results / page: 10

A kind of motor-driven synchronous method of target drone and system of actual ...
CN · CN109597393A · 北京航空航天大学 | 北京航空航天大学杭州创新研究院
Priority 2019-01-18 • Filed 2019-01-18 • Published 2019-04-09
Similar 4. the motor-driven synchronous method of target drone that actual situation as claimed in claim 2 combines, which is characterized in that the reception is described virtual Mission bit stream shows the task situation of virtual task and the flight dynamic and **threatening** environment of virtual ...

... system for virtual asset assisted extrusion and intrusion detection and **threat** ...
WO EP US AU CA · WO2015081182 · M. Shannon Lietz · Intuit Inc.
Priority 2014-02-03 • Filed 2015-03-11 • Granted 2017-06-20 • Published 2017-06-20
28. The system for virtual asset assisted extrusion detection in a **cloud** computing environment of claim 24 , wherein the suspect message copy data associated with a given suspect message is transferred to a specific analysis system of the one or more analysis systems for further analysis based, at ...

... virtual asset configured for extrusion and intrusion detection and **threat** ...
WO EP US AU CA · US10063582B2 · M. Shannon Lietz · Intuit Inc.
Priority 2014-02-03 • Filed 2018-02-23 • Granted 2018-07-23 • Published 2018-07-23
transferring the one or more suspect portions to the determined **threat** scoring services; assigning, by the determined **threat** scoring services, **threat** scores to the suspect message at least partially based on a potential impact of the suspect message's potential security **threat** on the virtual asset, ...

System and method for continuous AI management and **learning**
US · US11392860B2 · Roger Joseph Morin · Phacil, Llc
Priority 2018-11-07 • Filed 2019-01-18 • Granted 2022-07-26 • Published 2022-07-26
22 , 24 , 26 , 28 . In some implementations, the above noted data store may be, in whole or in part, distributed in a **cloud** computing topology. In this way, computer 12 and storage device 16 may refer to multiple devices, which may also be distributed throughout the network. In some implementations, ...

Automated container security
IN · IN201811027889A1 · Omar Santos · Cisco Technology, Inc.
Priority 2016-07-20 • Filed 2016-07-20 • Published 2018-01-25
after identifying a security **threat**, determining that a security patch is available for addressing the security **threat**, and **deploying** the security patch to the affected application container. 8 . The computer-implemented method of claim 1 , wherein applying a **threat** mitigation policy on the affected ...

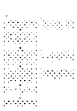
Systems and methods for cyber monitoring and alerting for connected aircraft
US · US11582257B2 · Amit Srivastav · Honeywell International Inc
Priority 2020-09-25 • Filed 2020-11-13 • Granted 2022-11-22 • Published 2022-11-22
classifying the anomaly event based on a predetermined level of **threat** severity. 10. The system of claim 8 , wherein the one or more processor configured to execute the instructions to perform operations further including: **deploying** the **learning** model on a user device, wherein the **learning** model is ...

Dynamic orchestration of machine **learning** functions on a distributed network
US · US11829882B2 · Charles Calvin Byers · Cisco Technology Inc
Priority 2019-01-09 • Filed 2019-01-09 • Granted 2023-11-28 • Published 2023-11-28
determining a reallocation of the first allocation of computing resources and the second allocation of resources based on the performance levels, wherein the reallocation comprises **deploying** workloads for the training of the ML models or the implementation of the trained ML models from a first ...

Personality sharing among drone swarm
US · US10831197B2 · Thomas D. Erickson · International Business Machines Corporation
Priority 2017-01-27 • Filed 2019-06-17 • Granted 2020-11-10 • Published 2020-11-10
Public **cloud**: the **cloud** infrastructure is made available to the general public or a large industry group and is owned by an organization selling **cloud** services. Hybrid **cloud**: the **cloud** infrastructure is a composition of two or more **clouds** (private, community, or public) that remain unique entities ...

... security apparatus, system, and method to analyze images to detect a **threat** ...
WO EP US AU CA · US11847676B2 · Lee FAIR · Chertoff Group, LLC
Priority 2018-06-20 • Filed 2022-05-13 • Granted 2023-12-19 • Published 2023-12-19
In a transportation security technique, images are stored that are received from image capturing equipment **deployed** at respective screening nodes. The images are analyzed using a machine **learning** model, where presence of a particular object in an image indicates that a **threat** condition exists at ...

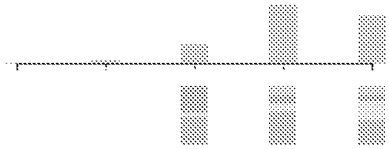
Threat mitigation system and method



WO EP US CA • US11093622B2 • Brian P. Murphy • Reliaquest Holdings, LLC
Priority 2018-06-06 • Filed 2019-06-05 • Granted 2021-08-31 • Published 2021-08-31
processing the plurality of security-relevant information sets using artificial learning/machine learning to identify one or more commonalities amongst the plurality of security-relevant information sets, wherein processing the plurality of security-relevant information sets using artificial ...

Next > >> About 34,459 results

Top 1000 results by filing date



Relative count of top 5 values

Assignees	Inventors	CPCs
Zscaler, Inc		7.1%
International Business Machines Corporation		6.7%
Sophos Limited		5.4%
Splunk Inc.		4.7%
Pure Storage, Inc		3.6%

Expand

Related landscapes

Engineering & Computer Science

General Engineering & Computer Science

Computing Systems

cloud deploy* learn* threat*

Everything

ADVANCED SEARCH

0 selected PAGE 1 1-10 of 235,987 Results

1 ARTICLE

Security Threats and Defensive Approaches in Machine Learning System Under Big Data Environment

Hongsong, Chen ; Yongpeng, Zhang ; Yongrui, Cao ; Bhargava, Bharat

Wireless personal communications, 2021-04, Vol.117 (4), p.3505-3525, Article 3505

Under big data environment, machine learning has been rapidly developed and widely used...

PEER REVIEWED

Get PDF | Read Online

Available Online

2 BOOK

The enterprise cloud : best practices for transforming legacy IT

Bond, James (Cloud chief technologist), author.

2015

Available Online

3 ARTICLE

A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting

HaddadPajouh, Hamed ; Dehghantanha, Ali ; Khayami, Raouf ; Choo, Kim-Kwang Raymond

Future Generation Computer Systems, 2018-08, Vol.85, p.88-96

Internet of Things (IoT) devices are increasingly deployed in different industries and for different purposes (e.g...

PEER REVIEWED OPEN ACCESS

Read Online

Available Online

4 BOOK

Cloud Attack Vectors Building Effective Cyber-Defense Strategies to Protect Cloud Resources

Haber, Morey J., author.; Chappell, J. B. (John Brian), author.; Hills, Christopher (Security strategist), author.

2022

Available Online

5 BOOK

The Cloud Computing Journey : Design and Deploy Resilient and Secure Multi-Cloud Systems with Practical Guidance

Gupta, Divit, author.; Rahi, Rohit, author.

2023

Available Online

6 BOOK

Mastering Cloud Security Posture Management (CSPM) : Secure Multi-Cloud Infrastructure Across AWS, Azure, and Google Cloud Using Proven Techniques.

Nomani, Qamar., Davila, Julie., Khan, Rehman.

2024

Available Online

7 BOOK

HYBRID CLOUD SECURITY PATTERNS leverage modern repeatable architecture patterns to secure your workloads on the cloud

Iyer, Sreekanth, author.

2022

Available Online

8

ARTICLE

Ensemble approach for network threat detection and classification on cloud computing

Krishnaveni, S. ; Prabakaran, S.

Concurrency and computation, 2021-02, Vol.33 (3), p.n/a

§§ *... Real Time Malicious Network Streams Samples were collected using Honeynet, which is deployed on cloud environment...* §§

PEER REVIEWED

Get PDF Read Online

Available Online

9

ARTICLE

Deploying Machine and Deep Learning Models for Efficient Data-Augmented Detection of COVID-19 Infections

Sedik, Ahmed ; Iliyasu, Abdullah M ; Abd El-Rahiem, Basma ; Abdel Samea, Mohammed E. ; Abdel-Raheem, Asmaa ; Hammad, Mohamed ; Peng, Jialiang ; Abd El-Samie, Fathi E. ; Abd El-Latif, Ahmed A.

Viruses, 2020-07, Vol.12 (7), p.769-

§§ *This generation faces existential threats because of the global assault of the novel Corona virus 2019 (i.e., COVID-19...* §§

PEER REVIEWED OPEN ACCESS

Get PDF Read Online

Available Online

10

ARTICLE

Federated Threat-Hunting Approach for Microservice-Based Industrial Cyber-Physical System

Abdel-Basset, Mohamed ; Hawash, Hossam ; Sallam, Karam

IEEE transactions on industrial informatics, 2022-03, Vol.18 (3), p.1905-1917

§§ *... This article presents a novel federated deep learning (DL) model (Fed-TH) for hunting cyber threats against ICPSs that captures the temporal and spatial representations of network data...* §§

Read Online

Available Online

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00116

Bibliographic Data

Application No: 18/361,748

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☐ No ☐ Met After Allowance

Verified and Acknowledged: /ALINA A BOUTAH/ Examiner's Signature | Initials

Title: Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
07/28/2023	709	2442	L0041B1CIP2C1
RULE			

APPLICANTS

LACEWORK, INC., MOUNTAIN VIEW, CA, UNITED STATES

INVENTORS

ÚLFAR ERLINGSSON, PALO ALTO, CA, UNITED STATES

YIJOU CHEN, CUPERTINO, CA, UNITED STATES

CONTINUING DATA

This application is a CON of 17671199 02/14/2022 PAT 11785104

17671199 is a CIP of 17504311 10/18/2021 PAT 11677772

17671199 has PRO of 63243013 09/10/2021

17504311 is a CON of 16665961 10/28/2019 PAT 11153339

16665961 is a CON of 16134794 09/18/2018 PAT 10581891

16134794 has PRO of 62650971 03/30/2018

16134794 has PRO of 62590986 11/27/2017

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

08/21/2023

STATE OR COUNTRY

UNITED STATES

ADDRESS

Lacework, Inc.
c/o Kennedy Lenart Spraggins LLP
797 Sam Bass Road #2559
ROUND ROCK, TX 78681
UNITED STATES

FILING FEE RECEIVED

$2,240

cloud deploy* learn* threat*

Everything

ADVANCED SEARCH

0 selected PAGE 1 1-10 of 235,987 Results

1 ARTICLE

Security Threats and Defensive Approaches in Machine Learning System Under Big Data Environment

Hongsong, Chen ; Yongpeng, Zhang ; Yongrui, Cao ; Bhargava, Bharat

Wireless personal communications, 2021-04, Vol.117 (4), p.3505-3525, Article 3505

Under big data environment, machine learning has been rapidly developed and widely used...

PEER REVIEWED

Get PDF | Read Online

Available Online

2 BOOK

The enterprise cloud : best practices for transforming legacy IT

Bond, James (Cloud chief technologist), author.

2015

Available Online

3 ARTICLE

A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting

HaddadPajouh, Hamed ; Dehghantanha, Ali ; Khayami, Raouf ; Choo, Kim-Kwang Raymond

Future Generation Computer Systems, 2018-08, Vol.85, p.88-96

Internet of Things (IoT) devices are increasingly deployed in different industries and for different purposes (e.g...

PEER REVIEWED OPEN ACCESS

Read Online

Available Online

4 BOOK

Cloud Attack Vectors Building Effective Cyber-Defense Strategies to Protect Cloud Resources

Haber, Morey J., author., Chappell, J. B. (John Brian), author.; Hills, Christopher (Security strategist), author.

2022

Available Online

5 BOOK

The Cloud Computing Journey : Design and Deploy Resilient and Secure Multi-Cloud Systems with Practical Guidance

Gupta, Divit, author.; Rahi, Rohit, author.

2023

Available Online

6 BOOK

Mastering Cloud Security Posture Management (CSPM) : Secure Multi-Cloud Infrastructure Across AWS, Azure, and Google Cloud Using Proven Techniques.

Nomani, Qamar., Davila, Julie., Khan, Rehman.

2024

Available Online

7 BOOK

HYBRID CLOUD SECURITY PATTERNS leverage modern repeatable architecture patterns to secure your workloads on the cloud

Iyer, Sreekanth, author.

2022

Available Online

8 ARTICLE

Ensemble approach for network threat detection and classification on cloud computing

Krishnaveni, S. ; Prabakaran, S.

Concurrency and computation, 2021-02, Vol.33 (3), p.n/a

§§ *... Real Time Malicious Network Streams Samples were collected using Honeynet, which is deployed on cloud environment...* §§

PEER REVIEWED

Get PDF Read Online

Available Online

9 ARTICLE

Deploying Machine and Deep Learning Models for Efficient Data-Augmented Detection of COVID-19 Infections

Sedik, Ahmed ; Iliyasu, Abdullah M ; Abd El-Rahiem, Basma ; Abdel Samea, Mohammed E. ; Abdel-Raheem, Asmaa ; Hammad, Mohamed ; Peng, Jialiang ; Abd El-Samie, Fathi E. ; Abd El-Latif, Ahmed A.

Viruses, 2020-07, Vol.12 (7), p.769-

§§ *This generation faces existential threats because of the global assault of the novel Corona virus 2019 (i.e., COVID-19...* §§

PEER REVIEWED OPEN ACCESS

Get PDF Read Online

Available Online

10 ARTICLE

Federated Threat-Hunting Approach for Microservice-Based Industrial Cyber-Physical System

Abdel-Basset, Mohamed ; Hawash, Hossam ; Sallam, Karam

IEEE transactions on industrial informatics, 2022-03, Vol.18 (3), p.1905-1917

§§ *... This article presents a novel federated deep learning (DL) model (Fed-TH) for hunting cyber threats against ICPSs that captures the temporal and spatial representations of network data...* §§

Read Online

Available Online

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00120

1 - 50

1. Distributed machine learning for anomaly detection

A hierarchical machine learning based infrastructure includes a first Machine Learning (ML) layer configured to execute within an enterprise network environment and locally learn statistics for a set of use cases and alert for deviations from learned distributions. The use cases are typically...

INTL BUSINESS MACHINES CORP

CN107301568 | China Patents | 2022-03-22 | 4

2. Distributed machine learning for anomaly detection

A hierarchical machine learning based infrastructure includes a first Machine Learning (ML) layer configured to execute within an enterprise network environment and locally learn statistics for a set of use cases and alert for deviations from learned distributions. The use cases are typically...

INTL BUSINESS MACHINES CORP

CN107301568A | China Applications | 2020-01-24 | 4

3. Safety defense system and method for closed-source power engineering control system

The invention discloses a safety defense system and a defense method of a closed-source power engineering control system. The security defense system includes: the system comprises a prediction module, a defense module, a detection module, a response module and a learning module, wherein the...

STATE GRID CORP OF CHINA SGCC [+3]

CN112788070A | China Applications | 2021-05-07 | 4

4. Distributed machine learning for anomaly detection

A tiered machine learning-based infrastructure comprises a first machine learning (ML) tier configured to execute within an enterprise network environment and that learns statistics for a set of use cases locally, and to alert deviations from the learned distributions. Use cases typically are...

INTL BUSINESS MACHINES CORP

US20200218992 | US Applications | 2020-07-09 | 4

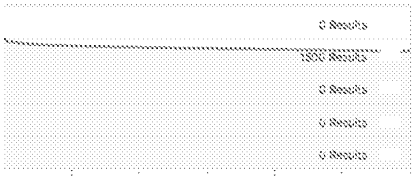
5. Distributed machine learning for anomaly detection

A tiered machine learning-based infrastructure comprises a first machine learning (ML) tier configured to execute within an enterprise network environment and that learns statistics for a set of use cases locally, and to alert deviations from the learned distributions. Use cases typically are...

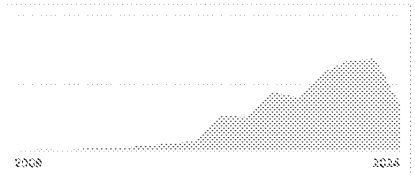
INTL BUSINESS MACHINES CORP

US11392910 | US Patents | 2022-08-16 | 4

Relevance



Publication Date



First Cur Assignees by Relevance

INTL BUSINESS MACHIN... (110)
STATE GRID CORP OF CH... (2)
MCAFEE LLC (3)
DR KALYANKUMAR DASA... (1)
JPMORGAN CHASE BAN... (3)
DR P V SARATH CHAND (1)
LACEWORK INC (37)
ZSCALER INC (107)

Charts based on top 1500 results

More Visuals

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00121

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	10003605	B2	2018-06-19	Muddu et al.	
	2	10116670	B2	2018-10-30	Muddu et al.	
	3	10148677	B2	2018-12-04	Muddu et al.	
	4	10158652	B2	2018-12-18	Muddu et al.	
	5	10205735	B2	2019-02-12	Apostolopoulos	
	6	10243970	B2	2019-03-26	Muddu et al.	
	7	10254848	B2	2019-04-09	Winternitz et al.	
	8	10338895	B2	2019-07-02	Zhang et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	9	10389738	B2	2019-08-20	Muddu et al.	
	10	10419463	B2	2019-09-17	Muddu et al.	
	11	10419465	B2	2019-09-17	Muddu et al.	
	12	10432639	B1	2019-10-01	Bebee et al.	
	13	10454889	B2	2019-10-22	HUANG	
	14	10459979	B2	2019-10-29	Piechowicz et al.	
	15	10462169	B2	2019-10-29	DURAIRAJ et al.	
	16	10491705	B2	2019-11-26	Oetting et al.	
	17	10496468	B2	2019-12-03	Gefen et al.	
	18	10534633	B2	2020-01-14	Hilemon et al.	
	19	10666668	B2	2020-05-26	Muddu et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	20	10673880	B1	2020-06-02	Pratt et al.	
	21	10693900	B2	2020-06-23	Zadeh et al.	
	22	10698954	B2	2020-06-30	Piechowicz et al.	
	23	10756982	B2	2020-08-25	Bai et al.	
	24	10771488	B2	2020-09-08	Verma et al.	
	25	10776191	B2	2020-09-15	Zheng et al.	
	26	10788570	B2	2020-09-29	Wilson	
	27	11036716	B2	2021-06-15	Griffith et al.	
	28	11044264	B2	2021-06-22	DURAIRAJ et al.	
	29	11082289	B2	2021-08-03	Dang et al.	
	30	11120343	B2	2021-09-14	Das et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	31	11126533	B2	2021-09-21	Knowles et al.	
	32	11194849	B2	2021-12-07	Lassoued et al.	
	33	11212299	B2	2021-12-28	Gamble et al.	
	34	11258807	B2	2022-02-22	Muddu et al.	
	35	11281519	B2	2022-03-22	Krishnaswamy et al.	
	36	11314789	B2	2022-04-26	Goldfarb	
	37	11411966	B2	2022-08-09	Muddu et al.	
	38	11463464	B2	2022-10-04	Zadeh et al.	
	39	11494787	B2	2022-11-08	Erickson et al.	
	40	11544138	B2	2023-01-03	Kapish et al.	
	41	11606272	B1	2023-03-14	Popelka et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	42	11636090	B2	2023-04-25	Li et al.	
	43	11640388	B2	2023-05-02	Yang et al.	
	44	11647034	B2	2023-05-09	Levin et al.	
	45	11658990	B2	2023-05-23	Shapoury	
	46	11669571	B2	2023-06-06	Binkley et al.	
	47	11693958	B1	2023-07-04	Steiman	
	48	11722554	B2	2023-08-08	Keren et al.	
	49	11734351	B2	2023-08-22	Binkley et al.	
	50	11734419	B1	2023-08-22	Mackle	
	51	11748473	B2	2023-09-05	Araujo et al.	
	52	11755576	B1	2023-09-12	Jiang et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	53	11755602	B2	2023-09-12	Smith Shawn et al.	
	54	11769098	B2	2023-09-26	Adinarayan et al.	
	55	11770387	B1	2023-09-26	Shivamoggi et al.	
	56	7233333	B2	2007-06-19	Lomask	
	57	7478246	B2	2009-01-13	Arndt et al.	
	58	7484091	B2	2009-01-27	Bade et al.	
	59	7526501	B2	2009-04-28	Albahari et al.	
	60	7707411	B2	2010-04-27	Bade et al.	
	61	7739211	B2	2010-06-15	Coffman et al.	
	62	7747559	B2	2010-06-29	Leitner et al.	
	63	7765431	B2	2010-07-27	Agha et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	64	8050907	B2	2011-11-01	Baisley et al.	
	65	8086852	B2	2011-12-27	Bade et al.	
	66	8140977	B2	2012-03-20	Kriss et al.	
	67	8160999	B2	2012-04-17	Jin et al.	
	68	8209204	B2	2012-06-26	Adler et al.	
	69	8301660	B2	2012-10-30	Yalamanchi	
	70	8490055	B2	2013-07-16	Basak	
	71	9043764	B2	2015-05-26	Ranganathan et al.	
	72	9053437	B2	2015-06-09	Adler et al.	
	73	9064210	B1	2015-06-23	Hart	
	74	9075618	B2	2015-07-07	Winternitz et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	75	9110873	B2	2015-08-18	Woodall et al.	
	76	9159024	B2	2015-10-13	Bhanot et al.	
	77	9189623	B1	2015-11-17	Lin et al.	
	78	9589069	B2	2017-03-07	Yang et al.	
	79	9591010	B1	2017-03-07	Muddu et al.	
	80	9600915	B2	2017-03-21	Winternitz et al.	
	81	9667641	B2	2017-05-30	Muddu et al.	
	82	9679243	B2	2017-06-13	Zou et al.	
	83	9699205	B2	2017-07-04	Muddu et al.	
	84	9710332	B1	2017-07-18	Fan et al.	
	85	9720703	B2	2017-08-01	Reick et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	86	9720704	B2	2017-08-01	Reick et al.	
	87	9727441	B2	2017-08-08	Agarwal et al.	
	88	9727604	B2	2017-08-08	Jin et al.	
	89	9813435	B2	2017-11-07	Muddu et al.	
	90	9824473	B2	2017-11-21	Winternitz et al.	
	91	9838410	B2	2017-12-05	Muddu et al.	
	92	9843837	B2	2017-12-12	Gopalan	
	93	9864672	B2	2018-01-09	Seto et al.	
	94	9985827	B2	2018-05-29	Li et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	1	20040225929	A1	2007-01-23	Agha et al.	
	2	20050246521	A1	2009-01-27	Bade et al.	
	3	20060025987	A1	2006-02-02	Baisley et al.	
	4	20060026419	A1	2009-01-13	Arndt et al.	
	5	20060109271	A1	2007-06-19	Lomask	
	6	20070214111	A1	2017-08-08	Jin et al.	
	7	20070282916	A1	2007-12-06	Albahari et al.	
	8	20080109730	A1	2008-05-08	Coffman et al.	
	9	20080147707	A1	2012-04-17	Jin et al.	
	10	20090006843	A1	2011-12-27	Bade et al.	
	11	20090007010	A1	2009-01-01	Kriss et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	12	20090063857	A1	2010-04-27	Bade et al.	
	13	20090307651	A1	2009-12-10	Senthil et al.	
	14	20090327328	A1	2015-08-18	Woodall et al.	
	15	20100042823	A1	2011-08-09	Arndt et al.	
	16	20110119100	A1	2011-05-19	Ruhl et al.	
	17	20110154287	A1	2011-06-23	Mukkamala et al.	
	18	20120143898	A1	2012-06-07	Bruno et al.	
	19	20120159333	A1	2012-06-21	Mital et al.	
	20	20130024412	A1	2013-01-24	Gong et al.	
	21	20130151453	A1	2013-06-13	Bhanot et al.	
	22	20140067750	A1	2015-05-26	Ranganathan et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	23	20140125672	A1	2015-07-07	Winternitz et al.	
	24	20140279779	A1	2017-06-13	Zou et al.	
	25	20150310649	A1	2017-03-21	Winternitz et al.	
	26	20160120070	A1	2016-04-28	Myrah et al.	
	27	20160357521	A1	2019-07-02	Zhang et al.	
	28	20170063888	A1	2017-03-02	Muddu et al.	
	29	20170063903	A1	2017-03-02	Muddu et al.	
	30	20170063905	A1	2017-03-02	Muddu et al.	
	31	20170063909	A1	2017-03-02	Muddu et al.	
	32	20170063911	A1	2017-03-02	Muddu et al.	
	33	20170070594	A1	2019-11-26	Oetting et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	34	20170102961	A1	2020-01-14	Hilemon et al.	
	35	20170118099	A1	2017-04-27	HUANG	
	36	20170142140	A1	2017-05-18	Muddu et al.	
	37	20170148197	A1	2017-05-25	Winternitz et al.	
	38	20170155570	A1	2017-06-01	Maheshwari et al.	
	39	20170155672	A1	2017-06-01	Muthukrishnan et al.	
	40	20170223036	A1	2017-08-03	Muddu et al.	
	41	20170346683	A1	2018-05-29	Li et al.	
	42	20180004835	A1	2018-01-04	Piechowicz et al.	
	43	20180004859	A1	2020-06-30	Piechowicz et al.	
	44	20180007145	A1	2019-10-29	Piechowicz et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	45	20180089132	A1	2018-03-29	Atta et al.	
	46	20180191781	A1	2018-07-05	Palani et al.	
	47	20180211425	A1	2018-07-26	Winternitz et al.	
	48	20180219888	A1	2018-08-02	Apostolopoulos	
	49	20180219897	A1	2018-08-02	Muddu et al.	
	50	20180359162	A1	2018-12-13	Savov et al.	
	51	20190042950	A1	2019-02-07	Lin et al.	
	52	20190050445	A1	2021-06-15	Griffith et al.	
	53	20190058626	A1	2019-02-21	Knowles et al.	
	54	20190075126	A1	2019-03-07	Muddu et al.	
	55	20190101622	A1	2019-04-04	Wilson	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	56	20190163555	A1	2019-05-30	Zheng et al.	
	57	20190227860	A1	2019-12-03	Gefen et al.	
	58	20190312898	A1	2019-10-10	Verma et al.	
	59	20190327251	A1	2019-10-24	Muddu et al.	
	60	20190342307	A1	2019-11-07	Gamble et al.	
	61	20190354554	A1	2019-11-21	Piechowicz et al.	
	62	20190356555	A1	2020-08-25	Bai et al.	
	63	20200014718	A1	2020-01-09	DURAIRAJ et al.	
	64	20200021607	A1	2020-01-16	Muddu et al.	
	65	20200175361	A1	2020-06-04	Che et al.	
	66	20200287923	A1	2020-09-10	Raghavendra et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	67	20200320106	A1	2022-04-26	Goldfarb	
	68	20200334293	A1	2020-10-22	Piechowicz et al.	
	69	20200351151	A1	2020-11-05	Dang et al.	
	70	20200412752	A1	2020-12-31	Shapoury	
	71	20210019209	A1	2021-01-21	Krishnaswamy et al.	
	72	20210232420	A1	2021-07-29	Dhruvakumar et al.	
	73	20210286798	A1	2021-09-16	Li et al.	
	74	20210294798	A1	2021-09-23	Binkley et al.	
	75	20210406917	A1	2021-12-30	Erickson et al.	
	76	20220004718	A1	2022-01-06	Quamar et al.	
	77	20220050840	A1	2022-02-17	Parravicini et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	78	20220058193	A1	2023-09-12	Smith Shawn et al.	
	79	20220067186	A1	2022-03-03	Thakur et al.	
	80	20220086179	A1	2023-05-09	Levin et al.	
	81	20220092481	A1	2022-03-24	Neithalath et al.	
	82	20220121741	A1	2023-09-05	Araujo et al.	
	83	20220124108	A1	2022-04-21	Gamble et al.	
	84	20220129803	A1	2022-04-28	Bikumala et al.	
	85	20220191226	A1	2022-06-16	Chan et al.	
	86	20220327119	A1	2022-10-13	Gasper et al.	
	87	20220350789	A1	2023-05-02	Yang et al.	
	88	20220374800	A1	2023-09-26	Adinarayan et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	89	20220376970	A1	2022-11-24	Chawathe et al.	
	90	20220382611	A1	2023-01-03	Kapish et al.	
	91	20220394082	A1	2022-12-08	Keren et al.	
	92	20220414072	A1	2022-12-29	Tandon et al.	
	93	20220414105	A1	2022-12-29	Umay et al.	
	94	20230025252	A1	2023-01-26	Erickson et al.	
	95	20230039566	A1	2023-02-09	Ghag et al.	
	96	20230052827	A1	2023-02-16	Araujo et al.	
	97	20230088960	A1	2023-03-23	Popelka et al.	
	98	20230096930	A1	2023-03-30	Dasdan	
	99	20230101773	A1	2023-03-30	Katahanas et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	100	20230138371	A1	2023-05-04	Bandukwala et al.	
	101	20230244523	A1	2023-08-03	Gorantla et al.	
	102	20230251960	A1	2023-08-10	Sharma et al.	
	103	20230275909	A1	2023-08-31	Shivamoggi et al.	
	104	20230291755	A1	2023-09-14	Siebel et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

EXAMINER SIGNATURE			
Examiner Signature	/ALINA A BOUTAH/	Date Considered	02/20/2024

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Edward J. Lenart/	Date (YYYY-MM-DD)	2023-12-07
Name/Print	Edward J. Lenart	Registration Number	63,665

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

Google cloud deployment

Sign in

All Images Videos News Forums More Tools

Examples Methods Steps Tools Services Models Vs Cloud Build Public cloud Manager

Cloud deployment is the process of deploying an application through one or more hosting models—software as a service (SaaS), platform as a service (PaaS) and/or infrastructure as a service (IaaS)—that leverage the cloud. This includes architecting, planning, implementing and operating workloads on cloud.

Cognizant
https://www.cognizant.com › glossary › cloud-deploym...

What is cloud deployment? - Cognizant

About featured snippets • Feedback

People also ask

What are the 4 types of deployment cloud services?

What is the difference between cloud build and deploy?

What is an example of a cloud deployment model?

What is cloud vs local deployment?

Feedback

Discussions and forums

Local vs Cloud deployment : r/mlops - Reddit

Reddit • r/mlops · 8 comments · 2mo ago

Cloud deployment model question : r/CCSP - Reddit

Reddit • r/CCSP · 10+ comments · 2y ago

See more

Google Cloud
https://cloud.google.com › ... › Documentation

Overview of Cloud Deploy

Cloud Deploy is a managed service that automates delivery of your applications to a series of target environments in a defined promotion sequence.
How a Cloud Deploy pipeline... · The Cloud Deploy delivery... · Approvals

GeeksforGeeks
https://www.geeksforgeeks.org › cloud-deployment-mo...

Cloud Deployment Models

May 3, 2023 — The cloud deployment model identifies the specific type of cloud environment based on ownership, scale, and access, as well as the cloud's ...

Things to know

Process
How does cloud deployment work

Example
Cloud deploy example

Models benefits
Benefits of deploying to cloud

Feedback

AWS Docs
https://docs.aws.amazon.com › ... › AWS Whitepaper

Types of cloud computing

A hybrid deployment is a way to connect infrastructure and applications between cloud-based resources and existing resources that are not located in the cloud.

Google Cloud
https://cloud.google.com › deploy

Cloud Deploy - Fully Managed Continuous Delivery

Cloud Deploy is an managed, opinionated, and secure continuous delivery service for GKE, Cloud Run, and Anthos. Managed progressions from dev to prod.
Learn more · Cloud Deploy documentation · Deploy an app to Cloud Run... · Pricing

LaunchDarkly
https://launchdarkly.com › blog › cloud-deployment-m...

5 Cloud Deployment Models: Which One Is Right for You?

Learn the five main cloud deployment and cloud service models—public cloud, private cloud, hybrid cloud, multi-cloud, and community cloud—and which models ...

Virtusa
https://www.virtusa.com › Digital Themes Glossary

What is Cloud Deployment?

Cloud deployment is the utilization of cloud environments to run applications through the use of different models, such as SaaS, PaaS, and IaaS.

SunTec Group
https://www.suntecgroup.com › blogs › what-is-cloud-d...

What is Cloud Deployment?

The software used to provide the services are managed centrally, while the services and applications can be accessed through the internet. The centralized ...

Amazon Web Services
https://aws.amazon.com › types-of-cloud-computing

Types of Cloud Computing - SaaS vs PaaS vs IaaS

Cloud Computing Deployment Models. Cloud. A cloud-based application is fully deployed in the cloud and all parts of the application run in the cloud.
Types Of Cloud Computing · Infrastructure As A Service... · Cloud Computing Deployment...

Related searches

cloud deployment **models**	**private** cloud deployment **model**
cloud deployment **services**	cloud deployment **process**
public cloud deployment **model**	cloud deployment **manager**
cloud deployment **tools**	cloud deployment **aws**

More results

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	11785104	B2	2023-10-10	Erlingsson et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	Alina Boutah
	Attorney Docket Number	L0041B1CIP2C1

	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ALINA A BOUTAH/	Date Considered	05/29/2024

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Edward J. Lenart/	Date (YYYY-MM-DD)	2024-05-29
Name/Print	Edward J. Lenart	Registration Number	63,665

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.A.B/

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	0	18/361748	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/02/20 09:29 AM
L2	32	((("LACEWORK") near3 ("INC"))).AS,AANM.	(USPAT)	OR	ON	ON	2024/02/20 09:29 AM
L3	64	((("ERLINGSSON") near3 ("ÚLFAR")) OR (("CHEN") near3 ("YIJOU"))).INV.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2024/02/20 09:30 AM
L4	250	("10003605" OR "10116670" OR "10148677" OR "10158652" OR "10205735" OR "10243970" OR "10254848" OR "10338895" OR "10389738" OR "10419463" OR "10419465" OR "10432639" OR "10454889" OR "10459979" OR "10462169" OR "10491705" OR "10496468" OR "10534633" OR "10666668" OR "10673880" OR "10693900" OR "10698954" OR "10756982" OR "10771488" OR "10776191" OR "10788570" OR "11036716" OR "11044264" OR "11082289" OR	(US-PGPUB; USPAT)	OR	ON	ON	2024/02/20 09:57 AM

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00151

		"11120343" OR "11126533" OR "11194849" OR "11212299" OR "11258807" OR "11281519" OR "11314789" OR "11411966" OR "11463464" OR "11494787" OR "11544138" OR "11606272" OR "11636090" OR "11640388" OR "11647034" OR "11658990" OR "11669571" OR "11693958" OR "11722554" OR "11734351" OR "11734419" OR "11748473" OR "11755576" OR "11755602" OR "11769098" OR "11770387" OR "20040225929" OR "20050246521" OR "20060025987" OR "20060026419" OR "20060109271" OR "20070214111" OR "20070282916" OR "20080109730" OR "20080147707" OR "20090006843" OR "20090007010" OR "20090063857" OR "20090307651" OR "20090327328" OR "20100042823" OR "20110119100" OR "20110154287" OR "20120143898" OR "20120159333" OR "20130024412" OR "20130151453" OR "20140067750" OR "20140125672" OR "20140279779" OR "20150310649" OR "20160120070" OR "20160357521" OR "20170063888" OR "20170063903" OR "20170063905" OR "20170063909" OR "20170063911" OR					

		"20170070594" OR "20170102961" OR "20170118099" OR "20170142140" OR "20170148197" OR "20170155570" OR "20170155672" OR "20170223036" OR "20170346683" OR "20180004835" OR "20180004859" OR "20180007145" OR "20180089132" OR "20180191781" OR "20180211425" OR "20180219888" OR "20180219897" OR "20180359162" OR "20190042950" OR "20190050445" OR "20190058626" OR "20190075126" OR "20190101622" OR "20190163555" OR "20190227860" OR "20190312898" OR "20190327251" OR "20190342307" OR "20190354554" OR "20190356555" OR "20200014718" OR "20200021607" OR "20200175361" OR "20200287923" OR "20200320106" OR "20200334293" OR "20200351151" OR "20200412752" OR "20210019209" OR "20210232420" OR "20210286798" OR "20210294798" OR "20210406917" OR "20220004718" OR "20220050840" OR "20220058193" OR "20220067186" OR "20220086179" OR "20220092481" OR "20220121741" OR "20220124108" OR "20220129803" OR "20220191226" OR "20220327119" OR "20220350789" OR "20220374800" OR "20220376970" OR "20220382611" OR					

		"20220394082" OR "20220414072" OR "20220414105" OR "20230025252" OR "20230039566" OR "20230052827" OR "20230088960" OR "20230096930" OR "20230101773" OR "20230138371" OR "20230244523" OR "20230251960" OR "20230275909" OR "20230291755" OR "7233333" OR "7478246" OR "7484091" OR "7526501" OR "7707411" OR "7739211" OR "7747559" OR "7765431" OR "8050907" OR "8086852" OR "8140977" OR "8160999" OR "8209204" OR "8301660" OR "8490055" OR "9043764" OR "9053437" OR "9064210" OR "9075618" OR "9110873" OR "9159024" OR "9189623" OR "9589069" OR "9591010" OR "9600915" OR "9667641" OR "9679243" OR "9699205" OR "9710332" OR "9720703" OR "9720704" OR "9727441" OR "9727604" OR "9813435" OR "9824473" OR "9838410" OR "9843837" OR "9864672" OR "9985827" OR "10033611" OR "10104071" OR "10115111" OR "10121000" OR "10122740" OR					

		"10127273" OR "10142357" OR "10149148" OR "10182058" OR "10205736" OR "10237254" OR "10237294" OR "10249266" OR "10331659" OR "10339309" OR "10367704" OR "10382303" OR "10382529" OR "10389742" OR "10419468" OR "10419469" OR "10425437" OR "10447526" OR "10454753" OR "10496263" OR "10496678" OR "10505818" OR "10510007" OR "10515095" OR "10521584" OR "10565373" OR "10581891" OR "10587609" OR "10592535" OR "10594718" OR "10599718" OR "10614200" OR "10642867" OR "10656979" OR "10664757" OR "10685295" OR "10701051" OR "10708082" OR "10735329" OR "10754940" OR "10775183" OR "10791131" OR "10797974" OR "10812497" OR "10824675" OR "10824813" OR "10885452").pn.					
L5	250	("10904007" OR "10904270" OR "10911470" OR "10951648" OR "10986114" OR "11036800" OR "11048492" OR "11080392" OR "11153339" OR "11233821" OR	(US-PGPUB; USPAT)	OR	ON	ON	2024/02/20 09:57 AM

		"11431735" OR "11489863" OR "11575693" OR "11677772" OR "20020059531" OR "20020161889" OR "20020184225" OR "20030037136" OR "20030179227" OR "20030233361" OR "20040015470" OR "20050060287" OR "20050102284" OR "20050102365" OR "20050108142" OR "20050188222" OR "20050231760" OR "20050246288" OR "20060036896" OR "20060085437" OR "20060090095" OR "20060259470" OR "20060288415" OR "20070050497" OR "20070118909" OR "20070130330" OR "20070162605" OR "20070162963" OR "20070168696" OR "20070169175" OR "20070225956" OR "20070266425" OR "20080034411" OR "20080065879" OR "20080072062" OR "20080148180" OR "20080151893" OR "20080155335" OR "20080244718" OR "20080263643" OR "20080270451" OR "20090019160" OR "20090165109" OR "20090177573" OR "20090222740" OR "20090228474" OR "20090271504" OR "20090287720" OR "20100094767" OR "20100114931" OR "20100172261" OR "20100217860" OR "20100274785" OR "20100309206" OR "20100329162" OR "20110023098" OR "20110029952" OR "20110055138" OR					

		"20110302631" OR "20120005243" OR "20120054732" OR "20120089875" OR "20120102029" OR "20120158858" OR "20120173541" OR "20120317149" OR "20120317151" OR "20120323956" OR "20130067100" OR "20130081118" OR "20130086667" OR "20130097320" OR "20130173915" OR "20130205357" OR "20130219295" OR "20130269007" OR "20130304915" OR "20140041005" OR "20140098101" OR "20140115001" OR "20140115011" OR "20140181944" OR "20140208191" OR "20140229607" OR "20140245443" OR "20140280068" OR "20140325631" OR "20140359558" OR "20140379716" OR "20150058619" OR "20150135312" OR "20150161201" OR "20150172321" OR "20150188751" OR "20150213598" OR "20150302440" OR "20150319185" OR "20150341379" OR "20150356144" OR "20160036837" OR "20160063226" OR "20160078365" OR "20160080204" OR "20160080404" OR "20160110434" OR "20160149937" OR "20160203411" OR "20160205125" OR "20160218911" OR "20160261544" OR "20160330183" OR "20160330206" OR "20160359592" OR "20160359872" OR "20160373428" OR "20170063830" OR					

		"20170063906" OR "20170063908" OR "20170063910" OR "20170063912" OR "20170076206" OR "20170085553" OR "20170086069" OR "20170111245" OR "20170116315" OR "20170118240" OR "20170134240" OR "20170147646" OR "20170163666" OR "20170230183" OR "20170249069" OR "20170251013" OR "20170257358" OR "20170262521" OR "20170272344" OR "20170277553" OR "20170277997" OR "20170279827" OR "20170286190" OR "20170288974" OR "20170330096" OR "20170337262" OR "20170353853" OR "20170359361" OR "20170366492" OR "20180013650" OR "20180019932" OR "20180020015" OR "20180025361" OR "20180034840" OR "20180039688" OR "20180063178" OR "20180067981" OR "20180069885" OR "20180084069" OR "20180096047" OR "20180097793" OR "20180103052" OR "20180115578" OR "20180123864" OR "20180124189" OR "20180137858" OR "20180139200" OR "20180173789" OR "20180174062" OR "20180181750" OR "20180227286" OR "20180248901" OR "20180268078" OR "20180288063" OR "20180329958" OR "20180336353" OR "20180357422" OR "20180367548" OR					

		"20190028327" OR "20190042879" OR "20190068627" OR "20190087480" OR "20190109870" OR "20190123973" OR "20190132224" OR "20190149553" OR "20190158524" OR "20190222597" OR "20190259033" OR "20190312796" OR "20190339965" OR "20190342282" OR "20190342311" OR "20190349305" OR "20190364067" OR "20190378050" OR "20200065857" OR "20200074341" OR "20200076685" OR "20200080856" OR "20200175042" OR "20200192690" OR "20200218579" OR "20200228555" OR "20200252376" OR "20200259852" OR "20200272740" OR "20200274894" OR "20200278892" OR "20200280592" OR "20200285737" OR "20200287927" OR "20200311644" OR "20200403860" OR "20200404008" OR "20210182248" OR "20210329019" OR "20210336976" OR "20210377287" OR "20220092668" OR "20220247769" OR "20220342690" OR "20220345480" OR "20220345481" OR "20220345483" OR "20220350931" OR "20220417273" OR "5584024" OR "5806062" OR "6347339" OR "6363411" OR "6434663" OR "6938084" OR "7054873" OR "7310733" OR "7529801" OR					

		"7562045" OR "7743153" OR "7797548" OR "7856544" OR "7926026" OR "7962635" OR "7996885" OR "8032925").pn.					
L6	80	("8037284" OR "8037521" OR "8103906" OR "8122122" OR "8151107" OR "8276197" OR "8291233" OR "8341711" OR "8351456" OR "8352589" OR "8359584" OR "8443442" OR "8497863" OR "8549002" OR "8561157" OR "8595262" OR "8607306" OR "8655989" OR "8671453" OR "8725587" OR "8826403" OR "8843646" OR "8862524" OR "8959608" OR "9021583" OR "9037273" OR "9053306" OR "9225730" OR "9231935" OR "9239873" OR "9246897" OR "9323806" OR "9332020" OR "9369450" OR "9391978" OR "9400882" OR "9430830" OR "9495522" OR "9497224" OR "9515999" OR "9516053" OR "9537851" OR "9558265" OR "9569869" OR "9582766" OR "9596253" OR "9596254" OR "9596295" OR "9602506" OR	(US-PGPUB; USPAT)	OR	ON	ON	2024/02/20 09:57 AM

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00160

		"9602526" OR "9639676" OR "9652875" OR "9654503" OR "9659337" OR "9665660" OR "9729416" OR "9734040" OR "9740744" OR "9741138" OR "9749339" OR "9753960" OR "9760619" OR "9781115" OR "9787705" OR "9805080" OR "9805140" OR "9811790" OR "9819671" OR "9830435" OR "9836183" OR "9852230" OR "9853968" OR "9887999" OR "9923911" OR "9942220" OR "9946800" OR "9953014" OR "9954842" OR "RE47937" OR "RE47952").pn.					
L7	547434	(H04L67/535 or G06F9/455 or G06F9/545 or G06F16/9024 or G06F16/9038 or G06F16/9535 or G06F16/9537 or G06F21/57 or H04L43/06 or H04L63/10 or H04L67/306 or G06F16/2456 or H04L41/08).cpc.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/02/20 10:02 AM
L8	3	17/671199	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO,	OR	ON	ON	2023/02/04 09:42 AM

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00161

			NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L8	1	"20190123973".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/02/20 10:24 AM
L9	4	17/671199	(US-PGPUB; USPAT)	OR	ON	ON	2024/02/20 11:57 AM
L20	166	cloud SAME behav$5 SAME (normal normali$7) SAME recommend$4	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/01/29 01:44 PM
L42	26	(alike similar$4) WITH cloud WITH deploy$5 WITH learn$4 WITH (other another)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/01/30 11:17 AM
L67	27	cloud WITH deploy$4 WITH (misconfigur$5 mis-configur$5)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO;	OR	ON	ON	2023/02/06 03:01 PM

			JPO; DERWENT; IBM_TDB)				
L77	5	17/671199	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/14 12:40 PM
L78	0	18/361748	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/14 12:52 PM
L79	0	18/361748	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/28 01:43 PM
L80	36	(Artificial Intelligence) More like doc: US-11785104-B2 Text: (US-20220247769-A1 OR US-11894984-B2	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB,	OR	ON	ON	2024/05/28 03:23 PM

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00163

		OR US-20220200869-A1 OR US-11770398-B1 OR US-11765249-B2 OR US-11895135-B2 OR US-11849000-B2 OR US-20220329616-A1 OR US-20230032686-A1 OR US-11818156-B1 OR US-20220224707-A1 OR US-20230275917-A1 OR US-11792284-B1 OR US-20240080329-A1 OR US-11909752-B1 OR US-20220400129-A1 OR US-20220311794-A1 OR US-20220215101-A1 OR US-20220303295-A1 OR US-11741238-B2).did.	HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L81	165604	(across cross) adj2 (customer user organization entit$4)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/28 03:36 PM
L82	3435	L81 SAME (cloud WITH deploy$4)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/28 03:36 PM
L83	2996	((across cross) adj2 (customer user organization entit$4))	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY,	OR	ON	ON	2024/05/28 03:37 PM

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00164

		WITH learn$4	CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L86	54	L83 SAME4 ((cloud WITH deploy$4))	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/28 03:37 PM
L87	316	L83 AND ((cloud WITH deploy$4))	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/28 05:07 PM
L88	241	L87 AND @ad<"20220214"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH,	OR	ON	ON	2024/05/28 05:08 PM

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00165

			TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L89	563640	(H04L67/535 or G06F9/455 or G06F9/545 or G06F16/9024 or G06F16/9038 or G06F16/9535 or G06F16/9537 or G06F21/57 or H04L43/06 or H04L63/10 or H04L67/306 or G06F16/2456 or H04L41/08).cpc.	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/28 05:09 PM
L90	38465	(H04L41/145 OR H04L67/10 OR H04L63/1408 OR H04L41/024 OR H04L41/0846 OR H04L41/0806 OR H04L41/0895).cpc.	(USPAT)	OR	ON	ON	2024/05/28 05:09 PM
L91	224260	H04L63/1425,1441,20,1416.cpc.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/28 05:09 PM
L92	60729	h04l67/535.cpc.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN,	OR	ON	ON	2024/05/28 05:09 PM

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00166

			WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L93	76	L88 AND (L92 L91 L90 L89)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/28 05:10 PM
L94	156	L65 AND threat	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/29 05:10 PM
L95	40	cloud WITH deploy$4 WITH (misconfigur$5 mis-configur$5)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/29 05:11 PM
L96	240	cloud SAME behav$5 SAME (normal normali$7) SAME recommend$4	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA,	OR	ON	ON	2024/05/29 05:11 PM

			EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N10	25930	h04l67/535.cpc.	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/29 05:07 PM
N11	83044	(H04L41/145 OR H04L67/10 OR H04L63/1408 OR H04L41/024 OR H04L41/0846 OR H04L41/0806 OR H04L41/0895).cpc.	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/29 05:07 PM
N12	1759	cloud WITH similar$7 WITH deploy$4	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/29 05:07 PM
N13	112457	(permission permit$4 admit$4 allow$4 admission approv$4 endors$7 privileg$$ warrant allowance) WITH level WITH (less reduc$4)	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/29 05:07 PM
N14	120	N5 AND N4	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/29 05:07 PM
N15	4	(N1 N2 N3) AND N6	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/29 05:07 PM
N16	37	(Artificial Intelligence) More like doc: US-20220247769-A1 Text: (US-11785104-B2 OR US-20220200869-A1 OR US-11894984-B2 OR US-11770398-B1 OR US-20220232025-A1 OR US-20220329616-A1 OR US-11895135-B2 OR US-20230032686-A1 OR US-20220224707-A1 OR US-11849000-B2 OR US-10425437-B1 OR US-	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/05/29 05:07 PM

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00168

		20220400129-A1 OR US-20220232024-A1 OR US-20230075355-A1 OR US-11818156-B1 OR US-10614071-B1 OR US-11470172-B1 OR US-11157502-B1 OR US-11637849-B1 OR US-11792284-B1).did.					
N17	120	N5 AND N4	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/29 05:11 PM
N18	1761	cloud WITH similar$7 WITH deploy$4	(US-PGPUB; USPAT)	OR	ON	ON	2024/05/31 10:58 AM

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/361,748	**05/29/2024 03:00:58 PM Z ET**	**L0041B1CIP2C1**

Title of Invention

Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4323	FILED BY	Ashley Jenkins
PATENT CENTER #	65718132	FILING DATE	07/28/2023
CUSTOMER #	182115	FIRST NAMED INVENTOR	ÚLFAR ERLINGSSON
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Edward Lenart

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
2024-05-29_L0041B1CIP2C1_IDS.pdf	4	Information Disclosure Statement (IDS) Form (SB08)	1252 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
2024-05-29_L0041B1CIP2C1_IDS.pdf	7372D0D435486D061E8F9B4DFDC5AFE6B23E8BAB597924210 41BD09D782E4AC4D8AE2CE2846CDD9DDE54CE4E25965CA1 6005B5D04131E1001098C7C6574D9445

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized

by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	18361748
Filing Date	2023-07-28
First Named Inventor	ÚLFAR ERLINGSSON
Art Unit	
Examiner Name	
Attorney Docket Number	L0041B1CIP2C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	11785104	B2	2023-10-10	Erlingsson et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Edward J. Lenart/	Date (YYYY-MM-DD)	2024-05-29
Name/Print	Edward J. Lenart	Registration Number	63,665

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UNITED STATES
PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

APPROVAL LETTER

APPLICATION #	FILING DATE	APPLICANT/PATENT UNDER REEXAMINATION
18/361,748	07/28/2023	ULFAR ERLINGSSON

Title of Invention

Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments

Electronic terminal disclaimer filed on 05/29/2024

☑ Approved

This patent is subject to a Terminal Disclaimer

Approved / Disapproved by: Electronic Terminal Disclaimer automatically approved

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A PRIOR PATENT

APPLICATION #	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET #
18361748	07/28/2023	ULFAR ERLINGSSON	L0041B1CIP2C1

Title of Invention

Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments

☑ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☑ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
LACEWORK, INC.	100%
Total	100%

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number(s)

Application #	Filing Date

as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the

instant application and is binding upon the grantee, its successors or assigns.
In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that any such patent granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

Patent #
11785104

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.
In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:

- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.



Terminal disclaimer fee under 37 CFR 1.20(d) included with Electronic Terminal Disclaimer request.

Applicant claims the following entity status:
Regular Undiscounted

I hereby declare that all statements made herein of my own knowledge are true and that all statemnts made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I certify, in accordance with 37 CFR 1.4(d)(4) that I am: An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

Signature	Name	Registration #
/Edward Lenart/	Edward Lenart	63665

* Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner). Form PTO/SB/96 may be used for making this certification. See MPEP 324.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/361,748	**05/29/2024 02:00:23 PM Z ET**	**L0041B1CIP2C1**

Title of Invention

Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4323	FILED BY	Edward Lenart
PATENT CENTER #	65715896	FILING DATE	07/28/2023
CUSTOMER #	182115	FIRST NAMED INVENTOR	ÚLFAR ERLINGSSON
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
petition-request.pdf	3	Terminal Disclaimer-Filed (Electronic)	48 KB
grantLetter.pdf	1	Terminal Disclaimer-Electronic-Approved	19 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
petition-request.pdf	C0BEFDFED373E0B708399B13241CA88316B2A8608E255CD6A4E4A2989045C9926080F64787F67D3420F9CCE0A0F56627FA0

A1254D937A6E04572243D5896B9C7

grantLetter.pdf

BCBCCAEC9F163C23949AC57D438FFDBF38DD973502AF5FC2
2F96DD09EEB39C091864DEEF792EB3573AA02A08EA426B741
FB4CA1863F48E8B4F53782B49D9E384

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/361,748	05/29/2024 02:00:23 PM Z ET	L0041B1CIP2C1

Title of Invention

Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4323	FILED BY	Edward Lenart
PATENT CENTER #	65715896	AUTHORIZED BY	-
CUSTOMER #	182115	FILING DATE	07/28/2023
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	ÚLFAR ERLINGSSON

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 2001	E20245SE00515631	Edward Lenart

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
1814	STATUTORY DISCLAIMER, INCLUDING TERMINAL DISCLAIMER	170.00	1	170.00
			TOTAL AMOUNT:	$170.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/361,748	**12/07/2023 01:15:29 PM Z ET**	**L0041B1CIP2C1**

Title of Invention

Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4323	FILED BY	Mindy Kennedy
PATENT CENTER #	63527035	FILING DATE	07/28/2023
CUSTOMER #	182115	FIRST NAMED INVENTOR	ÚLFAR ERLINGSSON
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Edward Lenart

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
2023-12-07_L0041B1CIP2C1_IDS.pdf	22	Information Disclosure Statement (IDS) Form (SB08)	1256 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
2023-12-07_L0041B1CIP2C1_IDS.pdf	AB01BC888DA1E872C327E2766F66C8BE39FC2D33667DB2F03368A9DA0051BD49BB91620134061BB4732298E55C8E91EF70BF3BA4B1E35D810A92FE80ADBE5FD6

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized

by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	10003605	B2	2018-06-19	Muddu et al.	
	2	10116670	B2	2018-10-30	Muddu et al.	
	3	10148677	B2	2018-12-04	Muddu et al.	
	4	10158652	B2	2018-12-18	Muddu et al.	
	5	10205735	B2	2019-02-12	Apostolopoulos	
	6	10243970	B2	2019-03-26	Muddu et al.	
	7	10254848	B2	2019-04-09	Winternitz et al.	
	8	10338895	B2	2019-07-02	Zhang et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	9	10389738	B2	2019-08-20	Muddu et al.	
	10	10419463	B2	2019-09-17	Muddu et al.	
	11	10419465	B2	2019-09-17	Muddu et al.	
	12	10432639	B1	2019-10-01	Bebee et al.	
	13	10454889	B2	2019-10-22	HUANG	
	14	10459979	B2	2019-10-29	Piechowicz et al.	
	15	10462169	B2	2019-10-29	DURAIRAJ et al.	
	16	10491705	B2	2019-11-26	Oetting et al.	
	17	10496468	B2	2019-12-03	Gefen et al.	
	18	10534633	B2	2020-01-14	Hilemon et al.	
	19	10666668	B2	2020-05-26	Muddu et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	20	10673880	B1	2020-06-02	Pratt et al.	
	21	10693900	B2	2020-06-23	Zadeh et al.	
	22	10698954	B2	2020-06-30	Piechowicz et al.	
	23	10756982	B2	2020-08-25	Bai et al.	
	24	10771488	B2	2020-09-08	Verma et al.	
	25	10776191	B2	2020-09-15	Zheng et al.	
	26	10788570	B2	2020-09-29	Wilson	
	27	11036716	B2	2021-06-15	Griffith et al.	
	28	11044264	B2	2021-06-22	DURAIRAJ et al.	
	29	11082289	B2	2021-08-03	Dang et al.	
	30	11120343	B2	2021-09-14	Das et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	31	11126533	B2	2021-09-21	Knowles et al.	
	32	11194849	B2	2021-12-07	Lassoued et al.	
	33	11212299	B2	2021-12-28	Gamble et al.	
	34	11258807	B2	2022-02-22	Muddu et al.	
	35	11281519	B2	2022-03-22	Krishnaswamy et al.	
	36	11314789	B2	2022-04-26	Goldfarb	
	37	11411966	B2	2022-08-09	Muddu et al.	
	38	11463464	B2	2022-10-04	Zadeh et al.	
	39	11494787	B2	2022-11-08	Erickson et al.	
	40	11544138	B2	2023-01-03	Kapish et al.	
	41	11606272	B1	2023-03-14	Popelka et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	42	11636090	B2	2023-04-25	Li et al.	
	43	11640388	B2	2023-05-02	Yang et al.	
	44	11647034	B2	2023-05-09	Levin et al.	
	45	11658990	B2	2023-05-23	Shapoury	
	46	11669571	B2	2023-06-06	Binkley et al.	
	47	11693958	B1	2023-07-04	Steiman	
	48	11722554	B2	2023-08-08	Keren et al.	
	49	11734351	B2	2023-08-22	Binkley et al.	
	50	11734419	B1	2023-08-22	Mackle	
	51	11748473	B2	2023-09-05	Araujo et al.	
	52	11755576	B1	2023-09-12	Jiang et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	53	11755602	B2	2023-09-12	Smith Shawn et al.	
	54	11769098	B2	2023-09-26	Adinarayan et al.	
	55	11770387	B1	2023-09-26	Shivamoggi et al.	
	56	7233333	B2	2007-06-19	Lomask	
	57	7478246	B2	2009-01-13	Arndt et al.	
	58	7484091	B2	2009-01-27	Bade et al.	
	59	7526501	B2	2009-04-28	Albahari et al.	
	60	7707411	B2	2010-04-27	Bade et al.	
	61	7739211	B2	2010-06-15	Coffman et al.	
	62	7747559	B2	2010-06-29	Leitner et al.	
	63	7765431	B2	2010-07-27	Agha et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	64	8050907	B2	2011-11-01	Baisley et al.	
	65	8086852	B2	2011-12-27	Bade et al.	
	66	8140977	B2	2012-03-20	Kriss et al.	
	67	8160999	B2	2012-04-17	Jin et al.	
	68	8209204	B2	2012-06-26	Adler et al.	
	69	8301660	B2	2012-10-30	Yalamanchi	
	70	8490055	B2	2013-07-16	Basak	
	71	9043764	B2	2015-05-26	Ranganathan et al.	
	72	9053437	B2	2015-06-09	Adler et al.	
	73	9064210	B1	2015-06-23	Hart	
	74	9075618	B2	2015-07-07	Winternitz et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	75	9110873	B2	2015-08-18	Woodall et al.	
	76	9159024	B2	2015-10-13	Bhanot et al.	
	77	9189623	B1	2015-11-17	Lin et al.	
	78	9589069	B2	2017-03-07	Yang et al.	
	79	9591010	B1	2017-03-07	Muddu et al.	
	80	9600915	B2	2017-03-21	Winternitz et al.	
	81	9667641	B2	2017-05-30	Muddu et al.	
	82	9679243	B2	2017-06-13	Zou et al.	
	83	9699205	B2	2017-07-04	Muddu et al.	
	84	9710332	B1	2017-07-18	Fan et al.	
	85	9720703	B2	2017-08-01	Reick et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	86	9720704	B2	2017-08-01	Reick et al.	
	87	9727441	B2	2017-08-08	Agarwal et al.	
	88	9727604	B2	2017-08-08	Jin et al.	
	89	9813435	B2	2017-11-07	Muddu et al.	
	90	9824473	B2	2017-11-21	Winternitz et al.	
	91	9838410	B2	2017-12-05	Muddu et al.	
	92	9843837	B2	2017-12-12	Gopalan	
	93	9864672	B2	2018-01-09	Seto et al.	
	94	9985827	B2	2018-05-29	Li et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	1	20040225929	A1	2007-01-23	Agha et al.	
	2	20050246521	A1	2009-01-27	Bade et al.	
	3	20060025987	A1	2006-02-02	Baisley et al.	
	4	20060026419	A1	2009-01-13	Arndt et al.	
	5	20060109271	A1	2007-06-19	Lomask	
	6	20070214111	A1	2017-08-08	Jin et al.	
	7	20070282916	A1	2007-12-06	Albahari et al.	
	8	20080109730	A1	2008-05-08	Coffman et al.	
	9	20080147707	A1	2012-04-17	Jin et al.	
	10	20090006843	A1	2011-12-27	Bade et al.	
	11	20090007010	A1	2009-01-01	Kriss et al.	

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00195

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	12	20090063857	A1	2010-04-27	Bade et al.	
	13	20090307651	A1	2009-12-10	Senthil et al.	
	14	20090327328	A1	2015-08-18	Woodall et al.	
	15	20100042823	A1	2011-08-09	Arndt et al.	
	16	20110119100	A1	2011-05-19	Ruhl et al.	
	17	20110154287	A1	2011-06-23	Mukkamala et al.	
	18	20120143898	A1	2012-06-07	Bruno et al.	
	19	20120159333	A1	2012-06-21	Mital et al.	
	20	20130024412	A1	2013-01-24	Gong et al.	
	21	20130151453	A1	2013-06-13	Bhanot et al.	
	22	20140067750	A1	2015-05-26	Ranganathan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	23	20140125672	A1	2015-07-07	Winternitz et al.	
	24	20140279779	A1	2017-06-13	Zou et al.	
	25	20150310649	A1	2017-03-21	Winternitz et al.	
	26	20160120070	A1	2016-04-28	Myrah et al.	
	27	20160357521	A1	2019-07-02	Zhang et al.	
	28	20170063888	A1	2017-03-02	Muddu et al.	
	29	20170063903	A1	2017-03-02	Muddu et al.	
	30	20170063905	A1	2017-03-02	Muddu et al.	
	31	20170063909	A1	2017-03-02	Muddu et al.	
	32	20170063911	A1	2017-03-02	Muddu et al.	
	33	20170070594	A1	2019-11-26	Oetting et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	34	20170102961	A1	2020-01-14	Hilemon et al.	
	35	20170118099	A1	2017-04-27	HUANG	
	36	20170142140	A1	2017-05-18	Muddu et al.	
	37	20170148197	A1	2017-05-25	Winternitz et al.	
	38	20170155570	A1	2017-06-01	Maheshwari et al.	
	39	20170155672	A1	2017-06-01	Muthukrishnan et al.	
	40	20170223036	A1	2017-08-03	Muddu et al.	
	41	20170346683	A1	2018-05-29	Li et al.	
	42	20180004835	A1	2018-01-04	Piechowicz et al.	
	43	20180004859	A1	2020-06-30	Piechowicz et al.	
	44	20180007145	A1	2019-10-29	Piechowicz et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	45	20180089132	A1	2018-03-29	Atta et al.	
	46	20180191781	A1	2018-07-05	Palani et al.	
	47	20180211425	A1	2018-07-26	Winternitz et al.	
	48	20180219888	A1	2018-08-02	Apostolopoulos	
	49	20180219897	A1	2018-08-02	Muddu et al.	
	50	20180359162	A1	2018-12-13	Savov et al.	
	51	20190042950	A1	2019-02-07	Lin et al.	
	52	20190050445	A1	2021-06-15	Griffith et al.	
	53	20190058626	A1	2019-02-21	Knowles et al.	
	54	20190075126	A1	2019-03-07	Muddu et al.	
	55	20190101622	A1	2019-04-04	Wilson	

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00199

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	56	20190163555	A1	2019-05-30	Zheng et al.	
	57	20190227860	A1	2019-12-03	Gefen et al.	
	58	20190312898	A1	2019-10-10	Verma et al.	
	59	20190327251	A1	2019-10-24	Muddu et al.	
	60	20190342307	A1	2019-11-07	Gamble et al.	
	61	20190354554	A1	2019-11-21	Piechowicz et al.	
	62	20190356555	A1	2020-08-25	Bai et al.	
	63	20200014718	A1	2020-01-09	DURAIRAJ et al.	
	64	20200021607	A1	2020-01-16	Muddu et al.	
	65	20200175361	A1	2020-06-04	Che et al.	
	66	20200287923	A1	2020-09-10	Raghavendra et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	67	20200320106	A1	2022-04-26	Goldfarb	
	68	20200334293	A1	2020-10-22	Piechowicz et al.	
	69	20200351151	A1	2020-11-05	Dang et al.	
	70	20200412752	A1	2020-12-31	Shapoury	
	71	20210019209	A1	2021-01-21	Krishnaswamy et al.	
	72	20210232420	A1	2021-07-29	Dhruvakumar et al.	
	73	20210286798	A1	2021-09-16	Li et al.	
	74	20210294798	A1	2021-09-23	Binkley et al.	
	75	20210406917	A1	2021-12-30	Erickson et al.	
	76	20220004718	A1	2022-01-06	Quamar et al.	
	77	20220050840	A1	2022-02-17	Parravicini et al.	

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00201

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	78	20220058193	A1	2023-09-12	Smith Shawn et al.	
	79	20220067186	A1	2022-03-03	Thakur et al.	
	80	20220086179	A1	2023-05-09	Levin et al.	
	81	20220092481	A1	2022-03-24	Neithalath et al.	
	82	20220121741	A1	2023-09-05	Araujo et al.	
	83	20220124108	A1	2022-04-21	Gamble et al.	
	84	20220129803	A1	2022-04-28	Bikumala et al.	
	85	20220191226	A1	2022-06-16	Chan et al.	
	86	20220327119	A1	2022-10-13	Gasper et al.	
	87	20220350789	A1	2023-05-02	Yang et al.	
	88	20220374800	A1	2023-09-26	Adinarayan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	89	20220376970	A1	2022-11-24	Chawathe et al.	
	90	20220382611	A1	2023-01-03	Kapish et al.	
	91	20220394082	A1	2022-12-08	Keren et al.	
	92	20220414072	A1	2022-12-29	Tandon et al.	
	93	20220414105	A1	2022-12-29	Umay et al.	
	94	20230025252	A1	2023-01-26	Erickson et al.	
	95	20230039566	A1	2023-02-09	Ghag et al.	
	96	20230052827	A1	2023-02-16	Araujo et al.	
	97	20230088960	A1	2023-03-23	Popelka et al.	
	98	20230096930	A1	2023-03-30	Dasdan	
	99	20230101773	A1	2023-03-30	Katahanas et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	100	20230138371	A1	2023-05-04	Bandukwala et al.	
	101	20230244523	A1	2023-08-03	Gorantla et al.	
	102	20230251960	A1	2023-08-10	Sharma et al.	
	103	20230275909	A1	2023-08-31	Shivamoggi et al.	
	104	20230291755	A1	2023-09-14	Siebel et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00204

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Edward J. Lenart/	Date (YYYY-MM-DD)	2023-12-07
Name/Print	Edward J. Lenart	Registration Number	63,665

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
18/361,748	07/28/2023		2240	L0041B1CIP2C1	20	3

CONFIRMATION NO. 4323

182115
Lacework, Inc.
c/o Kennedy Lenart Spraggins LLP
797 Sam Bass Road #2559
ROUND ROCK, TX 78681

FILING RECEIPT

OC000000086867149

Date Mailed: 08/23/2023

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

ÚLFAR ERLINGSSON, PALO ALTO, CA;
YIJOU CHEN, CUPERTINO, CA;

Applicant(s)

LACEWORK, INC., MOUNTAIN VIEW, CA;

Power of Attorney: The patent practitioners associated with Customer Number 182115

Domestic Priority data as claimed by applicant

This application is a CON of 17/671,199 02/14/2022
which is a CIP of 17/504,311 10/18/2021 PAT 11,677,772
which is a CON of 16/665,961 10/28/2019 PAT 11,153,339
which is a CON of 16/134,794 09/18/2018 PAT 10,581,891
which claims benefit of 62/650,971 03/30/2018
and claims benefit of 62/590,986 11/27/2017
and said 17/671,199 02/14/2022 claims benefit of 63/243,013 09/10/2021

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 08/21/2023

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 18/361,748**

Projected Publication Date: Request for Non-Publication Acknowledged

Non-Publication Request: Yes

Early Publication Request: No

Title

Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00209

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00210

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00211

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 18/361,748

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	320
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	700
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	800
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	* 0			OR	x =	0
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*				x =	0
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						420
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	2240

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	18361748
Filing Date	2023-07-28
First Named Inventor	ÚLFAR ERLINGSSON
Art Unit	
Examiner Name	
Attorney Docket Number	L0041B1CIP2C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	10033611	B1	2018-07-24	Linkous et al.	
	2	10104071	B2	2018-10-16	Gordon et al.	
	3	10115111	B2	2018-10-30	Miltonberger	
	4	10121000	B1	2018-11-06	Rivlin et al.	
	5	10122740	B1	2018-11-06	Finkelshtein et al.	
	6	10127273	B2	2018-11-13	Dickey	
	7	10142357	B1	2018-11-27	Tamersoy et al.	
	8	10149148	B2	2018-12-04	Zha et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	9	10182058	B2	2019-01-15	Xu	
	10	10205736	B2	2019-02-12	Rieke et al.	
	11	10237254	B2	2019-03-19	McDowell et al.	
	12	10237294	B1	2019-03-19	Zadeh et al.	
	13	10249266	B2	2019-04-02	Zamir	
	14	10331659	B2	2019-06-25	Ahuja et al.	
	15	10339309	B1	2019-07-02	Kling et al.	
	16	10367704	B2	2019-07-30	Giura et al.	
	17	10382303	B2	2019-08-13	Khanal et al.	
	18	10382529	B2	2019-08-13	WAN et al.	
	19	10389742	B2	2019-08-20	Reddy et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	20	10419468	B2	2019-09-17	Glatfelter et al.	
	21	10419469	B1	2019-09-17	Singh et al.	
	22	10425437	B1	2019-09-24	Bog et al.	
	23	10447526	B2	2019-10-15	Tucker et al.	
	24	10454753	B2	2019-10-22	Sasturkar et al.	
	25	10496263	B2	2019-12-03	So et al.	
	26	10496678	B1	2019-12-03	Tang	
	27	10505818	B1	2019-12-10	Yona et al.	
	28	10510007	B2	2019-12-17	Singhal et al.	
	29	10515095	B2	2019-12-24	Childress et al.	
	30	10521584	B1	2019-12-31	Mehr	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	31	10565373	B1	2020-02-18	Rao et al.	
	32	10581891	B1	2020-03-03	Kapoor et al.	
	33	10587609	B2	2020-03-10	Ebrahimi et al.	
	34	10592535	B2	2020-03-17	Ahn et al.	
	35	10594718	B1	2020-03-17	Deaguero et al.	
	36	10599718	B2	2020-03-24	Kumar et al.	
	37	10614200	B2	2020-04-07	Betz et al.	
	38	10642867	B2	2020-05-05	Palanciuc	
	39	10656979	B2	2020-05-19	Ishakian et al.	
	40	10664757	B2	2020-05-26	Lastras-Montano et al.	
	41	10685295	B1	2020-06-16	Ross et al.	

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00216

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	42	10701051	B2	2020-06-30	Ohsumi	
	43	10708082	B1	2020-07-07	Bakiaraj et al.	
	44	10735329	B2	2020-08-04	WANG et al.	
	45	10754940	B2	2020-08-25	Ohsumi	
	46	10775183	B2	2020-09-15	Ho et al.	
	47	10791131	B2	2020-09-29	Nor et al.	
	48	10797974	B2	2020-10-06	Giura et al.	
	49	10812497	B2	2020-10-20	Venkatramani et al.	
	50	10824675	B2	2020-11-03	Alonso et al.	
	51	10824813	B2	2020-11-03	Smith et al.	
	52	10885452	B1	2021-01-05	Garg	

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00217

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	53	10904007	B2	2021-01-26	Kim et al.	
	54	10904270	B2	2021-01-26	Muddu et al.	
	55	10911470	B2	2021-02-02	Muddu et al.	
	56	10951648	B2	2021-03-16	DORON et al.	
	57	10986114	B1	2021-04-20	Singh et al.	
	58	11036800	B1	2021-06-15	Kayyoor et al.	
	59	11048492	B2	2021-06-29	Jain et al.	
	60	11080392	B2	2021-08-03	Bennett et al.	
	61	11153339	B1	2021-10-19	Kapoor et al.	
	62	11233821	B2	2022-01-25	Yadav et al.	
	63	11431735	B2	2022-08-30	SHUA	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	64	11489863	B1	2022-11-01	Shua et al.	
	65	11575693	B1	2023-02-07	Muddu et al.	
	66	11677772	B1	2023-06-13	Kapoor et al.	
	67	5584024	A	1996-12-10	Shwartz	
	68	5806062	A	1998-09-08	Chen et al.	
	69	6347339	B1	2002-02-12	Morris et al.	
	70	6363411	B1	2002-03-26	Dugan et al.	
	71	6434663	B1	2002-08-13	Grimsrud et al.	
	72	6938084	B2	2005-08-30	Gamache et al.	
	73	7054873	B2	2006-05-30	Nordström et al.	
	74	7310733	B1	2007-12-18	Pearson et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	75	7529801	B2	2009-05-05	Moore et al.	
	76	7562045	B2	2009-07-14	Beadle et al.	
	77	7743153	B2	2010-06-22	Hall et al.	
	78	7797548	B2	2010-09-14	Pearson et al.	
	79	7856544	B2	2010-12-21	Schenfeld et al.	
	80	7926026	B2	2011-04-12	Klein et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020059531	A1	2002-05-16	On	
	2	20020161889	A1	2002-10-31	Gamache et al.	
	3	20020184225	A1	2002-12-05	Ghukasyan	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	4	20030037136	A1	2003-02-20	Labovitz et al.	
	5	20030179227	A1	2003-09-25	Ahmad et al.	
	6	20030233361	A1	2003-12-18	Cady	
	7	20040015470	A1	2004-01-22	Smith et al.	
	8	20050060287	A1	2005-03-17	Hellman et al.	
	9	20050102284	A1	2005-05-12	Srinivasan et al.	
	10	20050102365	A1	2005-05-12	Moore et al.	
	11	20050108142	A1	2005-05-19	Beadle et al.	
	12	20050188222	A1	2005-08-25	Motsinger et al.	
	13	20050231760	A1	2005-10-20	Minato	
	14	20050246288	A1	2005-11-03	Kimura et al.	

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00221

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	15	20060036896	A1	2006-02-16	Gamache et al.	
	16	20060085437	A1	2006-04-20	Brodhun et al.	
	17	20060090095	A1	2006-04-27	Massa et al.	
	18	20060259470	A1	2006-11-16	Chandrasekharan et al.	
	19	20060288415	A1	2006-12-21	Wong	
	20	20070050497	A1	2007-03-01	Haley et al.	
	21	20070118909	A1	2007-05-24	Hertzog et al.	
	22	20070130330	A1	2007-06-07	Ridel et al.	
	23	20070162605	A1	2007-07-12	Chalasani et al.	
	24	20070162963	A1	2007-07-12	Penet et al.	
	25	20070168696	A1	2007-07-19	Ridel et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	26	20070169175	A1	2007-07-19	Hall et al.	
	27	20070225956	A1	2007-09-27	Pratt et al.	
	28	20070266425	A1	2007-11-15	Cho	
	29	20080034411	A1	2008-02-07	Aoyama	
	30	20080065879	A1	2008-03-13	Song et al.	
	31	20080072062	A1	2008-03-20	Pearson et al.	
	32	20080148180	A1	2008-06-19	Liu et al.	
	33	20080151893	A1	2008-06-26	Nordmark et al.	
	34	20080155335	A1	2008-06-26	Klein et al.	
	35	20080244718	A1	2008-10-02	Frost et al.	
	36	20080263643	A1	2008-10-23	Jaiswal et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	37	20080270451	A1	2008-10-30	Thomsen et al.	
	38	20090019160	A1	2009-01-15	Schuler	
	39	20090165109	A1	2009-06-25	Hird	
	40	20090177573	A1	2009-07-09	Beadle et al.	
	41	20090222740	A1	2009-09-03	Yuan	
	42	20090228474	A1	2009-09-10	Chiu et al.	
	43	20090271504	A1	2009-10-29	Ginter et al.	
	44	20090287720	A1	2009-11-19	Herter et al.	
	45	20100094767	A1	2010-04-15	Miltonberger	
	46	20100114931	A1	2010-05-06	Xie et al.	
	47	20100172261	A1	2010-07-08	Shinbo et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	48	20100217860	A1	2010-08-26	Naidu et al.	
	49	20100274785	A1	2010-10-28	Procopiuc et al.	
	50	20100309206	A1	2010-12-09	Xie et al.	
	51	20100329162	A1	2010-12-30	Kadous et al.	
	52	20110023098	A1	2011-01-27	Pearson et al.	
	53	20110029952	A1	2011-02-03	Harrington	
	54	20110055138	A1	2011-03-03	Khanduja et al.	
	55	20110302631	A1	2011-12-08	Sureshchandra et al.	
	56	20120005243	A1	2012-01-05	Merwe et al.	
	57	20120054732	A1	2012-03-01	Jain et al.	
	58	20120089875	A1	2012-04-12	Faust et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	59	20120102029	A1	2012-04-26	Larson et al.	
	60	20120158858	A1	2012-06-21	Gkantsidis et al.	
	61	20120173541	A1	2012-07-05	Venkataramani	
	62	20120317149	A1	2012-12-13	Jagota et al.	
	63	20120317151	A1	2012-12-13	Ruf et al.	
	64	20120323956	A1	2012-12-20	Dumitru et al.	
	65	20130067100	A1	2013-03-14	Kuzin et al.	
	66	20130081118	A1	2013-03-28	Ge	
	67	20130086667	A1	2013-04-04	Haven	
	68	20130097320	A1	2013-04-18	Ritter et al.	
	69	20130173915	A1	2013-07-04	Haulund	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	70	20130205357	A1	2013-08-08	Bahnck et al.	
	71	20130205357	A1	2013-08-08	Bahnck et al.	
	72	20130219295	A1	2013-08-22	Feldman et al.	
	73	20130269007	A1	2013-10-10	Yoshigaki et al.	
	74	20130304915	A1	2013-11-14	KAWAI	
	75	20140041005	A1	2014-02-06	HE	
	76	20140098101	A1	2014-04-10	Friedlander et al.	
	77	20140115001	A1	2014-04-24	Arroyo et al.	
	78	20140115011	A1	2014-04-24	Buerner et al.	
	79	20140181944	A1	2014-06-26	Ahmed et al.	
	80	20140208191	A1	2014-07-24	Zaric et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	81	20140229607	A1	2014-08-14	Jung et al.	
	82	20140245443	A1	2014-08-28	Chakraborty	
	83	20140280068	A1	2014-09-18	DHOOPAR et al.	
	84	20140325631	A1	2014-10-30	Pearson et al.	
	85	20140359558	A1	2014-12-04	Chamberlain	
	86	20140379716	A1	2014-12-25	Branch et al.	
	87	20150058619	A1	2015-02-26	Sweet et al.	
	88	20150135312	A1	2015-05-14	Wada et al.	
	89	20150161201	A1	2015-06-11	Sadikov et al.	
	90	20150172321	A1	2015-06-18	Kirti et al.	
	91	20150188751	A1	2015-07-02	Vasseur et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	92	20150213598	A1	2015-07-30	Madabhushi et al.	
	93	20150302440	A1	2015-10-22	Monden et al.	
	94	20150319185	A1	2015-11-05	Kirti et al.	
	95	20150341379	A1	2015-11-26	Lefebvre et al.	
	96	20150356144	A1	2015-12-10	Chawla et al.	
	97	20160036837	A1	2016-02-04	Jain et al.	
	98	20160063226	A1	2016-03-03	Singh et al.	
	99	20160078365	A1	2016-03-17	Baumard	
	100	20160080204	A1	2016-03-17	MISHRA et al.	
	101	20160080404	A1	2016-03-17	KOHOUT et al.	
	102	20160110434	A1	2016-04-21	Kakaraddi et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	103	20160149937	A1	2016-05-26	KATMOR et al.	
	104	20160203411	A1	2016-07-14	Sadikov et al.	
	105	20160205125	A1	2016-07-14	Kim et al.	
	106	20160218911	A1	2016-07-28	WESSELS et al.	
	107	20160261544	A1	2016-09-08	Conover	
	108	20160330183	A1	2016-11-10	McDowell et al.	
	109	20160330206	A1	2016-11-10	Xu	
	110	20160359592	A1	2016-12-08	Kulshreshtha et al.	
	111	20160359872	A1	2016-12-08	Yadav et al.	
	112	20160373428	A1	2016-12-22	Shi	
	113	20170063830	A1	2017-03-02	Huang	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	114	20170063906	A1	2017-03-02	Muddu et al.	
	115	20170063908	A1	2017-03-02	Muddu et al.	
	116	20170063910	A1	2017-03-02	Muddu et al.	
	117	20170063912	A1	2017-03-02	Muddu et al.	
	118	20170076206	A1	2017-03-16	Lastras-Montano et al.	
	119	20170085553	A1	2017-03-23	Gordon et al.	
	120	20170086069	A1	2017-03-23	Liu	
	121	20170111245	A1	2017-04-20	Ishakian et al.	
	122	20170116315	A1	2017-04-27	Xiong et al.	
	123	20170118240	A1	2017-04-27	Reddy et al.	
	124	20170134240	A1	2017-05-11	Hévizi et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	125	20170147646	A1	2017-05-25	LEE et al.	
	126	20170163666	A1	2017-06-08	Venkatramani et al.	
	127	20170230183	A1	2017-08-10	Sweet et al.	
	128	20170249069	A1	2017-08-31	Zamir	
	129	20170251013	A1	2017-08-31	Kirti et al.	
	130	20170257358	A1	2017-09-07	Ebrahimi et al.	
	131	20170262521	A1	2017-09-14	Cho et al.	
	132	20170272344	A1	2017-09-21	Tang et al.	
	133	20170277553	A1	2017-09-28	Zada et al.	
	134	20170277997	A1	2017-09-28	Zong et al.	
	135	20170279827	A1	2017-09-28	Savalle et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	136	20170286190	A1	2017-10-05	Ishakian et al.	
	137	20170288974	A1	2017-10-05	Yoshihira et al.	
	138	20170330096	A1	2017-11-16	Gupta et al.	
	139	20170337262	A1	2017-11-23	Smith et al.	
	140	20170353853	A1	2017-12-07	Zha et al.	
	141	20170359361	A1	2017-12-14	Modani et al.	
	142	20170366492	A1	2017-12-21	Ho et al.	
	143	20180013650	A1	2018-01-11	Khanal et al.	
	144	20180019932	A1	2018-01-18	Giura et al.	
	145	20180020015	A1	2018-01-18	Munro et al.	
	146	20180025361	A1	2018-01-25	Llagostera et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	147	20180034840	A1	2018-02-01	Marquardt et al.	
	148	20180039688	A1	2018-02-08	Ahn et al.	
	149	20180063178	A1	2018-03-01	Jadhav et al.	
	150	20180067981	A1	2018-03-08	Ahuja et al.	
	151	20180069885	A1	2018-03-08	Patterson et al.	
	152	20180084069	A1	2018-03-22	Be'ery et al.	
	153	20180096047	A1	2018-04-05	Childress et al.	
	154	20180097793	A1	2018-04-05	Agarwal et al.	
	155	20180103052	A1	2018-04-12	Choudhury et al.	
	156	20180115578	A1	2018-04-26	Subbarayan et al.	
	157	20180123864	A1	2018-05-03	Tucker et al.	

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00234

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	158	20180124189	A1	2018-05-03	Edgington et al.	
	159	20180137858	A1	2018-05-17	Saxena et al.	
	160	20180139200	A1	2018-05-17	Gordon et al.	
	161	20180173789	A1	2018-06-21	Llagostera et al.	
	162	20180174062	A1	2018-06-21	Simo et al.	
	163	20180181750	A1	2018-06-28	Lamothe-Brassard	
	164	20180227286	A1	2018-08-09	Ohsumi	
	165	20180248901	A1	2018-08-30	Rieke	
	166	20180268078	A1	2018-09-20	Gianetto et al.	
	167	20180288063	A1	2018-10-04	Koottayi et al.	
	168	20180329958	A1	2018-11-15	Choudhury et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	169	20180336353	A1	2018-11-22	Manadhata et al.	
	170	20180357422	A1	2018-12-13	Telang et al.	
	171	20180367548	A1	2018-12-20	Stokes III et al.	
	172	20190028327	A1	2019-01-24	SILVA et al.	
	173	20190042879	A1	2019-02-07	MUNOZ	
	174	20190068627	A1	2019-02-28	Thampy	
	175	20190087480	A1	2019-03-21	Palanciuc	
	176	20190109870	A1	2019-04-11	BEDHAPUDI et al.	
	177	20190123973	A1	2019-04-25	Jeuk et al.	
	178	20190132224	A1	2019-05-02	VERMA et al.	
	179	20190149553	A1	2019-05-16	Xu	

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00236

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	180	20190158524	A1	2019-05-23	Zadeh et al.	
	181	20190222597	A1	2019-07-18	Crabtree et al.	
	182	20190259033	A1	2019-08-22	Reddy et al.	
	183	20190312796	A1	2019-10-10	Giura et al.	
	184	20190339965	A1	2019-11-07	Garvey et al.	
	185	20190342282	A1	2019-11-07	Carbune et al.	
	186	20190342311	A1	2019-11-07	Muddu et al.	
	187	20190349305	A1	2019-11-14	WANG et al.	
	188	20190364067	A1	2019-11-28	Yona et al.	
	189	20190378050	A1	2019-12-12	Edkin et al.	
	190	20200065857	A1	2020-02-27	Lagi et al.	

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00237

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	191	20200074341	A1	2020-03-05	He et al.	
	192	20200076685	A1	2020-03-05	Vaidya et al.	
	193	20200080856	A1	2020-03-12	Ho et al.	
	194	20200175042	A1	2020-06-04	Batruni	
	195	20200192690	A1	2020-06-18	Gupta et al.	
	196	20200218579	A1	2020-07-09	M et al.	
	197	20200228555	A1	2020-07-16	Wittenschlaeger	
	198	20200252376	A1	2020-08-06	Feng et al.	
	199	20200259852	A1	2020-08-13	Wolff et al.	
	200	20200272740	A1	2020-08-27	Obee et al.	
	201	20200274894	A1	2020-08-27	ARGOETI et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	202	20200278892	A1	2020-09-03	Nainar et al.	
	203	20200280592	A1	2020-09-03	Ithal et al.	
	204	20200285737	A1	2020-09-10	Kraus et al.	
	205	20200287927	A1	2020-09-10	Zadeh et al.	
	206	20200311644	A1	2020-10-01	WILLARD III et al.	
	207	20200403860	A1	2020-12-24	Lewis et al.	
	208	20200404008	A1	2020-12-24	Venkatramani et al.	
	209	20210182248	A1	2021-06-17	Jayanthi	
	210	20210329019	A1	2021-10-21	SHUA	
	211	20210336976	A1	2021-10-28	SHUA	
	212	20210377287	A1	2021-12-02	SHUA	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	213	20220092668	A1	2022-03-24	LU et al.	
	214	20220247769	A1	2022-08-04	Erlingsson et al.	
	215	20220342690	A1	2022-10-27	Shua	
	216	20220345480	A1	2022-10-27	Shua	
	217	20220345481	A1	2022-10-27	Shua	
	218	20220345483	A1	2022-10-27	Shua	
	219	20220350931	A1	2022-11-03	Shua	
	220	20220417273	A1	2022-12-29	Levin et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	110999250	CN	B	2021-11-05	Kirti et al.	Abstract only	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	2	114598840	CN	A	2022-06-07	Hua		☐
	3	2021052379	WO	A1	2021-03-25	Wu et al.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	AI-YASEEN et al., "Real-Time Intrusion Detection System Using Multi-Agent System", IAENG International Journal of Computer Science, volume 43, no. 1, February 2016, pp. 80-90, International Association of Engineers (IAENG), Hong Kong.	☐
	2	AKOGLU et al., "Graph-based Anomaly Detection and Description: A Survey", April 28, 2014.	☐
	3	AMIDON et al., “Program Fracture and Recombination for Efficient Automatic Code Reuse”, In 2015 IEEE High Performance Extreme Computing Conference (HPEC), September 2015, pp. 1-6, IEEE.org (online), DOI: 10.1109/HPEC.2015.7396314.	☐
	4	AMMAR et al., "Query Optimization Techniques in Graph Databases", International Journal of Database Management Systems (IIDMS), Vol. 8, No. 4, August 2016, pages 1-14 (Year: 2016).	☐
	5	BALASUBRAMANIYAN et al., "An Architecture For Intrusion Detection Using Autonomous Agents", In Proceedings 14th Annual Computer Security Applications Conference (Cat. No. 98EX217), 19 pages, June 1998, IEEE, DOI: 10.1109/CSAC.1998.738563.	☐
	6	BEUTEL et al., "User Behavior Modeling with Large-Scale Graph Analysis", Computer Science Department, Carnegie Mellon University, May 2016.	☐
	7	BUGIEL et al., "Towards Taming Privilege-Escalation Attacks on Android", In NOSS (Vol. 17, p. 19), 2012, February.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	8	CHANG et al., "Reality Bites - Progressive Querying and Result Visualization in Logical and VR Spaces", Proceedings of 1994 IEEE Symposium on Visual Languages, pp. 100-109, October 1994, IEEE, DOI: 10.1109NL.1994.363635.	☐
	9	CHESSON, "Communication And Control In A Cluster Network", ACM '74: Proceedings of the 1974 annual ACM conference - Volume 2, January 1974, pp 509-514, http://doi.org/10.1145/1408839 (Year 1974).	☐
	10	CROSBIE et al., “Defending a Computer System using Autonomous Agents”, docs.lib.purdue.edu (online), March 1995, 11 pages.	☐
	11	HAUTAMAKI et al., "Outlier Detection Using k-Nearest Neighbour Graph", Proceedings of the 17th International Conference on Pattern Recognition (ICPR 2004), Vol. 3, August 2004, IEEE, DOI: 10.1109/ICPR.2004.1334558.	☐
	12	HOOPER et al., "Medusa: a simple tool for interaction graph analysis", Bioinformatics, Vol. 21 no. 24, September 2005, pages 4432-4433, Oxford University Press (online), URL: https://academic.oup.com/bioinformatics/article/21/24/4432/179694.	☐
	13	KOUTRA et al., "Exploring and Making Sense of Large Graphs", Computer Science Department, Carnegie Mellon University, August 2015.	☐
	14	LEOPOLD et al., "A Visual Query System for the Specification and Scientific Analysis off Continual Queries", Proceedings, IEEE Symposia on Human-Centric Computing Languages and Environments (Cat. No.01TH8587), September 2001, pp. 203-211, IEEE, doi: 10.1109/HCC.2001.995260.	☐
	15	LIAO et al., "Visualizing Graph Dynamics And Similarity For Enterprise Network Security And Management", VizSec '10: Proceedings of the Seventh International Symposium on Visualization for Cyber Security, September 2010, pp. 34-45, URL: https://doi.org/10.1145/1850795.1850799.	☐
	16	LONG et al., “Automatic Input Rectification”, 2012 34th International Conference on Software Engineering (ICSE), June 2012, pp. 80-90, IEEE.org (online), DOI: 10.1109/ICSE.2012.6227204.	☐
	17	MATEESCU et al., "Join-Graph Propagation Algorithms", Journal of Artificial Intelligence Research, vol. 37, March 2010, pages 279-328, AI Access Foundation, Inc. (online), URL: https://doi.org/10.1613/jair.2842.	☐
	18	MORIANO et al., "Insider Threat Event Detection in User-System Interactions", MIST '17: Proceedings of the 2017 International Workshop on Managing Insider Security Threats, October 2017, pp 1-12, ACM Digital Library (online), URL: https://doi.Jrg/10.1145/3139923.3139928.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	19	PERKINS et al., “Automatically Patching Errors in Deployed Software”, Proceedings of the ACM SIGOPS 22nd Symposium on Operating Systems Principles, October 2009, pp 82-102, acm.org (online), URL: https://doi.org/10.1145/1629575.1629585.	☐
	20	RANSHOUS et al., "Anomaly detection in dynamic networks: a survey", WIREs Computational Statistics, volume 7, May/June 2015, pp. 223-247, Wiley Periodicals, Inc, United States.	☐
	21	RINARD, “Living In The Comfort Zone”, ACM SIGPLAN Notices, Volume 42, Issue 10, October 2007, pp. 611-622, acm.org (online), URL: https://doi.org/10.1145/1297105.1297072.	☐
	22	RINARD, “Manipulating Program Functionality to Eliminate Security Vulnerabilities”, In Moving Target Defense, January 2011, pp. 109-115. Springer, New York, NY.	☐
	23	SAMUEL et al., “Let’s Parse to Prevent Pwnage”, Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats (LEET’12), April 2012, 3 pages, acm.org (online), URL: https://www.usenix.org/conference/leet12/workshop-program/presentation/samuel.	☐
	24	SHEN et al., “Active Learning for Inference and Regeneration of Applications that Access Databases”, ACM Transactions on Programming Languages and Systems (TOPLAS), Volume 42, Issue 4, Article 18, January 2021, pp. 1-119, acm.org (online), URL: https://doi.org/10.1145/3430952.	☐
	25	TAMASSIA et al., "Graph Drawing for Security Visualization", In: Graph Drawing (GD 2008), Lecture Notes in Computer Science, vol 5417, Springer, Berlin, Heidelberg (online), URL: https://doi.org/10.1007/978-3-642-00219-9_2.	☐
	26	VAAS et al., "Detecting disguised processes using Application-Behavior Profiling", In 2017 IEEE International Symposium on Technologies for Homeland Security (HST), pp. 1-6, June 2017, IEEE, DOI: 10.1109/THS.2017.7943508.	☐
	27	VASILAKIS et al., “Supply-Chain Vulnerability Elimination via Active Learning and Regeneration”, Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, November 2021, pp. 1755-1770, acm.org (online), URL: https://doi.org/10.1145/3460120.3484736.	☐
	28	YU et al., "Recommending Join Queries Based on Path Frequency", 2015 12th Web Information System and Application Conference (WISA), September 2015, pp. 21-26, IEEE, DOI: 10.1109/WISA.2015.52.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Edward J. Lenart/	Date (YYYY-MM-DD)	2023-07-31
Name/Print	Edward J. Lenart	Registration Number	63,665

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00246

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/361,748	**07/31/2023 12:02:14 PM ET**	**L0041B1CIP2C1**

Title of Invention

Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4323	FILED BY	Mindy Kennedy
PATENT CENTER #	62530949	FILING DATE	-
CUSTOMER #	182115	FIRST NAMED INVENTOR	ÚLFAR ERLINGSSON
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Edward Lenart

Documents

TOTAL DOCUMENTS: 33

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
2023-07-31_L0041B1CIP2C1_IDS_1_OF_2.pdf	34	Information Disclosure Statement (IDS) Form (SB08)	1261 KB
2023-07-31_L0041B1CIP2C1_IDS_2_OF_2.pdf	11	Information Disclosure Statement (IDS) Form (SB08)	1254 KB
NPL_Rinard_LivingInTheComfortZone.pdf	11	Non Patent Literature	213 KB
NPL_Perkins_AutomaticallyPatchingErrors.pdf	16	Non Patent Literature	283 KB

NPL_Ranshous_AnomalyDetectionInDynamicNetworks.pdf	25	Non Patent Literature	493 KB
NPL_Rinard_ManipulatingProgramFunctionality.pdf	6	Non Patent Literature	79 KB
NPL_Mateescu_Join-GraphPropogation.pdf	50	Non Patent Literature	701 KB
NPL_Samuel_LetsParse.pdf	4	Non Patent Literature	141 KB
NPL_Long_AutomaticInputRectification.pdf	11	Non Patent Literature	1610 KB
NPL_Moriano_InsiderThreatEvent.pdf	12	Non Patent Literature	2137 KB
NPL_Vasilakis_SupplyChainVulnerability.pdf	16	Non Patent Literature	1167 KB
NPL_Vaas_DetectingDisguisedProcesses.pdf	6	Non Patent Literature	1083 KB
NPL_Yu_RecommendingJoinQueries.pdf	6	Non Patent Literature	611 KB
FOR_CN110999250B.pdf	1	Foreign Reference	76 KB
NPL_Tamassia_GraphDrawForSecurity.pdf	12	Non Patent Literature	2074 KB
NPL_Al-Yaseen_Real-timeIntrusion.pdf	11	Non Patent Literature	449 KB
NPL_Akoglu_GraphBasedAnomalyDetection.pdf	68	Non Patent Literature	806 KB
NPL_Amidon_ProgramFracture.pdf	6	Non Patent Literature	144 KB

NPL_Ammar_QueryOptimizationTechniques.pdf	14	Non Patent Literature	311 KB
NPL_Balasubramaniyan_AnArchitectureForIntrusion.pdf	19	Non Patent Literature	224 KB
NPL_Chang_RealityBitesProgressiveQuerying.pdf	10	Non Patent Literature	742 KB
FOR_WO2021052379A1.pdf	199	Foreign Reference	3106 KB
NPL_Crosbie_DefendingAComputerSystem.pdf	11	Non Patent Literature	289 KB
NPL_Chesson_CommunicationAndControl.pdf	6	Non Patent Literature	702 KB
FOR_CN114598840A.pdf	21	Foreign Reference	4446 KB
NPL_Hooper_Medusa-ASimpleTool.pdf	2	Non Patent Literature	214 KB
NPL_Hautamaki_OutlierDetectionUsingK-Nearest.pdf	4	Non Patent Literature	338 KB
NPL_Leopold_AVisualQuerySystem.pdf	9	Non Patent Literature	396 KB
NPL_Beutel_UserBehaviorModeling.pdf	275	Non Patent Literature	5352 KB
NPL_Bugiel_TowardsTamingPrivilege-Escalation.pdf	18	Non Patent Literature	5950 KB
NPL_Koutra_ExploringAndMakingSense.pdf	232	Non Patent Literature	3825 KB
NPL_Liao_VisualizingGraphDynamics.pdf	12	Non Patent Literature	4704 KB

NPL_Shen_ActiveLearningfor Inference.pdf	119	Non Patent Literature	23293 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
2023-07-31_L0041B1CIP2C1_IDS_1_OF_2.pdf	266F63691B21D8085585755BD25CB9F68D9A8F0403D2636137DCF13B824FCE0651C4987E9D72F7A7735B2B568F3B587F08727AA7E262AA9FC4B87542490272EB
2023-07-31_L0041B1CIP2C1_IDS_2_OF_2.pdf	F9D3F1DFC93895A20E991E01B9F8FA5530BD877D0398D8BF622A2622E2F20A098F2AB1DC25130C1A3125C7FA7BB36135751BA2843F404CAEE676914E09A6B371
NPL_Rinard_LivingInTheComfortZone.pdf	C5BAED094A9AB1CB7181900E57C0F93EBBFECADCDCC79172AE1604E28E1FB8C83DA67111D5529EC8B4156AA832CBCD335B3FFFC17A1FA8A7F9CDBBC979E16056
NPL_Perkins_AutomaticallyPatchingErrors.pdf	D1072E4E608A6280A3B1C10D8D2C06B5F60F52390F6038E98285E380686BC56C715EC8D507E016555EE6DBA51D70936B24F0184C8CBC44D1CF0852DF03C8F69C
NPL_Ranshous_AnomalyDetectionInDynamicNetworks.pdf	25E465CAC9E23F8E0F5C46C006FC398BBE2B21BE567F31704F18E9A79ADCCD956A6199D0C6D90B791E03075E18E95D90453E8B8FFFC84E6D495B0C48B3F692AB
NPL_Rinard_ManipulatingProgramFunctionality.pdf	420C43E1D140EC3BA786F8D78B387BCE53926B56F6B13BD431759A7978999ACEFF6FCDC2DC304236927C722CCAED2A2E399BDCF020A0FD3857E84915B414997E
NPL_Mateescu_Join-GraphPropogation.pdf	240C1B56027F98F776F7616A57CA1C63F6B2B6FA985197300E22D2DFA92FB757D28DC00DA5E4EBFE2EA583872A966C02D95F06D45F08CC280D635635D5697732
NPL_Samuel_LetsParse.pdf	4BD282FEA8C5BD2EFDB7EAE4091130539BA7AE2A70D87294C49985A95390F5484F7D8C8EA507D3FA761DF84D7FBCE018AA11B967DC7D4C1EF36D8C4B6ED5D88B

NPL_Long_AutomaticInputRectification.pdf	5B5AFA0391B3825FC11AB42870AF9DEC8197A77FAB600BE67667A0367748B48A30231C16BD5934C4CE4E8504D6664F17BB5AAFF78B96BFB6AD7DA0D863E1F4A5
NPL_Moriano_InsiderThreatEvent.pdf	883CDB3BE49DD3012BEB1F829023F06BB59D15BECEF2AB53AF27993E86FCA7363D8BF0600D1FFA9461393D0E3F69C7BCBA05F04BCC224A4DF995F22DB209A447
NPL_Vasilakis_SupplyChainVulnerability.pdf	9622653FABEEBC2BA0B3498E60500655B042037F55824FBF611E792B64A5023D444BDB15AC612E65512971211C6BF9AD675808C838CFD80F1E3F11C91E577A08
NPL_Vaas_DetectingDisguisedProcesses.pdf	A4CC045FC2C3A718E6D815CCEBC2F20E3B11D69453239F74EE37BC3FC19DF125DB1BB1431229BDAD797EC3B012247A6AE36D19EEE44FACA85710AA90F1F80C07
NPL_Yu_RecommendingJoinQueries.pdf	453387A31544F555B48A673B5B4BF42BB7A8247AC21511F5140B57B14F4D4E6F957DF84297CDFAA72436CC2B907AFC933F42BBBE4116C0858F35B25FE61D14C5
FOR_CN110999250B.pdf	96793C68D9A25DAB686B6938DC4936DD8E337EDA6660447B7E45C9EE204423176C797CF7B99C301C009BBD78A6F90035D98913EFA975EE20475EF485D1362CE3
NPL_Tamassia_GraphDrawForSecurity.pdf	50D27B55A1265D5471EA36A1A05254AB81F273FC80FDC0A0512A0958AB42CCDBF51B98BDE00A5938251DE58AAA00774A58494D97CFDE610EE76842E137049327
NPL_Al-Yaseen_Real-timeIntrusion.pdf	410D4DC41C77675E56DA21A96B493CF00C08E22AAE966408AE09E7FFFF61E430D32F54CEE2A0ABB6D9190159EFD3B8DF0BC6AD0A7E2F05333B07625264CA9B41
NPL_Akoglu_GraphBasedAnomalyDetection.pdf	B29A5D3C6B5D2B61818CB3610CDFEA65FE981A62778C3C145BA31E27B69F0EDE7FA6CDDFFF259BF50B3655BFF1BD581567422EB6CB933ACBBE7BE1AAF7FD8838
NPL_Amidon_ProgramFracture.pdf	A5163B5F289074A5B578A5C69BAFF222532D61A7130F7D19055A80163749BE9D25BC499F5B5165D8FF879208EDB8AFBF53389FB1AD5E83A0D7842ECA4B4AD44C

NPL_Ammar_QueryOptimizationTechniques.pdf	5450BE9D00EE222F51311A0E76BDDA29E49D0D42E050CBAE2AF6F481B5E00200026AC4F585E30704A41547DE02453168F935F48B22D259DA9E0E4311B4869C20
NPL_Balasubramaniyan_AnArchitectureForIntrusion.pdf	89D89D9869DCBBE55A4153A48E1BD4CED5FBF83E3D42AD8A7E6B48D2EF1F5988072BCDF32F79A066A708CE2E85D2EC0FF4036FD1EDF166D17C684E4027B7A93F
NPL_Chang_RealityBitesProgressiveQuerying.pdf	36FFFB3A06A3DD8F0977DF78B963E835CDBBFAA3F4C431BF41C6061D0A88FBC603019431A55DFF73C2E886FF223F487F0CFCBE6CFDF1E6AE13F907E045869F15
FOR_WO2021052379A1.pdf	E28E46DEC06679960DF97FD1F217367048D3CB2C8068268D9A35BB12DF38C30995F7F8BB1EF7775EC9BEE68234F8E2B30312F09EBF63B3C577B1737C6115E828
NPL_Crosbie_DefendingAComputerSystem.pdf	D65F6310889E53834E679AF8C8296FDC35FDEF9839D7158ABE5F2A6BD9498927D6B700DE6CEA8D6C6B4677FD19DA3D5AAC1E8B976A4BD92A3E4BDDC62348BE7B
NPL_Chesson_CommunicationAndControl.pdf	72FF001DF810C923A0A811B06C6EB03B8DCB29812B2E5FC76F8AC800444F1E1AED684B9055EDCDFD41263868D809822463E745D5D187C4B9A49DB3380167958C
FOR_CN114598840A.pdf	6A894AFE4310CB16E3C8A2F54BCA404FB035CF798A76E17F1530462D60ED21AE5E1203D15FAD59DCC79D54A8DE01811D686AB9186D99A7DE189FBB1CFE9773D7
NPL_Hooper_Medusa-ASimpleTool.pdf	BADCC82C81EB5A717282FE221B2DA79DDE5F844E1D77947C1B10A0172D6E1100A6FB314AF8BA7FA22B3A5A7BA555666C5C5E5399AE00399E9940DC3DE54E12A0
NPL_Hautamaki_OutlierDetectionUsingK-Nearest.pdf	8037EC36114C79375D3E058FD9739C2F3E8D02D00E4FA1A5C8902CC7711AFAE3651FE91633DB6A833E448F38163E626348404CADE416B2CE6362339C0CC6A057
NPL_Leopold_AVisualQuerySystem.pdf	2DBBCB42678A322C54D58BBD9BF7D8B950B37B081928F4644496E5B65635F403C142238EE625447929582DA9A964465FC4CE86113C586524BB9D20F7B25B73ED

NPL_Beutel_UserBehaviorModeling.pdf	F5DF9EE6942BFC7F40B394F4A813718E7C3FC191A3195EC077E7F91310D11ACB4DAB3D7D7BF9764D765C3331DF1669FA9FD2BD8F39B43A1ED3C0D1A00D3C2561
NPL_Bugiel_TowardsTamingPrivilege-Escalation.pdf	AB4A380C4B69D6746D2E55C35C8472398C45D815B9B14BA12ED45665EE24F28D6766733FFB6F9D371D9511FC8EB36DCC856F64F0C069B4818320B119E2488BB7
NPL_Koutra_ExploringAndMakingSense.pdf	234A544FE73F84AE279FC4F0975B640DD129EBAA9AA8A2C6DDCA07BD85B273404CD7CB34F0F0C5C39400ABC08DE842231FCD82267321DE58B9615011EF49C8C7
NPL_Liao_VisualizingGraphDynamics.pdf	655425F1461CA49285FC1541D4BC3C8213580A7412C032D76A7957A4F11F82BB8964C43BA5E0584A919AF7D9691F4CEAE02E75B735FB14DE75B16DE0B520832A
NPL_Shen_ActiveLearningforInference.pdf	982B2B58985D9117510766586BC7BCC699FD14BEF056536C729977E5FCA528984497775DA564A5F6D9107BD47132164756533 7288B06B5FDE2F34567F8B13F36

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(**Not for submission under 37 CFR 1.99)**

Application Number	18361748
Filing Date	2023-07-28
First Named Inventor	ÚLFAR ERLINGSSON
Art Unit	
Examiner Name	
Attorney Docket Number	L0041B1CIP2C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7962635	B2	2011-06-14	Naidu et al.	
	2	7996885	B2	2011-08-09	Jaiswal et al.	
	3	8032925	B2	2011-10-04	Cho	
	4	8037284	B2	2011-10-11	Schenfeld et al.	
	5	8037521	B2	2011-10-11	Minato	
	6	8103906	B1	2012-01-24	Alibakhsh et al.	
	7	8122122	B1	2012-02-21	Clingenpeel et al.	
	8	8151107	B2	2012-04-03	Song et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	9	8276197	B1	2012-09-25	Mangal et al.	
	10	8291233	B2	2012-10-16	Pearson et al.	
	11	8341711	B1	2012-12-25	Pennington et al.	
	12	8351456	B2	2013-01-08	Kadous et al.	
	13	8352589	B2	2013-01-08	Ridel et al.	
	14	8359584	B2	2013-01-22	Rao et al.	
	15	8443442	B2	2013-05-14	Wang et al.	
	16	8497863	B2	2013-07-30	Xie et al.	
	17	8549002	B2	2013-10-01	Herter et al.	
	18	8561157	B2	2013-10-15	Ge	
	19	8595262	B1	2013-11-26	Hayden	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	20	8607306	B1	2013-12-10	Bridge et al.	
	21	8655989	B2	2014-02-18	Ritter et al.	
	22	8671453	B2	2014-03-11	Underwood et al.	
	23	8725587	B2	2014-05-13	Beadle et al.	
	24	8826403	B2	2014-09-02	Bhaskaran et al.	
	25	8843646	B2	2014-09-23	Kuzin et al.	
	26	8862524	B2	2014-10-14	Zheng et al.	
	27	8959608	B2	2015-02-17	Ahmed et al.	
	28	9021583	B2	2015-04-28	Wittenstein et al.	
	29	9037273	B2	2015-05-19	Mikkelsen	
	30	9053306	B2	2015-06-09	Yoshigaki et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	31	9225730	B1	2015-12-29	Brezinski	
	32	9231935	B1	2016-01-05	Bridge et al.	
	33	9239873	B2	2016-01-19	Branch et al.	
	34	9246897	B2	2016-01-26	HE	
	35	9323806	B2	2016-04-26	Sadikov et al.	
	36	9332020	B2	2016-05-03	Thomas et al.	
	37	9369450	B1	2016-06-14	Barak et al.	
	38	9391978	B2	2016-07-12	Burch et al.	
	39	9400882	B2	2016-07-26	Pearson et al.	
	40	9430830	B2	2016-08-30	Madabhushi et al.	
	41	9495522	B2	2016-11-15	Singh et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	42	9497224	B2	2016-11-15	Sweet et al.	
	43	9515999	B2	2016-12-06	Ylonen	
	44	9516053	B1	2016-12-06	Muddu et al.	
	45	9537851	B2	2017-01-03	Gordon et al.	
	46	9558265	B1	2017-01-31	Tacchi et al.	
	47	9569869	B2	2017-02-14	Hesse et al.	
	48	9582766	B2	2017-02-28	Sadikov et al.	
	49	9596253	B2	2017-03-14	Chauhan et al.	
	50	9596254	B1	2017-03-14	Muddu et al.	
	51	9596295	B2	2017-03-14	Banadaki et al.	
	52	9602506	B2	2017-03-21	Kang et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	53	9602526	B2	2017-03-21	Liu et al.	
	54	9639676	B2	2017-05-02	Betz et al.	
	55	9652875	B2	2017-05-16	Vassilvitskii et al.	
	56	9654503	B1	2017-05-16	Kowalyshyn	
	57	9659337	B2	2017-05-23	Lee et al.	
	58	9665660	B2	2017-05-30	Wensel	
	59	9729416	B1	2017-08-08	Khanal et al.	
	60	9734040	B2	2017-08-15	Gounares	
	61	9740744	B2	2017-08-22	Stetson et al.	
	62	9741138	B2	2017-08-22	Friedlander et al.	
	63	9749339	B2	2017-08-29	Kadambe et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	64	9753960	B1	2017-09-05	Troyanovsky	
	65	9760619	B1	2017-09-12	Lattanzi et al.	
	66	9781115	B2	2017-10-03	Heise	
	67	9787705	B1	2017-10-10	Love et al.	
	68	9805080	B2	2017-10-31	Joshi et al.	
	69	9805140	B2	2017-10-31	Chakrabarti et al.	
	70	9811790	B2	2017-11-07	Ahern et al.	
	71	9819671	B2	2017-11-14	Ji	
	72	9830435	B2	2017-11-28	Haven	
	73	9836183	B1	2017-12-05	Love et al.	
	74	9852230	B2	2017-12-26	Fleury et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

	75	9853968	B2	2017-12-26	Shen et al.	
	76	9887999	B2	2018-02-06	DONG et al.	
	77	9923911	B2	2018-03-20	Vasseur et al.	
	78	9942220	B2	2018-04-10	Bajenov et al.	
	79	9946800	B2	2018-04-17	Qian et al.	
	80	9953014	B1	2018-04-24	Reshadi et al.	
	81	9954842	B2	2018-04-24	Huang	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	RE47937E1	E1	2020-04-07	Ramachandran et al.	
	2	RE47952E1	E1	2020-04-14	Ramachandran et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00261

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐
If you wish to add additional Foreign Patent Document citation information please click the Add button								Add

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐
If you wish to add additional non-patent literature document citation information please click the Add button			Add

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	18361748
	Filing Date	2023-07-28
	First Named Inventor	ÚLFAR ERLINGSSON
	Art Unit	
	Examiner Name	
	Attorney Docket Number	L0041B1CIP2C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Edward J. Lenart/	Date (YYYY-MM-DD)	2023-07-31
Name/Print	Edward J. Lenart	Registration Number	63,665

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Patent Translate
Powered by EPO and Google

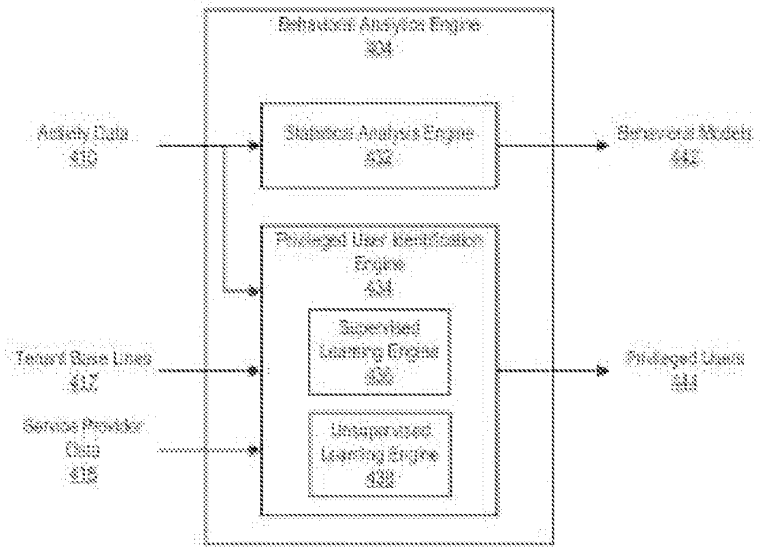
Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

ABSTRACT CN110999250B

[0001]

In various implementations, a security management and control system for monitoring and managing the security of cloud services can include automated techniques for identifying privileged users of a given cloud service. In various examples, the security management and control system can obtain activity logs from the cloud service, where the activity logs record actions performed by users of the organization while using the cloud service. In various examples, the security management and control system can identify actions in the activity log that are privileged with respect to the cloud service. In these and other examples, the security management and control system can use these actions in the activity log to identify privileged users. Once a privileged user is identified, the security management and control system can monitor the privileged user with a higher degree of scrutiny.



Espacenet

CN114598840A Intelligent badge movement track monitoring system and method

Applicants: HUA YUAN

Inventors: HUA YUAN

Classifications:

IPC ***G06K9/62; G06N3/04; G06N3/08; H04L67/10; H04L67/52; H04N7/18; H04W4/029;***

CPC **G06F18/23 (CN); G06N3/045 (CN); G06N3/08 (CN); H04L67/10 (CN); H04N7/18 (CN); H04W4/029 (CN);** Y02D30/70 (EP);

Priorities: CN202210043236A 2022-01-14

Application: CN202210043236A·2022-01-14

Publication: CN114598840A·2022-06-07

Published as: CN114598840A

Intelligent badge movement track monitoring system and method

Abstract

The invention discloses an intelligent badge action track monitoring system and method.The intelligent badge action track monitoring system comprises an automatic video recording module, a real-time communication module, a periphery recognition module, a track monitoring module and a track prediction module, and the output end of the automatic video recording module is connected with the input end of the real-time communication module; the output end of the real-time communication module is connected with the input end of the periphery identification module, the output end of the periphery identification module is connected with the input end of the track monitoring module, and the output end of the track monitoring module is connected with the input end of the track prediction module; according to the method, the action track of a badge wearer can be monitored in real time, other people can easily search and rescue the badge when the wearer is lost or missing, the personal safety of the wearer is guaranteed, the practicability is high, the action track prediction model is constructed and optimized by using an artificial intelligence algorithm, and even if the badge loses a signal, the badge can be quickly and accurately predicted. And the future action track of the badge wearer can be predicted according to the current action track, the work is reliable, and the application range is wide.

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

DESCRIPTION CN114598840A

Smart Badge Action Trajectory Monitoring System and Method

[0001]

technical field

[n0001]

The invention relates to the technical field of action track monitoring, in particular to a smart badge action track monitoring system and method.

[0003]

Background technique

[n0002]

A badge is a symbol worn on the body to indicate identity, occupation, honor and other meanings.

The smart badge, as the name suggests, refers to a badge with a microchip embedded in it.

At present, the common smart badges on the market mainly have functions such as lighting, positioning, communication, and video recording.

[n0003]

However, most of the existing smart badges cannot monitor the movement track of the badge wearer. When the wearer is lost or missing, it is difficult for others to search and rescue, and they do not have the image recognition function, so they cannot detect the scene and things around the badge wearer. Recognition increases the difficulty for others to find and search and rescue, and meets the needs of different wearers. In addition, when the badge loses signal, others cannot predict the future trajectory of the badge wearer based on the current trajectory. The reliability of the work is poor, and the scope of use is limited.

[0006]

Contents of the invention

[n0004]

The purpose of the present invention is to provide a smart badge action trajectory monitoring system and method to solve the

problems raised in the above-mentioned background technology.

[n0005]

In order to achieve the above object, the present invention provides the following technical solutions: a smart badge action track monitoring system, including an automatic video recording module, a real-time communication module, a peripheral identification module, a track monitoring module and a track prediction module, and the output end of the automatic video recording module is connected to a real-time The input end of the communication module, the output end of the real-time communication module are connected to the input end of the peripheral identification module, the output end of the peripheral identification module is connected to the input end of the trajectory monitoring module, and the output end of the trajectory monitoring module is connected to the input end of the trajectory prediction module.

[n0006]

Preferably, the automatic video recording module is composed of an image acquisition module, a satellite positioning module, a time stamp module, a video recording module, a video encoding module and a local storage module, the output of the image acquisition module is connected to the input of the satellite positioning module, and the satellite positioning The output end of the module is connected to the input end of the time stamp module, the output end of the time stamp module is connected to the input end of the video recording module, the output end of the video recording module is connected to the input end of the video encoding module, and the output end of the video encoding module is connected to the local storage module The input end of the local storage module is connected to the input end of the real-time communication module.

[n0007]

Preferably, the real-time communication module is composed of a 5G communication module, a 4G communication module, a satellite communication module, and a cloud storage module. The input terminals of the 5G communication module, the 4G communication module and the satellite communication module are all connected to the output terminals of the local storage module. The output ends of the communication module, the 4G communication module and the satellite communication module are all connected to the input end of the cloud storage module, and the output end of the cloud storage module is connected to the input end of the peripheral identification module.

[n0008]

Preferably, the peripheral recognition module is composed of a user login module, a video retrieval module, a video decoding module, an image processing module, a scene recognition module, a map reference module and a point correction module, and the input end of the user login module is connected to the cloud storage module The output terminal of the user login module is connected to the input terminal of the video retrieval module, the output terminal of the video retrieval module is connected to the input terminal of the video decoding module, and the output terminal of the video decoding module is connected to the input terminal of the image processing module. The output end of the module is connected to the input end of the scene recognition module, the output end of the scene recognition module is connected to the input end of the map reference module, the output end of the map reference module is connected to the input end of the point correction module, and the output end of the point correction module is connected to the track The input terminal of the monitoring module.

[n0009]

Preferably, the trajectory monitoring module is composed of a map loading module, a point anchor module, a time series labeling module, a point connection module, a trajectory generation module and a real-time monitoring module, and the input end of the map loading module is connected to the point correction module. Output terminal, the output terminal of the map loading module is connected to the input terminal of the point-position anchor module, the output terminal of the point-position anchor module is connected to the input terminal of the time series labeling module, and the output terminal of the time series labeling module is connected to the input terminal of the point-position connection module , the output end of the point-position connection module is connected to the input end of the trajectory generation module, the output end of the trajectory generation module is connected to the input end of the real-time monitoring module, and the output end of the real-time monitoring module is connected to the input end of the trajectory prediction module.

[n0010]

Preferably, the trajectory prediction module is composed of a data screening module, a model building module, a model optimization module and a real-time prediction module, the input of the data screening module is connected to the output of the real-time monitoring module, and the output of the data screening module is connected to the model building module The input end of the model construction module is connected to the input end of the model optimization module, and the output end of the model optimization module is connected to the input end of the real-time prediction module.

[n0011]

The method for monitoring the action track of the smart badge includes the following steps: Step 1, video recording; Step 2, communication; Step 3, identification; Step 4, monitoring; Step 5, prediction;

[n0012]

In the above step 1, the light and shadow image of the area in front of the badge is collected through the image acquisition module, and the shooting location of the light and shadow image is determined through the satellite positioning module, and then time stamped on the light and shadow image through the time stamp module, and recorded through the video recording module The image of the area in front of the badge for a period of time is encoded by the video encoding module and stored in the local storage module;

[n0013]

In the above step 2, upload the encoded video to the cloud through the 5G communication module, 4G communication module or satellite communication module according to the signal strength, and save it in the cloud storage module;

[n0014]

In the above step three, log in to the monitoring system in the cloud through the user login module, and retrieve the encoded video through the video retrieval module, after decoding by the video decoding module and grayscale processing by the image processing module, the scene recognition module recognizes the video in the video. Various scenes and things of various scenes, and compare the street view data in the satellite map through the map reference module, and then use the point correction module to correct the point where the badge is located on the electronic map;

[n0015]

In the above step 4, the satellite map is loaded through the map loading module, and the position of each action point on the satellite map is determined through the point anchoring module, and then the time sequence of each action point is marked through the time sequence labeling module, and according to the time sequence Each action point is connected into a line through the point connection module, and the action track of the badge is continuously generated on the satellite map after being processed by the track generation module, and then the action track of the badge is monitored in real time through the real-time monitoring module;

[n0016]

Among them, in the above step five, the historical data with strong correlation with the current action is screened out from the historical action trajectory of the badge through the data screening module, and the initial trajectory prediction model is constructed by using the deep learning algorithm through the model building module, and then optimized through the model The module uses the existing data of the current action to train the initial trajectory prediction model, optimizes the action trajectory prediction model, and predicts the action trajectory after the badge through the real-time prediction module.

[n0017]

Compared with the prior art, the beneficial effects of the present invention are: the smart badge action track monitoring system and method can monitor the action track of the badge wearer in real time, and when the wearer is lost or missing, others can easily find and search for it. The personal safety of the wearer is guaranteed; with image recognition

function, it can identify the scene and things around the badge wearer, and the positioning is more accurate, which reduces the difficulty of others to find and search and rescue, and meets the needs of different wearers; uses artificial intelligence The algorithm builds and optimizes the action trajectory prediction model. When the badge loses its signal, it can also predict the future action trajectory of the badge wearer based on the current action trajectory. It works reliably and has a wide range of applications.

[0021]

Description of drawings

[n0018]

Fig. 1 is a system structure diagram of the present invention;

[n0019]

Fig. 2 is a system flow chart of the present invention;

[n0020]

Fig. 3 is a flow chart of the method of the present invention;

[n0021]

In the figure: 1. Automatic video recording module; 11. Image acquisition module; 12. Satellite positioning module; 13. Time marking module; 14. Video recording module; 15. Video encoding module; 16. Local storage module; 2. Real-time communication module ;21. 5G communication module; 22. 4G communication module; 23. Satellite communication module; 24. Cloud storage module; 3. Peripheral identification module; 31. User login module; 34. Image processing module; 35. Scene recognition module; 36. Map reference module; 37. Point correction module; 4. Trajectory monitoring module; 41. Map loading module; 42. Point anchoring module; 43. Timing labeling module ;44. Point connection module; 45. Trajectory generation module; 46. Real-time monitoring module; 5. Trajectory prediction module; 51. Data screening module; 52. Model building module; 53. Model optimization module; 54. Real-time prediction module .

[0026]

Detailed ways

[n0022]

The following will clearly and completely describe the technical solutions in the embodiments of the present invention with reference to the accompanying drawings in the embodiments of the present invention. Obviously, the described embodiments are only some, not all, embodiments of the present invention.

Based on the embodiments of the present invention, all other embodiments obtained by persons of ordinary skill in the art without making creative efforts belong to the protection scope of the present invention.

[n0023]

Please refer to Fig. 1-2, an embodiment provided by the present invention: a smart badge action track monitoring system, including an automatic video recording module 1, a real-time communication module 2, a peripheral identification module 3, a track monitoring module 4 and a track prediction module 5, automatically The output end of the video recording module 1 is connected to the input end of the real-time communication module 2, and the output end of the real-time communication module 2 is connected to the input end of the peripheral identification module 3, and the output end of the peripheral identification module 3 is connected to the input end of the track monitoring module 4, and the track monitoring module The output end of 4 connects the input end of trajectory prediction module 5, and automatic video recording module 1 is made up of image acquisition module 11, satellite positioning

module 12, time stamp module 13, video recording module 14, video encoding module 15 and local storage module 16, image The output end of acquisition module 11 connects the input end of satellite positioning module 12, the output end of satellite positioning module 12 connects the input end of time stamp module 13, the output end of time stamp module 13 connects the input end of video recording module 14, video recording module The output end of 14 connects the input end of video coding module 15, and the output end of video coding module 15 connects the input end of local storage module 16, and the output end of local storage module 16 connects the input end of real-time communication module 2, and real-time communication module 2 consists of The 5G communication module 21, the 4G communication module 22, the satellite communication module 23, and the cloud storage module 24 are composed. The input terminals of the 5G communication module 21, the 4G communication module 22 and the satellite communication module 23 are all connected to the output terminals of the local storage module 16. 5G communication The output ends of the module 21, the 4G communication module 22 and the satellite communication module 23 are all connected to the input end of the cloud storage module 24, and the output end of the cloud storage module 24 is connected to the input end of the peripheral identification module 3, and the peripheral identification module 3 is logged into the module 31 by the user. , a video recording module 32, a video decoding module 33, an image processing module 34, a scene recognition module 35, a map reference module 36 and a point correction module 37, the input end of the user login module 31 is connected to the output end of the cloud storage module 24, The output end of the user login module 31 is connected to the input end of the video recording module 32, and the output end of the video recording module 32 is connected to the input end of the video decoding module 33, and the output end of the video decoding module 33 is connected to the input end of the image processing module 34, The output end of the image processing module 34 is connected to the input end of the scene recognition module 35, and the output end of the scene recognition module 35 is connected to the input end of the map reference module 36, and the output end of the map reference module 36 is connected to the input end of the point correction module 37, point The output end of the position correction module 37 is connected to the input end of the trajectory monitoring module 4, which has an image recognition function, and can identify scene objects around the wearer of the badge. The use requirements of the user; the track monitoring module 4 is composed of a map loading module 41, a point anchor module 42, a time series labeling module 43, a point connection module 44, a track generation module 45 and a real-time monitoring module 46. The map loading module 41 The input terminal is connected to the point correction module 3 7, the output of the map loading module 41 is connected to the input of the point anchor module 42, the output of the point anchor module 42 is connected to the input of the timing labeling module 43, and the output of the timing labeling module 43 is connected to the point The input end of bit connection module 44, the output end of point bit connection module 44 connects the input end of track generation module 45, the output end of track generation module 45 connects the input end of real-time monitoring module 46, the output end of real-time monitoring module 46 Connect the input terminal of the trajectory prediction module 5 to monitor the movement trajectory of the badge wearer in real time. When the wearer is lost or missing, it is easy for others to find and search for rescue, which ensures the personal safety of the wearer; the trajectory prediction module 5 is selected by data Module 51, model construction module 52, model optimization module 53 and real-time prediction module 54 are formed, the input end of data screening module 51 is connected the output end of real-time monitoring module 46, the output end of data screening module 51 is connected the input end of model construction module 52 , the output end of the model building module 52 is connected to the input end of the model optimization module 53, and the output end of the model optimization module 53 is connected to the input end of the real-time prediction module 54. When the badge loses signal, it can also predict the future of the badge wearer according to the current action trajectory Action track, reliable work, wide range of use.

[n0024]

Please refer to Fig. 3, an embodiment provided by the present invention: a smart badge action track monitoring method, including the following steps: Step 1, video recording; Step 2, communication; Step 3, identification; Step 4, monitoring; Step 5, prediction;

[n0025]

Wherein in the above-mentioned step one, the light and shadow image of the area in front of the badge is collected through the image acquisition module 11, and the shooting location of the light and shadow image is determined through the satellite positioning module 12, and then the time stamp is marked on the light and shadow image through the time stamp module 13, and through the video The recording module 14 records the

image of the area in front of the badge for a period of time, and saves it in the local storage module 16 after being encoded by the video encoding module 15;

[n0026]

Wherein in the above step 2, according to the signal strength, the coded video is uploaded to the cloud through the 5G communication module 21, the 4G communication module 22 or the satellite communication module 23, and stored in the cloud storage module 24;

[n0027]

Wherein in the above-mentioned step three, log in the monitoring system of the cloud through the user login module 31, and transfer the encoded video through the video retrieval module 32, after the video decoding module 33 decodes, the image processing module 34 grayscale processing, and then through the scene recognition module 35 recognize various scenes and things in the video, and compare the street view data in the satellite map through the map reference module 36, and then correct the point where the badge is located on the electronic map through the point correction module 37;

[n0028]

Wherein in above-mentioned step 4, load satellite map by map loading module 41, and determine the position of each action point on the satellite map by point position anchoring module 42, mark the time sequence of each action point by time series labeling module 43 again, And according to the time series, each action point is connected into a line through the point connection module 44, and the action track of the badge is continuously generated on the satellite map after being processed by the track generation module 45, and then the action track of the badge is monitored in real time by the real-time monitoring module 46 ;

[n0029]

Among them, in the above-mentioned step 5, the historical data with strong correlation with the current action is screened out from the historical action track of the badge through the data screening module 51, and the initial trajectory prediction model is constructed by using the deep learning algorithm through the model building module 52, and then passed The model optimization module 53 uses the existing data of the current action to train the initial trajectory prediction model, optimizes the action trajectory prediction model, and predicts the action trajectory after the badge through the real-time prediction module 54 .

[n0030]

Working principle: when the invention is used, the light and shadow image of the area in front of the badge is first collected through the image acquisition module 11, and the shooting location of the light and shadow image is determined through the satellite positioning module 12, and then the time stamp is marked on the light and shadow image through the time stamp module 13, And through the video recording module 14 to record the image of the area in front of the badge for a period of time, and save it in the local storage module 16 after being encoded by the video encoding module 15; The encoded video is uploaded to the cloud and stored in the cloud storage module 24; then the monitoring system in the cloud is logged in by the user login module 31, and the encoded video is retrieved by the video retrieval module 32, decoded by the video decoding module 33, and the image processing module 34 After the grayscale processing, the scene recognition module 35 is used to identify various scene objects in the video, and the map reference module 36 is used to compare the street view data in the satellite map, and then the point correction module 37 is used to correct the location of the badge on the electronic map. Finally, the satellite map is loaded by the map loading module 41, and the position of each action point on the satellite map is determined by the point anchor module 42, and then the timing of each action point is marked by the timing labeling module 43, and Each action point is connected into a line by the point connection module 44 according to timing, and the action track of the badge is continuously generated on the satellite map after being processed by the track generation module 45, and then the action track of the badge is monitored in real time by the real-time monitoring module 46; At the same time, the historical data with strong correlation with the current action can

be screened out from the historical action track of the badge through the data screening module 51, and the initial trajectory prediction model can be constructed by using the deep learning algorithm through the model building module 52, and then through the model optimization module 53 Use the existing data of the current action to train the trajectory prediction initial model, optimize the action trajectory prediction model, and predict the movement trajectory after the badge through the real-time prediction module 54. When the badge loses signal, it can also predict the badge wearer according to the current movement trajectory The future trajectory of action, reliable work, wide range of use, reduces the difficulty of others to find, search and rescue, and guarantees the personal safety of the wearer.

[n0031]

It will be apparent to those skilled in the art that the invention is not limited to the details of the above-described exemplary embodiments, but that the invention can be embodied in other specific forms without departing from the spirit or essential characteristics of the invention.

Accordingly, the embodiments should be regarded in all points of view as exemplary and not restrictive, the scope of the invention being defined by the appended claims rather than the foregoing description, and it is therefore intended that the scope of the invention be defined by the appended claims rather than by the foregoing description. All changes within the meaning and range of equivalents of the elements are embraced in the present invention.

Any reference sign in a claim should not be construed as limiting the claim concerned.

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

CLAIMS CN114598840A

1.

The smart badge action trajectory monitoring system includes an automatic video recording module (1), a real-time communication module (2), a peripheral identification module (3), a trajectory monitoring module (4) and a trajectory prediction module (5), and is characterized in that: the automatic The output end of the video recording module (1) is connected to the input end of the real-time communication module (2), the output end of the real-time communication module (2) is connected to the input end of the peripheral identification module (3), and the output end of the peripheral identification module (3) is connected to the track The input terminal of the monitoring module (4) and the output terminal of the trajectory monitoring module (4) are connected to the input terminal of the trajectory prediction module (5).

2.

The smart badge action trajectory monitoring system according to claim 1, characterized in that: the automatic video recording module (1) consists of an image acquisition module (11), a satellite positioning module (12), a time stamp module (13), a video recording module Module (14), video coding module (15) and local storage module (16) form, the output end of image acquisition module (11) connects the input end of satellite positioning module (12), the output end of satellite positioning module (12) connects The input end of the time stamp module (13), the output end of the time stamp module (13) is connected to the input end of the video recording module (14), and the output end of the video recording module (14) is connected to the input end of the video encoding module (15), The output end of the video encoding module (15) is connected to the input end of the local storage module (16), and the output end of the local storage module (16) is connected to the input end of the real-time communication module (2).

3.

The smart badge action track monitoring system according to claim 2, characterized in that: the real-time communication module (2) consists of a 5G communication module (21), a 4G communication module (22), a satellite communication module (23), and cloud storage module (24), the input ends of the 5G communication module (21), the 4G communication module (22) and the satellite communication module (23) are all connected to the output end of the local storage module (16), the 5G communication module (21), the 4G communication module The output ends of the module (22) and the satellite communication module (23) are both connected to the input end of the cloud storage module (24), and the output end of the cloud storage module (24) is connected to the input end of the peripheral identification module (3).

4.

The smart badge action trajectory monitoring system according to claim 3, characterized in that: the peripheral identification module (3) consists of a user login module (31), a video retrieval module (32), a video decoding module (33), an image processing module (34), scene recognition module (35), map reference module (36) and point correction module (37), the input

end of user login module (31) is connected to the output end of cloud storage module (24), and the user The output end of login module (31) connects the input end of video recording module (32), the output end of video recording module (32) connects the input end of video decoding module (33), and the output end of video decoding module (33) Connect the input end of image processing module (34), the output end of image processing module (34) connects the input end of scene recognition module (35), the output end of scene recognition module (35) connects the input end of map reference module (36) , the output end of the map reference module (36) is connected to the input end of the point correction module (37), and the output end of the point correction module (37) is connected to the input end of the track monitoring module (4).

5.

The smart badge action trajectory monitoring system according to claim 4, characterized in that: the trajectory monitoring module (4) consists of a map loading module (41), a point anchor module (42), a time sequence labeling module (43), Point connection module (44), trajectory generation module (45) and real-time monitoring module (46) are formed, and the input terminal of map loading module (41) connects the output end of point correction module (37), and map loading module (41) is connected to the input of the point anchor module (42), the output of the point anchor module (42) is connected to the input of the timing labeling module (43), and the output of the timing labeling module (43) is connected to the point The input end of the bit connection module (44), the output end of the point-bit connection module (44) connects the input end of the track generation module (45), and the output end of the track generation module (45) connects the real-time monitoring module (46) The input end, the output end of the real-time monitoring module (46) is connected to the input end of the trajectory prediction module (5).

6.

The smart badge action trajectory monitoring system according to claim 5, characterized in that: the trajectory prediction module (5) consists of a data screening module (51), a model building module (52), a model optimization module (53) and real-time prediction Module (54) is formed, and the input end of data screening module (51) connects the output end of real-time monitoring module (46), and the output end of data screening module (51) connects the input end of model construction module (52), and model construction module (The output end of 52) is connected to the input end of the model optimization module (53), and the output end of the model optimization module (53) is connected to the input end of the real-time prediction module (54).

7.

The method for monitoring the action track of an intelligent badge includes the following steps: step 1, video recording; step 2, communication; step 3, identification; step 4, monitoring; step 5, prediction; it is characterized in that:

Wherein in the above-mentioned step one, the light and shadow image of the area in front of the badge is collected by the image acquisition module (11), and the shooting location of the light and shadow image is determined by the satellite positioning module (12), and then the light and shadow image is marked by the time stamp module (13) Timestamp, and record the image of a period of time in front of the badge by the video recording module (14), and save it in the local storage module (16) after being encoded by the video encoding module (15);

Wherein in the above-mentioned step 2, upload the encoded video to the cloud through the 5G communication module (21), 4G communication module (22) or satellite communication module (23) according to the signal strength, and store it in the cloud storage module (24);

Wherein in the above-mentioned step three, log in the monitoring system of the cloud through the user login module (31), and transfer the coded video through the video retrieval module (32), decode through the video decoding module (33), and image processing module (34) grayscale After processing, identify the various scene objects in the video by the scene recognition module (35), and compare the street view data in the satellite map by the map reference module (36), and then correct the badge on the electronic screen by the point correction module (37). The point on the map;

Wherein in above-mentioned step 4, load satellite map by map loading module (41), and determine the position of each action point on the satellite map by point position anchoring module (42), mark each action point by timing labeling module (43) again The timing of the action points, and according to the timing, each action point is connected into a line through the point connection module (44), and the action trajectory of the badge is continuously generated on the satellite map after being processed by the trajectory generation module (45), and then passed. The real-time monitoring module (46) monitors the action track of the badge in real time;

Among them, in the above step five, the historical data with strong correlation with the current action is screened out from the historical action trajectory of the badge through the data screening module (51), and the initial trajectory prediction is constructed through the model building module (52) using a deep learning algorithm. Model, and then use the existing data of the current action to train the trajectory prediction initial model through the model optimization module (53), optimize the action trajectory prediction model, and predict the action trajectory after the badge through the real-time prediction module (54).

(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114598840 A
(43)申请公布日 2022.06.07

(21)申请号 202210043236.8
(22)申请日 2022.01.14
(71)申请人 华元
地址 广东省深圳市福田区中康路128号卓越城一期一栋1205
(72)发明人 华元
(74)专利代理机构 北京知无忧专利代理有限公司 11880
专利代理师 李伟新
(51)Int.Cl.
H04N 7/18(2006.01)
H04W 4/029(2018.01)
H04L 67/10(2022.01)
H04L 67/52(2022.01)
G06N 3/04(2006.01)
G06N 3/08(2006.01)
G06K 9/62(2022.01)

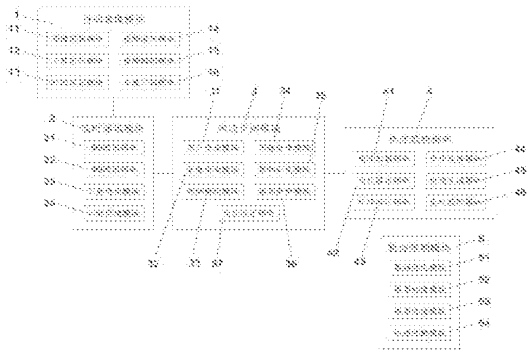
权利要求书2页 说明书5页 附图2页

(54)发明名称

智能徽章行动轨迹监控系统及方法

(57)摘要

本发明公开了智能徽章行动轨迹监控系统及方法，包括自动录像模块、实时通讯模块、周边识别模块、轨迹监控模块和轨迹预测模块，所述自动录像模块的输出端连接实时通讯模块的输入端，实时通讯模块的输出端连接周边识别模块的输入端，周边识别模块的输出端连接轨迹监控模块的输入端，轨迹监控模块的输出端连接轨迹预测模块的输入端；该发明可实时监控徽章佩带者的行动轨迹，在佩带者走丢或失踪的情况下，他人易于寻找和搜救，保障了佩带者的人身安全，实用性强，且利用人工智能算法构建并优化出行动轨迹预测模型，即便徽章失去了信号，也能根据当前行动轨迹预测徽章佩带者的未来行动轨迹，工作可靠，使用范围广。



CN 114598840 A

1.智能徽章行动轨迹监控系统，包括自动录像模块(1)、实时通讯模块(2)、周边识别模块(3)、轨迹监控模块(4)和轨迹预测模块(5)，其特征在于：所述自动录像模块(1)的输出端连接实时通讯模块(2)的输入端，实时通讯模块(2)的输出端连接周边识别模块(3)的输入端，周边识别模块(3)的输出端连接轨迹监控模块(4)的输入端，轨迹监控模块(4)的输出端连接轨迹预测模块(5)的输入端。

2.根据权利要求1所述的智能徽章行动轨迹监控系统，其特征在于：所述自动录像模块(1)由图像采集模块(11)、卫星定位模块(12)、时间标记模块(13)、视频录制模块(14)、视频编码模块(15)和本地存储模块(16)组成，图像采集模块(11)的输出端连接卫星定位模块(12)的输入端，卫星定位模块(12)的输出端连接时间标记模块(13)的输入端，时间标记模块(13)的输出端连接视频录制模块(14)的输入端，视频录制模块(14)的输出端连接视频编码模块(15)的输入端，视频编码模块(15)的输出端连接本地存储模块(16)的输入端，本地存储模块(16)的输出端连接实时通讯模块(2)的输入端。

3.根据权利要求2所述的智能徽章行动轨迹监控系统，其特征在于：所述实时通讯模块(2)由5G通讯模块(21)、4G通讯模块(22)、卫星通讯模块(23)、云端存储模块(24)组成，5G通讯模块(21)、4G通讯模块(22)和卫星通讯模块(23)的输入端均连接本地存储模块(16)的输出端，5G通讯模块(21)、4G通讯模块(22)和卫星通讯模块(23)的输出端均连接云端存储模块(24)的输入端，云端存储模块(24)的输出端连接周边识别模块(3)的输入端。

4.根据权利要求3所述的智能徽章行动轨迹监控系统，其特征在于：所述周边识别模块(3)由用户登录模块(31)、录像调取模块(32)、视频解码模块(33)、图像处理模块(34)、场景识别模块(35)、地图参照模块(36)和点位校正模块(37)组成，用户登录模块(31)的输入端连接云端存储模块(24)的输出端，用户登录模块(31)的输出端连接录像调取模块(32)的输入端，录像调取模块(32)的输出端连接视频解码模块(33)的输入端，视频解码模块(33)的输出端连接图像处理模块(34)的输入端，图像处理模块(34)的输出端连接场景识别模块(35)的输入端，场景识别模块(35)的输出端连接地图参照模块(36)的输入端，地图参照模块(36)的输出端连接点位校正模块(37)的输入端，点位校正模块(37)的输出端连接轨迹监控模块(4)的输入端。

5.根据权利要求4所述的智能徽章行动轨迹监控系统，其特征在于：所述轨迹监控模块(4)由地图加载模块(41)、点位锚定模块(42)、时序标注模块(43)、点位连线模块(44)、轨迹生成模块(45)和实时监控模块(46)组成，地图加载模块(41)的输入端连接点位校正模块(37)的输出端，地图加载模块(41)的输出端连接点位锚定模块(42)的输入端，点位锚定模块(42)的输出端连接时序标注模块(43)的输入端，时序标注模块(43)的输出端连接点位连线模块(44)的输入端，点位连线模块(44)的输出端连接轨迹生成模块(45)的输入端，轨迹生成模块(45)的输出端连接实时监控模块(46)的输入端，实时监控模块(46)的输出端连接轨迹预测模块(5)的输入端。

6.根据权利要求5所述的智能徽章行动轨迹监控系统，其特征在于：所述轨迹预测模块(5)由数据筛选模块(51)、模型构建模块(52)、模型优化模块(53)和实时预测模块(54)组成，数据筛选模块(51)的输入端连接实时监控模块(46)的输出端，数据筛选模块(51)的输出端连接模型构建模块(52)的输入端，模型构建模块(52)的输出端连接模型优化模块(53)的输入端，模型优化模块(53)的输出端连接实时预测模块(54)的输入端。

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00278

7.智能徽章行动轨迹监控方法，包括以下步骤：步骤一，录像；步骤二，通讯；步骤三，识别；步骤四，监控；步骤五，预测；其特征在于：

其中上述步骤一中，通过图像采集模块(11)采集到徽章前方区域的光影图像，并通过卫星定位模块(12)确定光影图像的拍摄地点，再通过时间标记模块(13)给光影图像标记上时间戳，并通过视频录制模块(14)录制徽章前方区域一段时间的影像，经视频编码模块(15)编码后保存到本地存储模块(16)中；

其中上述步骤二中，根据信号强度通过5G通讯模块(21)、4G通讯模块(22)或卫星通讯模块(23)将编码录像上传给云端，并保存在云端存储模块(24)中；

其中上述步骤三中，通过用户登录模块(31)登入云端的监控系统，并通过录像调取模块(32)调取编码录像，经视频解码模块(33)解码、图像处理模块(34)灰度处理后，再通过场景识别模块(35)识别出录像中的各种场景事物，并通过地图参照模块(36)比照卫星地图中的街景数据，进而通过点位校正模块(37)校正徽章在电子地图上所处的点位；

其中上述步骤四中，通过地图加载模块(41)加载卫星地图，并通过点位锚定模块(42)确定各个行动点位在卫星地图上的位置，再通过时序标注模块(43)标注上各个行动点位的时序，并根据时序通过点位连线模块(44)将各个行动点位连接成线，经轨迹生成模块(45)处理后持续的在卫星地图上生成徽章的行动轨迹，进而通过实时监控模块(46)实时监控徽章的行动轨迹；

其中上述步骤五中，通过数据筛选模块(51)从徽章的历史行动轨迹中筛选出与当前行动相关性较强的历史数据，并通过模型构建模块(52)利用深度学习算法构建出轨迹预测初始模型，再通过模型优化模块(53)利用当前行动已有数据对轨迹预测初始模型进行训练，优化出行动轨迹预测模型，并通过实时预测模块(54)预测出徽章之后的行动轨迹。

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00279

智能徽章行动轨迹监控系统及方法

技术领域

[0001] 本发明涉及行动轨迹监控技术领域，具体为智能徽章行动轨迹监控系统及方法。

背景技术

[0002] 徽章，是一种佩带在身上用来表示身份、职业、荣誉等含义的标志。而智能徽章，顾名思义指的是一种内嵌有微芯片的徽章。目前，市面上常见的智能徽章主要具有灯光、定位、通讯、录像等功能。

[0003] 然而，现有的智能徽章大多无法监控徽章佩带者的行动轨迹，在佩带者走丢或失踪的情况下，他人寻找、搜救困难，且不具备图像识别功能，无法对徽章佩带者周边的场景事物进行识别，增加了他人寻找、搜救的难度，满足了不同佩带者的使用需求，另外徽章失去信号时，他人无法根据当前行动轨迹预测徽章佩带者的未来行动轨迹，工作可靠性差，使用范围有限。

发明内容

[0004] 本发明的目的在于提供智能徽章行动轨迹监控系统及方法，以解决上述背景技术中提出的问题。

[0005] 为实现上述目的，本发明提供如下技术方案：智能徽章行动轨迹监控系统，包括自动录像模块、实时通讯模块、周边识别模块、轨迹监控模块和轨迹预测模块，所述自动录像模块的输出端连接实时通讯模块的输入端，实时通讯模块的输出端连接周边识别模块的输入端，周边识别模块的输出端连接轨迹监控模块的输入端，轨迹监控模块的输出端连接轨迹预测模块的输入端。

[0006] 优选的，所述自动录像模块由图像采集模块、卫星定位模块、时间标记模块、视频录制模块、视频编码模块和本地存储模块组成，图像采集模块的输出端连接卫星定位模块的输入端，卫星定位模块的输出端连接时间标记模块的输入端，时间标记模块的输出端连接视频录制模块的输入端，视频录制模块的输出端连接视频编码模块的输入端，视频编码模块的输出端连接本地存储模块的输入端，本地存储模块的输出端连接实时通讯模块的输入端。

[0007] 优选的，所述实时通讯模块由5G通讯模块、4G通讯模块、卫星通讯模块、云端存储模块组成，5G通讯模块、4G通讯模块和卫星通讯模块的输入端均连接本地存储模块的输出端，5G通讯模块、4G通讯模块和卫星通讯模块的输出端均连接云端存储模块的输入端，云端存储模块的输出端连接周边识别模块的输入端。

[0008] 优选的，所述周边识别模块由用户登录模块、录像调取模块、视频解码模块、图像处理模块、场景识别模块、地图参照模块和点位校正模块组成，用户登录模块的输入端连接云端存储模块的输出端，用户登录模块的输出端连接录像调取模块的输入端，录像调取模块的输出端连接视频解码模块的输入端，视频解码模块的输出端连接图像处理模块的输入端，图像处理模块的输出端连接场景识别模块的输入端，场景识别模块的输出端连接地图

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00280

参照模块的输入端，地图参照模块的输出端连接点位校正模块的输入端，点位校正模块的输出端连接轨迹监控模块的输入端。

[0009] 优选的，所述轨迹监控模块由地图加载模块、点位锚定模块、时序标注模块、点位连线模块、轨迹生成模块和实时监控模块组成，地图加载模块的输入端连接点位校正模块的输出端，地图加载模块的输出端连接点位锚定模块的输入端，点位锚定模块的输出端连接时序标注模块的输入端，时序标注模块的输出端连接点位连线模块的输入端，点位连线模块的输出端连接轨迹生成模块的输入端，轨迹生成模块的输出端连接实时监控模块的输入端，实时监控模块的输出端连接轨迹预测模块的输入端。

[0010] 优选的，所述轨迹预测模块由数据筛选模块、模型构建模块、模型优化模块和实时预测模块组成，数据筛选模块的输入端连接实时监控模块的输出端，数据筛选模块的输出端连接模型构建模块的输入端，模型构建模块的输出端连接模型优化模块的输入端，模型优化模块的输出端连接实时预测模块的输入端。

[0011] 智能徽章行动轨迹监控方法，包括以下步骤：步骤一，录像；步骤二，通讯；步骤三，识别；步骤四，监控；步骤五，预测；

[0012] 其中上述步骤一中，通过图像采集模块采集到徽章前方区域的光影图像，并通过卫星定位模块确定光影图像的拍摄地点，再通过时间标记模块给光影图像标记上时间戳，并通过视频录制模块录制徽章前方区域一段时间的影像，经视频编码模块编码后保存到本地存储模块中；

[0013] 其中上述步骤二中，根据信号强度通过5G通讯模块、4G通讯模块或卫星通讯模块将编码录像上传给云端，并保存在云端存储模块中；

[0014] 其中上述步骤三中，通过用户登录模块登入云端的监控系统，并通过录像调取模块调取编码录像，经视频解码模块解码、图像处理模块灰度处理后，再通过场景识别模块识别出录像中的各种场景事物，并通过地图参照模块比照卫星地图中的街景数据，进而通过点位校正模块校正徽章在电子地图上所处的点位；

[0015] 其中上述步骤四中，通过地图加载模块加载卫星地图，并通过点位锚定模块确定各个行动点位在卫星地图上的位置，再通过时序标注模块标注上各个行动点位的时序，并根据时序通过点位连线模块将各个行动点位连接成线，经轨迹生成模块处理后持续的在卫星地图上生成徽章的行动轨迹，进而通过实时监控模块实时监控徽章的行动轨迹；

[0016] 其中上述步骤五中，通过数据筛选模块从徽章的历史行动轨迹中筛选出与当前行动相关性较强的历史数据，并通过模型构建模块利用深度学习算法构建出轨迹预测初始模型，再通过模型优化模块利用当前行动已有数据对轨迹预测初始模型进行训练，优化出行动轨迹预测模型，并通过实时预测模块预测出徽章之后的行动轨迹。

[0017] 与现有技术相比，本发明的有益效果是：该智能徽章行动轨迹监控系统及方法，实时监控徽章佩带者的行动轨迹，在佩带者走丢或失踪的情况下，他人易于寻找和搜救，保障了佩带者的人身安全；具备图像识别功能，能对徽章佩带者周边的场景事物进行识别，定位更加准确，降低了他人寻找、搜救的难度，满足了不同佩带者的使用需求；利用人工智能算法构建并优化出行动轨迹预测模型，徽章失去信号时，也能根据当前行动轨迹预测徽章佩带者的未来行动轨迹，工作可靠，使用范围广。

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00281

附图说明

[0018] 图1为本发明的系统结构图；

[0019] 图2为本发明的系统流程图；

[0020] 图3为本发明的方法流程图；

[0021] 图中：1、自动录像模块；11、图像采集模块；12、卫星定位模块；13、时间标记模块；14、视频录制模块；15、视频编码模块；16、本地存储模块；2、实时通讯模块；21、5G通讯模块；22、4G通讯模块；23、卫星通讯模块；24、云端存储模块；3、周边识别模块；31、用户登录模块；32、录像调取模块；33、视频解码模块；34、图像处理模块；35、场景识别模块；36、地图参照模块；37、点位校正模块；4、轨迹监控模块；41、地图加载模块；42、点位锚定模块；43、时序标注模块；44、点位连线模块；45、轨迹生成模块；46、实时监控模块；5、轨迹预测模块；51、数据筛选模块；52、模型构建模块；53、模型优化模块；54、实时预测模块。

具体实施方式

[0022] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0023] 请参阅图1-2，本发明提供的一种实施例：智能徽章行动轨迹监控系统，包括自动录像模块1、实时通讯模块2、周边识别模块3、轨迹监控模块4和轨迹预测模块5，自动录像模块1的输出端连接实时通讯模块2的输入端，实时通讯模块2的输出端连接周边识别模块3的输入端，周边识别模块3的输出端连接轨迹监控模块4的输入端，轨迹监控模块4的输出端连接轨迹预测模块5的输入端，自动录像模块1由图像采集模块11、卫星定位模块12、时间标记模块13、视频录制模块14、视频编码模块15和本地存储模块16组成，图像采集模块11的输出端连接卫星定位模块12的输入端，卫星定位模块12的输出端连接时间标记模块13的输入端，时间标记模块13的输出端连接视频录制模块14的输入端，视频录制模块14的输出端连接视频编码模块15的输入端，视频编码模块15的输出端连接本地存储模块16的输入端，本地存储模块16的输出端连接实时通讯模块2的输入端，实时通讯模块2由5G通讯模块21、4G通讯模块22、卫星通讯模块23、云端存储模块24组成，5G通讯模块21、4G通讯模块22和卫星通讯模块23的输入端均连接本地存储模块16的输出端，5G通讯模块21、4G通讯模块22和卫星通讯模块23的输出端均连接云端存储模块24的输入端，云端存储模块24的输出端连接周边识别模块3的输入端，周边识别模块3由用户登录模块31、录像调取模块32、视频解码模块33、图像处理模块34、场景识别模块35、地图参照模块36和点位校正模块37组成，用户登录模块31的输入端连接云端存储模块24的输出端，用户登录模块31的输出端连接录像调取模块32的输入端，录像调取模块32的输出端连接视频解码模块33的输入端，视频解码模块33的输出端连接图像处理模块34的输入端，图像处理模块34的输出端连接场景识别模块35的输入端，场景识别模块35的输出端连接地图参照模块36的输入端，地图参照模块36的输出端连接点位校正模块37的输入端，点位校正模块37的输出端连接轨迹监控模块4的输入端，具备图像识别功能，能对徽章佩带者周边的场景事物进行识别，定位更加准确，降低了他人寻找、搜救的难度，满足了不同佩带者的使用需求；轨迹监控模块4由地图加载模块41、点位

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00282

锚定模块42、时序标注模块43、点位连线模块44、轨迹生成模块45和实时监控模块46组成，地图加载模块41的输入端连接点位校正模块37的输出端，地图加载模块41的输出端连接点位锚定模块42的输入端，点位锚定模块42的输出端连接时序标注模块43的输入端，时序标注模块43的输出端连接点位连线模块44的输入端，点位连线模块44的输出端连接轨迹生成模块45的输入端，轨迹生成模块45的输出端连接实时监控模块46的输入端，实时监控模块46的输出端连接轨迹预测模块5的输入端，实时监控徽章佩带者的行动轨迹，在佩带者走丢或失踪的情况下，他人易于寻找和搜救，保障了佩带者的人身安全；轨迹预测模块5由数据筛选模块51、模型构建模块52、模型优化模块53和实时预测模块54组成，数据筛选模块51的输入端连接实时监控模块46的输出端，数据筛选模块51的输出端连接模型构建模块52的输入端，模型构建模块52的输出端连接模型优化模块53的输入端，模型优化模块53的输出端连接实时预测模块54的输入端，徽章失去信号时，也能根据当前行动轨迹预测徽章佩带者的未来行动轨迹，工作可靠，使用范围广。

[0024] 请参阅图3，本发明提供的一种实施例：智能徽章行动轨迹监控方法，包括以下步骤：步骤一，录像；步骤二，通讯；步骤三，识别；步骤四，监控；步骤五，预测；

[0025] 其中上述步骤一中，通过图像采集模块11采集到徽章前方区域的光影图像，并通过卫星定位模块12确定光影图像的拍摄地点，再通过时间标记模块13给光影图像标记上时间戳，并通过视频录制模块14录制徽章前方区域一段时间的影像，经视频编码模块15编码后保存到本地存储模块16中；

[0026] 其中上述步骤二中，根据信号强度通过5G通讯模块21、4G通讯模块22或卫星通讯模块23将编码录像上传给云端，并保存在云端存储模块24中；

[0027] 其中上述步骤三中，通过用户登录模块31登入云端的监控系统，并通过录像调取模块32调取编码录像，经视频解码模块33解码、图像处理模块34灰度处理后，再通过场景识别模块35识别出录像中的各种场景事物，并通过地图参照模块36比照卫星地图中的街景数据，进而通过点位校正模块37校正徽章在电子地图上所处的点位；

[0028] 其中上述步骤四中，通过地图加载模块41加载卫星地图，并通过点位锚定模块42确定各个行动点位在卫星地图上的位置，再通过时序标注模块43标注上各个行动点位的时序，并根据时序通过点位连线模块44将各个行动点位连接成线，经轨迹生成模块45处理后持续的在卫星地图上生成徽章的行动轨迹，进而通过实时监控模块46实时监控徽章的行动轨迹；

[0029] 其中上述步骤五中，通过数据筛选模块51从徽章的历史行动轨迹中筛选出与当前行动相关性较强的历史数据，并通过模型构建模块52利用深度学习算法构建出轨迹预测初始模型，再通过模型优化模块53利用当前行动已有数据对轨迹预测初始模型进行训练，优化出行动轨迹预测模型，并通过实时预测模块54预测出徽章之后的行动轨迹。

[0030] 工作原理：该发明使用时，先通过图像采集模块11采集到徽章前方区域的光影图像，并通过卫星定位模块12确定光影图像的拍摄地点，再通过时间标记模块13给光影图像标记上时间戳，并通过视频录制模块14录制徽章前方区域一段时间的影像，经视频编码模块15编码后保存到本地存储模块16中；接着根据信号强度通过5G通讯模块21、4G通讯模块22或卫星通讯模块23将编码录像上传给云端，并保存在云端存储模块24中；然后通过用户登录模块31登入云端的监控系统，并通过录像调取模块32调取编码录像，经视频解码模块

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00283

33解码、图像处理模块34灰度处理后，再通过场景识别模块35识别出录像中的各种场景事物，并通过地图参照模块36比照卫星地图中的街景数据，进而通过点位校正模块37校正徽章在电子地图上所处的点位；最后通过地图加载模块41加载卫星地图，并通过点位锚定模块42确定各个行动点位在卫星地图上的位置，再通过时序标注模块43标注上各个行动点位的时序，并根据时序通过点位连线模块44将各个行动点位连接成线，经轨迹生成模块45处理后持续的在卫星地图上生成徽章的行动轨迹，进而通过实时监控模块46实时监控徽章的行动轨迹；同时可通过数据筛选模块51从徽章的历史行动轨迹中筛选出与当前行动相关性较强的历史数据，并通过模型构建模块52利用深度学习算法构建出轨迹预测初始模型，再通过模型优化模块53利用当前行动已有数据对轨迹预测初始模型进行训练，优化出行动轨迹预测模型，并通过实时预测模块54预测出徽章之后的行动轨迹，徽章失去信号时，也能根据当前行动轨迹预测徽章佩带者的未来行动轨迹，工作可靠，使用范围广，降低了他人寻找、搜救的难度，保障了佩带者的人身安全。

[0031] 对于本领域技术人员而言，显然本发明不限于上述示范性实施例的细节，而且在不背离本发明的精神或基本特征的情况下，能够以其他的具体形式实现本发明。因此，无论从哪一点来看，均应将实施例看作是示范性的，而且是非限制性的，本发明的范围由所附权利要求而不是上述说明限定，因此旨在将落在权利要求的等同要件的含义和范围内的所有变化囊括在本发明内。不应将权利要求中的任何附图标记视为限制所涉及的权利要求。

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00284

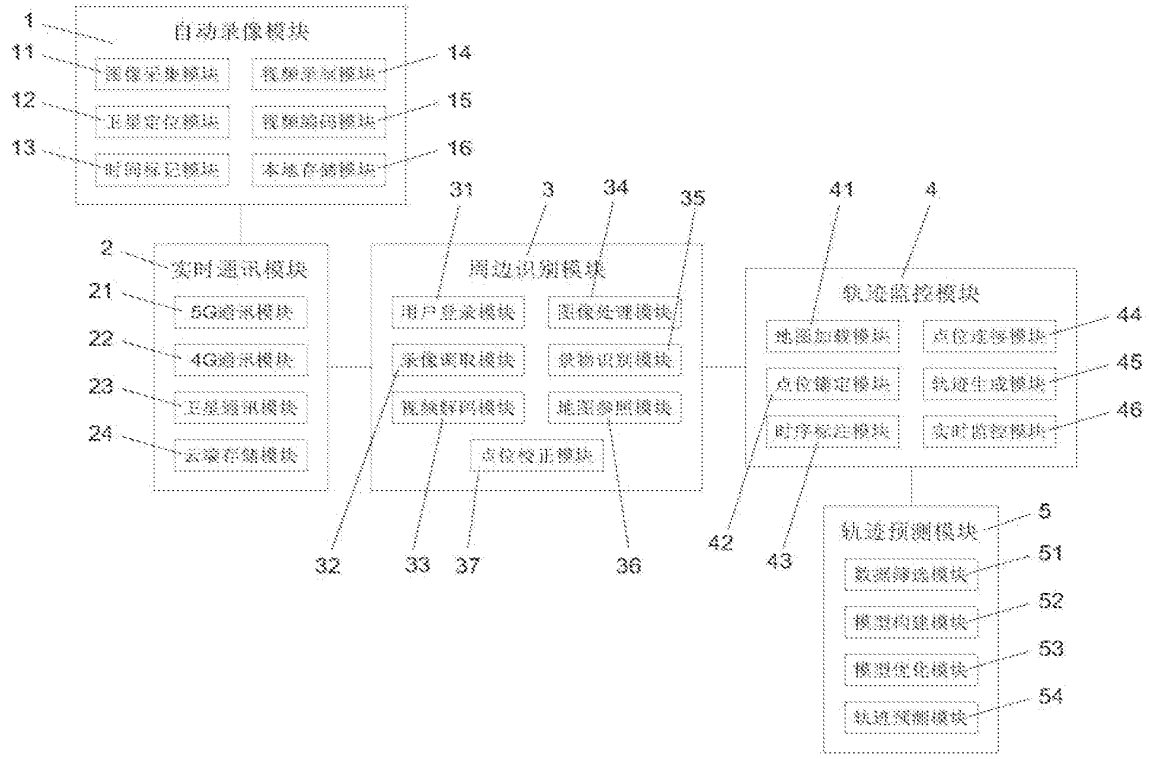


图1

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00285

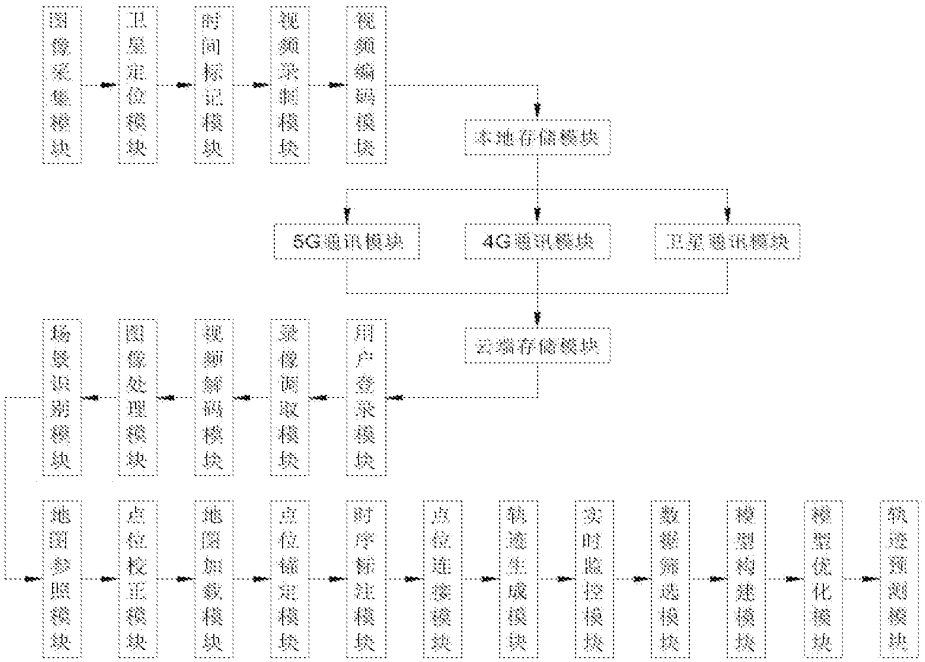


图2

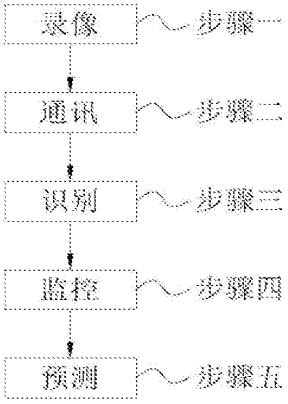


图3

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00286

Espacenet

WO2021052379A1 DATA STREAM TYPE IDENTIFICATION METHOD AND RELATED DEVICES

Applicants: HUAWEI TECH CO LTD [CN]

Inventors: WU JUN [CN],HU XINYU [CN],WANG YALI [CN],SI XIAOYUN [CN]

Classifications:

IPC ***H04L12/851;***

CPC **G06N20/00 (KR); G06N3/08 (KR); H04L41/145 (CN); H04L47/20 (US); H04L47/24 (EP); H04L47/2441 (US); H04L47/2475 (KR); H04L47/2483 (EP,CN,KR); H04L65/403 (EP,KR); H04L65/762 (EP); H04L65/80 (KR); H04L69/16 (KR); H04L69/22 (CN,US);** G06N20/00 (EP); G06N3/08 (EP); H04L65/80 (EP);

Priorities: CN201910872990A 2019-09-16

Application: CN2020115693W·2020-09-16

Publication: WO2021052379A1·2021-03-25

Published as: **BR112022004814A2; CN112511457A; CN112511457B; CN114465962A; EP4024791A1; EP4024791A4; JP2022548136A; KR20220053658A; US2022210082A1;** WO2021052379A1

DATA STREAM TYPE IDENTIFICATION METHOD AND RELATED DEVICES

Abstract

A data stream type identification method and related devices. The method comprises: obtaining at least one first confidence level of a current data stream corresponding to at least one data stream type according to message characteristics of the current data stream and a behavior recognition model, the behavior recognition model being a model obtained on the basis of a plurality of data stream samples; obtaining at least one second confidence level of the current data stream corresponding to at least one data stream type according to the characteristic information of the current data stream and a content recognition model, the content recognition model being a model obtained on the basis of one or more historical data streams; and determining the data stream type of the current data stream according to the at least one first confidence level and the at least one second confidence level. The data stream type can be more accurately identified using the present method.

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

CLAIMS WO2021052379A1

1.

A method for identifying a data stream type, comprising:

Obtain at least one first confidence degree corresponding to at least one data flow type of the current data flow according to the packet characteristics and behavior recognition model of the current data flow, wherein the behavior recognition model is a report based on a plurality of data flow samples The model obtained by the text feature and the data flow type; the message feature includes one or more of message length, message transmission speed, message interval time and message direction;

Obtaining at least one second confidence degree of the current data flow corresponding to the at least one data flow type according to the feature information and the content identification model of the current data flow, wherein the feature information includes a destination address and a protocol type, The content recognition model is a model obtained according to characteristic information and data flow types of one or more historical data flows, and the data flow type of the historical data flows is obtained according to the behavior recognition model;

Determine the data flow type of the current data flow according to the at least one first confidence level and the at least one second confidence level.

2.

The method according to claim 1, wherein the determining the data stream type of the current data stream according to the at least one first confidence degree and the at least one second confidence degree comprises:

calculating a composite confidence level corresponding to the first data flow type based on the first confidence level corresponding to the first data flow type and the second confidence level corresponding to the first data flow type, the first data flow type A data stream type is any one of the at least one data stream type;

If the comprehensive confidence degree corresponding to the first data flow type is greater than a first preset threshold, determine that the data flow type of the current data flow is the first data flow type.

3.

The method according to claim 1, wherein the determining the data flow type of the current data flow according to the at least one first confidence level and the at least one second confidence level comprises:

According to the first confidence degree corresponding to the first data stream type, the weight value of the first confidence degree, the second confidence degree corresponding to the first data stream type, and the weight value of the second confidence degree The weight value calculates the comprehensive confidence corresponding to the first data flow type, and the first data flow type is any one of the at least one data flow type;

If the comprehensive confidence degree corresponding to the first data flow type is greater than a first preset threshold, determine that the data flow type of the current data flow is the first data flow type.

4.

The method according to claim 2 or 3, characterized in that the method further comprises:

If the comprehensive confidence corresponding to the first data flow type is less than a second preset threshold, send the characteristic information of the current data flow and the information of the first data flow type to the device, and the second The preset threshold is greater than the first preset threshold;

receiving first information sent by the device, where the first information is obtained by the device according to the characteristic information of the current data flow and the identification information of the first data flow type;

Updating the content recognition model according to the first information to obtain a new content recognition model.

5.

The method according to claim 2 or 3, further comprising:

If the comprehensive confidence corresponding to the first data stream type is less than a second preset threshold, then update the content recognition model according to the feature information of the current data stream and the first data stream type information, so as to A new content recognition model is obtained, and the second preset threshold is greater than the first preset threshold.

6.

The method according to claim 5, wherein updating the content recognition model according to the characteristic information of the current data stream and the type information of the first data stream to obtain a new content recognition model comprises:

If the feature information of the first record among the multiple records is the same as the feature information of the current data stream but the data stream type of the first record is different from the first data stream type, then the updating the data stream type to the first data stream type to obtain a second record; each of the multiple records includes feature information and a data stream type;

and performing training on a plurality of records including the second record to obtain a new content recognition model.

7.

The method according to any one of claims 1-6, wherein after determining the data flow type of the current data flow according to the at least one first confidence level and the at least one second confidence level, Also includes:

Sending the information of the data flow type of the current data flow to an operation and maintenance support system OSS, where the information of the data flow type of the current data flow is used by the OSS to generate a flow control policy for the current data flow.

8.

The method according to any one of claims 1-7, wherein the message length includes one or more of Ethernet frame length, IP length, transport protocol length, and header length in the message, and the Transmission protocols include Transmission Control Protocol TCP and/or User Datagram Protocol UDP.

9.

A method for identifying a data stream type, comprising:

The characteristic information of the current data stream sent by the receiving device and the information of the data stream type;

generating first information according to the characteristic information of the current data flow and the information of the data flow type;

sending the first information to the device for updating a content recognition model, the content recognition model being used to obtain at least one second confidence level corresponding to at least one data stream type, wherein the content recognition model is A model obtained according to characteristic information and data flow types of one or more historical data streams, the data flow type of the historical data streams is obtained according to a behavior recognition model, and

the behavior recognition model is a report based on multiple data flow samples A model obtained by using a packet feature and a data flow type, and the packet feature includes one or more of packet length, packet transmission speed, packet interval time, and packet direction.

10.

The method according to claim 9, wherein the generating the first information according to the characteristic information of the current data flow and the information of the data flow type includes:

If the feature information of the first record among the multiple records is the same as the feature information of the current data stream but the data stream type of the first record is different from the data stream type of the current data stream, then the first The data flow type of the record is updated to the data flow type of the current data flow to obtain a second record; each record in the plurality of records includes characteristic information and a data flow type;

and performing training on a plurality of records including the second record to obtain a new content recognition model.

11.

A data flow type identification device, characterized in that the device is a first device, and the first device includes a memory and a processor, wherein the memory is used to store a computer program, and the processor calls the computer Programs that perform the following actions:

Obtain at least one first confidence degree corresponding to at least one data flow type of the current data flow according to the packet characteristics and behavior recognition model of the current data flow, wherein the behavior recognition model is a report based on a plurality of data flow samples The model obtained by the text feature and the data flow type; the message feature includes one or more of message length, message transmission speed, message interval time and message direction;

Obtaining at least one second confidence degree of the current data flow corresponding to the at least one data flow type according to the feature information and the content identification model of the current data flow, wherein the feature information includes a destination address and a protocol type, The content recognition model is a model obtained according to characteristic information and data flow types of one or more historical data flows, and the data flow type of the historical data flows is obtained according to the behavior recognition model;

Determine the data flow type of the current data flow according to the at least one first confidence level and the at least one second confidence level.

12.

The device according to claim 11, wherein the determining the data stream type of the current data stream according to the at least one first confidence degree and the at least one second confidence degree is specifically:

calculating a composite confidence level corresponding to the first data flow type based on the first confidence level corresponding to the first data flow type and the second confidence level corresponding to the first data flow type, the first data flow type A data stream type is any one of the at least one data stream type;

If the comprehensive confidence degree corresponding to the first data flow type is greater than a first preset threshold, determine that the data flow type of the current data flow is the first data flow type.

13.

The device according to claim 11, wherein the determining the data stream type of the current data stream according to the at least one first confidence degree and the at least one second confidence degree is specifically:

According to the first confidence degree corresponding to the first data stream type, the weight value of the first confidence degree, the second confidence degree corresponding to the first data stream type, and the weight value of the second confidence degree The weight value calculates the comprehensive confidence corresponding to the first data flow type, and the first data flow type is any one of the at least one data flow type;

If the comprehensive confidence degree corresponding to the first data flow type is greater than a first preset threshold, determine that the data flow type of the current data flow is the first data flow type.

14.

The device according to claim 12 or 13, wherein the first device further comprises a transceiver, and the processor is further configured to:

If the comprehensive confidence corresponding to the first data stream type is less than a second preset threshold, sending the characteristic information of the current data stream and the first data stream type to a second device through the transceiver information, the second preset threshold is greater than the first preset threshold;

receiving, by the transceiver, first information sent by the second device, where the first information is obtained by the second device according to the characteristic information of the current data stream and the identification information of the first data stream type ;

Updating the content recognition model according to the first information to obtain a new content recognition model.

15.

The device according to claim 12 or 13, wherein the processor is further configured to:

If the comprehensive confidence corresponding to the first data stream type is less than a second preset threshold, then update the content recognition model according to the feature information of the current data stream and the first data stream type information, so as to A new content recognition model is obtained, and the second preset threshold is greater than the first preset threshold.

16.

The device according to claim 15, wherein the content recognition model is updated according to the characteristic information of the current data stream and the type information of the first data stream to obtain a new content recognition model, specifically :

If the feature information of the first record among the multiple records is the same as the feature information of the current data stream but the data stream type of the first record is different from the first data stream type, then the updating the data stream type to the first data stream type to obtain a second record; each of the multiple records includes feature information and a data stream type;

and performing training on a plurality of records including the second record to obtain a new content recognition model.

17.

The device according to any one of claims 11-16, wherein the first device further comprises a transceiver, and the processor is further configured to: After the at least one second confidence degree determines the data flow type of the current data flow, the information of the data flow type of the current data flow is sent to the operation and maintenance support system OSS through the transceiver, and the data flow of the current data flow The information of the flow type is used by the OSS to generate a flow control policy for the current data flow.

18.

The device according to any one of claims 11-17, wherein the packet length includes one or more of the Ethernet frame length, IP length, transport protocol length, and header length in the packet, and the Transmission protocols include Transmission Control Protocol TCP and/or User Datagram Protocol UDP.

19.

A data flow type identification device, the device is a first device, characterized in that the first device includes a memory, a processor and a transceiver, wherein the memory is used to store a computer program, and the processor calls The computer program is used to perform the following operations:

receiving, through the transceiver, the characteristic information of the current data flow and the information of the type of the data flow sent by the second device;

generating first information according to the characteristic information of the current data flow and the information of the data flow type;

Sending the first information to the second device via the transceiver for updating a content recognition model, the content recognition model being used to obtain at least one second confidence level corresponding to at least one data stream type, wherein , the content recognition model is a model obtained according to the feature information and data flow types of one or more historical data streams, the data flow type of the historical data streams is obtained according to a behavior recognition model, and the behavior recognition model is based on A model obtained from packet characteristics and data flow types of multiple data flow samples, where the packet characteristics include one or more of packet length, packet transmission speed, packet interval time, and packet direction.

20.

The device according to claim 19, wherein the first information is generated according to the characteristic information of the current data flow and the information of the data flow type, specifically:

If the feature information of the first record among the multiple records is the same as the feature information of the current data stream but the data stream type of the first record is different from the data stream type of the current data stream, then the first The data flow type of the record is updated to the data flow type of the current data flow to obtain a second record; each record in the plurality of records includes characteristic information and a data flow type;

and performing training on a plurality of records including the second record to obtain a new content recognition model.

21.

A device for identifying a data stream type, characterized by comprising a unit for performing the method according to any one of claims 1-10

22.

A computer-readable storage medium, wherein a computer program is stored in the computer-readable storage medium, and when the computer program is run on a processor, the method according to any one of claims 1-10 is realized.

23.

A computer program product, characterized in that the computer program product is stored in a memory, and when the computer program product is run on a processor, the method according to any one of claims 1-10 is implemented.

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

DESCRIPTION WO2021052379A1

A data flow type identification method and related equipment

[0001]

This application claims the priority of the Chinese patent application with the application number 201910872990.0 and the title of the invention "A data stream type identification method and related equipment" filed on September 16, 2019, the entire contents of which are incorporated by reference in this application . technical field

[0002]

The present invention relates to the field of computer technology and communication, and further relates to the application of artificial intelligence (AI) in the field of computer technology and communication, in particular to a data flow type identification method and related equipment.

Background technique

[0003]

With the rapid development of computer technology, more and more enterprises use private office applications for office work, such as desktop cloud, voice conferencing, video conferencing, etc. are all private office applications.

In order to reasonably arrange the traffic of each service and improve service reliability, it is usually necessary to reasonably configure QoS priority and real-time route selection. The premise of QoS priority and real-time route selection is to know which type of application (that is, which type of data flow) the current office application belongs to.

[0004]

At present, the following two methods are mainly used to know the type of office application: the first method is based on manual identification, mainly manually configuring rules to match keywords in network traffic (including header data, payload data, etc.), so as to identify App types.

However, the manual identification method is time-consuming and labor-intensive, and with the dynamics brought about by the cloudification of enterprise office applications, transmission encryption is usually performed for safety, which makes it difficult to manually set the identification rules for application types, which makes it difficult to it is difficult to identify the application type. The second method is to use offline learning, which is mainly to collect sample data in advance, then manually or use third-party tools to label the sample data, and then use machine learning or neural network algorithms to model the offline model of the labeled sample data train. The offline trained model is used to infer the application type of live network traffic. However, every time an enterprise application is modified or updated, the trained model may not be usable; in addition, the implementation of private applications is not standardized, and the applicable models for the same type of applications in different enterprises are different. That is to say, when the model trained above is used for type recognition of a modified or updated application or another enterprise's application, the recognition accuracy may not be high.

[0005]

How to quickly and accurately identify the application type (also referred to as the data flow type) of the office application is a technical issue that is being studied by those skilled in the art.

[0006]

Contents of the invention

[0007]

The embodiment of the invention discloses a data flow type identification method and related equipment, which can more accurately identify the data flow type.

[0008]

In the first aspect, the embodiment of the present application provides a method for identifying a data flow type, the method including:

[0009]

Obtain at least one first confidence degree corresponding to at least one data flow type of the current data flow according to the packet characteristics and behavior recognition model of the current data flow, wherein the behavior recognition model is a report based on a plurality of data flow samples The model obtained by the text feature and the data flow type; the message feature includes one or more of message length, message transmission speed, message interval time and message direction;

[0010]

Obtaining at least one second confidence degree of the current data flow corresponding to the at least one data flow type according to the feature information and the content identification model of the current data flow, wherein the feature information includes a destination address and a protocol type, The content recognition model is a model obtained according to characteristic information and data flow types of one or more historical data flows, and the data flow type of the historical data flows is obtained according to the behavior recognition model;

[0011]

Determine the data flow type of the current data flow according to the at least one first confidence level and the at least one second confidence level.

[0012]

In the above method, a behavior recognition model and a content recognition model are involved. The behavior recognition model is obtained by pre-training the message characteristics and data flow types of multiple data flow samples, and the content recognition model is based on the characteristic information of the data flow and the behavior model. The identified data flow type is trained, so the content recognition model is an online learning model; the behavior recognition model can recognize some basic (or typical) data flow types of data flow, and certain characteristics of the same type of data flow (such as message length, message transmission speed, etc.) may change during the subsequent transmission process, so the type of the data flow can be identified from other aspects (such as destination address, protocol type, etc.) in combination with the online learning characteristics of the content recognition model. The hedging behavior recognition model recognizes the data flow type of the data flow in the process of data flow transmission. Therefore, this application adopts the recognition method of combining the behavior recognition model and the content recognition model to improve the recognition accuracy of the data flow type of the data flow , which also improves the generalization of identification, and can be applied to various scenarios such as application cloud deployment, application transmission encryption, and private applications.

[0013]

With reference to the first aspect, in a first possible implementation manner of the first aspect, determining the data flow type

of the current data flow according to the at least one first confidence level and the at least one second confidence level, include:

[0014]

According to the first confidence degree corresponding to the first data stream type, the weight value of the first confidence degree, the second confidence degree corresponding to the first data stream type, and the weight value of the second confidence degree The weight value calculates the comprehensive confidence corresponding to the first data flow type, and the first data flow type is any one of the at least one data flow type;

[0015]

If the comprehensive confidence degree corresponding to the first data flow type is greater than a first preset threshold, determine that the data flow type of the current data flow is the first data flow type.

[0016]

In the above method, according to the degree of influence of the content recognition model and the behavior recognition model on the final recognition result, the weights of the confidence degrees are respectively configured for the two models (the weight configured for the behavior recognition model is the weight of the first confidence degree, which is The weight configured by the content recognition model is the weight of the second confidence degree), so the comprehensive confidence calculated based on the weights of the two confidence degrees can better reflect the actual type of the current data flow.

In addition, introducing a first preset threshold to measure whether the corresponding data flow type is desirable can improve the efficiency and accuracy of determining the data flow type.

[0017]

In combination with the first aspect, or any of the above possible implementation manners of the first aspect, in a second possible implementation manner of the first aspect, the method further includes:

[0018]

If the comprehensive confidence corresponding to the first data flow type is less than a second preset threshold, send the characteristic information of the current data flow and the information of the first data flow type to the device, and the second The preset threshold is greater than the first preset threshold;

[0019]

receiving first information sent by the device, where the first information is obtained by the device according to the characteristic information of the current data flow and the identification information of the first data flow type;

[0020]

Updating the content recognition model according to the first information to obtain a new content recognition model.

[0021]

In combination with the first aspect, or any of the above possible implementation manners of the first aspect, the third possible implementation manner of the first aspect further includes:

[0022]

If the comprehensive confidence corresponding to the first data stream type is less than a second preset threshold, then update the content recognition model according to the feature information of the current data stream and the first data stream type information, so as to A new content recognition model is obtained, and the second preset threshold is greater than the first preset threshold.

[0023]

In the above method, the inventor of the present application uses the identification result of the data stream type of the current data stream to correct the content recognition model.

Specifically, a second preset threshold is introduced, and when the comprehensive confidence corresponding to the first data stream type is less than the second preset threshold, relevant information about the current data stream is sent to the device for training, so as to use To obtain a new content recognition model to make the next identification result more accurate.

[0024]

With reference to the first aspect, or any of the above possible implementation manners of the first aspect, in a fourth possible implementation manner of the first aspect, the The stream type information updates the content recognition model to obtain a new content recognition model, including:

[0025]

If the feature information of the first record among the multiple records is the same as the feature information of the current data stream but the data stream type of the first record is different from the first data stream type, then the updating the data stream type to the first data stream type to obtain a second record; each of the multiple records includes feature information and a data stream type;

[0026]

and performing training on a plurality of records including the second record to obtain a new content recognition model.

[0027]

That is to say, if the feature information of the historical data flow is the same as that of the current data flow but the data flow type is different in the identified record, update the data flow type in the record to the current data flow This is mainly to adapt to the flexible deployment of cloud resources. For example, the same cloud resource is used for video conferencing in the previous period, and is used for desktop cloud in the next period. The data flow type is updated to desktop cloud, so that the data flow type of the current data flow can still be accurately identified in the case of elastic deployment of cloud resources.

[0028]

With reference to the first aspect, or any of the above possible implementation manners of the first aspect, in a fifth possible implementation manner of the first aspect, the After determining the data flow type of the current data flow with two confidence degrees, it also includes:

[0029]

Sending the information of the data flow type of the current data flow to an operation and maintenance support system OSS, where the information of the data flow type of the current data flow is used by the OSS to generate a flow control policy for the current data flow.

[0030]

That is to say, after the data flow type of the current data flow is determined, the relevant information of the current data flow type is notified to the OSS system, so that the OSS system can generate an Stream flow control policy, for example, when the first data stream type of the current data stream is video stream of video conference, define its corresponding flow control policy as the priority transmission policy, that is, when there are multiple data streams to be transmitted, the priority Transmit the current data stream.

[0031]

in combination with the first aspect, or any of the above possible implementations of the first aspect, in the sixth possible implementation of the first aspect, the packet length includes the Ethernet frame length in the packet, the IP length, the transmission One or more of protocol length and header length, the transmission protocol includes transmission control protocol TCP and/or user datagram protocol UDP.

[0032]

in a second aspect, an embodiment of the present application provides a method for identifying a data stream type, the method including:

[0033]

The characteristic information of the current data stream sent by the receiving device and the information of the data stream type;

[0034]

generating first information according to the characteristic information of the current data flow and the information of the data flow type;

[0035]

sending the first information to the device for updating a content recognition model, the content recognition model being used to obtain at least one second confidence level corresponding to at least one data stream type, wherein the content recognition model is A model obtained according to characteristic information and data flow types of one or more historical data streams, the data flow type of the historical data streams is obtained according to a behavior recognition model, and the behavior recognition model is a report based on multiple data flow samples A model obtained by using a packet feature and a data flow type, and the packet feature includes one or more of packet length, packet transmission speed, packet interval time, and packet direction.

[0036]

in the above method, a behavior recognition model and a content recognition model are involved. The behavior recognition model is obtained by pre-training the message characteristics and data flow types of multiple data flow samples, and the content recognition model is based on the characteristic information of the data flow and the behavior model. The identified data flow type is trained, so the content recognition model is an online learning model; the behavior recognition model can recognize some basic (or typical) data flow types of data flow, and certain characteristics of the same type of data flow (such as message length, message transmission speed, etc.) may change during the subsequent transmission process, so the type of the data flow can be identified from other aspects (such as destination address, protocol type, etc.) in combination with the online learning characteristics of the content recognition model. The hedging behavior recognition model recognizes the data flow type of the data flow in the process of data flow transmission. Therefore, this application adopts the recognition method of combining the behavior recognition model and the content recognition model to improve the recognition accuracy of the data flow type of the data flow , also improves the generalization of identification, and can be applied to various scenarios such as application cloud deployment, application transmission encryption, and private applications.

[0037]

In a third aspect, an embodiment of the present application provides a data stream type identification device, including a memory and a processor, wherein the memory is used to store a computer program, and the processor invokes the computer program to perform the following operations:

[0038]

Obtain at least one first confidence degree corresponding to at least one data flow type of the current data flow according to the packet characteristics and behavior recognition model of the current data flow, wherein the behavior recognition model is a report based on a plurality of data flow samples The model obtained by the texi

feature and the data flow type; the message feature includes one or more of message length, message transmission speed, message interval time and message direction;

[0039]

Obtaining at least one second confidence degree of the current data flow corresponding to the at least one data flow type according to the feature information and the content identification model of the current data flow, wherein the feature information includes a destination address and a protocol type, The content recognition model is a model obtained according to characteristic information and data flow types of one or more historical data flows, and the data flow type of the historical data flows is obtained according to the behavior recognition model;

[0040]

Determine the data flow type of the current data flow according to the at least one first confidence level and the at least one second confidence level.

[0041]

In the above method, a behavior recognition model and a content recognition model are involved. The behavior recognition model is obtained by pre-training the message characteristics and data flow types of multiple data flow samples, and the content recognition model is based on the characteristic information of the data flow and the behavior model. The identified data flow type is trained, so the content recognition model is an online learning model; the behavior recognition model can recognize some basic (or typical) data flow types of data flow, and certain characteristics of the same type of data flow (such as message length, message transmission speed, etc.) may change during the subsequent transmission process, so the type of the data flow can be identified from other aspects (such as destination address, protocol type, etc.) in combination with the online learning characteristics of the content recognition model. The hedging behavior recognition model recognizes the data flow type of the data flow in the process of data flow transmission. Therefore, this application adopts the recognition method of combining the behavior recognition model and the content recognition model to improve the recognition accuracy of the data flow type of the data flow , which also improves the generalization of identification, and can be applied to various scenarios such as application cloud deployment, application transmission encryption, and private applications.

[0042]

With reference to the third aspect, in a first possible implementation manner of the third aspect, determining the data flow type of the current data flow according to the at least one first confidence level and the at least one second confidence level, Specifically:

[0043]

According to the first confidence degree corresponding to the first data stream type, the weight value of the first confidence degree, the second confidence degree corresponding to the first data stream type, and the weight value of the second confidence degree The weight value calculates the comprehensive confidence corresponding to the first data flow type, and the first data flow type is any one of the at least one data flow type;

[0044]

If the comprehensive confidence degree corresponding to the first data flow type is greater than a first preset threshold, determine that the data flow type of the current data flow is the first data flow type.

[0045]

In the above operation, according to the degree of influence of the content recognition model and the behavior recognition model on the final recognition result, the weights of the confidence degrees are respectively configured for the two models (the weight configured for the behavior recognition model is the

weight of the first confidence degree, which is The weight configured by the content recognition model is the weight of the second confidence degree), so the comprehensive confidence calculated based on the weights of the two confidence degrees can better reflect the actual type of the current data flow.

In addition, introducing a first preset threshold to measure whether the corresponding data flow type is desirable can improve the efficiency and accuracy of determining the data flow type.

[0046]

With reference to the third aspect, or any of the foregoing possible implementation manners of the third aspect, in a second possible implementation manner of the third aspect, the device further includes a transceiver, and the processor is further configured to:

[0047]

If the comprehensive confidence corresponding to the first data stream type is less than a second preset threshold, sending the feature information of the current data stream and the first data stream type to other devices through the transceiver information, the second preset threshold is greater than the first preset threshold;

[0048]

receiving the first information sent by the other device through the transceiver, the first information is obtained by the other device according to the characteristic information of the current data flow and the identification information of the first data flow type;

[0049]

Updating the content recognition model according to the first information to obtain a new content recognition model.

[0050]

With reference to the third aspect, or any of the foregoing possible implementation manners of the third aspect, in a third possible implementation manner of the third aspect, the processor is further configured to:

[0051]

If the comprehensive confidence corresponding to the first data stream type is less than a second preset threshold, then update the content recognition model according to the feature information of the current data stream and the first data stream type information, so as to A new content recognition model is obtained, and the second preset threshold is greater than the first preset threshold.

[0052]

In the above method, the inventor of the present application uses the identification result of the data stream type of the current data stream to correct the content recognition model.

Specifically, a second preset threshold is introduced, and when the comprehensive confidence corresponding to the first data stream type is less than the second preset threshold, relevant information about the current data stream is sent to the device for training, so as to use To obtain a new content recognition model to make the next identification result more accurate.

[0053]

With reference to the third aspect, or any of the above possible implementation manners of the third aspect, in a fourth possible implementation manner of the third aspect, the The flow type information updates the content recognition model to obtain a new content recognition model, specifically:

[0054]

If the feature information of the first record among the multiple records is the same as the feature information of the current data stream but the data stream type of the first record is different from the first data stream type, then the updating the data stream type to the first data stream type to obtain a second record; each of the multiple records includes feature information and a data stream type;

[0055]

and performing training on a plurality of records including the second record to obtain a new content recognition model.

[0056]

That is to say, if the feature information of the historical data flow is the same as that of the current data flow but the data flow type is different in the identified record, update the data flow type in the record to the current data flow This is mainly to adapt to the flexible deployment of cloud resources. For example, the same cloud resource is used for video conferencing in the previous period, and is used for desktop cloud in the next period; The data flow type is updated to desktop cloud, so that the data flow type of the current data flow can still be accurately identified in the case of elastic deployment of cloud resources.

[0057]

With reference to the third aspect, or any of the foregoing possible implementation manners of the third aspect, in a fifth possible implementation manner of the third aspect, the device further includes a transceiver, and the processor is further configured to: After determining the data flow type of the current data flow according to the at least one first confidence degree and the at least one second confidence degree, sending the data flow type of the current data flow to the operation and maintenance support system OSS through the transceiver information about the data flow type, the information about the data flow type of the current data flow is used by the OSS to generate a flow control policy for the current data flow.

[0058]

That is to say, after the data flow type of the current data flow is determined, the relevant information of the current data flow type is notified to the OSS system, so that the OSS system can generate an Stream flow control policy, for example, when the first data stream type of the current data stream is video stream of video conference, define its corresponding flow control policy as the priority transmission policy, that is, when there are multiple data streams to be transmitted, the priority Transmit the current data stream.

[0059]

In combination with the third aspect, or any of the above possible implementations of the third aspect, in the sixth possible implementation of the third aspect, the packet length includes the Ethernet frame length in the packet, the IP length, the transmission One or more of protocol length and header length, the transmission protocol includes transmission control protocol TCP and/or user datagram protocol UDP.

[0060]

In a fourth aspect, an embodiment of the present application provides a data stream type identification device, including a memory, a processor, and a transceiver, wherein the memory is used to store a computer program, and the processor invokes the computer program to perform the following operations :

[0061]

receiving, through the transceiver, the characteristic information of the current data stream and the information of the data stream type sent by other devices;

[0062]

generating first information according to the characteristic information of the current data flow and the information of the data flow type;

[0063]

Sending the first information to the other device through the transceiver for updating a content recognition model, the content recognition model is used to obtain at least one second confidence level corresponding to at least one data flow type, wherein, The content recognition model is a model obtained according to characteristic information and data flow types of one or more historical data flows, and the data flow type of the historical data flow is obtained according to a behavior recognition model, and the behavior recognition model is based on multiple A model obtained from the packet characteristics and data flow types of a data flow sample, the packet characteristics include one or more of packet length, packet transmission speed, packet interval time, and packet direction.

[0064]

The above operations involve a behavior recognition model and a content recognition model. The behavior recognition model is pre-trained from the message characteristics and data flow types of multiple data flow samples, while the content recognition model is based on the characteristic information of the data flow and the behavior model The identified data flow type is trained, so the content recognition model is an online learning model; the behavior recognition model can recognize some basic (or typical) data flow types of data flow, and certain characteristics of the same type of data flow (such as message length, message transmission speed, etc.) may change during the subsequent transmission process, so the type of the data flow can be identified from other aspects (such as destination address, protocol type, etc.) in combination with the online learning characteristics of the content recognition model. The hedging behavior recognition model recognizes the data flow type of the data flow in the process of data flow transmission. Therefore, this application adopts the recognition method of combining the behavior recognition model and the content recognition model to improve the recognition accuracy of the data flow type of the data flow , which also improves the generalization of identification, and can be applied to various scenarios such as application cloud deployment, application transmission encryption, and private applications.

[0065]

In the fifth aspect, the embodiment of the present application provides a data flow type identification device, the device includes:

[0066]

The first identification unit is configured to obtain at least one first confidence level corresponding to at least one data flow type of the current data flow according to the packet characteristics and the behavior recognition model of the current data flow, wherein the behavior recognition model is based on A model obtained from packet characteristics and data flow types of multiple data flow samples; the packet characteristics include one or more of packet length, packet transmission speed, packet interval time, and packet direction;

[0067]

The second identification unit is configured to obtain at least one second confidence level of the current data stream corresponding to the at least one data stream type according to the feature

information of the current data stream and a content identification model, wherein the feature information is including the destination address and protocol type, the content recognition model is a model obtained according to the characteristic information and data flow type of one or more historical data flows, and the data flow type of the historical data flow is obtained according to the behavior recognition model ;

[0068]

A determining unit, configured to determine the data stream type of the current data stream according to the at least one first confidence level and the at least one second confidence level.

[0069]

Among the above-mentioned devices, a behavior recognition model and a content recognition model are involved. The behavior recognition model is pre-trained by the message characteristics and data flow types of multiple data flow samples, and the content recognition model is based on the characteristic information of the data flow and the behavior model The identified data flow type is trained, so the content recognition model is an online learning model; the behavior recognition model can recognize some basic (or typical) data flow types of data flow, and certain characteristics of the same type of data flow (such as message length, message transmission speed, etc.) may change during the subsequent transmission process, so the type of the data flow can be identified from other aspects (such as destination address, protocol type, etc.) in combination with the online learning characteristics of the content recognition model. The hedging behavior recognition model recognizes the data flow type of the data flow in the process of data flow transmission. Therefore, this application adopts the recognition method of combining the behavior recognition model and the content recognition model to improve the recognition accuracy of the data flow type of the data flow , which also improves the generalization of identification, and can be applied to various scenarios such as application cloud deployment, application transmission encryption, and private applications.

[0070]

With reference to the fifth aspect, in a first possible implementation manner of the fifth aspect, the determining unit is configured to determine the current data flow according to the at least one first confidence level and the at least one second confidence level The data flow type of , specifically:

[0071]

used for according to the first confidence level corresponding to the first data flow type, the weight value of the first confidence level, the second confidence level corresponding to the first data flow type, and the second confidence level The weight value of the degree calculates the comprehensive confidence degree corresponding to the first data flow type, and the first data flow type is any one of the at least one data flow type;

[0072]

If the comprehensive confidence degree corresponding to the first data flow type is greater than a first preset threshold, it is determined that the data flow type of the current data flow is the first data flow type.

[0073]

In the above-mentioned equipment, according to the degree of influence of the content recognition model and the behavior recognition model on the final recognition result respectively, the weights of the confidence degrees are respectively configured for the two

models (the weight configured for the behavior recognition model is the weight of the first confidence degree, which is The weight configured by the content recognition model is the weight of the second confidence degree), so the comprehensive confidence calculated based on the weights of the two confidence degrees can better reflect the actual type of the current data flow.

In addition, introducing a first preset threshold to measure whether the corresponding data flow type is desirable can improve the efficiency and accuracy of determining the data flow type.

[0074]

With reference to the fifth aspect, or any of the foregoing possible implementation manners of the fifth aspect, in a second possible implementation manner of the fifth aspect, the device further includes:

[0075]

A first sending unit, configured to send the characteristic information of the current data flow and the first information about the type of data flow, the second preset threshold is greater than the first preset threshold;

[0076]

a receiving unit, configured to receive first information sent by the other device, where the first information is obtained by the other device according to the characteristic information of the current data stream and the identification information of the first data stream type;

[0077]

An updating unit, configured to update the content recognition model according to the first information to obtain a new content recognition model

[0078]

In combination with the fifth aspect, or any of the above possible implementation manners of the fifth aspect, the third possible implementation manner of the fifth aspect further includes:

[0079]

An updating unit, configured to update according to the characteristic information of the current data stream and the information of the first data stream type when the comprehensive confidence corresponding to the first data stream type is less than a second preset threshold The content recognition model is used to obtain a new content recognition model, and the second preset threshold is greater than the first preset threshold.

[0080]

In the above method, the inventor of the present application uses the identification result of the data stream type of the current data stream to correct the content recognition model.

Specifically, a second preset threshold is introduced, and when the comprehensive confidence corresponding to the first data stream type is less than the second preset threshold, relevant information about the current data stream is sent to the device for training, so as to use To obtain a new content recognition model to make the next identification result more accurate.

[0081]

With reference to the fifth aspect, or any of the above possible implementation manners of the fifth aspect, in a fourth possible implementation manner of the fifth aspect, the The flow type information updates the content recognition model to obtain a new content recognition model, specifically:

[0082]

If the feature information of the first record among the multiple records is the same as the feature information of the current data stream but the data stream type of the first record is different from the first data stream type, then the updating the data stream type to the first data stream type to obtain a second record; each of the multiple records includes feature information and a data stream type;

[0083]

and performing training on a plurality of records including the second record to obtain a new content recognition model

[0084]

That is to say, if the feature information of the historical data flow is the same as that of the current data flow but the data flow type is different in the identified record, update the data flow type in the record to the current data flow This is mainly to adapt to the flexible deployment of cloud resources. For example, the same cloud resource is used for video conferencing in the previous period, and is used for desktop cloud in the next period; The data flow type is updated to desktop cloud, so that the data flow type of the current data flow can still be accurately identified in the case of elastic deployment of cloud resources.

[0085]

With reference to the fifth aspect, or any of the foregoing possible implementation manners of the fifth aspect, in a fifth possible implementation manner of the fifth aspect, the device further includes:

[0086]

The second sending unit is configured to, after the determining unit determines the data flow type of the current data flow according to the at least one first confidence degree and the at least one second confidence degree, send the information to the operation and maintenance support system OSS information about the data flow type of the current data flow, and the information about the data flow type of the current data flow is used by the OSS to generate a flow control policy for the current data flow.

[0087]

That is to say, after the data flow type of the current data flow is determined, the relevant information of the current data flow type is notified to the OSS system, so that the OSS system can generate an Stream flow control policy, for example, when the first data stream type of the current data stream is video stream of video conference, define its corresponding flow control policy as the priority transmission policy, that is, when there are multiple data streams to be transmitted, the priority Transmit the current data stream.

[0088]

In combination with the fifth aspect, or any of the above possible implementations of

the fifth aspect, in the sixth possible implementation of the fifth aspect, the packet length includes the Ethernet frame length in the packet, the IP length, the transmission One or more of protocol length and header length, the transmission protocol includes transmission control protocol TCP and/or user datagram protocol UDP.

[0089]

in a sixth aspect, the embodiment of the present application provides a device for identifying a data stream type, which includes:

[0090]

The receiving unit is used to receive the characteristic information of the current data flow and the information of the data flow type sent by other devices;

[0091]

a generating unit, configured to generate first information according to the characteristic information of the current data stream and the information of the data stream type;

[0092]

A sending unit, configured to send the first information to the other device for updating a content recognition model, and the content recognition model is used to obtain at least one second confidence level corresponding to at least one data stream type, wherein, The content recognition model is a model obtained according to characteristic information and data flow types of one or more historical data flows, and the data flow type of the historical data flow is obtained according to a behavior recognition model, and the behavior recognition model is based on multiple A model obtained from the packet characteristics and data flow types of a data flow sample, the packet characteristics include one or more of packet length, packet transmission speed, packet interval time, and packet direction.

[0093]

Among the above-mentioned devices, a behavior recognition model and a content recognition model are involved. The behavior recognition model is pre-trained by the message characteristics and data flow types of multiple data flow samples, and the content recognition model is based on the characteristic information of the data flow and the behavior model The identified data flow type is trained, so the content recognition model is an online learning model; the behavior recognition model can recognize some basic (or typical) data flow types of data flow, and certain characteristics of the same type of data flow (such as message length, message transmission speed, etc.) may change during the subsequent transmission process, so the type of the data flow can be identified from other aspects (such as destination address, protocol type, etc.) in combination with the online learning characteristics of the content recognition model. The hedging behavior recognition model recognizes the data flow type of the data flow in the process of data flow transmission. Therefore, this application adopts the recognition method of combining the behavior recognition model and the content recognition model to improve the recognition accuracy of the data flow type of the data flow , which also improves the generalization of identification, and can be applied to various scenarios such as application cloud deployment, application transmission encryption, and private applications.

[0094]

in the seventh aspect, the embodiments of the present application provide a computer-readable storage medium, where a computer program is stored in the computer-readable storage medium, and when it is run on a processor, the first aspect or any possibility of the first aspect can be realized. implementation of the described method.

[0096]

in an eighth aspect, an embodiment of the present application provides a computer program product, the computer program product is stored in a memory, and when the computer program product is run on a processor, the first aspect or any possible implementation of the first aspect can be realized. Implement the method described by.

[0096]

in the ninth aspect, the embodiment of the present application provides a data stream type identification system, the system includes a first device and a second device, wherein the second device is the third aspect above, or any possible one of the third aspect or the fifth aspect, or the data flow type identification device described in any possible implementation of the fifth aspect; the first device is the above fourth aspect, or any possible implementation of the fourth aspect manner, or the sixth aspect, or the device for identifying the data stream type described in any possible implementation manner of the sixth aspect.

[0097]

In the embodiment of the present application, it involves a behavior recognition model and a content recognition model. The behavior recognition model is pre-trained by the message characteristics and data flow types of multiple data flow samples, and the content recognition model is based on the characteristic information of the data flow and the The data flow type identified by the behavior model is trained, so the content recognition model is an online learning model; the behavior recognition model can recognize some basic (or typical) data flow types of data flow, and certain characteristics of the same type of data flow (such as message length, message transmission speed, etc.) may change during the subsequent transmission process, so the type of data flow is identified from other aspects (such as destination address, protocol type, etc.) in combination with the online learning characteristics of the content recognition model , can hedge against the recognition error of the data flow type of the data flow by the behavior recognition model in the process of data flow transmission, so this application adopts the recognition method of combining the behavior recognition model and the content recognition model to improve the recognition of the data flow type of the data flow Accuracy also improves the generalization of recognition, and can be applied to various scenarios such as application cloud deployment, application transmission encryption, and private applications.

Description of drawings

[0098]

The accompanying drawings used in the embodiments of the present invention are introduced below.

[0099]

FIG. 1 is a schematic diagram of the architecture of a data stream type

identification system provided by an embodiment of the present invention;

[0100]

FIG. 2A is a schematic diagram of a scene of a content recognition model and a behavior recognition model provided by an embodiment of the present invention;

[0101]

Fig. 2B is a schematic structural diagram of a classification model provided by an embodiment of the present invention;

[0102]

Fig. 2C is a schematic structural diagram of a classification model provided by an embodiment of the present invention;

[0103]

Fig. 2D is a schematic structural diagram of a classification model provided by an embodiment of the present invention;

[0104]

FIG. 3 is a schematic flowchart of a method for identifying a data stream type provided by an embodiment of the present invention;

[0105]

FIG. 4 is a schematic diagram of scenarios of data stream a and data stream b provided by an embodiment of the present invention;

[0106]

Fig. 5 is a sample schematic diagram of a data flow record provided by an embodiment of the present invention;

[0107]

Fig. 6 is a sample schematic diagram of a data flow record provided by an embodiment of the present invention;

[0108]

FIG. 7 is a schematic structural diagram of a second device provided by an embodiment of the present invention;

[0109]

Fig. 8 is a schematic structural diagram of a first device provided by an embodiment of the present invention;

[0110]

FIG. 9 is a schematic structural diagram of another second device provided by an embodiment of the present invention;

[0111]

Fig. 10 is a schematic structural diagram of another first device provided by an embodiment of the present invention.

Detailed ways

[0112]

Embodiments of the present invention will be described below with reference to the drawings in the embodiments of the present invention.

[0113]

Please refer to FIG. 1. FIG. 1 is a schematic diagram of the architecture of a data flow type identification system provided by an embodiment of the present invention, the system includes an operation and maintenance support system (operational system support, OSS) 101, a server 102, a forwarding device 103, a terminal 104, wherein the number of terminals 104 can be multiple, and only 6 are shown in the figure as an example. The terminals 104 are used to run various applications, such as video conferencing applications, audio conferencing applications, desktop cloud applications, etc. , the data stream types (also referred to as application types) of the data streams generated by different applications are often different.

In the embodiment of the present application, the data flow generated by the terminal 104 needs to be sent to the destination device through the forwarding device 103 first, wherein the forwarding device may include a router, a switch, etc., and the number of forwarding devices 103 may be one or more, for example , there is one router and three switches; another example, there is only one switch, another example, there are three switches, and so on.

The aforementioned server 102 may be one server or a server cluster composed of multiple servers.

[0114]

Wherein, how to send the data flow generated by the terminal 104 on the terminal 104 and how to forward it on the forwarding device 103 can be carried out according to the traffic control policy generated by the OSS101. For example, when the traffic control policy stipulates that the video conferencing application When the generated data stream has the highest priority, if there are multiple data streams including the data stream generated by the video conference application to be sent on the terminal 104 or the forwarding device 103, the data stream generated by the video conference application will be transmitted first data flow

It should be noted that the flow control policy is generated by OSS 101 based on the data flow type of the current data flow.

In the embodiment of the present application, the data flow type of the current data flow used by the OSS 101 to generate the traffic control policy is determined by the second device.

[0115]

As shown in Figure 2A, the second device needs to use a behavior recognition model and a content recognition model when determining the data flow type of the current data flow, where the parameters of the

model may include but not limited to the confidence weight vector (w1, w2) , the first preset threshold 81 of the data flow type, and the second preset threshold 82, wherein the first preset threshold can also be called the classification threshold, which is used to measure whether to classify the data flow type into a certain category, the second preset threshold Set the threshold, also known as the model update threshold, to measure when to update the content recognition model.

These model parameters will be described in more detail in the subsequent method flow.

Wherein, the input of the content identification model when performing data flow type identification on the current data flow may include feature information (such as destination IP, destination port, protocol type, etc.), and the behavior identification model when performing data flow type identification on the current data flow The input may include message information (such as message length, message transmission speed, message interval time, message direction, etc.).

The second device obtains the final data flow type based on the confidence obtained by the content recognition model and the confidence obtained by the behavior recognition model based on the confidence weight vector (w1, w2); in this process, if the content is determined by the second preset threshold 82 If the recognition model needs to be updated, the parameters required for updating the content recognition model are acquired.

[0116]

Optionally, the parameters required for updating may be obtained by the second device through training on some data stream related information, or may be obtained by the first device through training on some data stream related information, and then sent to the second device Two equipment.

[0117]

In the embodiment of this application, the second device may be the above-mentioned OSS101, or the above-mentioned server 102, or the above-mentioned forwarding device 103; in addition, the first device may be the above-mentioned OSS101, or the above-mentioned server 102, or is the forwarding device 103 described above.

With reference to the above description, the first device and the second device may be the same device or different devices.

Moreover, when neither the first device nor the second device is the above-mentioned server 102, it can be considered that there is no server 102 in the architecture shown in FIG. 1 .

[0118]

It should be noted that the above content recognition model is essentially a classification model, as shown in Figure 2B, the classification model can be a tree model, as shown in Figure 2C, the classification model can also be a neural network model, as shown in Figure 2D, The classification model can also be a support vector machine (support vector machine, SVM) model, and the

classification model can also be other forms of models.

Optionally, since the above-mentioned content recognition model is classified by extracting features of input vectors (such as characteristic information such as destination internet protocol (internet protocol, IP) address, destination port number, protocol type, etc.), the content recognition model Data flows with the same destination IP address, the same protocol type, and the same port number can be identified as the same data flow type; data flows with the same network segment, the same protocol type, and similar port numbers can be identified as the same data flow type; The transmission control protocol (transmission control protocol, TCP) traffic whose port number is 20 (the well-known port number of the file transfer protocol (file transfer protocol, FTP)) is identified as the data flow type for downloading.

[0119]

In addition, some information about the current data stream that the second device needs to use when identifying the data stream type of the current data stream can be sent to the second device by the terminal 104 or other devices, or collected by the second device itself.

[0120]

Please refer to FIG. 3. FIG. 3 is a method for identifying a data stream type provided by an embodiment of the present invention. The method can be implemented based on the architecture shown in FIG. 1. The method includes but is not limited to the following steps:

[0121]

Step S301: The second device obtains at least one first confidence level corresponding to at least one data flow type of the current data flow according to the packet characteristics and the behavior recognition model of the current data flow.

[0122]

Specifically, the behavior recognition model is a model obtained according to the message characteristics and data flow types of multiple data flow samples; optionally, the multiple data flow samples can be offline samples, that is, the behavior recognition model can be offline The trained model.

The plurality of data stream samples may also be pre-selected typical (or representative) samples. For example, the packets of data streams used in video conferencing usually have a relatively long packet length, but occasionally When the file length is relatively short, the relatively long message length can better reflect that the current data flow is the data flow of the video conference application. Therefore, when selecting the data flow related to the video conference application, try to choose Long such representative as data stream samples.

Optionally, the data flow types of the multiple data flow samples may be determined, that is, manually labeled.

Since the behavior recognition model is a model obtained according to the packet characteristics and data flow types of multiple data flow samples, the behavior recognition model can reflect some relationships between the packet characteristics and data flow types in a data flow. Therefore, when the message characteristics of the current data flow are input to the behavior recognition model, it can predict the tendency (or probability) that the current data flow belongs to a certain or certain data flow types to a certain extent, reflecting the tendency (or probability) of the current data flow. Probability) parameters can also be called confidence.

[0123]

in the embodiment of the present application, the message characteristics may include one or more of message length, message transmission speed, message interval time, and message direction. Optionally, the message length includes message One or more of Ethernet frame length, IP length, transmission protocol length, and header length, where the transmission protocol includes Transmission Control Protocol TCP and/or User Datagram Protocol UDP.

Of course, besides the features exemplified here, the message features can also include other features, for example, the maximum value, minimum value, mean value, variance, quantiles etc.

The packet feature may be input into the behavior recognition model in the form of a vector, for example, in the form of (length of packet, transmission speed of packet, interval time between packets).

in addition, the data stream type in this embodiment of the present application may also be called an application type.

[0124]

In the first possible situation, there may be N data stream types, and N is greater than or equal to 1. The embodiment of the present application can estimate (or predict) the confidence that the current data stream belongs to each of the N data stream types , that is, to obtain N first confidence levels corresponding to N data flow types of the current data flow, for example, if the N data flow types refer to the data flow type of video conference, the data flow of voice conference type, the data flow type of the desktop cloud, then, it is necessary to estimate the first confidence degree of the current data flow belonging to the data flow type of the video conference, the first confidence degree of the data flow type of the voice conference, and the first confidence degree of the data flow type of the desktop cloud through the behavior recognition model. The first confidence level for the stream type.

If the N data stream types refer to the data stream types of the video conference, it is necessary to estimate the first confidence that the current data stream belongs to the data stream type of the video conference through a behavior

recognition model.

[0125]

In the second possible situation, there may be multiple types of data streams, but the embodiment of the present application focuses on one of the data stream types, so the embodiment of the present application only estimates (or predicts) that the current data stream belongs to the focused data stream type Confidence degree, that is, to obtain a first confidence degree corresponding to a data flow type of the current data flow, for example, if the multiple data flow types refer to the data flow type of the video conference, the data flow of the voice conference Stream type, desktop cloud data stream type, but the embodiment of the present application only focuses on the video conference data stream type, so it is only necessary to estimate the first confidence level that the current data stream belongs to the video conference data stream type through the behavior recognition model.

[0126]

Step S202: The second device obtains at least one second confidence level of the current data stream corresponding to the at least one data stream type according to the characteristic information of the current data stream and the content recognition model.

[0127]

Specifically, the content recognition model is a model obtained according to feature information and data flow types of one or more historical data flows.

Optionally, the one or more historical data streams may be online data streams, that is, one or more data streams that have been continuously generated for a period of time before that, and the data stream type of the historical data streams is identified by the above behavior It is obtained by model identification, that is, the content identification model may be a model obtained by online training.

Since the content recognition model is a model obtained according to the characteristic information and data flow types of one or more historical data streams, the content recognition model can reflect some relationship between the characteristic information in a data stream and the data flow type, Therefore, when the characteristic information of the current data flow is input to the content recognition model, it can predict the tendency (or probability) of the current data flow belonging to a certain or certain data flow types to a certain extent, reflecting the tendency (or probability)) parameter can also be called confidence.

[0128]

in the embodiment of the present application, the feature information may include one or more of the destination address, protocol type, and port number, where the destination address may be an IP address, or a destination MAC address, or other forms of The address; of course, the feature information may include other features besides the features exemplified here.

Further, the feature information here may be target-specific information, for example, target IP, target port, and so on.

The feature information may be input into the content recognition model in the form of a vector, which may be in the form of (ip, port, protocol), for example, it may be (10.29.74.5, 8443, 6).

It can also be in the form of (mac, port, protocol), for example, it can be (05FA1525EEFF, 8443, 6).

Of course, it can also be in other forms, and will not give examples one by one here.

[0129]

In the first possible situation, there may be N data stream types, and the embodiment of the present application can estimate (or predict) the confidence that the current data stream belongs to each of the N data stream types, that is, obtain the current N second confidence levels corresponding to N data flow types of the data flow, for example, if the N data flow types refer to the data flow type of the video conference, the data flow type of the voice conference, or the data flow of the desktop cloud flow type, then it is necessary to use the content recognition model to estimate the second confidence degree of the data flow type belonging to the video conference, the second confidence degree of the data flow type belonging to the voice conference, and the second confidence degree of the data flow type belonging to the desktop cloud through the content recognition model. Confidence.

If the N data stream types refer to the data stream types of the video conference, it is necessary to estimate the second confidence degree that the current data stream belongs to the data stream type of the video conference through the content recognition model.

[0130]

In the second possible situation, there may be multiple types of data streams, but the embodiment of the present application focuses on one of the data stream types, so the embodiment of the present application only estimates (or predicts) that the current data stream belongs to the focused data stream type Confidence degree, that is, to obtain a

second confidence degree corresponding to a data flow type of the current data flow, for example, if the multiple data flow types refer to the data flow type of the video conference, the data flow of the voice conference Stream type, desktop cloud data stream type, but the embodiment of the present application only focuses on the video conference data stream type, so it is only necessary to estimate the second confidence level that the current data stream belongs to the video conference data stream type through the content recognition model.

[0131]

Step S303: The second device determines the data stream type of the current data stream according to the at least one first confidence level and the at least one second confidence level.

[0132]

Specifically, because at least one first confidence level can characterize the data type tendency of the current data flow to a certain extent, and at least one second confidence level can also characterize the data flow type tendency of the current data flow to a certain extent, so the two Comprehensive consideration can obtain a more accurate and credible data flow type tendency, so as to obtain the data flow type of the current data flow.

[0133]

In an optional solution, which data flow type has the largest comprehensive confidence, then determine the data flow type as the data flow type of the current data flow, for example, according to the first confidence of the data flow type of the video conference degree and the second confidence degree of the data flow type of the video conference, the comprehensive confidence degree of the data flow type of the video conference is 0.7; according to the first confidence degree of the data flow type of the voice conference and the second The comprehensive confidence degree of the data flow type of the voice conference determined by the second confidence degree is 0.2; the data of the desktop cloud determined according to the first confidence degree of the data flow type of the desktop cloud and the second confidence degree of the data flow type of the desktop cloud The integrated confidence of the stream type is 0.1; since the integrated confidence of the data

stream type of the video conference is the largest, the data stream type of the current data stream is determined as the data stream type of the video conference.

[0134]

in yet another optional solution, the determining the data stream type of the current data stream according to at least one first confidence degree and at least one second confidence degree may specifically be: according to all data stream types corresponding to the first data stream type The first confidence level, the weight value of the first confidence level, the second confidence level corresponding to the first data stream type, and the weight value of the second confidence level are calculated corresponding to the first data The comprehensive confidence of the flow type, the first data flow type is any one of the at least one data flow type, that is to say, each data flow type in the at least one data flow type satisfies the first A characteristic of a data stream type

if the comprehensive confidence corresponding to the first data stream type is greater than a first preset threshold, then determine that the data stream type of the current data stream is the first data stream type, for example, if it corresponds to a video conference If the comprehensive confidence degree of the data stream type is greater than the first preset threshold, it is determined that the data stream type of the current data stream is the data stream type of the video conference; if the comprehensive confidence level corresponding to the data stream type of the desktop cloud If the degree is greater than the first preset threshold, it is determined that the data flow type of the current data flow is the data flow type of the desktop cloud.

[0135]

For example, if the confidence weight vector (w1, w2) is (0.4, 0.6), that is, the first confidence weight (which can also be considered as the weight of the behavior recognition model) is 0.6, and the second confidence weight (which can also be considered as is the weight of the content recognition model) is 0.4, and the first preset threshold 01 of the data flow type is equal to 0.5.

At the beginning of the data flow type identification of the second device, because the content recognition model has not been fully trained, the behavior recognition model can identify the data flow type of the input data flow, but the content recognition model cannot perform data flow identification on the input flow data. The identification of the flow type, so at first the confidence level identified by the content identification model corresponding to any data flow type is 0.

[0136]

If there are two data streams of the desktop cloud, as shown in Figure 4, the horizontal axis represents the serial number of the data stream, and the vertical axis represents the length of the packet. If the packet length is greater than 0, it is an uplink packet, and if the packet length is less than 0, it is a downlink packet; Both data flow a and data flow b are data flow types of the desktop cloud. Among them, data flow b has upstream packets, which is relatively more representative of the characteristics of the desktop cloud scene. Therefore, the packet behavior of data flow b is considered to be typical. the behavior of.

Data flow a has no uplink packets for a long period of time, so it cannot clearly indicate that it is a desktop cloud scenario, so the packet behavior of data flow a is considered to be atypical behavior; the behavior recognition model is usually based on the data flow of typical behavior After training, the behavior recognition model can recognize the data flow type of data flow b, but cannot recognize the data flow type of data flow a.

The feature information of data stream a and data stream b is as follows.

[0137]

The protocol type of data flow a is TCP, the destination IP address is 10.129.74.5, and the destination port number is 8443.

[0138]

The protocol type of data flow b is TCP, the destination IP address is 10.129.56.39, and the destination port

number is 443.

[0139]

Then, for the data stream a, the content recognition model identifies the data stream type of the desktop cloud, the data stream type of the voice conference, and the data stream type of the video conference with a second confidence level of 0.

The behavior recognition model is based on the packet feature recognition. The first confidence level of the data flow type of the desktop cloud is 0.5, the first confidence level of the data flow type of the voice conference is 0, and the data flow type of the video conference is the first confidence level. A confidence level is 0.

Therefore, the comprehensive confidence corresponding to these three data flow types is as follows.

[0140]

Desktop cloud: 0*0.4+0.5*0.6=0.3, less than θ1, so the current data flow is not the data flow type of desktop cloud.

[0141]

Voice conference: 0*0.4+0*0.6=0, less than θ1, so the current data stream is not the data stream type of voice conference.

[0142]

Video conference: 0*0.4+0*0.6=0, less than θ1, so the current data stream is not the data stream type of video conference.

[0143]

Then, for the data flow b, the content recognition model identifies the data flow type of the desktop cloud, the data flow type of the voice conference, and the data flow type of the video conference with a second confidence level of 0.

The behavior recognition model is based on the message

characteristics. The first confidence level of the data flow type of the desktop cloud is 0.9, the first confidence level of the data flow type of the voice conference is 0, and the data flow type of the video conference is the first confidence level. A confidence level is 0.

Therefore, the comprehensive confidence corresponding to these three data flow types is as follows.

[0144]

Desktop cloud: 0*0.4+0.9*0.6=0.54, greater than θ1, so the current data flow is the data flow type of desktop cloud.

[0145]

Voice conference: 0*0.4+0*0.6=0, less than θ1, so the current data stream is not the data stream type of voice conference.

[0146]

Video conference: 0*0.4+0*0.6=0, less than θ1, so the current data stream is not the data stream type of video conference.

[0147]

In the embodiment of the present application, the content recognition model can also be updated, and two different update solutions are provided below.

[0148]

Solution 1, if the comprehensive confidence corresponding to the first data stream type is greater than a first preset threshold and less than a second preset threshold θ2, then the second device sends the characteristics of the current data stream to the first device information and the information of the first data stream type, the second preset threshold is greater than the first preset threshold.

For example, for data flow a, the comprehensive confidence level of 0.3 corresponding to the data flow type of the desktop cloud is not in the interval (θ1, θ2), so there is no need to send the feature information of the current data flow and the desktop cloud information to the first device. Information about the type of data stream; for another example, for data stream b, the comprehensive confidence of 0.54 corresponding to the data stream type of the desktop cloud is not in the interval (θ1, θ2), so the current data stream needs to be sent to the first device The characteristic information (such as destination IP address 10.129.56.39, destination port number 443, protocol type TCP type) and the information of the data flow type of the desktop cloud (such as name, identification and other information).

[0149]

Correspondingly, the first device receives the feature information of the current data stream and the information of the first data stream type sent by the second device, that is, there is one more data stream record on the first device, as shown in Figure 5, more A record for stream b is created.

Then, the first device obtains the first information according to the feature information of the current data stream and the information of the first data stream type, for example, some parameters that affect the calculation confidence.

Optionally, the first information belongs to the model file, so it can be transmitted as a model file. The ai model file of the common open source keras

library is an h5 file/json file; the ai model file of the open source sklearn library is a pkl/m file.

These files are binary and are used to save the structure of the model and the weight of the model.

[0150]

Next, the second device receives the first information sent by the first device, and then updates the content recognition model according to the first information to obtain a new content recognition model.

In the record of data flow b, the destination IP address is 10.129.56.39, the destination port number is 443, and the protocol type is TCP, which together correspond to the data flow type of the desktop cloud. When flow b is estimated, the estimated second confidence level corresponding to the data flow type of the desktop cloud is 1.

Optionally, since the characteristic information of data flow a is similar to that of data flow b, for example, the destination IP address is in the same network segment, the port number is similar, and the protocol type is similar, therefore, the updated content recognition model can be When estimating the input data flow a, the estimation result will be closer to the estimation result of the data flow b, for example, the estimated second confidence level corresponding to the data flow type of the desktop cloud may be 0.8.

[0151]

When data flow a and data flow b appear in the subsequent network and need to estimate the data flow type, the execution process is as follows.

[0152]

The confidence weight vector (w1, w2), the first preset threshold θ1, and the second preset threshold θ2 remain unchanged.

[0153]

Then, for data stream a, the second confidence level for the content recognition model to identify the data stream type of desktop cloud is 0.6, and the second confidence level for identifying the data stream type of voice conference and video conference is both 0.

The behavior recognition model is based on the packet feature recognition. The first confidence level of the data flow type of the desktop cloud is 0.5, the first confidence level of the data flow type of the voice conference is 0, and the data flow type of the video conference is the first confidence level. A confidence level is 0.

Therefore, the comprehensive confidence corresponding to these three data flow types is as follows.

[0154]

Desktop cloud: 0.6*0.4+0.5*0.6=0.54, greater than θ1, so the current data flow is the data flow type of desktop cloud.

[0155]

Voice conference: 0*0.4+0*0.6=0, less than θ1, so the current data stream is not the data stream type of voice conference.

[0156]

Video conference: 0*0.4+0*0.6=0, less than θ1, so the current data stream is not the data stream type of video conference.

[0157]

Since the second confidence level of 0.54 for identifying the data flow type of the desktop cloud is within the interval (θ1, θ2), it is necessary to send the characteristic information of the current data flow and the information of the data flow type of the desktop cloud to the first device, so as to it is used to update the content recognition model in the future (the update principle has been introduced earlier,

and will not be repeated here).

[0158]

Then, for data flow b, the second confidence level of the content recognition model for identifying the data flow type of the desktop cloud type is 1, and the second confidence level for identifying the data flow type of the voice conference and the data flow type of the video conference is equal to 1. is 0.

The behavior recognition model is based on the message characteristics. The first confidence level of the data flow type of the desktop cloud is 0.9, the first confidence level of the data flow type of the voice conference is 0, and the data flow type of the video conference is the first confidence level. A confidence level is 0.

Therefore, the comprehensive confidence corresponding to these three data flow types is as follows.

[0159]

Desktop cloud: 1*0.4+0.9*0.6=0.94, greater than θ1, so the current data flow is the data flow type of desktop cloud

[0160]

Voice conference: 0*0.4+0*0.6=0, less than θ1, so the current data stream is not the data stream type of voice conference.

[0161]

Video conference: 0*0.4+0*0.6=0, less than θ1, so the current data stream is not the data stream type of video conference.

[0162]

Since the second confidence level 0.94 for identifying the data flow type of the desktop cloud is not in the interval (01, 02), there is no need to send the characteristic information of the current data flow and the information of the data flow type of the desktop cloud to the first device.

[0163]

There are cloud-based elastic deployment scenarios in the network. For example,

the destination IP address is 10.128.56.39, the destination port number is 443, and the cloud resource whose protocol type is TCP changes from providing services for desktop clouds to providing services for video conferencing.

For this scenario, the first information obtained by the first device based on the feature information of the current data stream and the information

of
the
first
data
stream
type
rnay
include:
if
the
feature
information
of
the
first
record
among
the
multiple
records
is
the
same
as
the
The
feature
information
of
the
current
data
stream
is
the
same
but
the
data
stream
type
of
the
first
record
is
different
from
the
first
data
stream
type,
then
update
the
data
stream

type of the first record to the first data stream type, to obtain a second record; each of the multiple records includes feature information and a data flow type; and then trains the multiple records including the second record to obtain the first information.

[0164]

For example, the protocol type of data stream c is TCP,

the destination IP address is 10.128.56.39, and the destination port number is 443.

[0166]

Then, for data flow c, the second confidence degree of the content recognition model for identifying the data flow type of the desktop cloud data flow type is 1, and the second confidence degree for identifying the data flow type of the

voice conference and the video conference data flow type is equal to 1. is 0.

The behavior recognition model is based on packet features. The first confidence level of the data flow type of the desktop cloud is 0, the first confidence level of the data flow type of the voice conference is 0, and the first confidence

level of the data flow type of the video conference is identified. The confidence level is 0.9.

Therefore, the comprehensive confidence corresponding to these three data flow types is as follows.

[0166]

Desktop cloud: 1*0.4+0*0.6=0.4, which is less than θ1, so the current data flow is not the data flow type of desktop cloud.

[0167]

Voice conference: 0*0.4+0*0.6=0, less than 01, so the current data stream is not the data stream type of voice conference.

[0168]

Video conference: 0*0.4+0.9*0.6=0.54, greater than 01, so the current data stream is the data stream type of video conference.

[0169]

Since the second confidence level 0.54 for identifying the data stream type

of the video conference is within the interval (θ1, θ2), it is necessary to send the characteristic information of the current data stream and the information of the data stream type of the desktop cloud to the first device.

Correspondingly, the first device receives the feature information of the current data flow and the information of the first

data flow type sent by the second device, that is, there is a data flow record on the first device, as shown in Figure 6, multiple Created a record for data stream c.

[0170]

Comparing Figure 6 and Figure 5, it can be found that compared with the records for data flow c and data flow

b,
the
data
flow
type
(i.e.
application
category)
is
different
but
the
characteristic
information
(such
as
destination
IP
address,
destination
port
number
and
protocol
type
)
are
the
same,
so
modify
the
existing
records
so
that
the
data
flow
type
corresponding
to
the
protocol
type
TCP,
destination
IP
address
10.129.56.39,
and
destination
port
number
443
is
the
data

flow
type
of
the
video
conference,
not
the
data
flow
corresponding
to
the
desktop
cloud
Type,
the
record
before
modification
is
the
first
record,
and
the
record
after
modification
is
the
second
record.

[0171]

It
can
be
understood
that
after
the
first
record
is
updated
to
the
second
record,
and
the
content
recognition
model
is
updated

based on the first information obtained through the training of the second record, when the above data stream c is input to the updated content recognition model again, it is recognized as a desktop The second confidence degree of the cloud data flow type is 0, and the second confidence degree of identifying it as a video conference

data
flow
type
is
1.

[0172]

Solution
2,
if
the
comprehensive
confidence
corresponding
to
the
first
data
stream
type
is
less
than
a
second
preset
threshold,
the
second
device
does
not
need
to
send
the
characteristic
information
of
the
current
data
stream
and
the
information
of
the
first
data
stream
type
to
the
second
device.
A

device updates the content identification model by itself according to the feature information of the current data stream and the first data stream type information to obtain a new content identification model, and the second preset threshold is greater than the specified the first preset threshold.

Optionally, if the feature information of the first record among the multiple

records is the same as the feature information of the current data stream but the data stream type of the first record is different from the first data stream type, the second device updating the data stream type of the first record to the first data stream type to obtain a second record; each record in the plurality

of records includes characteristic information and a data stream type; Record multiple records for training to get a new content recognition model.

For ease of understanding, reference may be made to the above-mentioned solution 1 for specific principles, and the second device may replace the operations performed by the first device in the above-mentioned solution.

[0173]

Step S304: the second device sends information about the data flow type of the current data flow to the operation and maintenance support system OSS.

[0174]

Specifically, the second device may send information about the data flow type of the current data flow to the OSS each time the data flow type of the

current
data
flow
is
determined,
for
example,
when
the
data
flow
type
of
the
data
flow
a
is
generated
for
the
first
time,
send
The
OSS
sends
the
information
of
the
data
flow
type
of
data
flow
a,
when
generating
the
data
flow
type
of
data
flow
b
for
the
first
time,
sends
the
information
of
the
data

flow
type
of
data
flow
b
to
OSS,
and
generates
the
data
flow
type
of
data
flow
a
for
the
second
time
,
send
the
information
of
the
data
flow
type
of
data
flow
a
to
OSS,
when
generating
the
data
flow
type
of
data
flow
b
for
the
second
time,
send
the
information
of
data
flow
type

of
data
flow
b
to
OSS;
when
generating
the
data
flow
type
of
data
flow
c,
Send
the
information
of
the
data
flow
type
of
the
data
flow
c
to
the
OSS.

It
can
be
understood
that,
if
the
second
device
is
the
OSS,
the
above
step
S304
does
not
need
to
be
performed.

[0175]

Step

S305: The OSS generates a flow control policy for the current data flow according to the data flow type information of the current data flow.

For example, if the data flow type information of the current data flow indicates that the current data flow is a data flow type of a video desktop cloud, or a data flow

type of a video conference, the current data flow is defined as a high-priority QoS.

[0176]

Step S306: the OSS sends the traffic control policy to the forwarding device or the terminal.

[0177]

Specifically, the forwarding device 103 may be a device such as a router or a switch, and the terminal 104

is a device that outputs the above-mentioned current data flow.

if the forwarding device or terminal knows that the current data flow belongs to the high-priority QoS according to the flow control policy, when it finds that there are multiple data flows to be sent, it will send the current data flow configured as the high

priority first.

[0178] In the method described in Figure 3, a behavior recognition model and a content recognition model are involved. The behavior recognition model is obtained by pre-training the message characteristics and data flow types of multiple data flow samples, and the content recognition model is based on the characteristics of the data flow.

The information and the data flow type identified by the behavior model are trained, so the content recognition model is an online learning model; the behavior recognition model can recognize some basic (or typical) data flow types of data flow, and the same type of data flow Some characteristics (such as packet length, packet transmission speed, etc.) may

change during the subsequent transmission process, so combined with the online learning characteristics of the content recognition model from other aspects (such as destination address, protocol type, etc.) Type identification can offset the identification error of the data flow type of the data flow by the behavior identification model in the process of data flow transmission. The recognition

accuracy of the type also improves the generalization of the recognition, and can be applied to various scenarios such as application cloud deployment, application transmission encryption, and private applications.

[0178]

The method of the embodiment of the present invention has been described in detail above, and the device of the embodiment of the present invention is

provided below.

[0180]

Please refer to FIG. 7. FIG. 7 is a schematic structural diagram of a data flow type identification device 70 provided by an embodiment of the present invention. The device 70 may be the second device in the method embodiment shown in FIG. 3, and the device 70 may include the first An

identification unit 701. a second identification unit 702 and a determination unit 703. wherein the detailed description of each unit is as follows.

[0181]

The first identification unit 701 is configured to obtain at least one first confidence degree corresponding to at least one data flow type of the current data flow according to

the packet characteristics and the behavior recognition model of the current data flow, wherein the behavior recognition model is A model obtained according to packet characteristics and data flow types of multiple data flow samples; the packet characteristics include one or more of packet length, packet transmission speed, packet interval time, and packet direction;

[0182]

The

second identification unit 702 is configured to obtain at least one second confidence degree of the current data stream corresponding to the at least one data stream type according to the characteristic information of the current data stream and a content recognition model, wherein the feature The information includes destination address and protocol type, and the content recognition

model
is
a
model
obtained
according
to
the
characteristic
information
and
data
flow
type
of
one
or
more
historical
data
flows,
and
the
data
flow
type
of
the
historical
data
flow
is
obtained
according
to
the
behavior
recognition
model
of;

[0183]

A
determining
unit
703,
configured
to
determine
a
data
stream
type
of
the
current
data

stream according to the at least one first confidence level and the at least one second confidence level.

[0184]

Among the above-mentioned devices, a behavior recognition model and a content recognition model are involved. The behavior recognition model is pre-trained by the message characteristics and data flow types of multiple data flow samples, and

the
content
recognition
model
is
based
on
the
characteristic
information
of
the
data
flow
and
the
behavior
model
The
identified
data
flow
type
is
trained,
so
the
content
recognition
model
is
an
online
learning
model;
the
behavior
recognition
model
can
recognize
some
basic
(or
typical)
data
flow
types
of
data
flow,
and
certain
characteristics
of
the
same
type

of
data
flow
(such
as
message
length,
message
transmission
speed,
etc.)
may
change
during
the
subsequent
transmission
process,
so
the
type
of
the
data
flow
can
be
identified
from
other
aspects
(such
as
destination
address,
protocol
type,
etc.)
in
combination
with
the
online
learning
characteristics
of
the
content
recognition
model.
The
hedging
behavior
recognition
model
recognizes
the
data

flow
type
of
the
data
flow
in
the
process
of
data
flow
transmission
Therefore,
this
application
adopts
the
recognition
method
of
combining
the
behavior
recognition
model
and
the
content
recognition
model
to
improve
the
recognition
accuracy
of
the
data
flow
type
of
the
data
flow
,
which
also
improves
the
generalization
of
identification,
and
can
be
applied
to

various scenarios such as application cloud deployment, application transmission encryption, and private applications.

[0185]

In a possible implementation manner, the determining unit 703 is configured to determine the data flow type of the current data flow according to the at least one first confidence level and the at least one second confidence level, specifically:

[0186]

used
for
according
to
the
first
confidence
level
corresponding
to
the
first
data
flow
type,
the
weight
value
of
the
first
confidence
level,
the
second
confidence
level
corresponding
to
the
first
data
flow
type,
and
the
second
confidence
level
The
weight
value
of
the
degree
calculates
the
comprehensive
confidence
degree
corresponding
to
the
first
data
flow
type,
and

the
first
data
flow
type
is
any
one
of
the
at
least
one
data
flow
type;

[0187]

if
the
comprehensive
confidence
degree
corresponding
to
the
first
data
flow
type
is
greater
than
a
first
preset
threshold,
determine
that
the
data
flow
type
of
the
current
data
flow
is
the
first
data
flow
type.

[0188]

in the above equipment, according to the degree of influence of the content recognition model and the behavior recognition model on the final recognition result respectively, the weights of the confidence degrees are respectively configured for the two models (the weight configured for the behavior recognition model is the weight of the first confidence degree, which is The

weight
configured
by
the
content
recognition
model
is
the
weight
of
the
second
confidence
degree),
so
the
comprehensive
confidence
calculated
based
on
the
weights
of
the
two
confidence
degrees
can
better
reflect
the
actual
type
of
the
current
data
flow.

in
addition,
introducing
a
first
preset
threshold
to
measure
whether
the
corresponding
data
flow
type
is
desirable
can

improve the efficiency and accuracy of determining the data flow type.

[0189]

In yet another possible implementation manner, the device 70 further includes.

[0190]

The first sending unit is configured to, when the comprehensive confidence corresponding to the first data stream type is less than a second preset threshold, send to other devices (the

first device in the method embodiment shown in FIG.) sending the characteristic information of the current data flow and the information of the first data flow type, the second preset threshold is greater than the first preset threshold;

[0191]

The receiving unit is configured to receive the first information sent by the other device (the

first device in the method embodiment shown in Figure 3), the first information is the other device (the method embodiment shown in Figure 3 The first device in) obtains it according to the feature information of the current data stream and the identification information of the first data stream type;

[0192]

An updating unit, configured

to update the content recognition model according to the first information to obtain a new content recognition model.

[0193]

In yet another possible implementation, the device 70 also includes:

[0194]

An updating unit, configured to update according to the characteristic information of the current data stream and the information of the first data stream

type when the comprehensive confidence corresponding to the first data stream type is less than a second preset threshold The content recognition model is used to obtain a new content recognition model, and the second preset threshold is greater than the first preset threshold.

[0195]

In the above method, the inventor of the present application uses

the identification result of the data stream type of the current data stream to correct the content recognition model.

Specifically, a second preset threshold is introduced, and when the comprehensive confidence corresponding to the first data stream type is less than the second preset threshold, relevant information about the current data stream is sent to the device for

training,
so
as
to
use
To
obtain
a
new
content
recognition
model
to
make
the
next
identification
result
more
accurate.

[0198]

In
yet
another
possible
implementation
manner,
the
updating
of
the
content
recognition
model
according
to
the
characteristic
information
of
the
current
data
stream
and
the
type
information
of
the
first
data
stream
to
obtain
a

new content recognition model is specifically:

[0197]

if the feature information of the first record among the multiple records is the same as the feature information of the current data stream but the data stream type of the first record is different from the first data stream type, then the updating the data stream type to

the first data stream type to obtain a second record; each of the multiple records includes feature information and a data stream type;

[0198]

and performing training on a plurality of records including the second record to obtain a new content recognition model.

[0199]

That is to say, if the feature information of the

historical data flow is the same as that of the current data flow but the data flow type is different in the identified record, update the data flow type in the record to the current data flow This is mainly to adapt to the flexible deployment of cloud resources. For example, the same cloud resource is used for

video conferencing in the previous period, and is used for desktop cloud in the next period. The data flow type is updated to desktop cloud, so that the data flow type of the current data flow can still be accurately identified in the case of elastic deployment of cloud resources.

[0200]

In yet another possible implementation

manner, the device 70 further includes:

[0201]

The second sending unit is configured to, after the determining unit determines the data flow type of the current data flow according to the at least one first confidence degree and the at least one second confidence degree, send the information to the operation and maintenance support system OSS

information about the data flow type of the current data flow, and the information about the data flow type of the current data flow is used by the OSS to generate a flow control policy for the current data flow.

[0202]

That is to say, after the data flow type of the current data flow is

determined,
the
relevant
information
of
the
current
data
flow
type
is
notified
to
the
OSS
system,
so
that
the
OSS
system
can
generate
an
Stream
flow
control
policy,
for
example,
when
the
first
data
stream
type
of
the
current
data
stream
is
video
stream
of
video
conference,
define
its
corresponding
flow
control
policy
as
the
priority
transmission
policy,

that
is,
when
there
are
multiple
data
streams
to
be
transmitted,
the
priority
Transmit
the
current
data
stream

[0203]

In
yet
another
possible
implementation,
the
message
length
includes
one
or
more
of
the
Ethernet
frame
length,
IP
length,
transmission
protocol
length,
and
header
length
in
the
message,
and
the
transmission
protocol
includes
Transmission
Control
Protocol
TCP

and
/or
User
Datagram
Protocol
UDP.

[0204]

It
should
be
noted
that
the
implementation
of
each
unit
may
also
refer
to
the
corresponding
description
of
the
method
embodiment
shown
in
FIG.
3

[0205]

Please
refer
to
FIG.
8.
FIG.
8
is
a
schematic
structural
diagram
of
a
data
stream
type
identification
device
80

provided by an embodiment of the present invention. The device 80 may be the first device in the method embodiment shown in FIG. 3, and the device 80 may include receiving A unit 801, a generating unit 802, and a sending unit 803, wherein the detailed description of each unit is as follows.

[0206]

The receiving

unit
801
is
configured
to
receive
characteristic
information
of
the
current
data
stream
and
information
of
the
data
stream
type
sent
by
other
devices
(the
second
device
in
the
method
embodiment
shown
in
FIG.
3
);

[0297]

A
generating
unit
802,
configured
to
generate
first
information
according
to
the
characteristic
information
of
the
current
data
flow

and
the
information
of
the
data
flow
type;

[0208]

The
sending
unit
803
is
configured
to
send
the
first
information
to
the
other
device
(the
second
device
in
the
method
embodiment
shown
in
FIG.
3
),
so
as
to
update
the
content
recognition
model,
and
the
content
recognition
model
is
used
to
obtain
the
corresponding
AI

least one second degree of confidence in at least one data stream type, wherein the content recognition model is a model obtained from the feature information and data stream types of one or more historical data streams, and the data stream type of the historical data streams it is obtained according to the behavior recognition model, which is

a model obtained according to the packet characteristics and data flow types of multiple data flow samples, and the packet characteristics include packet length, packet transmission speed, and packet interval One or more of time and message direction.

[0208]

In the above-mentioned device 80, a behavior recognition model and a content recognition model are involved.

The behavior recognition model is pre-trained by packet characteristics and data flow types of multiple data flow samples, and the content recognition model is based on the characteristic information of the data flow and the behavior The data flow type identified by the model is trained, so the content recognition model is an online learning model; the

behavior
recognition
model
can
recognize
some
basic
(or
typical)
data
flow
types
of
data
flow,
and
certain
characteristics
of
the
same
type
of
data
flow
(
For
example,
the
length
of
the
message,
the
speed
of
message
transmission,
etc.)
may
change
during
the
subsequent
transmission
process,
so
the
type
of
the
data
flow
is
identified
from
other
aspects

(such as destination address, protocol type, etc.) in combination with the online learning characteristics of the content recognition model, it can hedge the recognition error of the data flow type of the data flow by the behavior recognition model in the process of data flow transmission Therefore, this application adopts the recognition method of combining the behavior recognition

model
and
the
content
recognition
model
to
improve
the
recognition
accuracy
of
the
data
flow
type
of
the
data
flow
it
also
improves
the
generalization
of
identification,
and
can
be
applied
to
various
scenarios
such
as
application
cloud
deployment,
application
transmission
encryption,
and
private
applications.

[0210]

It
should
be
noted
that
the
implementation
of
each
unit

may
also
refer
to
the
corresponding
description
of
the
method
embodiment
shown
in
FIG.
3
.

[0211]

Please
refer
to
FIG.
9.
FIG.
9
is
a
device
90
provided
by
an
embodiment
of
the
present
invention.
The
device
90
may
be
the
second
device
in
the
method
embodiment
shown
in
FIG.
3,
and
the
device
90

includes a processor 901, a memory 902 and a transceiver 903. The processor 901, the memory 902, and the transceiver 903 are connected to each other through a bus.

[0212]

Memory 902 includes, but is not limited to, random access memory (random access memory. RAM), read-only memory (read-only memory. ROM), erasable programmable read-only

memory (erasable programmable read only memory. EPROM), or Portable read-only memory (compact disc read-only memory. CD-ROM), the memory 902 is used for related computer programs and data.

The transceiver 903 is used to receive and transmit data.

[0213]

The processor 901 may be one or more central processing units (central processing unit, CPU).

in the case where the processor 901 is a CPU, the CPU may be a single-core CPU or a multi-core CPU.

[0214]

The processor 901 reads the computer program code stored in the memory 902 to perform the following operations:

[0215]

Obtain at least one first confidence degree corresponding to at least

one
data
flow
type
of
the
current
data
flow
according
to
the
packet
characteristics
and
behavior
recognition
model
of
the
current
data
flow,
wherein
the
behavior
recognition
model
is
a
report
based
on
a
plurality
of
data
flow
samples
The
model
obtained
by
the
text
feature
and
the
data
flow
type;
the
message
feature
includes
one
or
more

of message length, message transmission speed, message interval time and message direction.

[0216]

Obtaining at least one second confidence degree of the current data flow corresponding to the at least one data flow type according to the feature information and the content identification model of the current data flow, wherein the feature information includes a destination

address and a protocol type, The content recognition model is a model obtained according to characteristic information and data flow types of one or more historical data flows, and the data flow type of the historical data flows is obtained according to the behavior recognition model;

[0217]

Determine the data flow type of the current data

flow according to the at least one first confidence level and the at least one second confidence level.

[0218]

The above operations involve a behavior recognition model and a content recognition model. The behavior recognition model is pre-trained from the message characteristics and data flow types of multiple data flow samples, while the content recognition

model
is
based
on
the
characteristic
information
of
the
data
flow
and
the
behavior
model
The
identified
data
flow
type
is
trained,
so
the
content
recognition
model
is
an
online
learning
model;
the
behavior
recognition
model
can
recognize
some
basic
(or
typical)
data
flow
types
of
data
flow,
and
certain
characteristics
of
the
same
type
of
data
flow

(such as message length, message transmission speed, etc.) may change during the subsequent transmission process, so the type of the data flow can be identified from other aspects (such as destination address, protocol type, etc.) in combination with the online learning characteristics of the content recognition model. The hedging behavior recognition model recognizes the data flow type of

the
data
flow
in
the
process
of
data
flow
transmission.
Therefore,
this
application
adopts
the
recognition
method
of
combining
the
behavior
recognition
model
and
the
content
recognition
model
to
improve
the
recognition
accuracy
of
the
data
flow
type
of
the
data
flow
,
which
also
improves
the
generalization
of
identification,
and
can
be
applied
to
various
scenarios
such

as
application
cloud
deployment,
application
transmission
encryption,
and
private
applications.

[0219]

In
a
possible
implementation
manner,
the
determining
the
data
stream
type
of
the
current
data
stream
according
to
the
at
least
one
first
confidence
degree
and
the
at
least
one
second
confidence
degree
is
specifically:

[0220]

According
to
the
first
confidence
degree
corresponding

to
the
first
data
stream
type,
the
weight
value
of
the
first
confidence
degree,
the
second
confidence
degree
corresponding
to
the
first
data
stream
type,
and
the
weight
value
of
the
second
confidence
degree
The
weight
value
calculates
the
comprehensive
confidence
corresponding
to
the
first
data
flow
type,
and
the
first
data
flow
type
is
any
one
of

the
at
least
one
data
flow
type;

[0221]

if
the
comprehensive
confidence
degree
corresponding
to
the
first
data
flow
type
is
greater
than
a
first
preset
threshold,
determine
that
the
data
flow
type
of
the
current
data
flow
is
the
first
data
flow
type.

[0222]

in
the
above
operation,
according
to
the
degree
of

influence of the content recognition model and the behavior recognition model on the final recognition result, the weights of the confidence degrees are respectively configured for the two models (the weight configured for the behavior recognition model is the weight of the first confidence degree, which is The weight configured by the content recognition model is the weight

of
the
second
confidence
degree),
so
the
comprehensive
confidence
calculated
based
on
the
weights
of
the
two
confidence
degrees
can
better
reflect
the
actual
type
of
the
current
data
flow.

In
addition,
introducing
a
first
preset
threshold
to
rmeasure
whether
the
corresponding
data
flow
type
is
desirable
can
improve
the
efficiency
and
accuracy
of
determining
the
data
flow

type.

[0223]

in a possible implementation manner, the processor is further configured to:

[0224]

if the comprehensive confidence corresponding to the first data stream type is less than a second preset threshold, send the The characteristic information of the current data stream and the information of the first data stream type, the second preset

threshold
is
greater
than
the
first
preset
threshold;

[0225]

Receive
the
first
information
sent
by
the
other
device
(the
first
device
in
the
method
embodiment
as
shown
in
Figure
3
)
through
the
transceiver,
and
the
first
information
is
the
other
device
(the
first
device
in
the
method
embodiment
as
shown
in
Figure
3
)
The

first
device
in
)
obtains
it
according
to
the
feature
information
of
the
current
data
stream
and
the
identification
information
of
the
first
data
stream
type;

[0226]

Updating
the
content
recognition
model
according
to
the
first
information
to
obtain
a
new
content
recognition
model.

[0227]

In
yet
another
possible
implementation
manner,
the
processor
is

further configured to:

[0228]

If the comprehensive confidence corresponding to the first data stream type is less than a second preset threshold, then update the content recognition model according to the feature information of the current data stream and the first data stream type information, so as to A new content recognition model is obtained, and

the second preset threshold is greater than the first preset threshold.

[0328]

In the above method, the inventor of the present application uses the identification result of the data stream type of the current data stream to correct the content recognition model.

Specifically, a second preset threshold is introduced, and when the comprehensive confidence corresponding to

the
first
data
stream
type
is
less
than
the
second
preset
threshold,
relevant
information
about
the
current
data
stream
is
sent
to
the
device
for
training,
so
as
to
use
To
obtain
a
new
content
recognition
model
to
make
the
next
identification
result
more
accurate.

[0230]

In
yet
another
possible
implementation
manner,
the
updating
of
the

content recognition model according to the characteristic information of the current data stream and the type information of the first data stream to obtain a new content recognition model is specifically:

[0231]

if the feature information of the first record among the multiple records is the same as the feature information of the current data stream

but
the
data
stream
type
of
the
first
record
is
different
from
the
first
data
stream
type,
then
the
updating
the
data
stream
type
to
the
first
data
stream
type
to
obtain
a
second
record;
each
of
the
multiple
records
includes
feature
information
and
a
data
stream
type;

[0232]

and
performing
training
on
a
plurality
of

records including the second record to obtain a new content recognition model.

[0233]

That is to say, if the feature information of the historical data flow is the same as that of the current data flow but the data flow type is different in the identified record, update the data flow type in the record to

the current data flow This is mainly to adapt to the flexible deployment of cloud resources. For example, the same cloud resource is used for video conferencing in the previous period, and is used for desktop cloud in the next period; The data flow type is updated to desktop cloud, so that the data flow type of the

current
data
flow
can
still
be
accurately
identified
in
the
case
of
elastic
deployment
of
cloud
resources

[0234]

In
yet
another
possible
implementation
manner,
the
processor
is
further
configured
to,
after
determining
the
data
stream
type
of
the
current
data
stream
according
to
the
at
least
one
first
confidence
level
and
the
at
least
one
second

confidence
level
.
sending
information
about
the
data
flow
type
of
the
current
data
flow
to
an
operation
and
maintenance
support
system
OSS
through
the
transceiver,
where
the
information
about
the
data
flow
type
of
the
current
data
flow
is
used
by
the
OSS
to
generate
traffic
control
strategy.

[0238]

That
is
to
say,
after
the

data flow type of the current data flow is determined, the relevant information of the current data flow type is notified to the OSS system, so that the OSS system can generate an Stream flow control policy, for example, when the first data stream type of the current data stream is video stream of video conference, define its

corresponding flow control policy as the priority transmission policy, that is, when there are multiple data streams to be transmitted, the priority Transmit the current data stream.

[0238]

In yet another possible implementation, the message length includes one or more of the Ethernet frame length, IP length, transmission protocol length, and header length in the message,

and
the
transmission
protocol
includes
Transmission
Control
Protocol
TCP
and
/or
User
Datagram
Protocol
UDP.

[0237]

It
should
be
noted
that
the
implementation
of
each
operation
may
also
refer
to
the
corresponding
description
of
the
method
embodiment
shown
in
FIG.
3
.

[0238]

Please
refer
to
FIG.
10.
FIG.
10
is
a
device
100

provided by an embodiment of the present invention. The device 100 may be the first device in the method embodiment shown in FIG. 3, and the device 100 includes a processor 1001, a memory 1002 and a transceiver 1003. The processor 1001, the memory 1002, and the transceiver 1003 are connected to each other through a bus.

[0238]

Memory 1002 includes, but is not limited to, random access memory (random access memory, RAM), read-only memory (read-only memory, ROM), erasable programmable read-only memory (erasable programmable read only memory, EPROM), or Portable read-only memory (compact disc read-only memory, CD-ROM), the memory 1002 is used for related computer programs and data.

The transceiver 1003 is used to receive and transmit data.

[0240]

The processor 1001 may be one or more central processing units (central processing unit, CPU) in the case where the processor 1001 is a CPU, the CPU may be a single-core CPU or a multi-core CPU.

[0241]

The processor 1001 reads

the computer program code stored in the memory 1002 to perform the following operations:

[0242]

Receive, through the transceiver, the characteristic information of the current data stream and the information of the data stream type sent by other devices (the second device in the method embodiment shown in FIG. 3);

[0243]

generating first

information according to the characteristic information of the current data flow and the information of the data flow type;

[0244]

Send the first information to the other device (the second device in the method embodiment shown in FIG. 3) through the transceiver, so as to update the content recognition model, and the content recognition model

is
used
to
obtain
the
corresponding
At
least
one
second
degree
of
confidence
of
at
least
one
data
flow
type,
wherein
the
content
recognition
model
is
a
model
obtained
according
to
characteristic
information
and
data
flow
types
of
one
or
more
historical
data
flows,
and
the
data
flow
type
of
the
historical
data
flow
is
Obtained
according
to

the behavior recognition model, the behavior recognition model is a model obtained according to the packet characteristics and data flow types of multiple data flow samples, and the packet characteristics include packet length, packet transmission speed, and packet interval time One or more of message direction.

[0245]

The above operations involve a behavior recognition model and

a
content
recognition
model.
The
behavior
recognition
model
is
pre-
trained
from
the
message
characteristics
and
data
flow
types
of
multiple
data
flow
samples,
while
the
content
recognition
model
is
based
on
the
characteristic
information
of
the
data
flow
and
the
behavior
model
The
identified
data
flow
type
is
trained,
so
the
content
recognition
model
is
an
online

learning model; the behavior recognition model can recognize some basic (or typical) data flow types of data flow, and certain characteristics of the same type of data flow (such as message length, message transmission speed, etc.) may change during the subsequent transmission process, so the type of the data flow can be identified from other aspects (such as

destination address, protocol type, etc.) in combination with the online learning characteristics of the content recognition model. The hedging behavior recognition model recognizes the data flow type of the data flow in the process of data flow transmission. Therefore, this application adopts the recognition method of combining the behavior recognition model and the content recognition model to improve

the
recognition
accuracy
of
the
data
flow
type
of
the
data
flow
,
which
also
improves
the
generalization
of
identification,
and
can
be
applied
to
various
scenarios
such
as
application
cloud
deployment,
application
transmission
encryption,
and
private
applications.

[0248]

It
should
be
noted
that
the
implementation
of
each
operation
may
also
refer
to
the
corresponding
description

of
the
method
embodiment
shown
in
FIG.
3
.

[0247]

It
should
be
noted
that
any
device
embodiment
described
above
is
only
illustrative,
and
the
units
described
as
separate
components
may
or
may
not
be
physically
separated,
and
the
components
shown
as
units
may
or
may
not
be
A
physical
unit
can
be
located
in
one

place, or it can be distributed to multiple network units.

Part or all of the modules can be selected according to actual needs to achieve the purpose of the solution of this embodiment.

In addition, in the drawings of the embodiments of network devices or hosts provided by the present invention, the connection relationship between modules indicates

that they have communication connections, which can be specifically implemented as one or more communication buses or signal lines.

It can be understood and implemented by those skilled in the art without creative effort.

[0248]

The embodiment of the present invention also provides a chip system, the chip system includes at least one processor, a memory

and an interface circuit, the memory, the transceiver and the at least one processor are interconnected through lines, and the at least one memory A computer program is stored in the computer; when the computer program is executed by the processor, the method flow shown in FIG. 3 is realized.

[0249]

An embodiment of the present

invention also provides a computer-readable storage medium, where a computer program is stored in the computer-readable storage medium, and when the computer program is run on a processor, the method flow shown in FIG. 3 is implemented.

[0250]

An embodiment of the present invention also provides a computer program product, and when the computer

program product is run on a processor, the flow of the method shown in FIG. 3 is realized.

[0251]

In summary, this application involves a behavior recognition model and a content recognition model. The behavior recognition model is pre-trained from the message characteristics and data flow types of multiple data flow samples, and the content

recognition model is based on the characteristic information and data flow characteristics of the data flow. it is trained by the data flow type identified by the behavior model, so the content recognition model is an online learning model; the behavior recognition model can recognize some basic (or typical) data flow types of data flow, and some of

the same type of data flow Features (such as packet length, packet transmission speed, etc.) may change during the subsequent transmission process, so the type of data flow is analyzed from other aspects (such as destination address, protocol type, etc.) in combination with the online learning characteristics of the content recognition model. Recognition can offset the recognition error

of
the
data
flow
type
of
the
data
flow
by
the
behavior
recognition
model
in
the
process
of
data
flow
transmission.
Therefore,
this
application
adopts
the
recognition
method
combining
the
behavior
recognition
model
and
the
content
recognition
model
to
improve
the
accuracy
of
the
data
flow
type
The
recognition
accuracy
also
improves
the
generalization
of
recognition,
and
can

be applied to various scenarios such as application cloud deployment, application transmission encryption, and private applications.

[0282]

Those of ordinary skill in the art can understand that all or part of the processes in the methods of the above embodiments are realized. The processes can be completed by computer programs or hardware related to the computer

programs. The computer programs can be stored in computer-readable storage media. The computer programs During execution, it may include the processes of the foregoing method embodiments.

The aforementioned storage medium includes. ROM or random access memory RAM, magnetic disk or optical disk, and other various media that can store computer program codes

[0253]

The first

device,
the
first
confidence
level,
the
first
data
stream
type,
the
first
preset
threshold,
the
first
information,
and
the
"first"
in
the
first
record
mentioned
in
the
embodiment
of
the
present
invention
are
only
used
for
name
identification,
not
Represents
the
first
in
order.

The
same
rule
applies
to
"second,"
"third,"
and
"fourth,"
etc.

However,
the
"first"

in the first identifier mentioned in the embodiment of the present invention represents the first in order.

The same rule applies to "Nth".

[0254]

The specific embodiments described above have further described the purpose, technical solutions and beneficial effects of the present invention in detail. it should be understood that the above descriptions are only specific

embodiments of the present invention and are not intended to limit the scope of the present invention. Protection scope, all modifications, substitutions, improvements, etc. made on the basis of the technical solution of the present invention shall be included in the protection scope of the present invention.

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2021 年 3 月 25 日 (25.03.2021)

WIPO | PCT

(10) 国际公布号
WO 2021/052379 A1

(51) 国际专利分类号：
H04L 12/851 (2013.01)

(21) 国际申请号： PCT/CN2020/115693

(22) 国际申请日： 2020 年 9 月 16 日 (16.09.2020)

(25) 申请语言： 中文

(26) 公布语言： 中文

(30) 优先权：
201910872990.0 2019年9月16日 (16.09.2019) CN

(71) 申请人：华为技术有限公司 (**HUAWEI TECHNOLOGIES CO., LTD.**) [CN/CN]；中国广东省深圳市龙岗区坂田华为总部办公楼，**Guangdong** 518129 (**CN**)。

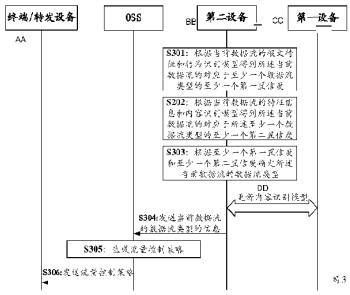
(72) 发明人：吴俊 (**WU, Jim**)；中国广东省深圳市龙岗区坂田华为总部办公楼，**Guangdong** 518129 (**CN**)。胡新宇 (**HU, Xinyu**)；中国广东省深圳市龙岗区坂田华为总部办公楼，**Guangdong** 518129 (**CN**)。王雅莉 (**WANG, Yali**)；中国广东省深圳市龙岗区坂田华为总部办公楼，**Guangdong** 518129 (**CN**)。司晓云 (**SI, Xiaoyun**)；中国广东省深圳市龙岗区坂田华为总部办公楼，**Guangdong** 518129 (**CN**)。

(81) 指定国（除另有指明，要求每一种可提供的国家保护）：AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国（除另有指明，要求每一种可提供的地区保护）：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,

(54) **Title** :DATA STREAM TYPE IDENTIFICATION METHOD AND RELATED DEVICES

(54) 发明名称：一种数据流类型识别方法及相关设备



S301 Obtain at least one first confidence level of a current data stream corresponding to at least one data stream type according to message characteristics of the current data stream and a behavior recognition model
S302 Obtain at least one second confidence level of the current data stream corresponding to at least one data stream type according to the characteristic information of the current data stream and a content recognition model
S303 Determine the data stream type of the current data stream according to the at least one first confidence level and the at least one second confidence level
S304 Send information of the data stream type of the current data stream
S305 Generate a traffic control policy
S306 Send the traffic control policy
AA Terminal/forwarding device
BB Second device
CC First device
DD Update the content to the model

(57) **Abstract** : A data stream type identification method and related devices. The method comprises: obtaining at least one first confidence level of a current data stream corresponding to at least one data stream type according to message characteristics of the current data stream and a behavior recognition model, the behavior recognition model being a model obtained on the basis of a plurality of data stream samples; obtaining at least one second confidence level of the current data stream corresponding to at least one data stream type according to the characteristic information of the current data stream and a content recognition model, the content recognition model being a model obtained on the basis of one or more historical data streams; and determining the data stream type of the current data stream according to the at least one first confidence level and the at least one second confidence level. The data stream type can be more accurately identified using the present method.

(57) 摘要：一种数据流类型识别方法及相关设备。该方法根据当前数据流的报文特征和行为识别模型得到当前数据流的对应于至少一个数据流类型的至少一个第一置信度，行为识别模型为根据多个数据流样本得到的模型；根据当前数据流的特征信息和内容识别模型得到当前数据流的对应于至少一个数据流类型的至少一个第二置信度，内容识别模型为根据一条或多条历史数据流得到的模型；根据至少一个第一置信度和至少一个第二置信度确定当前数据流的数据流类型。采用该方法能够更准确地识别出数据流类型。

WO 2021/052379 A1

[见续页]

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00448

RO, RS, SE, SI, SK, SM, TR),OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：
- 包括国际检索报告（条约第21条(3)）。

一种数据流类型识别方法及相关设备

本申请要求于2019年9月16日提交的申请号为201910872990.0、发明名称为“一种数据流类型识别方法及相关设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及计算机技术领域和通信领域，进一步涉及人工智能(Artificial Intelligence, AI)在计算机技术领域和通信领域的应用，尤其涉及一种数据流类型识别方法及相关设备。

背景技术

随着计算机技术的迅猛发展，越来越多的企业使用私有的办公类应用进行办公，如桌面云、语音会议、视频会议等均属于私有的办公类应用。为了合理安排各业务的流量提高业务的可靠性，通常需要合理配置QoS优先级、实时选路等。而QoS优先级、实时选路等的前提是需要获知当前的办公应用属于哪种类型的应用(即哪种数据流类型)。

目前主要采用如下两种方式来获知办公应用的类型：第一种，基于人工识别的方式，主要是手工配置规则来匹配网络流量中的关键字(包括报头数据、载荷数据等)，从而识别出应用类型。然而，人工识别的方式耗时耗力，而且随着企业办公应用云化带来的动态性，出于安全通常会进行传输加密，这就导致人工难以设定出应用类型的识别规则，从而很难识别出应用类型。第二种，采用离线学习的方式，主要是预先采集样本数据，然后通过人工或使用第三方工具对样本数据进行标注，然后对标注过的样本数据使用机器学习或者神经网络的算法进行模型的离线训练。将离线训练好的模型，用于推理现网流量的应用类型。但是，企业应用每次进行改动或更新，都可能训练出的模型无法使用；另外，私有应用的实现没有规范，不同企业的同类型应用，适用的模型也不一样。即以上训练出的模型在用于改动、更新后的应用或另一个企业的应用的类型识别时，都可能出现识别准确率不高的问题。

如何快速准确地识别出办公应用的应用类型(也称数据流类型)是本领域的技术人员正在研究的技术问题。

发明内容

本发明实施例公开了一种数据流类型识别方法及相关设备，能够更准确地识别出数据流类型。

第一方面，本申请实施例提供一种数据流类型识别方法，该方法包括：

根据当前数据流的报文特征和行为识别模型得到所述当前数据流的对应于至少一个数据流类型的至少一个第一置信度，其中，所述行为识别模型为根据多个数据流样本的报文特征和数据流类型得到的模型；所述报文特征包括报文长度、报文传输速度、报文间隔时间和报文方向中的一项或者多项；

根据所述当前数据流的特征信息和内容识别模型得到所述当前数据流的对应于所述至少一个数据流类型的至少一个第二置信度，其中，所述特征信息包括目的地址和协议类型，所述内容识别模型为根据一条或多条历史数据流的特征信息和数据流类型得到的模型，所述历史数据流的数据流类型是根据所述行为识别模型得到的；

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00450

根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型。

上述方法中，涉及行为识别模型和内容识别模型，行为识别模型为由多个数据流样本的报文特征和数据流类型预先训练得到，而内容识别模型是基于数据流的特征信息和由行为模型识别出的数据流类型训练得到，因此内容识别模型就是一个在线学习模型；行为识别模型能够识别出一些基本(或说典型)数据流的数据流类型，同样类型的数据流的某些特征(例如报文长度、报文传输速度等)可能在后续传输过程中发生变化，因此结合内容识别模型的在线学习特性从其他方面(如目的地址、协议类型等)对该数据流的类型进行识别，能够对冲行为识别模型在数据流传输过程中对数据流的数据流类型的识别误差，因此本申请采用行为识别模型和内容识别模型相结合的识别方式，提高了数据流的数据流类型的识别准确度，也提升了识别的泛化性，能够适用于应用云化部署、应用传输加密、私有应用等多种场景。

结合第一方面，在第一方面的第一种可能的实现方式中，所述根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型，包括：

根据对应于第一数据流类型的所述第一置信度、所述第一置信度的权重值、对应于所述第一数据流类型的所述第二置信度和所述第二置信度的权重值计算对应于所述第一数据流类型的综合置信度，所述第一数据流类型为所述至少一个数据流类型中的任意一个；

若对应于所述第一数据流类型的所述综合置信度大于第一预设阈值，则确定所述当前数据流的数据流类型为所述第一数据流类型。

在上述方法中，预先根据内容识别模型和行为识别模型各自对最终识别结果的影响程度，分别为两种模型配置置信度的权重(为行为识别模型配置的权重为第一置信度的权重，为内容识别模型配置的权重为第二置信度的权重)，因此基于这两个置信度的权重计算出的综合置信度更能体现当前数据流的实际类型。另外，引入第一预设阈值来衡量对应的数据流类型是否可取，能够提高确定数据流类型的效率和准确性。

结合第一方面，或者第一方面的上述任一种可能的实现方式，在第一方面的第二种可能的实现方式中，所述方法还包括：

若对应于所述第一数据流类型的所述综合置信度小于第二预设阈值，则向设备发送所述当前数据流的特征信息和所述第一数据流类型的信息，所述第二预设阈值大于所述第一预设阈值；

接收所述设备发送的第一信息，所述第一信息是所述设备根据所述当前数据流的特征信息和所述第一数据流类型的标识信息得到的；

根据所述第一信息更新所述内容识别模型，以得到新的内容识别模型。

结合第一方面，或者第一方面的上述任一种可能的实现方式，在第一方面的第三种可能的实现方式中，还包括：

若对应于所述第一数据流类型的所述综合置信度小于第二预设阈值，则根据所述当前数据流的特征信息和所述第一数据流类型信息更新所述内容识别模型，以得到新的内容识别模型，所述第二预设阈值大于所述第一预设阈值。

上述方法中，本申请发明人利用当前数据流的数据流类型的认定结果对内容识别模型进行校正。具体的，引入了第二预设阈值，在对应于所述第一数据流类型的所述综合置信度小于第二预设阈值时，将当前数据流的相关信息发送给设备进行训练，以用于获得新的内容识别模型，以使得下一次的认定结果更加准确。

结合第一方面，或者第一方面的上述任一种可能的实现方式，在第一方面的第四种可能

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00451

的实现方式中，所述根据所述当前数据流的特征信息和所述第一数据流类型信息更新所述内容识别模型，以得到新的内容识别模型，包括：

若多条记录中的第一记录的特征信息与所述当前数据流的特征信息相同但所述第一记录的数据流类型与所述第一数据流类型不同，则将所述第一记录的数据流类型更新为所述第一数据流类型，以获得第二记录；所述多条记录中的每一条记录包括特征信息和数据流类型；

对包括所述第二记录的多条记录进行训练，以得到新的内容识别模型。

也即是说，如果在已经识别过的记录中，存在历史数据流的特征信息与当前数据流的特征信息相同但数据流类型不同的情况，则将记录中的数据流类型更新为当前数据流的第一数据流类型，这主要是为了适应云资源的弹性部署，例如，同样的云资源在前一段时间用于视频会议，在下一段时间用于桌面云；采用上述方法能够在下一段时间内及时将数据流类型更新为桌面云，从而在弹性部署云资源的情况下仍然可以准确识别出当前数据流的数据流类型。

结合第一方面，或者第一方面的上述任一种可能的实现方式，在第一方面的第五种可能的实现方式中，所述根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型之后，还包括：

向运维支持系统 OSS 发送所述当前数据流的数据流类型的信息，所述当前数据流的数据流类型的所述信息用于所述 OSS 生成针对所述当前数据流的流量控制策略。

也即是说，在确定出当前数据流的数据流类型之后，将当前数据流类型的相关信息通知给 OSS 系统，这样 OSS 系统就可以基于当前数据流的数据流类型来生成针对所述当前数据流的流量控制策略，例如当前数据流的第一数据流类型为视频会议的视频流时，将其对应的流量控制策略定义为优先传输的策略，即当有多个数据流待传输时，优先传输该当前数据流。

结合第一方面，或者第一方面的上述任一种可能的实现方式，在第一方面的第六种可能的实现方式中，所述报文长度包括报文中以太帧长度、IP 长度、传输协议长度和报头长度中的一项或者多项，所述传输协议包括传输控制协议 TCP 和/或用户数据报协议 UDP。

第二方面，本申请实施例提供一种数据流类型识别方法，该方法包括：

接收设备发送的当前数据流的特征信息和数据流类型的信息；

根据所述当前数据流的特征信息和数据流类型的信息生成第一信息；

向所述设备发送所述第一信息，以用于更新内容识别模型，所述内容识别模型用于得到对应于至少一个数据流类型的至少一个第二置信度，其中，所述内容识别模型为根据一条或多条历史数据流的特征信息和数据流类型得到的模型，所述历史数据流的数据流类型是根据行为识别模型得到的，所述行为识别模型为根据多个数据流样本的报文特征和数据流类型得到的模型，所述报文特征包括报文长度、报文传输速度、报文间隔时间和报文方向中的一项或者多项。

上述方法中，涉及行为识别模型和内容识别模型，行为识别模型为由多个数据流样本的报文特征和数据流类型预先训练得到，而内容识别模型是基于数据流的特征信息和由行为模型识别出的数据流类型训练得到，因此内容识别模型就是一个在线学习模型；行为识别模型能够识别出一些基本（或说典型）数据流的数据流类型，同样类型的数据流的某些特征（例如报文长度、报文传输速度等）可能在后续传输过程中发生变化，因此结合内容识别模型的在线学习特性从其他方面（如目的地址、协议类型等）对该数据流的类型进行识别，能够对冲行为识别模型在数据流传输过程中对数据流的数据流类型的识别误差，因此本申请采用行为识别模型和内容识别模型相结合的识别方式，提高了数据流的数据流类型的识别准确度，

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00452

也提升了识别的泛化性，能够适用于应用云化部署、应用传输加密、私有应用等多种场景。

第三方面，本申请实施例提供一种数据流类型识别设备，包括存储器和处理器，其中，所述存储器用于存储计算机程序，所述处理器调用所述计算机程序，用于执行如下操作：

根据当前数据流的报文特征和行为识别模型得到所述当前数据流的对应于至少一个数据流类型的至少一个第一置信度，其中，所述行为识别模型为根据多个数据流样本的报文特征和数据流类型得到的模型；所述报文特征包括报文长度、报文传输速度、报文间隔时间和报文方向中的一项或者多项；

根据所述当前数据流的特征信息和内容识别模型得到所述当前数据流的对应于所述至少一个数据流类型的至少一个第二置信度，其中，所述特征信息包括目的地址和协议类型，所述内容识别模型为根据一条或多条历史数据流的特征信息和数据流类型得到的模型，所述历史数据流的数据流类型是根据所述行为识别模型得到的；

根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型。

上述方法中，涉及行为识别模型和内容识别模型，行为识别模型为由多个数据流样本的报文特征和数据流类型预先训练得到，而内容识别模型是基于数据流的特征信息和由行为模型识别出的数据流类型训练得到，因此内容识别模型就是一个在线学习模型；行为识别模型能够识别出一些基本(或说典型)数据流的数据流类型，同样类型的数据流的某些特征(例如报文长度、报文传输速度等)可能在后续传输过程中发生变化，因此结合内容识别模型的在线学习特性从其他方面(如目的地址、协议类型等)对该数据流的类型进行识别，能够对冲行为识别模型在数据流传输过程中对数据流的数据流类型的识别误差，因此本申请采用行为识别模型和内容识别模型相结合的识别方式，提高了数据流的数据流类型的识别准确度，也提升了识别的泛化性，能够适用于应用云化部署、应用传输加密、私有应用等多种场景。

结合第三方面，在第三方面的第一种可能的实现方式中，所述根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型，具体为：

根据对应于第一数据流类型的所述第一置信度、所述第一置信度的权重值、对应于所述第一数据流类型的所述第二置信度和所述第二置信度的权重值计算对应于所述第一数据流类型的综合置信度，所述第一数据流类型为所述至少一个数据流类型中的任意一个；

若对应于所述第一数据流类型的所述综合置信度大于第一预设阈值，则确定所述当前数据流的数据流类型为所述第一数据流类型。

在上述操作中，预先根据内容识别模型和行为识别模型各自对最终识别结果的影响程度，分别为两种模型配置置信度的权重(为行为识别模型配置的权重为第一置信度的权重，为内容识别模型配置的权重为第二置信度的权重)，因此基于这两个置信度的权重计算出的综合置信度更能体现当前数据流的实际类型。另外，引入第一预设阈值来衡量对应的数据流类型是否可取，能够提高确定数据流类型的效率和准确性。

结合第三方面，或者第三方面的上述任一种可能的实现方式，在第三方面的第二种可能的实现方式中，所述设备还包括收发器，所述处理器还用于：

若对应于所述第一数据流类型的所述综合置信度小于第二预设阈值，则通过所述收发器向其他设备发送所述当前数据流的特征信息和所述第一数据流类型的信息，所述第二预设阈值大于所述第一预设阈值；

通过所述收发器接收所述其他设备发送的第一信息，所述第一信息是所述其他设备根据

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00453

所述当前数据流的特征信息和所述第一数据流类型的标识信息得到的；

根据所述第一信息更新所述内容识别模型，以得到新的内容识别模型。

结合第三方面，或者第三方面的上述任一种可能的实现方式，在第三方面的第三种可能的实现方式中，所述处理器还用于：

若对应于所述第一数据流类型的所述综合置信度小于第二预设阈值，则根据所述当前数据流的特征信息和所述第一数据流类型信息更新所述内容识别模型，以得到新的内容识别模型，所述第二预设阈值大于所述第一预设阈值。

上述方法中，本申请发明人利用当前数据流的数据流类型的认定结果对内容识别模型进行校正。具体的，引入了第二预设阈值，在对应于所述第一数据流类型的所述综合置信度小于第二预设阈值时，将当前数据流的相关信息发送给设备进行训练，以用于获得新的内容识别模型，以使得下一次的认定结果更加准确。

结合第三方面，或者第三方面的上述任一种可能的实现方式，在第三方面的第四种可能的实现方式中，所述根据所述当前数据流的特征信息和所述第一数据流类型信息更新所述内容识别模型，以得到新的内容识别模型，具体为：

若多条记录中的第一记录的特征信息与所述当前数据流的特征信息相同但所述第一记录的数据流类型与所述第一数据流类型不同，则将所述第一记录的数据流类型更新为所述第一数据流类型，以获得第二记录；所述多条记录中的每一条记录包括特征信息和数据流类型；

对包括所述第二记录的多条记录进行训练，以得到新的内容识别模型。

也即是说，如果在已经识别过的记录中，存在历史数据流的特征信息与当前数据流的特征信息相同但数据流类型不同的情况，则将记录中的数据流类型更新为当前数据流的第一数据流类型，这主要是为了适应云资源的弹性部署，例如，同样的云资源在前一段时间用于视频会议，在下一段时间用于桌面云；采用上述方法能够在下一段时间内及时将数据流类型更新为桌面云，从而在弹性部署云资源的情况下仍然可以准确识别出当前数据流的数据流类型。

结合第三方面，或者第三方面的上述任一种可能的实现方式，在第三方面的第五种可能的实现方式中，所述设备还包括收发器，所述处理器还用于，在所述根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型之后，通过所述收发器向运维支持系统 OSS 发送所述当前数据流的数据流类型的信息，所述当前数据流的数据流类型的所述信息用于所述 OSS 生成针对所述当前数据流的流量控制策略。

也即是说，在确定出当前数据流的数据流类型之后，将当前数据流类型的相关信息通知给 OSS 系统，这样 OSS 系统就可以基于当前数据流的数据流类型来生成针对所述当前数据流的流量控制策略，例如当前数据流的第一数据流类型为视频会议的视频流时，将其对应的流量控制策略定义为优先传输的策略，即当有多个数据流待传输时，优先传输该当前数据流。

结合第三方面，或者第三方面的上述任一种可能的实现方式，在第三方面的第六种可能的实现方式中，所述报文长度包括报文中以太帧长度、IP 长度、传输协议长度和报头长度中的一项或者多项，所述传输协议包括传输控制协议 TCP 和/或用户数据报协议 UDP。

第四方面，本申请实施例提供一种数据流类型识别设备，包括存储器、处理器和收发器，其中，存储器用于存储计算机程序，所述处理器调用所述计算机程序，用于执行如下操作：

通过所述收发器接收其他设备发送的当前数据流的特征信息和数据流类型的信息；

根据所述当前数据流的特征信息和数据流类型的信息生成第一信息；

通过所述收发器向所述其他设备发送所述第一信息，以用于更新内容识别模型，所述内

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00454

容识别模型用于得到对应于至少一个数据流类型的至少一个第二置信度，其中，所述内容识别模型为根据一条或多条历史数据流的特征信息和数据流类型得到的模型，所述历史数据流的数据流类型是根据行为识别模型得到的，所述行为识别模型为根据多个数据流样本的报文特征和数据流类型得到的模型，所述报文特征包括报文长度、报文传输速度、报文间隔时间和报文方向中的一项或者多项。

上述操作中，涉及行为识别模型和内容识别模型，行为识别模型为由多个数据流样本的报文特征和数据流类型预先训练得到，而内容识别模型是基于数据流的特征信息和由行为模型识别出的数据流类型训练得到，因此内容识别模型就是一个在线学习模型；行为识别模型能够识别出一些基本(或说典型)数据流的数据流类型，同样类型的数据流的某些特征(例如报文长度、报文传输速度等)可能在后续传输过程中发生变化，因此结合内容识别模型的在线学习特性从其他方面(如目的地址、协议类型等)对该数据流的类型进行识别，能够对冲行为识别模型在数据流传输过程中对数据流的数据流类型的识别误差，因此本申请采用行为识别模型和内容识别模型相结合的识别方式，提高了数据流的数据流类型的识别准确度，也提升了识别的泛化性，能够适用于应用云化部署、应用传输加密、私有应用等多种场景。

第五方面，本申请实施例提供一种数据流类型识别设备，该设备包括：

第一识别单元，用于根据当前数据流的报文特征和行为识别模型得到所述当前数据流的对应于至少一个数据流类型的至少一个第一置信度，其中，所述行为识别模型为根据多个数据流样本的报文特征和数据流类型得到的模型;所述报文特征包括报文长度、报文传输速度、报文间隔时间和报文方向中的一项或者多项；

第二识别单元，用于根据所述当前数据流的特征信息和内容识别模型得到所述当前数据流的对应于所述至少一个数据流类型的至少一个第二置信度，其中，所述特征信息包括目的地址和协议类型，所述内容识别模型为根据一条或多条历史数据流的特征信息和数据流类型得到的模型，所述历史数据流的数据流类型是根据所述行为识别模型得到的；

确定单元，用于根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型。

上述设备中，涉及行为识别模型和内容识别模型，行为识别模型为由多个数据流样本的报文特征和数据流类型预先训练得到，而内容识别模型是基于数据流的特征信息和由行为模型识别出的数据流类型训练得到，因此内容识别模型就是一个在线学习模型；行为识别模型能够识别出一些基本(或说典型)数据流的数据流类型，同样类型的数据流的某些特征(例如报文长度、报文传输速度等)可能在后续传输过程中发生变化，因此结合内容识别模型的在线学习特性从其他方面(如目的地址、协议类型等)对该数据流的类型进行识别，能够对冲行为识别模型在数据流传输过程中对数据流的数据流类型的识别误差，因此本申请采用行为识别模型和内容识别模型相结合的识别方式，提高了数据流的数据流类型的识别准确度，也提升了识别的泛化性，能够适用于应用云化部署、应用传输加密、私有应用等多种场景。

结合第五方面，在第五方面的第一种可能的实现方式中，所述确定单元，用于根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型，具体为：

用于根据对应于第一数据流类型的所述第一置信度、所述第一置信度的权重值、对应于所述第一数据流类型的所述第二置信度和所述第二置信度的权重值计算对应于所述第一数据流类型的综合置信度，所述第一数据流类型为所述至少一个数据流类型中的任意一个；

若对应于所述第一数据流类型的所述综合置信度大于第一预设阈值，则确定所述当前数

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00455

据流的数据流类型为所述第一数据流类型。

在上述设备中,预先根据内容识别模型和行为识别模型各自对最终识别结果的影响程度,分别为两种模型配置置信度的权重 (为行为识别模型配置的权重为第一置信度的权重,为内容识别模型配置的权重为第二置信度的权重),因此基于这两个置信度的权重计算出的综合置信度更能体现当前数据流的实际类型。另外,引入第一预设阈值来衡量对应的数据流类型是否可取,能够提高确定数据流类型的效率和准确性。

结合第五方面,或者第五方面的上述任一种可能的实现方式,在第五方面的第二种可能的实现方式中,所述设备还包括:

第一发送单元,用于在对应于所述第一数据流类型的所述综合置信度小于第二预设阈值的情况下,向其他设备发送所述当前数据流的特征信息和所述第一数据流类型的信息,所述第二预设阈值大于所述第一预设阈值;

接收单元,用于接收所述其他设备发送的第一信息,所述第一信息是所述其他设备根据所述当前数据流的特征信息和所述第一数据流类型的标识信息得到的;

更新单元,用于根据所述第一信息更新所述内容识别模型,以得到新的内容识别模型。

结合第五方面,或者第五方面的上述任一种可能的实现方式,在第五方面的第三种可能的实现方式中,还包括:

更新单元,用于在对应于所述第一数据流类型的所述综合置信度小于第二预设阈值的情况下,根据所述当前数据流的特征信息和所述第一数据流类型信息更新所述内容识别模型,以得到新的内容识别模型,所述第二预设阈值大于所述第一预设阈值。

上述方法中,本申请发明人利用当前数据流的数据流类型的认定结果对内容识别模型进行校正。具体的,引入了第二预设阈值,在对应于所述第一数据流类型的所述综合置信度小于第二预设阈值时,将当前数据流的相关信息发送给设备进行训练,以用于获得新的内容识别模型,以使得下一次的认定结果更加准确。

结合第五方面,或者第五方面的上述任一种可能的实现方式,在第五方面的第四种可能的实现方式中,所述根据所述当前数据流的特征信息和所述第一数据流类型信息更新所述内容识别模型,以得到新的内容识别模型,具体为:

若多条记录中的第一记录的特征信息与所述当前数据流的特征信息相同但所述第一记录的数据流类型与所述第一数据流类型不同,则将所述第一记录的数据流类型更新为所述第一数据流类型,以获得第二记录;所述多条记录中的每一条记录包括特征信息和数据流类型;

对包括所述第二记录的多条记录进行训练,以得到新的内容识别模型。

也即是说,如果在已经识别过的记录中,存在历史数据流的特征信息与当前数据流的特征信息相同但数据流类型不同的情况,则将记录中的数据流类型更新为当前数据流的第一数据流类型,这主要是为了适应云资源的弹性部署,例如,同样的云资源在前一段时间用于视频会议,在下一段时间用于桌面云;采用上述方法能够在下一段时间内及时将数据流类型更新为桌面云,从而在弹性部署云资源的情况下仍然可以准确识别出当前数据流的数据流类型。

结合第五方面,或者第五方面的上述任一种可能的实现方式,在第五方面的第五种可能的实现方式中,所述设备还包括:

第二发送单元,用于在所述确定单元;f艮据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型之后,向运维支持系统 OSS 发送所述当前数据流的数据流类型的信息,所述当前数据流的数据流类型的所述信息用于所述 OSS 生成针对所述当前数据流的流量控制策略。

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00456

也即是说，在确定出当前数据流的数据流类型之后，将当前数据流类型的相关信息通知给 OSS 系统，这样 OSS 系统就可以基于当前数据流的数据流类型来生成针对所述当前数据流的流量控制策略，例如当前数据流的第一数据流类型为视频会议的视频流时，将其对应的流量控制策略定义为优先传输的策略，即当有多个数据流待传输时，优先传输该当前数据流。

结合第五方面，或者第五方面的上述任一种可能的实现方式，在第五方面的第六种可能的实现方式中，所述报文长度包括报文中以太帧长度、IP 长度、传输协议长度和报头长度中的一项或者多项，所述传输协议包括传输控制协议 TCP 和/或用户数据报协议 UDP。

第六方面，本申请实施例提供一种数据流类型识别设备，该设备包括：

接收单元，用于接收其他设备发送的当前数据流的特征信息和数据流类型的信息；

生成单元，用于根据所述当前数据流的特征信息和数据流类型的信息生成第一信息；

发送单元，用于向所述其他设备发送所述第一信息，以用于更新内容识别模型，所述内容识别模型用于得到对应于至少一个数据流类型的至少一个第二置信度，其中，所述内容识别模型为根据一条或多条历史数据流的特征信息和数据流类型得到的模型，所述历史数据流的数据流类型是根据行为识别模型得到的，所述行为识别模型为根据多个数据流样本的报文特征和数据流类型得到的模型，所述报文特征包括报文长度、报文传输速度、报文间隔时间和报文方向中的一项或者多项。

上述设备中，涉及行为识别模型和内容识别模型，行为识别模型为由多个数据流样本的报文特征和数据流类型预先训练得到，而内容识别模型是基于数据流的特征信息和由行为模型识别出的数据流类型训练得到，因此内容识别模型就是一个在线学习模型；行为识别模型能够识别出一些基本（或说典型）数据流的数据流类型，同样类型的数据流的某些特征（例如报文长度、报文传输速度等）可能在后续传输过程中发生变化，因此结合内容识别模型的在线学习特性从其他方面（如目的地址、协议类型等）对该数据流的类型进行识别，能够对冲行为识别模型在数据流传输过程中对数据流的数据流类型的识别误差，因此本申请采用行为识别模型和内容识别模型相结合的识别方式，提高了数据流的数据流类型的识别准确度，也提升了识别的泛化性，能够适用于应用云化部署、应用传输加密、私有应用等多种场景。

第七方面，本申请实施例提供一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机程序，当其在处理器上运行时，实现第一方面或者第一方面的任意可能的实现方式所描述的方法。

第八方面，本申请实施例提供一种计算机程序产品，所述计算机程序产品存储在存储器上，当所述计算机程序产品在处理器上运行时，实现第一方面或者第一方面的任意可能的实现方式所描述的方法。

第九方面，本申请实施例提供了一种数据流类型识别系统，该系统包括第一设备和第二设备，其中，所述第二设备为上述第三方面，或者第三方面的任一可能的实现方式，或者第五方面，或者第五方面的任一可能的实现方式所描述的数据流类型识别设备；所述第一设备为上述第四方面，或者第四方面的任一可能的实现方式，或者第六方面，或者第六方面的任一可能的实现方式所描述的数据流类型识别设备。

本申请实施例中，涉及行为识别模型和内容识别模型，行为识别模型为由多个数据流样本的报文特征和数据流类型预先训练得到，而内容识别模型是基于数据流的特征信息和由行为模型识别出的数据流类型训练得到，因此内容识别模型就是一个在线学习模型；行为识别模型能够识别出一些基本（或说典型）数据流的数据流类型，同样类型的数据流的某些特征（例如报文长度、报文传输速度等）可能在后续传输过程中发生变化，因此结合内容识别模

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00457

型的在线学习特性从其他方面（如目的地址、协议类型等）对该数据流的类型进行识别，能够对冲行为识别模型在数据流传输过程中对数据流的数据流类型的识别误差，因此本申请采用行为识别模型和内容识别模型相结合的识别方式，提高了数据流的数据流类型的识别准确度，也提升了识别的泛化性，能够适用于应用云化部署、应用传输加密、私有应用等多种场景。

附图说明

以下对本发明实施例用到的附图进行介绍。

图 1 是本发明实施例提供的一种数据流类型的识别系统的架构示意图；

图 2A 是本发明实施例提供的内容识别模型和行为识别模型的场景示意图；

图 2B 是本发明实施例提供的一种分类模型的结构示意图；

图 2C 是本发明实施例提供的一种分类模型的结构示意图；

图 2D 是本发明实施例提供的一种分类模型的结构示意图；

图 3 是本发明实施例提供的一种数据流类型识别方法的流程示意图；

图 4 是本发明实施例提供的数据流 a 和数据流 b 的场景示意图；

图 5 是本发明实施例提供的数据流记录的样例示意图；

图 6 是本发明实施例提供的数据流记录的样例示意图；

图 7 是本发明实施例提供的一种第二设备的结构示意图；

图 8 是本发明实施例提供的一种第一设备的结构示意图；

图 9 是本发明实施例提供的又一种第二设备的结构示意图；

图 10 是本发明实施例提供的又一种第一设备的结构示意图。

具体实施方式

下面结合本发明实施例中的附图对本发明实施例进行描述。

请参见图 1，图 1 是本发明实施例提供的一种数据流类型的识别系统的架构示意图，该系统包括运维支持系统（operational system support，OSS）101、服务器 102、转发设备 103、终端 104，其中，终端 104 的数量可以为多个，图中仅以 6 个为例进行了示意，终端 104 上用于运行各种应用，例如，视频会议应用、语音会议应用、桌面云应用等等，不同的应用所产生的数据流的数据流类型（也称应用类型）往往不同。本申请实施例中，终端 104 所产生的数据流需要先通过转发设备 103 发往目的设备，其中，转发设备可以包括路由器、交换机等，转发设备 103 的数量可以是一个也可以是多个，例如，存在一个路由器和三个交换机；再如，仅存在一个交换机；再如，存在三个交换机，等等。上述服务器 102 可以为一个服务器或者多个服务器组成的服务器集群。

其中，终端 104 所产生的数据流在该终端 104 上该如何发送，以及在转发设备 103 上该如何转发，都可以按照 OSS 101 生成的流量控制策略来进行，例如，当流量控制策略规定视频会议应用所产生的数据流具有最高优先级时，假若在终端 104，或者转发设备 103 上有包括视频会议应用所产生的数据流在内的多种数据流需要发送时，会优先传输视频会议应用所产生的数据流。需要说明的是，该流量控制策略由 OSS 101 基于当前数据流的数据流类型来生成的。本申请实施例中，OSS 101 生成流量控制策略所用到的当前数据流的数据流类型是通过第二设备来确定的。

如图 2A 所示，第二设备在确定当前数据流的数据流类型的时候需要用到行为识别模型

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00458

和内容识别模型，其中，模型的参数可以包括但不限于置信度权重向量（w1，w2）、数据流类型的第一预设阈值01、第二预设阈值02，其中，第一预设阈值也可以称为分类阈值，用于衡量是否将数据流类型划分到某一类；第二预设阈值也称为模型更新阈值，用于衡量何时对内容识别模型进行更新。这些模型参数将在后续的方法流程中做更具体的阐述。其中，内容识别模型在对当前数据流进行数据流类型识别时的输入可以包括特征信息（如目的IP、目的端口、协议类型等），行为识别模型在对当前数据流进行数据流类型识别时的输入可以包括报文信息（如报文长度、报文传输速度、报文间隔时间、报文方向等）。第二设备对内容识别模型得到的置信度和行为识别模型得到的置信度基于置信度权重向量（w1，w2）得到最终的数据流类型；这个过程中，如果通过第二预设阈值02确定内容识别模型需要进行更新，则获取更新内容识别模型所需的参数。

可选的，更新所需要用到的参数可以是第二设备通过对一些数据流的相关信息进行训练得到，也可以是第一设备通过对一些数据流的相关信息进行训练得到，然后发送给第二设备。

本申请实施例中，该第二设备可以是上述OSS 101，也可以是上述服务器102，也可以是上述转发设备103；另外，该第一设备可以是上述OSS 101，也可以是上述服务器102，也可以是上述转发设备103。结合以上描述，该第一设备与该第二设备可以是相同的设备，也可以是不同的设备。并且，当第一设备和第二设备都不是上述服务器102时，可以认为图1所示的架构的中不存在服务器102。

需要说明的是，上述内容识别模型实质上是一个分类模型，如图2B所示，分类模型可以是树模型，如图2C所示，分类模型还可以是神经网络模型，如图2D所示，分类模型还可以是支持向量机（support vector machine，SVM）模型，当分类模型还可以是其他形式的模型。可选的，由于上述内容识别模型是通过提取输入的向量（如目的互联网协议（internet protocol，IP）地址、目的端口号、协议类型等特征信息）的特征来分类得到的，因此该内容识别模型可以将同一目的IP地址，同一协议类型，相同端口号的数据流识别为相同的数据流类型；将同一网段，同一协议类型，相近端口号的数据流识别为相同的数据流类型；将目的端口号是20（文件传输协议（file transfer protocol，FTP）的知名端口号）的传输控制协议（transmission control protocol，TCP）流量识别为下载的数据流类型。

另外，该第二设备在识别当前数据流的数据流类型时需要用到的一些关于当前数据流的信息，都可以由终端104或者其他设备发送给第二设备，或者第二设备自己采集得到。

请参见图3，图3是本发明实施例提供的一种数据流类型识别方法，该方法可以基于图1所示的架构来实现，该方法包括但不限于如下步骤：

步骤S301：第二设备根据当前数据流的报文特征和行为识别模型得到所述当前数据流的对应于至少一个数据流类型的至少一个第一置信度。

具体地，所述行为识别模型为根据多个数据流样本的报文特征和数据流类型得到的模型；可选的，该多个数据流样本可以为离线样本，即该行为识别模型可以为离线训练得到的模型。该多个数据流样本还可以为预先挑选的比较典型（或说有代表性）的样本，例如，视频会议应用的数据流的报文大多时候的报文长度比较长，但是也会偶尔出现报文长度比较短的时候，相比而言，报文长度比较长更能反映当前数据流为视频会议应用的数据流，因此，在选择关于视频会议应用的数据流时，尽量选择报文长度比较长的这种有代表性的作为数据流样本。可选的，该多个数据流样本的数据流类型可以是认为确定的，即人工打标签。由于所述行为识别模型为根据多个数据流样本的报文特征和数据流类型得到的模型，因此该行为识别模型

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00459

能够反映一个数据流中的报文特征与数据流类型之间的一些关系，因此，当向该行为识别模型输入当前数据流的报文特征时，其能够一定程度上预测该当前数据流属于某个或者某些数据流类型的倾向（或者说概率），体现倾向（或者说概率）的参数也可以称为置信度。

本申请实施例中，所述报文特征可以包括报文长度、报文传输速度、报文间隔时间和报文方向中的一项或者多项，可选的，所述报文长度包括报文中以太帧长度、IP长度、传输协议长度和报头长度中的一项或者多项，所述传输协议包括传输控制协议TCP和/或用户数据报协议UDP。当然，报文特征除了包括这里举例的特征外，还可以包括其他特征，例如，报文长度、报文传输速度、报文间隔时间和报文方向中的最大值、最小值、均值、方差、分位数等。该报文特征可以是以向量的形式输入到行为识别模型中，例如可以是（报文长度，报文传输速度，报文间隔时间）这种形式。另外，本申请实施例中的数据流类型还可以称之为应用类型。

第一种可能情况中，数据流类型可能有N个，N大于或者等于1，本申请实施例可以估计（或者说预测）出当前数据流属于该N个数据流类型中每个类型的置信度，即得到所述当前数据流的对应于N个数据流类型的N个第一置信度，举例来说，假若该N个数据流类型指的是视频会议的数据流类型、语音会议的数据流类型、桌面云的数据流类型，那么，需要通过行为识别模型估计当前数据流属于视频会议的数据流类型的第一置信度、属于语音会议的数据流类型的第一置信度、属于桌面云的数据流类型的第一置信度。假若N个数据流类型指的是视频会议的数据流类型，则需要通过行为识别模型估计当前数据流属于视频会议的数据流类型的第一置信度。

第二种可能情况，数据流类型可能有多个，但本申请实施例重点关注其中一个数据流类型，因此本申请实施例只估计（或者说预测）当前数据流属于该重点关注的数据流类型的置信度，即得到所述当前数据流的对应于一个数据流类型的一个第一置信度，举例来说，假若该多个数据流类型指的是视频会议的数据流类型、语音会议的数据流类型、桌面云的数据流类型，但本申请实施例只关注视频会议的数据流类型，因此只需通过行为识别模型估计当前数据流属于视频会议的数据流类型的第一置信度即可。

步骤S202：第二设备根据所述当前数据流的特征信息和内容识别模型得到所述当前数据流的对应于所述至少一个数据流类型的至少一个第二置信度。

具体地，所述内容识别模型为根据一条或多条历史数据流的特征信息和数据流类型得到的模型。可选的，该一条或者多条历史数据流可以为在线数据流，即在此之前的一段时间内持续产生的一条或者多条数据流，所述历史数据流的数据流类型是由上述行为识别模型识别得到的，即该内容识别模型可以为在线训练得到的模型。由于所述内容识别模型为根据一条或者多条历史数据流的特征信息和数据流类型得到的模型，因此该内容识别模型能够反映一个数据流中的特征信息与数据流类型之间的一些关系，因此，当向该内容识别模型输入当前数据流的特征信息时，其能够一定程度上预测该当前数据流属于某个或者某些数据流类型的倾向（或者说概率），体现倾向（或者说概率）的参数也可以称为置信度。

本申请实施例中，所述特征信息可以包括目的地址、协议类型、端口号中的一项或者多项，其中，目的地址可以为IP地址，也可以为目的MAC地址，还可以为其他形式的地址；当然，特征信息除了包括这里举例的特征外，还可以包括其他特征。进一步地，这里的特征信息可以是针对目标的信息，例如，目标IP，目标端口等。该特征信息可以是以向量的形式输入到内容识别模型中，可以是（ip，port，protocol）这种形式，例如可以为（10.29.74.5，8443，6）。也可以是（mac，port，protocol）这种形式，例如可以为（05FA1525EEFF，8443，

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00460

6)。当然还可以是其他形式，此处不再一一举例。

第一种可能情况中，数据流类型可能有 N 个，本申请实施例可以估计 (或者说预测) 出当前数据流属于该 N 个数据流类型中每个类型的置信度，即得到所述当前数据流的对应于 N 个数据流类型的 N 个第二置信度，举例来说，假若该 N 个数据流类型指的是视频会议的数据流类型、语音会议的数据流类型、桌面云的数据流类型，那么，需要通过内容识别模型估计当前数据流属于视频会议的数据流类型的第二置信度、属于语音会议的数据流类型的第二置信度、属于桌面云的数据流类型的第二置信度。假若 N 个数据流类型指的是视频会议的数据流类型，则需要通过内容识别模型估计当前数据流属于视频会议的数据流类型的第二置信度。

第二种可能情况，数据流类型可能有多个，但本申请实施例重点关注其中一个数据流类型，因此本申请实施例只估计 (或者说预测) 当前数据流属于该重点关注的数据流类型的置信度，即得到所述当前数据流的对应于一个数据流类型的一个第二置信度，举例来说，假若该多个数据流类型指的是视频会议的数据流类型、语音会议的数据流类型、桌面云的数据流类型，但本申请实施例只关注视频会议的数据流类型，因此只需通过内容识别模型估计当前数据流属于视频会议的数据流类型的第二置信度即可。

步骤 S303：第二设备根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型。

具体地，因为至少一个第一置信度能够在一定程度上表征当前数据流的数据类型倾向，至少一个第二置信度也可以在一定程度上表征当前数据流的数据流类型倾向，因此对两者进行综合考虑可以获得更准确可信的数据流类型倾向，从而得出当前数据流的数据流类型。

一种可选的方案中，得到的哪种数据流类型的综合置信度最大，则将该数据流类型确定为当前数据流的数据流类型，例如，根据视频会议的数据流类型的第一置信度和视频会议的数据流类型的第二置信度确定出的视频会议的数据流类型的综合置信度为 0.7；根据语音会议的数据流类型的第一置信度和语音会议的数据流类型的第二置信度确定出的语音会议的数据流类型的综合置信度为 0.2；根据桌面云的数据流类型的第一置信度和桌面云的数据流类型的第二置信度确定出的桌面云的数据流类型的综合置信度为 0.1；由于视频会议的数据流类型的综合置信度最大，因此将当前数据流的数据流类型确定为视频会议的数据流类型。

又一种可选的方案中，所述根据至少一个第一置信度和至少一个第二置信度确定所述当前数据流的数据流类型，可以具体为：根据对应于第一数据流类型的所述第一置信度、所述第一置信度的权重值、对应于所述第一数据流类型的所述第二置信度和所述第二置信度的权重值计算对应于所述第一数据流类型的综合置信度，所述第一数据流类型为所述至少一个数据流类型中的任意一个，也即是说，该至少一个数据流类型中的每个数据流类型均满足这里的第一数据流类型的特征。若对应于所述第一数据流类型的所述综合置信度大于第一预设阈值，则确定所述当前数据流的数据流类型为所述第一数据流类型，例如，假若对应于视频会议的数据流类型的所述综合置信度大于第一预设阈值，则确定所述当前数据流的数据流类型为视频会议的数据流类型；假若对应于桌面云的数据流类型的所述综合置信度大于第一预设阈值，则确定所述当前数据流的数据流类型为桌面云的数据流类型。

举例来说，假若置信度权重向量 (w1，w2) 为 (0.4，0.6)，即第一置信度权重 (也可以认为是行为识别模型的权重) 为 0.6，第二置信度权重 (也可以认为是内容识别模型的权重) 为 0.4、数据流类型的第一预设阈值01 等于 0.5。在第二设备进行数据流类型识别之初，由于内容识别模型未得到充分训练，因此行为识别模型能够对输入的数据流进行数据流类型的识别，而内容识别模型无法对输入的流数据进行数据流类型的识别，因此起初内容识别模型识

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00461

别的对应于任何数据流类型的置信度均为0。

假若存在两条桌面云的数据流，如图4所示，横轴代表数据流序号，纵轴代表报文长度，报文长度大于0为上行报文，报文长度小于0为下行报文；数据流a和数据流b均为桌面云的数据流类型，其中，数据流b有上行的报文，相对来说更能代表桌面云场景的特性，因此认为数据流b的报文行为是典型的行为。数据流a在很长一段时间内没有上行报文，无法明显表明其为桌面云场景，因此认为数据流a的报文行为是不典型的行为；行为识别模型通常是通过对典型行为的数据流进行训练得到，因此行为识别模型能够识别出数据流b的数据流类型，但无法识别出数据流a的数据流类型。数据流a和数据流b的特征信息如下。

数据流a的协议类型是TCP，目的IP地址是10.129.74.5，目的端口号是8443。

数据流b的协议类型是TCP，目的IP地址是10.129.56.39，目的端口号是443。

那么针对数据流a，内容识别模型识别是桌面云的数据流类型、语音会议的数据流类型、视频会议的数据流类型的第二置信度均是0。行为识别模型基于报文特征识别是桌面云的数据流类型的第一置信度是0.5、识别是语音会议的数据流类型的第一置信度均是0、识别是视频会议的数据流类型的第一置信度是0。因此，对应于这三种数据流类型的综合置信度如下。

桌面云：0*0.4+0.5*0.6=0.3，小于01，因此当前数据流不是桌面云的数据流类型。

语音会议：0*0.4+0*0.6=0，小于01，因此当前数据流不是语音会议的数据流类型。

视频会议：0*0.4+0*0.6=0，小于01，因此当前数据流不是视频会议的数据流类型。

那么针对数据流b，内容识别模型识别是桌面云的数据流类型、语音会议的数据流类型、视频会议的数据流类型的第二置信度均是0。行为识别模型基于报文特征识别是桌面云的数据流类型的第一置信度是0.9、识别是语音会议的数据流类型的第一置信度均是0、识别是视频会议的数据流类型的第一置信度是0。因此，对应于这三种数据流类型的综合置信度如下。

桌面云：0*0.4+0.9*0.6=0.54，大于01，因此当前数据流是桌面云的数据流类型。

语音会议：0*0.4+0*0.6=0，小于01，因此当前数据流不是语音会议的数据流类型。

视频会议：0*0.4+0*0.6=0，小于01，因此当前数据流不是视频会议的数据流类型。

本申请实施例中，该内容识别模型还可以进行更新，下面提供两种不同的更新方案。

方案一，若对应于所述第一数据流类型的所述综合置信度大于第一预设阈值且小于第二预设阈值02，则第二设备向第一设备发送所述当前数据流的特征信息和所述第一数据流类型的信息，所述第二预设阈值大于所述第一预设阈值。例如，针对数据流a来说，对应于桌面云的数据流类型的综合置信度0.3不在区间（01，02）内，因此无需向第一设备发送所述当前数据流的特征信息和桌面云的数据流类型的信息；再如，针对数据流b来说，对应于桌面云的数据流类型的综合置信度0.54不在区间（01，02）内，因此需要向第一设备发送所述当前数据流的特征信息（如目的IP地址10.129.56.39、目的端口号443、协议类TCP型）和桌面云的数据流类型的信息（如名称、标识等信息）。

相应的，第一设备接收第二设备发送的所述当前数据流的特征信息和所述第一数据流类型的信息，即该第一设备上就多了一条数据流记录，如图5，多了一条针对数据流b的记录。然后，该第一设备根据当前数据流的特征信息和所述第一数据流类型的信息得到的第一信息，例如，对计算置信度有影响的一些参数。可选的，第一信息属于模型文件，因此可以以模型文件的方式传输，常见开源keras库的ai模型文件是h5文件/json文件；开源skleam库的ai模型文件是pkl/m文件。这些文件都是二进制的，用于保存模型的结构、模型的权重。

接着，第二设备接收第一设备发送的第一信息，然后根据所述第一信息更新所述内容识别模型，以得到新的内容识别模型。由于数据流b的记录中，目的IP地址为10_129_56_39、

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00462

目的端口号为443、协议类型为TCP共同对应的是桌面云的数据流类型，因此，更新后的内容识别模型再对输入的数据流b进行估计时，估计出的对应于桌面云的数据流类型的第二置信度为1。可选的，由于数据流a的特征信息与数据流b的特征信息有相似之处，例如，目的IP地址在同一网段，端口号相似，协议类型相似，因此，更新后的内容识别模型再对输入的数据流a进行估计时，估计的结果会更接近对数据流b的估计结果，例如，估计出的对应于桌面云的数据流类型的第二置信度可能为0.6。

后续网络中再出现数据流a和数据流b需要估计数据流类型时，执行流程如下。

置信度权重向量 (w1，w2)、第一预设阈值01、第二预设阈值02依旧不变。

那么针对数据流a，内容识别模型识别是桌面云的数据流类型的第二置信度为0.6，识别是语音会议的数据流类型、视频会议的数据流类型的第二置信度均是0。行为识别模型基于报文特征识别是桌面云的数据流类型的第一置信度是0.5、识别是语音会议的数据流类型的第一置信度均是0、识别是视频会议的数据流类型的第一置信度是0。因此，对应于这三种数据流类型的综合置信度如下。

桌面云：0.6*0.4+0.5*0.6=0.54 ，大于01，因此当前数据流是桌面云的数据流类型。

语音会议：0*0.4+0*0.6=0 ，小于01，因此当前数据流不是语音会议的数据流类型。

视频会议：0*0.4+0*0.6=0 ，小于01，因此当前数据流不是视频会议的数据流类型。

由于识别是桌面云的数据流类型的第二置信度0.54在区间（01，02）内，因此需要向第一设备发送所述当前数据流的特征信息和桌面云的数据流类型的信息，以用于后续对内容识别模型进行更新 (更新原理前面已有介绍，此处不再赘述)。

那么针对数据流b，内容识别模型识别是桌面云的数据流类型的数据流类型的第二置信度是1、识别是语音会议的数据流类型、视频会议的数据流类型的第二置信度均是0。行为识别模型基于报文特征识别是桌面云的数据流类型的第一置信度是0.9、识别是语音会议的数据流类型的第一置信度均是0、识别是视频会议的数据流类型的第一置信度是0。因此，对应于这三种数据流类型的综合置信度如下。

桌面云：1*0.4+0.9*0.6=0.94 ，大于01，因此当前数据流是桌面云的数据流类型。

语音会议：0*0.4+0*0.6=0 ，小于01，因此当前数据流不是语音会议的数据流类型。

视频会议：0*0.4+0*0.6=0 ，小于01，因此当前数据流不是视频会议的数据流类型。

由于识别是桌面云的数据流类型的第二置信度0.94不在区间（01，02）内，因此不需要向第一设备发送所述当前数据流的特征信息和桌面云的数据流类型的信息。

在网络中存在云化的弹性部署场景，例如，目的IP地址为10.129.56.39，目的端口号为443，协议类型为TCP的云资源从为桌面云提供服务变成为视频会议提供服务。针对这种场景，上述第一设备根据当前数据流的特征信息和所述第一数据流类型的信息得到的第一信息，可以包括：若多条记录中的第一记录的特征信息与所述当前数据流的特征信息相同但所述第一记录的数据流类型与所述第一数据流类型不同，则将所述第一记录的数据流类型更新为所述第一数据流类型，以获得第二记录；所述多条记录中的每一条记录包括特征信息和数据流类型；然后对包括所述第二记录的多条记录进行训练，以得到第一信息。

举例来说，数据流c的协议类型是TCP，目的IP地址是10.129.56.39，目的端口号是443。

那么针对数据流c，内容识别模型识别是桌面云的数据流类型的数据流类型的第二置信度是1、识别是语音会议的数据流类型、视频会议的数据流类型的第二置信度均是0。行为识别模型基于报文特征识别是桌面云的数据流类型的第一置信度是0、识别是语音会议的数据流类型的第一置信度是0、识别是视频会议的数据流类型的第一置信度是0.9。因此，对应于

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00463

这三种数据流类型的综合置信度如下。

桌面云：1*0.4+0*0.6=0.4，小于01，因此当前数据流不是桌面云的数据流类型。

语音会议：0*0.4+0*0.6=0，小于01，因此当前数据流不是语音会议的数据流类型。

视频会议：0*0.4+0.9*0.6=0.54，大于01，因此当前数据流是视频会议的数据流类型。

由于识别是视频会议的数据流类型的第二置信度0.54在区间（01，02）内，因此需要向第一设备发送所述当前数据流的特征信息和桌面云的数据流类型的信息。相应的，第一设备接收第二设备发送的所述当前数据流的特征信息和所述第一数据流类型的信息，即该第一设备上就有了一条数据流记录，如图6，多了一条针对数据流c的记录。

对比图6和图5就可以发现，针对数据流c的记录与针对数据流b的记录相比，数据流类型（即应用类别）不同但特征信息（如目的IP地址、目的端口号和协议类型）相同，因此修改已有的记录，使得协议类型TCP、目的IP地址10.129.56.39、目的端口号443共同对应的数据流类型为视频会议的数据流类型，而不再是桌面云对应的数据流类型，修改前的记录即为第一记录，修改后的记录即为第二记录。

可以理解，将第一记录更新为第二记录之后，基于第二记录训练得到的第一信息来更新内容识别模型后，上述数据流c再次输入到更新后的内容识别模型时，识别其为桌面云的数据流类型的第二置信度为0，识别其为视频会议的数据流类型的第二置信度为1。

方案二，若对应于所述第一数据流类型的所述综合置信度小于第二预设阈值，第二设备无需将当前数据流的特征信息和所述第一数据流类型的信息发送给第一设备，则而是由自己根据所述当前数据流的特征信息和所述第一数据流类型信息更新所述内容识别模型，以得到新的内容识别模型，所述第二预设阈值大于所述第一预设阈值。可选的，若多条记录中的第一记录的特征信息与所述当前数据流的特征信息相同但所述第一记录的数据流类型与所述第一数据流类型不同，则第二设备将所述第一记录的数据流类型更新为所述第一数据流类型，以获得第二记录；所述多条记录中的每一条记录包括特征信息和数据流类型；对包括所述第二记录的多条记录进行训练，以得到新的内容识别模型。为了便于理解，具体原理可以参照上述方案一，由该第二设备替代上述方案一种第一设备执行的操作即可。

步骤S304：第二设备向运维支持系统OSS发送所述当前数据流的数据流类型的信息。

具体地，第二设备可以在每次确定出当前数据流的数据流类型时，向OSS发送当前数据流的数据流类型的信息，例如，第一次生成数据流a的数据流类型时，向OSS发送数据流a的数据流类型的信息，第一次生成数据流b的数据流类型时，向OSS发送数据流b的数据流类型的信息，第二次生成数据流a的数据流类型时，向OSS发送数据流a的数据流类型的信息，第二次生成数据流b的数据流类型时，向OSS发送数据流b的数据流类型的信息；生成数据流c的数据流类型时，向OSS发送数据流c的数据流类型的信息。可以理解的是，假若第二设备为该OSS，则不需要执行上述步骤S304。

步骤S305：OSS根据当前数据流的数据流类型的信息生成针对当前数据流的流量控制策略。例如，如果当前数据流的数据流类型信息表明该当前数据流为视频桌面云的数据流类型，或者视频会议的数据流类型，则将当前数据流定义为高优先级的QoS。

步骤S306：OSS向转发设备或者终端发送所述流量控制策略。

具体地，该转发设备103可以为路由器或者交换机等设备，该终端104为输出上述当前数据流的设备。假若转发设备或者终端根据流量控制策略获知当前数据流属于高优先级的QoS，则在发现有多种数据流待发送时，优先发送被配置为高优先级的当前数据流。

在图3所描述的方法中，涉及行为识别模型和内容识别模型，行为识别模型为由多个数

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00464

据流样本的报文特征和数据流类型预先训练得到，而内容识别模型是基于数据流的特征信息和由行为模型识别出的数据流类型训练得到，因此内容识别模型就是一个在线学习模型；行为识别模型能够识别出一些基本（或说典型）数据流的数据流类型，同样类型的数据流的某些特征（例如报文长度、报文传输速度等）可能在后续传输过程中发生变化，因此结合内容识别模型的在线学习特性从其他方面（如目的地址、协议类型等）对该数据流的类型进行识别，能够对冲行为识别模型在数据流传输过程中对数据流的数据流类型的识别误差，因此本申请采用行为识别模型和内容识别模型相结合的识别方式，提高了数据流的数据流类型的识别准确度，也提升了识别的泛化性，能够适用于应用云化部署、应用传输加密、私有应用等多种场景。

上述详细阐述了本发明实施例的方法，下面提供了本发明实施例的装置。

请参见图7，图7是本发明实施例提供的一种数据流类型识别设备70的结构示意图，该设备70可以为图3所示方法实施例中的第二设备，该设备70可以包括第一识别单元701、第二识别单元702和确定单元703，其中，各个单元的详细描述如下。

第一识别单元701，用于根据当前数据流的报文特征和行为识别模型得到所述当前数据流的对应于至少一个数据流类型的至少一个第一置信度，其中，所述行为识别模型为根据多个数据流样本的报文特征和数据流类型得到的模型；所述报文特征包括报文长度、报文传输速度、报文间隔时间和报文方向中的一项或者多项；

第二识别单元702，用于根据所述当前数据流的特征信息和内容识别模型得到所述当前数据流的对应于所述至少一个数据流类型的至少一个第二置信度，其中，所述特征信息包括目的地址和协议类型，所述内容识别模型为根据一条或多条历史数据流的特征信息和数据流类型得到的模型，所述历史数据流的数据流类型是根据所述行为识别模型得到的；

确定单元703，用于根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型。

上述设备中，涉及行为识别模型和内容识别模型，行为识别模型为由多个数据流样本的报文特征和数据流类型预先训练得到，而内容识别模型是基于数据流的特征信息和由行为模型识别出的数据流类型训练得到，因此内容识别模型就是一个在线学习模型；行为识别模型能够识别出一些基本（或说典型）数据流的数据流类型，同样类型的数据流的某些特征（例如报文长度、报文传输速度等）可能在后续传输过程中发生变化，因此结合内容识别模型的在线学习特性从其他方面（如目的地址、协议类型等）对该数据流的类型进行识别，能够对冲行为识别模型在数据流传输过程中对数据流的数据流类型的识别误差，因此本申请采用行为识别模型和内容识别模型相结合的识别方式，提高了数据流的数据流类型的识别准确度，也提升了识别的泛化性，能够适用于应用云化部署、应用传输加密、私有应用等多种场景。

在一种可能的实现方式中，所述确定单元703，用于根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型，具体为：

用于根据对应于第一数据流类型的所述第一置信度、所述第一置信度的权重值、对应于所述第一数据流类型的所述第二置信度和所述第二置信度的权重值计算对应于所述第一数据流类型的综合置信度，所述第一数据流类型为所述至少一个数据流类型中的任意一个；

若对应于所述第一数据流类型的所述综合置信度大于第一预设阈值，则确定所述当前数据流的数据流类型为所述第一数据流类型。

在上述设备中，预先根据内容识别模型和行为识别模型各自对最终识别结果的影响程度，

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00465

分别为两种模型配置置信度的权重 (为行为识别模型配置的权重为第一置信度的权重，为内容识别模型配置的权重为第二置信度的权重),因此基于这两个置信度的权重计算出的综合置信度更能体现当前数据流的实际类型。另外，引入第一预设阈值来衡量对应的数据流类型是否可取，能够提高确定数据流类型的效率和准确性。

在又一种可能的实现方式中，所述设备 70 还包括：

第一发送单元，用于在对应于所述第一数据流类型的所述综合置信度小于第二预设阈值的情况下，向其他设备 (如图 3 所示方法实施例中的第一设备) 发送所述当前数据流的特征信息和所述第一数据流类型的信息，所述第二预设阈值大于所述第一预设阈值；

接收单元，用于接收所述其他设备 (如图 3 所示方法实施例中的第一设备) 发送的第一信息，所述第一信息是所述其他设备 (如图 3 所示方法实施例中的第一设备) 根据所述当前数据流的特征信息和所述第一数据流类型的标识信息得到的；

更新单元，用于根据所述第一信息更新所述内容识别模型，以得到新的内容识别模型。

在又一种可能的实现方式中，该设备 70 还包括：

更新单元，用于在对应于所述第一数据流类型的所述综合置信度小于第二预设阈值的情况下，根据所述当前数据流的特征信息和所述第一数据流类型信息更新所述内容识别模型，以得到新的内容识别模型，所述第二预设阈值大于所述第一预设阈值。

上述方法中，本申请发明人利用当前数据流的数据流类型的认定结果对内容识别模型进行校正。具体的，引入了第二预设阈值，在对应于所述第一数据流类型的所述综合置信度小于第二预设阈值时，将当前数据流的相关信息发送给设备进行训练，以用于获得新的内容识别模型，以使得下一次的认定结果更加准确。

在又一种可能的实现方式中，所述根据所述当前数据流的特征信息和所述第一数据流类型信息更新所述内容识别模型，以得到新的内容识别模型，具体为：

若多条记录中的第一记录的特征信息与所述当前数据流的特征信息相同但所述第一记录的数据流类型与所述第一数据流类型不同，则将所述第一记录的数据流类型更新为所述第一数据流类型，以获得第二记录；所述多条记录中的每一条记录包括特征信息和数据流类型；

对包括所述第二记录的多条记录进行训练，以得到新的内容识别模型。

也即是说，如果在已经识别过的记录中，存在历史数据流的特征信息与当前数据流的特征信息相同但数据流类型不同的情况，则将记录中的数据流类型更新为当前数据流的第一数据流类型，这主要是为了适应云资源的弹性部署，例如，同样的云资源在前一段时间用于视频会议，在下一段时间用于桌面云；采用上述方法能够在下一段时间内及时将数据流类型更新为桌面云，从而在弹性部署云资源的情况下仍然可以准确识别出当前数据流的数据流类型。

在又一种可能的实现方式中，所述设备 70 还包括：

第二发送单元，用于在所述确定单元根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型之后，向运维支持系统 **OSS** 发送所述当前数据流的数据流类型的信息，所述当前数据流的数据流类型的所述信息用于所述 **OSS** 生成针对所述当前数据流的流量控制策略。

也即是说，在确定出当前数据流的数据流类型之后，将当前数据流类型的相关信息通知给 **OSS** 系统，这样 **OSS** 系统就可以基于当前数据流的数据流类型来生成针对所述当前数据流的流量控制策略，例如当前数据流的第一数据流类型为视频会议的视频流时，将其对应的流量控制策略定义为优先传输的策略，即当有多个数据流待传输时，优先传输该当前数据流。

在又一种可能的实现方式中，所述报文长度包括报文中以太帧长度、**IP** 长度、传输协议

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00466

长度和报头长度中的一项或者多项，所述传输协议包括传输控制协议 TCP 和/或用户数据报协议 UDP。

需要说明的是，各个单元的实现还可以对应参照图 3 所示的方法实施例的相应描述。

请参见图 8，图 8 是本发明实施例提供的一种数据流类型识别设备 80 的结构示意图，该设备 80 可以为图 3 所示方法实施例中的第一设备，该设备 80 可以包括接收单元 801、生成单元 802 和发送单元 803，其中，各个单元的详细描述如下。

接收单元 801，用于接收其他设备（如图 3 所示方法实施例中的第二设备）发送的当前数据流的特征信息和数据流类型的信息；

生成单元 802，用于根据所述当前数据流的特征信息和数据流类型的信息生成第一信息；

发送单元 803，用于向所述其他设备（如图 3 所示方法实施例中的第二设备）发送所述第一信息，以用于更新内容识别模型，所述内容识别模型用于得到对应于至少一个数据流类型的至少一个第二置信度，其中，所述内容识别模型为根据一条或多条历史数据流的特征信息和数据流类型得到的模型，所述历史数据流的数据流类型是根据行为识别模型得到的，所述行为识别模型为根据多个数据流样本的报文特征和数据流类型得到的模型，所述报文特征包括报文长度、报文传输速度、报文间隔时间和报文方向中的一项或者多项。

上述设备 80 中，涉及行为识别模型和内容识别模型，行为识别模型为由多个数据流样本的报文特征和数据流类型预先训练得到，而内容识别模型是基于数据流的特征信息和由行为模型识别出的数据流类型训练得到，因此内容识别模型就是一个在线学习模型；行为识别模型能够识别出一些基本（或说典型）数据流的数据流类型，同样类型的数据流的某些特征（例如报文长度、报文传输速度等）可能在后续传输过程中发生变化，因此结合内容识别模型的在线学习特性从其他方面（如目的地址、协议类型等）对该数据流的类型进行识别，能够对冲行为识别模型在数据流传输过程中对数据流的数据流类型的识别误差，因此本申请采用行为识别模型和内容识别模型相结合的识别方式，提高了数据流的数据流类型的识别准确度，也提升了识别的泛化性，能够适用于应用云化部署、应用传输加密、私有应用等多种场景。

需要说明的是，各个单元的实现还可以对应参照图 3 所示的方法实施例的相应描述。

请参见图 9，图 9 是本发明实施例提供的一种设备 90，该设备 90 可以为图 3 所示方法实施例中的第二设备，该设备 90 包括处理器 901、存储器 902 和收发器 903，所述处理器 901、存储器 902 和收发器 903 通过总线相互连接。

存储器 902 包括但不限于是随机存储记忆体（random access memory，RAM）、只读存储器（read-only memory，ROM）、可擦除可编程只读存储器（erasable programmable read only memory，EPROM）、或便携式只读存储器（compact disc read-only memory，CD-ROM），该存储器 902 用于相关计算机程序及数据。收发器 903 用于接收和发送数据。

处理器 901 可以是一个或多个中央处理器（central processing unit，CPU），在处理器 901 是一个 CPU 的情况下，该 CPU 可以是单核 CPU，也可以是多核 CPU。

处理器 901 读取所述存储器 902 中存储的计算机程序代码，用于执行以下操作：

根据当前数据流的报文特征和行为识别模型得到所述当前数据流的对应于至少一个数据流类型的至少一个第一置信度，其中，所述行为识别模型为根据多个数据流样本的报文特征和数据流类型得到的模型；所述报文特征包括报文长度、报文传输速度、报文间隔时间和报文方向中的一项或者多项；

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00467

根据所述当前数据流的特征信息和内容识别模型得到所述当前数据流的对应于所述至少一个数据流类型的至少一个第二置信度，其中，所述特征信息包括目的地址和协议类型，所述内容识别模型为根据一条或多条历史数据流的特征信息和数据流类型得到的模型，所述历史数据流的数据流类型是根据所述行为识别模型得到的；

根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型。

上述操作中，涉及行为识别模型和内容识别模型，行为识别模型为由多个数据流样本的报文特征和数据流类型预先训练得到，而内容识别模型是基于数据流的特征信息和由行为模型识别出的数据流类型训练得到，因此内容识别模型就是一个在线学习模型；行为识别模型能够识别出一些基本（或说典型）数据流的数据流类型，同样类型的数据流的某些特征（例如报文长度、报文传输速度等）可能在后续传输过程中发生变化，因此结合内容识别模型的在线学习特性从其他方面（如目的地址、协议类型等）对该数据流的类型进行识别，能够对冲行为识别模型在数据流传输过程中对数据流的数据流类型的识别误差，因此本申请采用行为识别模型和内容识别模型相结合的识别方式，提高了数据流的数据流类型的识别准确度，也提升了识别的泛化性，能够适用于应用云化部署、应用传输加密、私有应用等多种场景。

在一种可能的实现方式中，所述根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型，具体为：

根据对应于第一数据流类型的所述第一置信度、所述第一置信度的权重值、对应于所述第一数据流类型的所述第二置信度和所述第二置信度的权重值计算对应于所述第一数据流类型的综合置信度，所述第一数据流类型为所述至少一个数据流类型中的任意一个；

若对应于所述第一数据流类型的所述综合置信度大于第一预设阈值，则确定所述当前数据流的数据流类型为所述第一数据流类型。

在上述操作中，预先根据内容识别模型和行为识别模型各自对最终识别结果的影响程度，分别为两种模型配置置信度的权重（为行为识别模型配置的权重为第一置信度的权重，为内容识别模型配置的权重为第二置信度的权重），因此基于这两个置信度的权重计算出的综合置信度更能体现当前数据流的实际类型。另外，引入第一预设阈值来衡量对应的数据流类型是否可取，能够提高确定数据流类型的效率和准确性。

在一种可能的实现方式中，所述处理器还用于：

若对应于所述第一数据流类型的所述综合置信度小于第二预设阈值，则通过所述收发器向其他设备（如图3所示方法实施例中的第一设备）发送所述当前数据流的特征信息和所述第一数据流类型的信息，所述第二预设阈值大于所述第一预设阈值；

通过所述收发器接收所述其他设备（如图3所示方法实施例中的第一设备）发送的第一信息，所述第一信息是所述其他设备（如图3所示方法实施例中的第一设备）根据所述当前数据流的特征信息和所述第一数据流类型的标识信息得到的；

根据所述第一信息更新所述内容识别模型，以得到新的内容识别模型。

在又一种可能的实现方式中，所述处理器还用于：

若对应于所述第一数据流类型的所述综合置信度小于第二预设阈值，则根据所述当前数据流的特征信息和所述第一数据流类型信息更新所述内容识别模型，以得到新的内容识别模型，所述第二预设阈值大于所述第一预设阈值。

上述方法中，本申请发明人利用当前数据流的数据流类型的认定结果对内容识别模型进行校正。具体的，引入了第二预设阈值，在对应于所述第一数据流类型的所述综合置信度小

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00468

于第二预设阈值时，将当前数据流的相关信息发送给设备进行训练，以用于获得新的内容识别模型，以使得下一次的认定结果更加准确。

在又一种可能的实现方式中，所述根据所述当前数据流的特征信息和所述第一数据流类型信息更新所述内容识别模型，以得到新的内容识别模型，具体为：

若多条记录中的第一记录的特征信息与所述当前数据流的特征信息相同但所述第一记录的数据流类型与所述第一数据流类型不同，则将所述第一记录的数据流类型更新为所述第一数据流类型，以获得第二记录；所述多条记录中的每一条记录包括特征信息和数据流类型；

对包括所述第二记录的多条记录进行训练，以得到新的内容识别模型。

也即是说，如果在已经识别过的记录中，存在历史数据流的特征信息与当前数据流的特征信息相同但数据流类型不同的情况，则将记录中的数据流类型更新为当前数据流的第一数据流类型，这主要是为了适应云资源的弹性部署，例如，同样的云资源在前一段时间用于视频会议，在下一段时间用于桌面云；采用上述方法能够在下一段时间内及时将数据流类型更新为桌面云，从而在弹性部署云资源的情况下仍然可以准确识别出当前数据流的数据流类型。

在又一种可能的实现方式中，所述处理器还用于，在所述根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型之后，通过所述收发器向运维支持系统 OSS 发送所述当前数据流的数据流类型的信息，所述当前数据流的数据流类型的所述信息用于所述 OSS 生成针对所述当前数据流的流量控制策略。

也即是说，在确定出当前数据流的数据流类型之后，将当前数据流类型的相关信息通知给 OSS 系统，这样 OSS 系统就可以基于当前数据流的数据流类型来生成针对所述当前数据流的流量控制策略，例如当前数据流的第一数据流类型为视频会议的视频流时，将其对应的流量控制策略定义为优先传输的策略，即当有多个数据流待传输时，优先传输该当前数据流。

在又一种可能的实现方式中，所述报文长度包括报文中以太帧长度、IP 长度、传输协议长度和报头长度中的一项或者多项，所述传输协议包括传输控制协议 TCP 和/或用户数据报协议 UDP。

需要说明的是，各个操作的实现还可以对应参照图 3 所示的方法实施例的相应描述。

请参见图 10，图 10 是本发明实施例提供的一种设备 100，该设备 100 可以为图 3 所示方法实施例中的第一设备，该设备 100 包括处理器 1001、存储器 1002 和收发器 1003，所述处理器 1001、存储器 1002 和收发器 1003 通过总线相互连接。

存储器 1002 包括但不限于是随机存储记忆体（random access memory，RAM）、只读存储器（read-only memory，ROM）、可擦除可编程只读存储器（erasable programmable read only memory，EPROM）、或便携式只读存储器（compact disc read-only memory，CD-ROM），该存储器 1002 用于相关计算机程序及数据。收发器 1003 用于接收和发送数据。

处理器 1001 可以是一个或多个中央处理器（central processing unit，CPU），在处理器 1001 是一个 CPU 的情况下，该 CPU 可以是单核 CPU，也可以是多核 CPU。

处理器 1001 读取所述存储器 1002 中存储的计算机程序代码，用于执行以下操作：

通过所述收发器接收其他设备（如图 3 所示方法实施例中的第二设备）发送的当前数据流的特征信息和数据流类型的信息；

根据所述当前数据流的特征信息和数据流类型的信息生成第一信息；

通过所述收发器向所述其他设备（如图 3 所示方法实施例中的第二设备）发送所述第一信息，以用于更新内容识别模型，所述内容识别模型用于得到对应于至少一个数据流类型的

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00469

至少一个第二置信度，其中，所述内容识别模型为根据一条或多条历史数据流的特征信息和数据流类型得到的模型，所述历史数据流的数据流类型是根据行为识别模型得到的，所述行为识别模型为根据多个数据流样本的报文特征和数据流类型得到的模型，所述报文特征包括报文长度、报文传输速度、报文间隔时间和报文方向中的一项或者多项。

上述操作中，涉及行为识别模型和内容识别模型，行为识别模型为由多个数据流样本的报文特征和数据流类型预先训练得到，而内容识别模型是基于数据流的特征信息和由行为模型识别出的数据流类型训练得到，因此内容识别模型就是一个在线学习模型；行为识别模型能够识别出一些基本(或说典型)数据流的数据流类型，同样类型的数据流的某些特征(例如报文长度、报文传输速度等)可能在后续传输过程中发生变化，因此结合内容识别模型的在线学习特性从其他方面(如目的地址、协议类型等)对该数据流的类型进行识别，能够对冲行为识别模型在数据流传输过程中对数据流的数据流类型的识别误差，因此本申请采用行为识别模型和内容识别模型相结合的识别方式，提高了数据流的数据流类型的识别准确度，也提升了识别的泛化性，能够适用于应用云化部署、应用传输加密、私有应用等多种场景。

需要说明的是，各个操作的实现还可以对应参照图3所示的方法实施例的相应描述。

需说明的是，以上描述的任意装置实施例都仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。另外，本发明提供的网络设备或主机的实施例附图中，模块之间的连接关系表示它们之间具有通信连接，具体可以实现为一条或多条通信总线或信号线。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

本发明实施例还提供一种芯片系统，所述芯片系统包括至少一个处理器，存储器和接口电路，所述存储器、所述收发器和所述至少一个处理器通过线路互联，所述至少一个存储器中存储有计算机程序；所述计算机程序被所述处理器执行时，实现图3所示的方法流程。

本发明实施例还提供一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机程序，当其在处理器上运行时，实现图3所示的方法流程。

本发明实施例还提供一种计算机程序产品，当所述计算机程序产品在处理器上运行时，实现图3所示的方法流程得以实现。

综上所述，本申请涉及行为识别模型和内容识别模型，行为识别模型为由多个数据流样本的报文特征和数据流类型预先训练得到，而内容识别模型是基于数据流的特征信息和由行为模型识别出的数据流类型训练得到，因此内容识别模型就是一个在线学习模型；行为识别模型能够识别出一些基本(或说典型)数据流的数据流类型，同样类型的数据流的某些特征(例如报文长度、报文传输速度等)可能在后续传输过程中发生变化，因此结合内容识别模型的在线学习特性从其他方面(如目的地址、协议类型等)对该数据流的类型进行识别，能够对冲行为识别模型在数据流传输过程中对数据流的数据流类型的识别误差，因此本申请采用行为识别模型和内容识别模型相结合的识别方式，提高了数据流的数据流类型的识别准确度，也提升了识别的泛化性，能够适用于应用云化部署、应用传输加密、私有应用等多种场景。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，该流程可以由计算机程序来计算机程序相关的硬件完成，该计算机程序可存储于计算机可读取存储介质中，该计算机程序在执行时，可包括如上述各方法实施例的流程。而前述的存储介质包括：ROM

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00470

或随机存储记忆体 RAM、磁碟或者光盘等各种可存储计算机程序代码的介质。

本发明实施例中提到的第一设备、第一置信度、第一数据流类型、第一预设阈值第一信息以及第一记录中的“第一”只是用来做名字标识，并不代表顺序上的第一。该规则同样适用于“第二”、“第三”和“第四”等。然而，本发明实施例中提到的第一个标识中的“第一个”代表顺序上的第一。该规则同样适用于“第 N 个”。

以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上，所做的任何修改、替换、改进等，均应包括在本发明的保护范围之内。

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00471

权利要求书

1、一种数据流类型识别方法，其特征在于，包括：

根据当前数据流的报文特征和行为识别模型得到所述当前数据流的对应于至少一个数据流类型的至少一个第一置信度，其中，所述行为识别模型为根据多个数据流样本的报文特征和数据流类型得到的模型；所述报文特征包括报文长度、报文传输速度、报文间隔时间和报文方向中的一项或者多项；

根据所述当前数据流的特征信息和内容识别模型得到所述当前数据流的对应于所述至少一个数据流类型的至少一个第二置信度，其中，所述特征信息包括目的地址和协议类型，所述内容识别模型为根据一条或多条历史数据流的特征信息和数据流类型得到的模型，所述历史数据流的数据流类型是根据所述行为识别模型得到的；

根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型。

2、根据权利要求1所述的方法，其特征在于，所述根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型，包括：

根据对应于第一数据流类型的所述第一置信度和对应于所述第一数据流类型的所述第二置信度计算对应于所述第一数据流类型的综合置信度，所述第一数据流类型为所述至少一个数据流类型中的任意一个；

若对应于所述第一数据流类型的所述综合置信度大于第一预设阈值，则确定所述当前数据流的数据流类型为所述第一数据流类型。

3、根据权利要求1所述的方法，其特征在于，所述根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型，包括：

根据对应于第一数据流类型的所述第一置信度、所述第一置信度的权重值、对应于所述第一数据流类型的所述第二置信度和所述第二置信度的权重值计算对应于所述第一数据流类型的综合置信度，所述第一数据流类型为所述至少一个数据流类型中的任意一个；

若对应于所述第一数据流类型的所述综合置信度大于第一预设阈值，则确定所述当前数据流的数据流类型为所述第一数据流类型。

4、根据权利要求2或3所述的方法，其特征在于，所述方法还包括：

若对应于所述第一数据流类型的所述综合置信度小于第二预设阈值，则向设备发送所述当前数据流的特征信息和所述第一数据流类型的信息，所述第二预设阈值大于所述第一预设阈值；

接收所述设备发送的第一信息，所述第一信息是所述设备根据所述当前数据流的特征信息和所述第一数据流类型的标识信息得到的；

根据所述第一信息更新所述内容识别模型，以得到新的内容识别模型。

5、根据权利要求2或3所述的方法，其特征在于，还包括：

若对应于所述第一数据流类型的所述综合置信度小于第二预设阈值，则根据所述当前数据流的特征信息和所述第一数据流类型信息更新所述内容识别模型，以得到新的内容识别模型，所述第二预设阈值大于所述第一预设阈值。

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00472

6、根据权利要求5所述的方法，其特征在于，所述根据所述当前数据流的特征信息和所述第一数据流类型信息更新所述内容识别模型，以得到新的内容识别模型，包括：

若多条记录中的第一记录的特征信息与所述当前数据流的特征信息相同但所述第一记录的数据流类型与所述第一数据流类型不同，则将所述第一记录的数据流类型更新为所述第一数据流类型，以获得第二记录；所述多条记录中的每一条记录包括特征信息和数据流类型；

对包括所述第二记录的多条记录进行训练，以得到新的内容识别模型。

7、根据权利要求1-6任一项所述的方法，其特征在于，所述根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型之后，还包括：

向运维支持系统OSS发送所述当前数据流的数据流类型的信息，所述当前数据流的数据流类型的信息用于所述OSS生成针对所述当前数据流的流量控制策略。

8、根据权利要求1-7任一项所述的方法，其特征在于，所述报文长度包括报文中以太帧长度、IP长度、传输协议长度和报头长度中的一项或者多项，所述传输协议包括传输控制协议TCP和/或用户数据报协议UDP。

9、一种数据流类型识别方法，其特征在于，包括：

接收设备发送的当前数据流的特征信息和数据流类型的信息；

根据所述当前数据流的特征信息和数据流类型的信息生成第一信息；

向所述设备发送所述第一信息，以用于更新内容识别模型，所述内容识别模型用于得到对应于至少一个数据流类型的至少一个第二置信度，其中，所述内容识别模型为根据一条或多条历史数据流的特征信息和数据流类型得到的模型，所述历史数据流的数据流类型是根据行为识别模型得到的，所述行为识别模型为根据多个数据流样本的报文特征和数据流类型得到的模型，所述报文特征包括报文长度、报文传输速度、报文间隔时间和报文方向中的一项或者多项。

10、根据权利要求9所述的方法，其特征在于，所述根据所述当前数据流的特征信息和数据流类型的信息生成第一信息，包括：

若多条记录中的第一记录的特征信息与所述当前数据流的特征信息相同但所述第一记录的数据流类型与所述当前数据流的数据流类型不同，则将所述第一记录的数据流类型更新为所述当前数据流的数据流类型，以获得第二记录；所述多条记录中的每一条记录包括特征信息和数据流类型；

对包括所述第二记录的多条记录进行训练，以得到新的内容识别模型。

11、一种数据流类型识别设备，其特征在于，所述设备是第一设备，所述第一设备包括存储器和处理器，其中，所述存储器用于存储计算机程序，所述处理器调用所述计算机程序，用于执行如下操作：

根据当前数据流的报文特征和行为识别模型得到所述当前数据流的对应于至少一个数据流类型的至少一个第一置信度，其中，所述行为识别模型为根据多个数据流样本的报文特征和数据流类型得到的模型；所述报文特征包括报文长度、报文传输速度、报文间隔时间和报

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00473

文方向中的一项或者多项；

根据所述当前数据流的特征信息和内容识别模型得到所述当前数据流的对应于所述至少一个数据流类型的至少一个第二置信度，其中，所述特征信息包括目的地址和协议类型，所述内容识别模型为根据一条或多条历史数据流的特征信息和数据流类型得到的模型，所述历史数据流的数据流类型是根据所述行为识别模型得到的；

根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型。

12、根据权利要求11所述的设备，其特征在于，所述根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型，具体为：

根据对应于第一数据流类型的所述第一置信度和对应于所述第一数据流类型的所述第二置信度计算对应于所述第一数据流类型的综合置信度，所述第一数据流类型为所述至少一个数据流类型中的任意一个；

若对应于所述第一数据流类型的所述综合置信度大于第一预设阈值，则确定所述当前数据流的数据流类型为所述第一数据流类型。

13、根据权利要求11所述的设备，其特征在于，所述根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型，具体为：

根据对应于第一数据流类型的所述第一置信度、所述第一置信度的权重值、对应于所述第一数据流类型的所述第二置信度和所述第二置信度的权重值计算对应于所述第一数据流类型的综合置信度，所述第一数据流类型为所述至少一个数据流类型中的任意一个；

若对应于所述第一数据流类型的所述综合置信度大于第一预设阈值，则确定所述当前数据流的数据流类型为所述第一数据流类型。

14、根据权利要求12或13所述的设备，其特征在于，所述第一设备还包括收发器，所述处理器还用于：

若对应于所述第一数据流类型的所述综合置信度小于第二预设阈值，则通过所述收发器向第二设备发送所述当前数据流的特征信息和所述第一数据流类型的信息，所述第二预设阈值大于所述第一预设阈值；

通过所述收发器接收所述第二设备发送的第一信息，所述第一信息是所述第二设备根据所述当前数据流的特征信息和所述第一数据流类型的标识信息得到的；

根据所述第一信息更新所述内容识别模型，以得到新的内容识别模型。

15、根据权利要求12或13所述的设备，其特征在于，所述处理器还用于：

若对应于所述第一数据流类型的所述综合置信度小于第二预设阈值，则根据所述当前数据流的特征信息和所述第一数据流类型信息更新所述内容识别模型，以得到新的内容识别模型，所述第二预设阈值大于所述第一预设阈值。

16、根据权利要求15所述的设备，其特征在于，所述根据所述当前数据流的特征信息和所述第一数据流类型信息更新所述内容识别模型，以得到新的内容识别模型，具体为：

若多条记录中的第一记录的特征信息与所述当前数据流的特征信息相同但所述第一记录

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00474

的数据流类型与所述第一数据流类型不同，则将所述第一记录的数据流类型更新为所述第一数据流类型，以获得第二记录；所述多条记录中的每一条记录包括特征信息和数据流类型；

对包括所述第二记录的多条记录进行训练，以得到新的内容识别模型。

17、根据权利要求 11-16 任一项所述的设备，其特征在于，所述第一设备还包括收发器，所述处理器还用于，在所述根据所述至少一个第一置信度和所述至少一个第二置信度确定所述当前数据流的数据流类型之后，通过所述收发器向运维支持系统 OSS 发送所述当前数据流的数据流类型的信息，所述当前数据流的数据流类型的所述信息用于所述 OSS 生成针对所述当前数据流的流量控制策略。

18、根据权利要求 11-17 任一项所述的设备，其特征在于，所述报文长度包括报文中以太帧长度、IP 长度、传输协议长度和报头长度中的一项或者多项，所述传输协议包括传输控制协议 TCP 和/或用户数据报协议 UDP。

19、一种数据流类型识别设备，所述设备是第一设备，其特征在于，所述第一设备包括存储器、处理器和收发器，其中，所述存储器用于存储计算机程序，所述处理器调用所述计算机程序，用于执行如下操作：

通过所述收发器接收第二设备发送的当前数据流的特征信息和数据流类型的信息；

根据所述当前数据流的特征信息和数据流类型的信息生成第一信息；

通过所述收发器向所述第二设备发送所述第一信息，以用于更新内容识别模型，所述内容识别模型用于得到对应于至少一个数据流类型的至少一个第二置信度，其中，所述内容识别模型为根据一条或多条历史数据流的特征信息和数据流类型得到的模型，所述历史数据流的数据流类型是根据行为识别模型得到的，所述行为识别模型为根据多个数据流样本的报文特征和数据流类型得到的模型，所述报文特征包括报文长度、报文传输速度、报文间隔时间和报文方向中的一项或者多项。

20、根据权利要求 19 所述的设备，其特征在于，所述根据所述当前数据流的特征信息和数据流类型的信息生成第一信息，具体为：

若多条记录中的第一记录的特征信息与所述当前数据流的特征信息相同但所述第一记录的数据流类型与所述当前数据流的数据流类型不同，则将所述第一记录的数据流类型更新为所述当前数据流的数据流类型，以获得第二记录；所述多条记录中的每一条记录包括特征信息和数据流类型；

对包括所述第二记录的多条记录进行训练，以得到新的内容识别模型。

21、一种数据流类型识别设备，其特征在于，包括用于执行权利要求 1-10 任一项所述的方法的单元。

22、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中存储有计算机程序，当其在处理器上运行时，实现权利要求 1-10 任一所述的方法。

23、一种计算机程序产品，其特征在于，所述计算机程序产品存储在存储器上，当所述计算机程序产品在处理器上运行时，实现权利要求 1-10 任一项所述的方法。

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00475

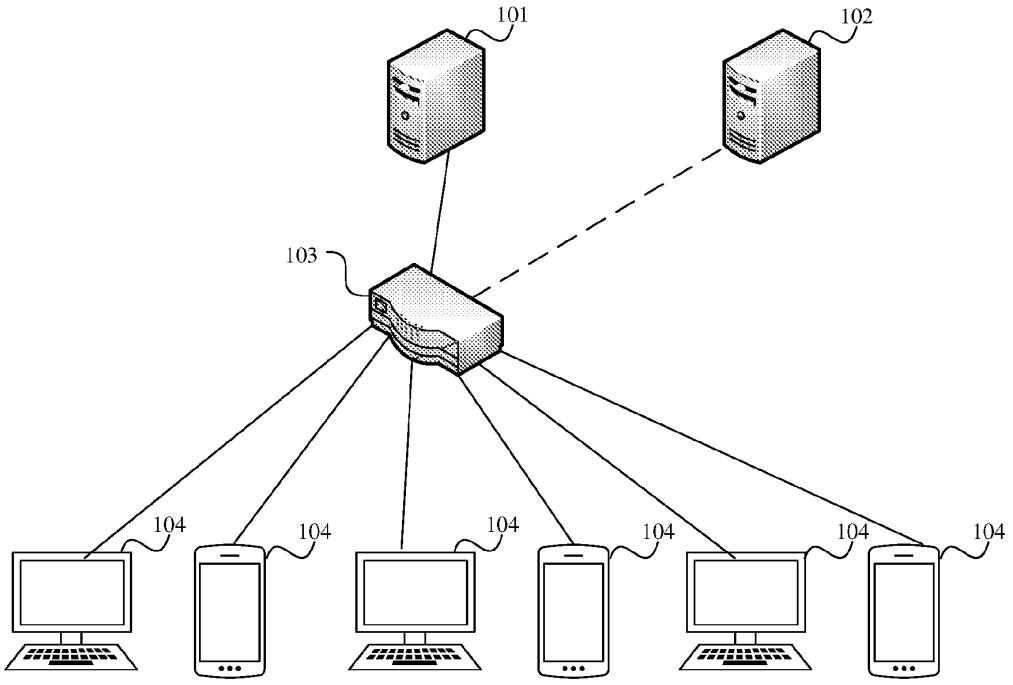


图 1

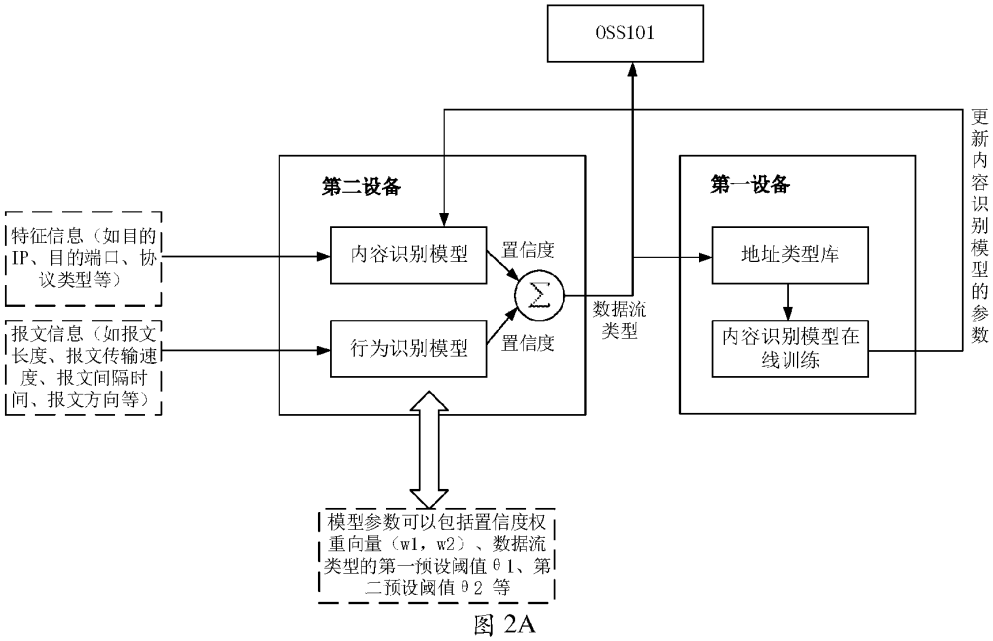


图 2A

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00476

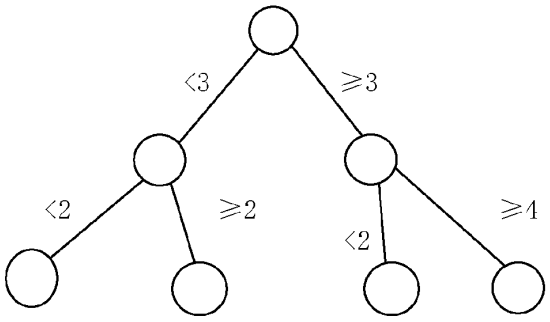


图 2B

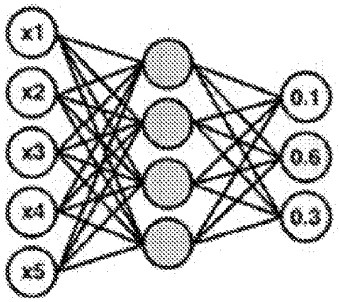


图 2C

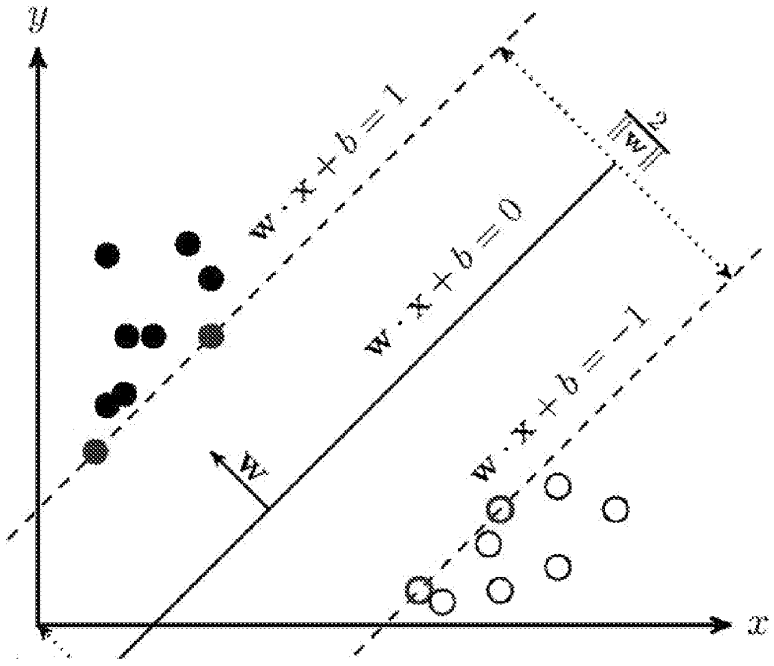


图 2D

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00477

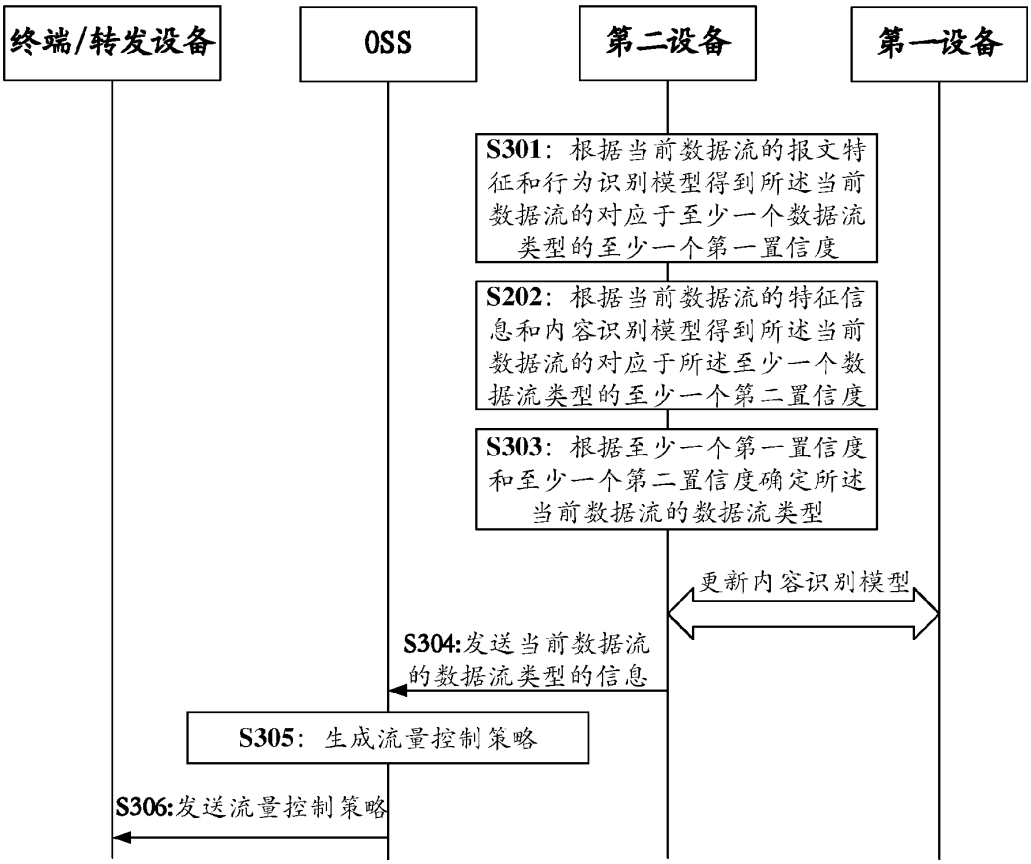


图 3

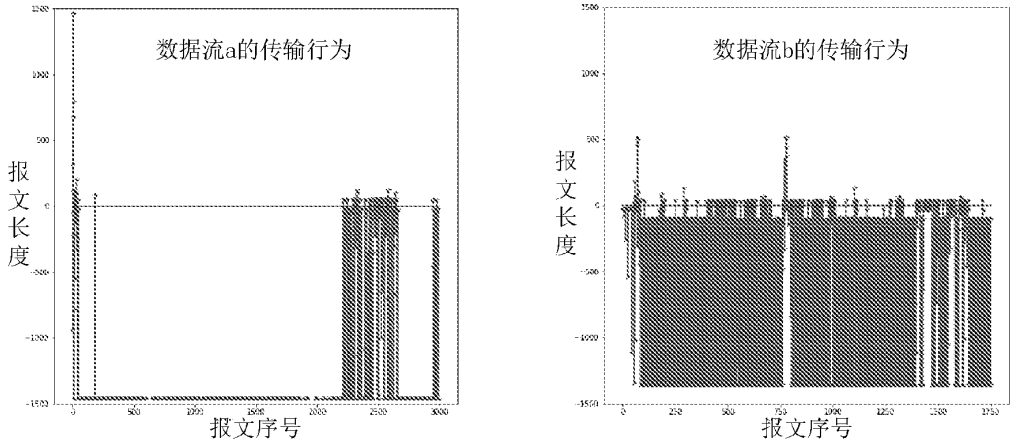


图 4

IP地址	端口	协议	数据流类型
10.129.56.39	443	TCP	桌面云

图 5

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00478

IP地址	端口	协议	数据流类型
10.129.56.39	443	TCP	视频会议

图 6

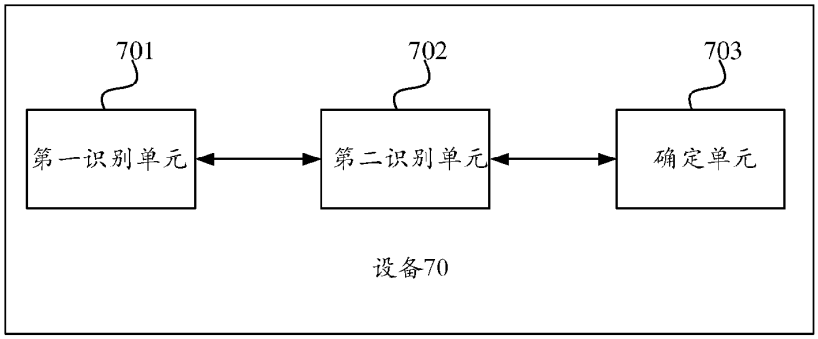


图 7

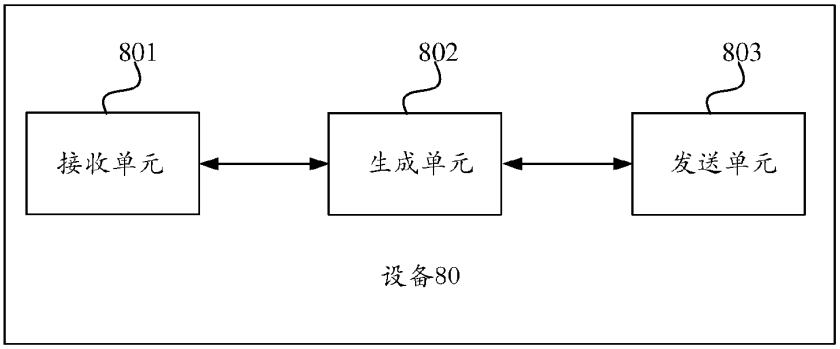


图 8

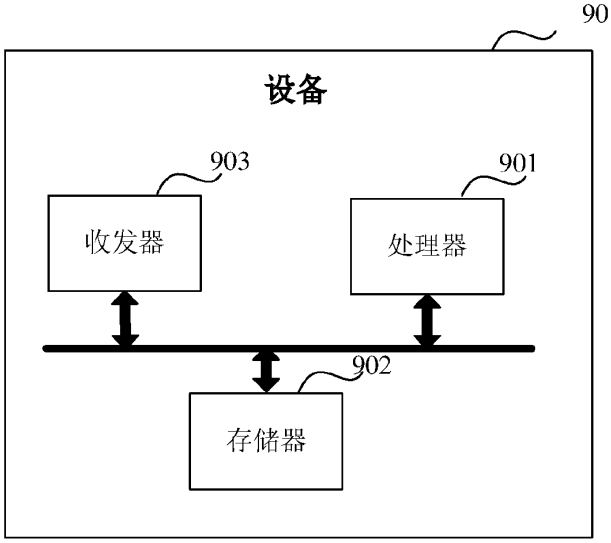


图 9

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00479

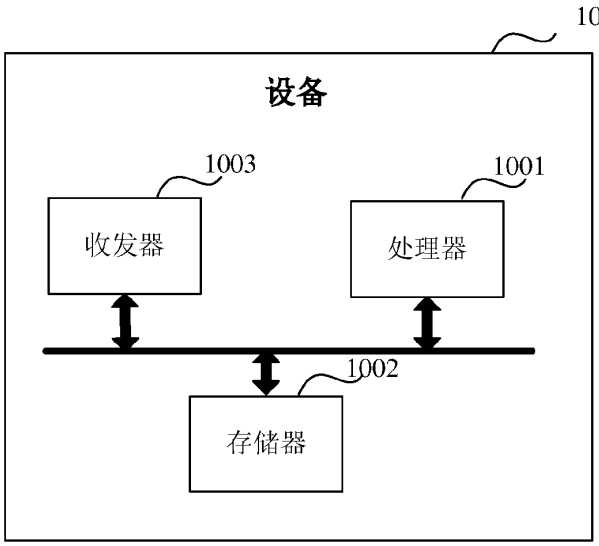


图 10

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00480

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/115693

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/851(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: 网络 ,数据 ,流 ,报文 ,类型 ,分类 ,识别 ,置信度 ,相似度 ,概率 ,特征 ,行为 ,内容 ,模型 ,历史 network, data, flow, message, type, classification, identify, confidence, probability, feature, behavior, content, model, history

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 107360032 A (CHINA SOUTHERN POWER GRID CO., LTD.) 17 November 2017 (2017-11-17) description, paragraphs 0066-0127	9-10, 19-23
Y	CN 108667747 A (SHENZHEN INSTITUTE OF INFORMATION TECHNOLOGY) 16 October 2018 (2018-10-16) description, paragraphs 0051-0103	9-10,19-23
A	CN 107360032 A (CHINA SOUTHERN POWER GRID CO., LTD.) 17 November 2017 (2017-11-17) description, paragraphs 0066-0127	1-8, 11-18
A	CN 108900432 A (SUN YAT-SEN UNIVERSITY) 27 November 2018 (2018-11-27) entire document	1-23
A	CN 110048962 A (GUANGDONG UNIVERSITY OF TECHNOLOGY) 23 July 2019 (2019-07-23) entire document	1-23
A	WO 2011114060 A2 (THALES) 22 September 2011 (2011-09-22) entire document	1-23

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 December 2020	**16 December 2020**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/115693

C. **DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	周丁丁 等 (ZHOU, Dingding et al.). "基于贝叶斯更新机制的流量分类算法 (Traffic Classification Based on Bayesian Updating Method)" *系统仿真学报 (Journal of System Simulation)*, Vol. 25, No. 11, 30 November 2013 (2013-11-30), entire document	1-23

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/115693

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	107360032	A	17 November 2017	None			
CN	108667747	A	16 October 2018	None			
CN	108900432	A	27 November 2018	None			
CN	110048962	A	23 July 2019	None			
WO	2011114060	A2	22 September 2011	US	2013117205	A1	09 May 2013
				SG	184120	A1	30 October 2012
				ES	2546129	T3	18 September 2015
				EP	2548337	A2	23 January 2013
				FR	2957738	B1	20 April 2012
				PT	2548337	E	16 October 2015
				MY	157412	A	15 June 2016
				FR	2957738	A1	23 September 2011

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00483

国际检索报告

国际申请号
PCT/CN2020/115693

A. 主题的分类

H04L 12/851(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNPAT,CNKI,WPI,EPODOC:网络，数据，流，报文，类型，分类，识别，置信度，相似度，概率，特征，行为，内容，模型，历史，network, data, flow, message, type, classification, identify, confidence, probability, feature, behavior, content, model, history

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
Y	CN 107360032 A (中国南方电网有限责任公司) 2017年 11月 17日 (2017-11-17) 说明书第0066-0127段	9-10,19-23
Y	CN 108667747 A (深圳信息职业技术学院) 2018年 10月 16日 (2018-10-16) 说明书第0051-0103段	9-10,19-23
A	CN 107360032 A (中国南方电网有限责任公司) 2017年 11月 17日 (2017-11-17) 说明书第0066-0127段	1-8,11-18
A	CN 108900432 A (中山大学) 2018年 11月 27日 (2018-11-27) 全文	1-23
A	CN 110048962 A (广东工业大学) 2019年 7月 23日 (2019-07-23) 全文	1-23
A	WO 2011114060 A2 (THALES) 2011年 9月 22日 (2011-09-22) 全文	1 23
A	周丁丁等. "基于贝叶斯更新机制的流量分类算法" 系统仿真学报, 第25卷, 第11期, 2013年 11月 30日 (2013-11-30), 全文	1-23

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型:

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 12月 4日	2020年 12月 16日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 靳晶 电话号码 86-(10)-53961790

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00484

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/115693

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	107360032	A	2017年 11月 17日	无			
CN	108667747	A	2018年 10月 16日	无			
CN	108900432	A	2018年 11月 27日	无			
CN	110048962	A	2019年 7月 23日	无			
WO	2011114060	A2	2011年 9月 22日	US	2013117205	A1	2013年 5月 9日
				SG	184120	A1	2012年 10月 30日
				ES	2546129	T3	2015年 9月 18日
				EP	2548337	A2	2013年 1月 23日
				FR	2957738	B1	2012年 4月 20日
				PT	2548337	E	2015年 10月 16日
				MY	157412	A	2016年 6月 15日
				FR	2957738	A1	2011年 9月 23日

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00485

DOCKET NUMBER: **LACEP073**

ASSIGNMENT-STATEMENT

Title of Invention: **LEARNING FROM SIMILAR CLOUD DEPLOYMENTS**

As a below named inventor, I hereby declare that:

This declaration is directed to the attached application, or (if following box is checked):

[ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I have reviewed and understand the contents of the application, including the claims.

I am aware of the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in 37 CFR Section 1.56.

Whereas, I ("ASSIGNOR") have made certain inventions, improvements, and discoveries (herein referred to as the "Invention") disclosed in the above-identified patent application and further identified by the Docket Number provided above in the header of this document;

Whereas, Lacework, Inc., (herein referred to as the "ASSIGNEE"), a corporation organized and existing under the laws of the State of Delaware, with a principal office at 6201 America Center Drive, Suite 200, San Jose, CA 95002 (herein referred to as "Lacework"), desires to acquire, and each undersigned inventor desires to grant to Lacework, the entire worldwide right, title, and interest in and to the Invention and in and to any and all patent applications and patents directed thereto;

Now, therefore, for good and valuable consideration, the receipt and sufficiency thereof being hereby acknowledged, I hereby sell or have sold, assign or have assigned, and otherwise transfer or have transferred to the ASSIGNEE, its successors, legal representatives, and assigns, my entire worldwide right, title, and interest in and to the Invention, the above-identified United States patent application, and any and all other patent applications and patents for the Invention which may be applied for or granted therefor in the United States and in all foreign countries and jurisdictions, including all divisions, continuations, reissues, reexaminations, renewals, extensions, counterparts, substitutes, and extensions thereof, and all rights of priority resulting from the filing of such applications and granting of such patents. In addition, I hereby authorize and request the Director of the United States Patent and Trademark Office to issue any United States Patent, and foreign patent authorities to issue any foreign patent, granted for the Invention, to the ASSIGNEE, its successors, legal representatives, and assigns, my entire worldwide right, title, and interest in and to the same to be held and enjoyed by the ASSIGNEE, its successors, legal representatives, and assigns to the full end of the terms for which any and all such patents may be granted, as fully and entirely as would have been held and enjoyed by me had this Assignment not been made; and I agree to execute any and all documents and instruments and perform all lawful acts reasonably related to recording this Assignment or perfecting title to the Invention and all related patents and applications, in the ASSIGNEE, its successors, legal representatives, and assigns, whenever requested by the ASSIGNEE, its successors, legal representatives, or assigns.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00486

I acknowledge my prior and ongoing obligations to sell, assign, and transfer my rights under this Assignment to the ASSIGNEE and am unaware of any reason why I may not have the full and unencumbered right to sell, assign, and transfer my rights hereby sold, assigned, and transferred, and have not executed, and will not execute, any document or instrument in conflict herewith. I also hereby grant the ASSIGNEE, its successors, legal representatives, and assigns, the right to insert in this Assignment any further identification (including, but not limited to, patent Application Number) which may be necessary or desirable for recordation of this Assignment. This Assignment is governed by the substantive laws of the State of Delaware, and any disputes will be resolved in a Delaware state court or federal court sited in Delaware.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. § 1001 by fine or imprisonment of not more than five (5) years, or both.

Signature: / Úlfar Erlingsson / Date: 02/11/2022

(1) Legal Name of Inventor: **ÚLFAR ERLINGSSON**

Signature: / Yijou Chen / Date: 02/11/2022

(2) Legal Name of Inventor: **YIJOU CHEN**

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00487

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	L0041B1CIP2C1
	Application Number	
Title of Invention	Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	ÚLFAR		ERLINGSSON	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	PALO ALTO	State/Province	CA	Country of Residence	US

Mailing Address of Inventor:

Address 1	391 SAN ANTONIO ROAD
Address 2	FLOOR 3

City	MOUNTAIN VIEW	State/Province	CA
Postal Code	94040	**Country**	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	YIJOU		CHEN	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	CUPERTINO	State/Province	CA	Country of Residence	US

Mailing Address of Inventor:

Address 1	391 SAN ANTONIO ROAD
Address 2	FLOOR 3

City	MOUNTAIN VIEW	State/Province	CA
Postal Code	94040	**Country**	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	L0041B1CIP2C1
	Application Number	
Title of Invention	Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments	

☐ **An Address is being provided for the correspondence Information of this application.**			
Customer Number	182115		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments		
Attorney Docket Number	L0041B1CIP2C1	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	49	**Suggested Figure for Publication (if any)**	

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☒ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	182115		

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	L0041B1CIP2C1
	Application Number	
Title of Invention	Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments	

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Continuation of	17671199	2022-02-14
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
17671199	Continuation in part of	17504311	2021-10-18
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
17504311	Continuation of	16665961	2019-10-28	11153339	2021-10-19

Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
16665961	Continuation of	16134794	2018-09-18	10581891	2020-03-03

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
16134794	Claims benefit of provisional	62650971	2018-03-30
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
16134794	Claims benefit of provisional	62590986	2017-11-27
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
17671199	Claims benefit of provisional	63243013	2021-09-10
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.			Add

Foreign Priority Information:

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	L0041B1CIP2C1
	Application Number	
Title of Invention	Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments	

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	L0041B1CIP2C1
	Application Number	
Title of Invention	Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	L0041B1CIP2C1
	Application Number	
Title of Invention	Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◉ Assignee	○ Legal Representative under 35 U.S.C. 117	○ Joint Inventor
○ Person to whom the inventor is obligated to assign.	○ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	LACEWORK, INC.		
Mailing Address Information For Applicant:			
Address 1	391 SAN ANTONIO ROAD		
Address 2	FLOOR 3		
City	MOUNTAIN VIEW	**State/Province**	CA
Country	US	Postal Code	94040
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	L0041B1CIP2C1
	Application Number	
Title of Invention	Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments	

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Jason Fletcher/			Date (YYYY-MM-DD)	2023-07-28
First Name	Jason	Last Name	Fletcher	Registration Number	68,044

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (01-22)
Approved for use through 05/31/2024. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	L0041B1CIP2C1
	Application Number	
Title of Invention	Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1 The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3 A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent CooperationTreaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00496

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	UNKNOWN
Filing Date	HEREWITH
First Named Inventor	ÚLFAR ERLINGSSON
Title	Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments
Art Unit	UNKNOWN
Examiner Name	UNKNOWN
Attorney Docket Number	L0041B1CIP2C1

SIGNATURE of Applicant or Patent Practitioner

Signature	/Jason Fletcher/	Date (Optional)	2023-07-28
Name	Jason Fletcher	Registration Number	68,044
Title (if Applicant is a juristic entity)	Patent Practitioner for Applicant		
Applicant Name (if Applicant is a juristic entity)	Lacework, Inc.		

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc Code: PA..

Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 182115

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

Lacework, Inc.

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature	/ Michael Moore /	Date (Optional)	
Name	Michael Moore		
Title	Vice President, Privacy and Intellectual Property		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

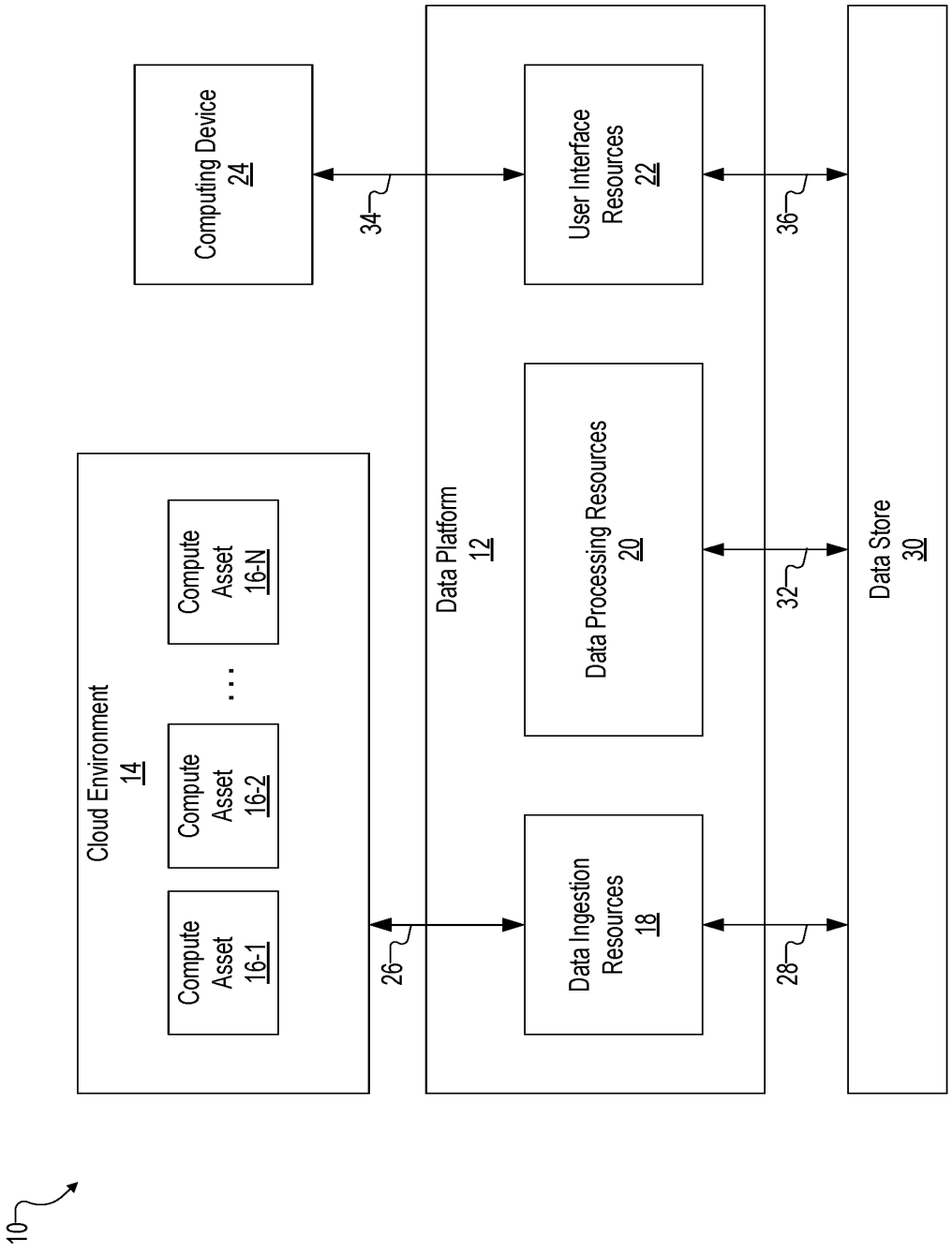

10
Cloud Environment
14
Compute Asset 16-1
Compute Asset 16-2
Compute Asset 16-N
26
Data Platform
12
Data Ingestion Resources
18
Data Processing Resources
20
User Interface Resources
22
28
32
34
36
Computing Device
24
Data Store
30

Fig. 1A

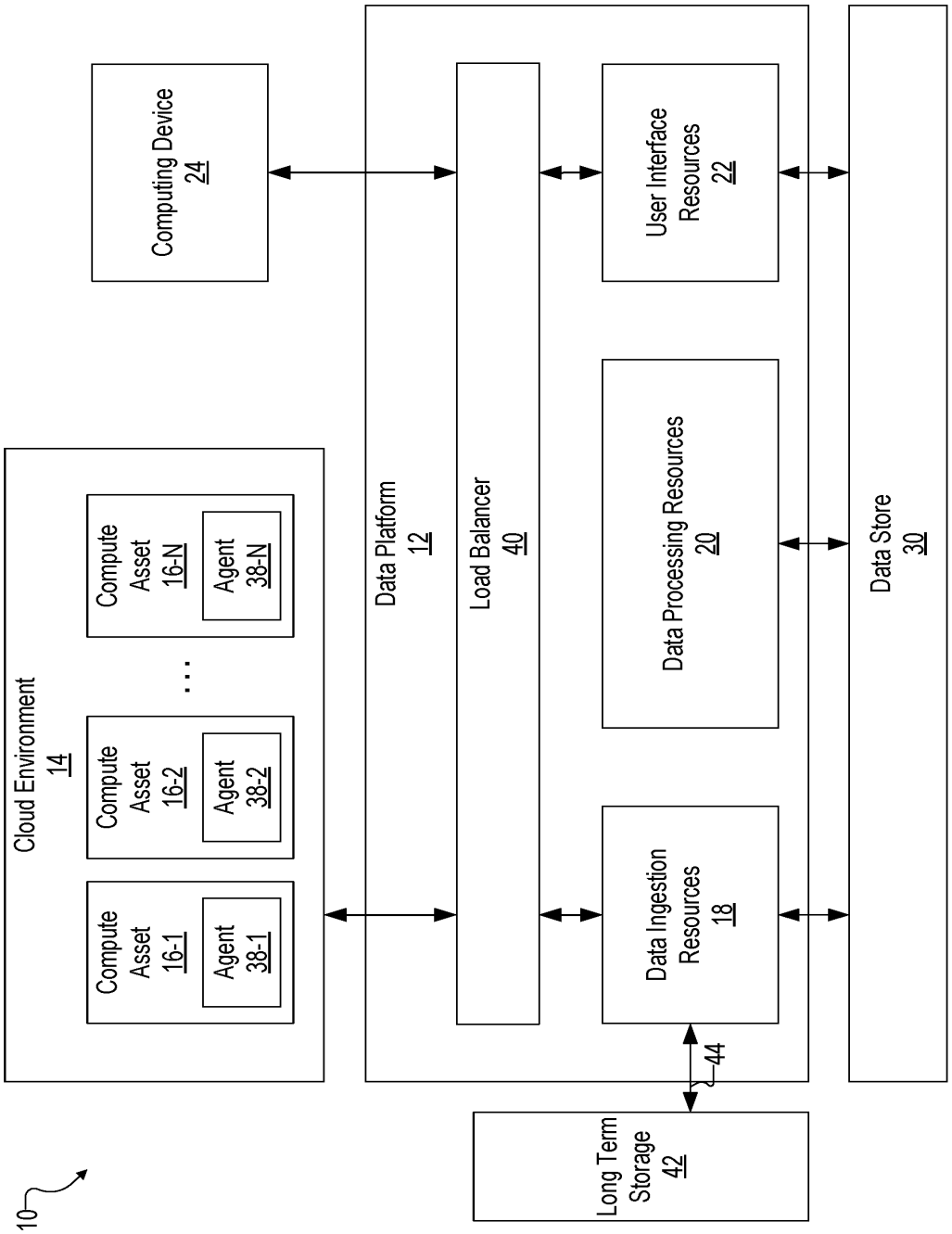

10
Cloud Environment
14
Compute Asset 16-1
Agent 38-1
Compute Asset 16-2
Agent 38-2
Compute Asset 16-N
Agent 38-N
Computing Device
24
Data Platform
12
Load Balancer
40
Data Ingestion Resources
18
Data Processing Resources
20
User Interface Resources
22
Data Store
30
44
Long Term Storage
42

Fig. 1B

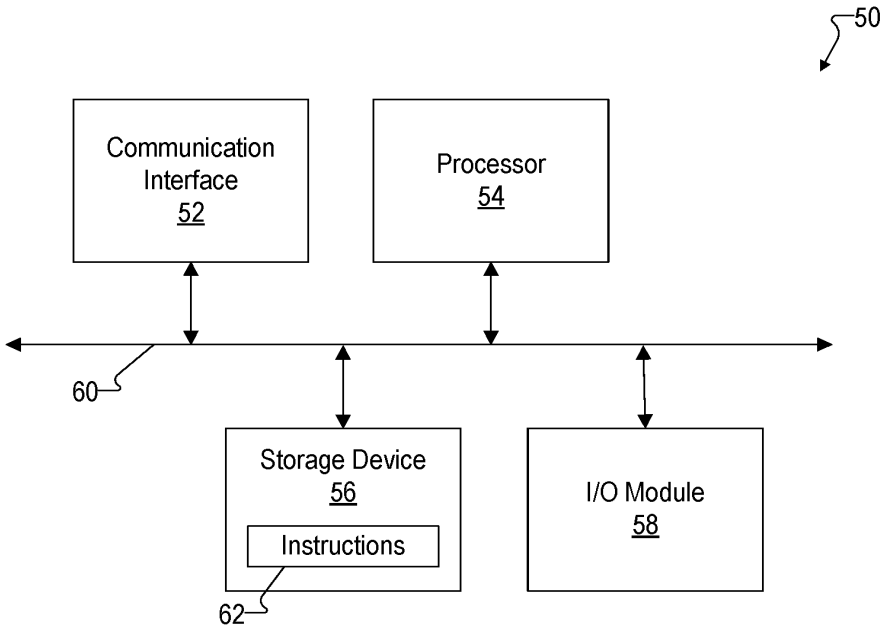

50
Communication Interface 52
Processor 54
60
Storage Device 56
Instructions
62
I/O Module 58

Fig. 1C

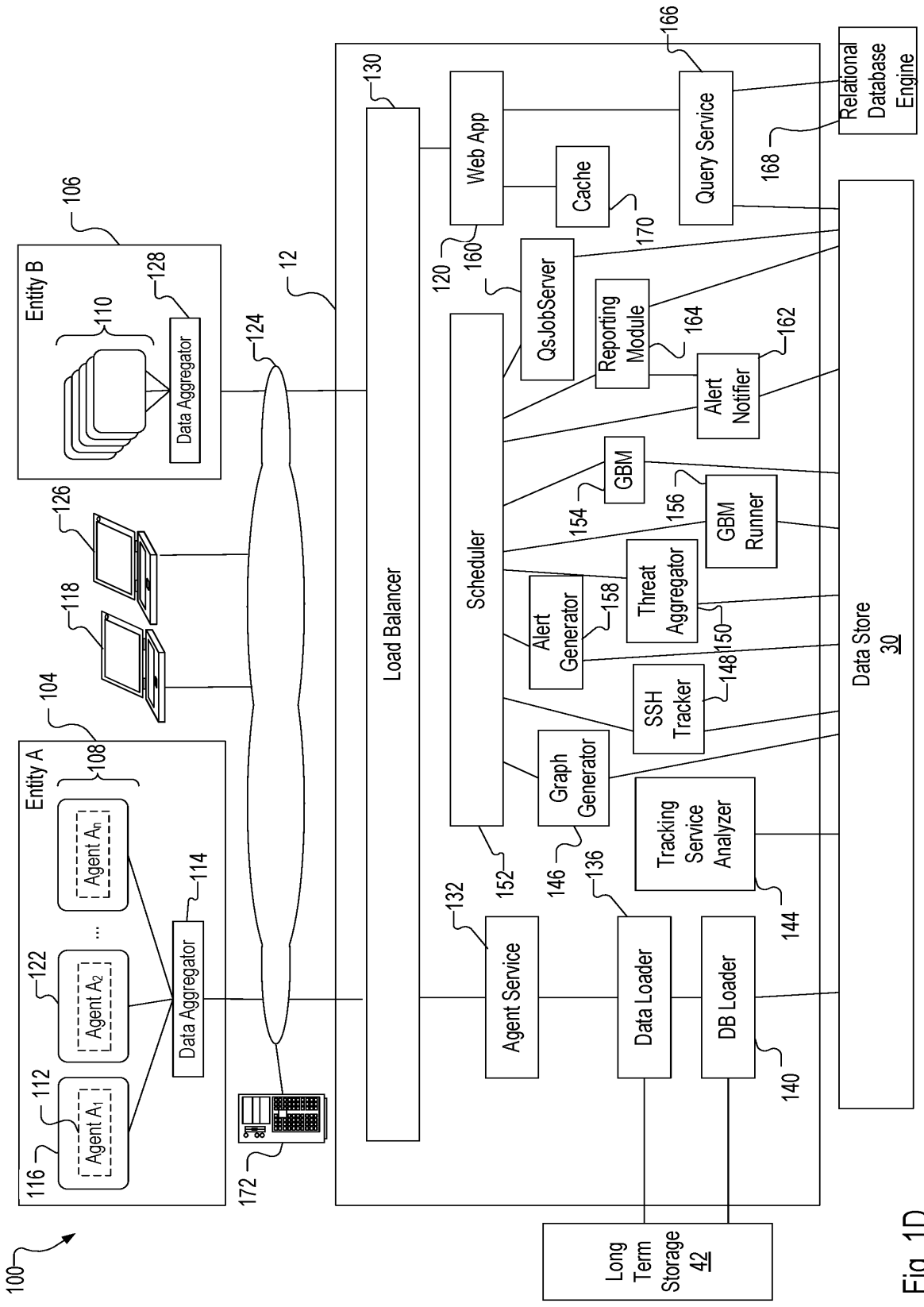

100
Entity A
104
108
Agent A_n
Agent A_2
Agent A_1
112
122
116
114
Data Aggregator
Entity B
106
110
128
Data Aggregator
126
118
172
12
124
Load Balancer
130
Web App
Cache
Query Service
166
Relational Database Engine
168
170
120
160
QsJobServer
Reporting Module
164
Alert Notifier
162
Scheduler
GBM
154
GBM Runner
156
Alert Generator
158
Threat Aggregator
150
SSH Tracker
148
Graph Generator
146
Tracking Service Analyzer
144
152
132
136
Agent Service
Data Loader
DB Loader
140
Data Store
30
Long Term Storage
42

Fig. 1D

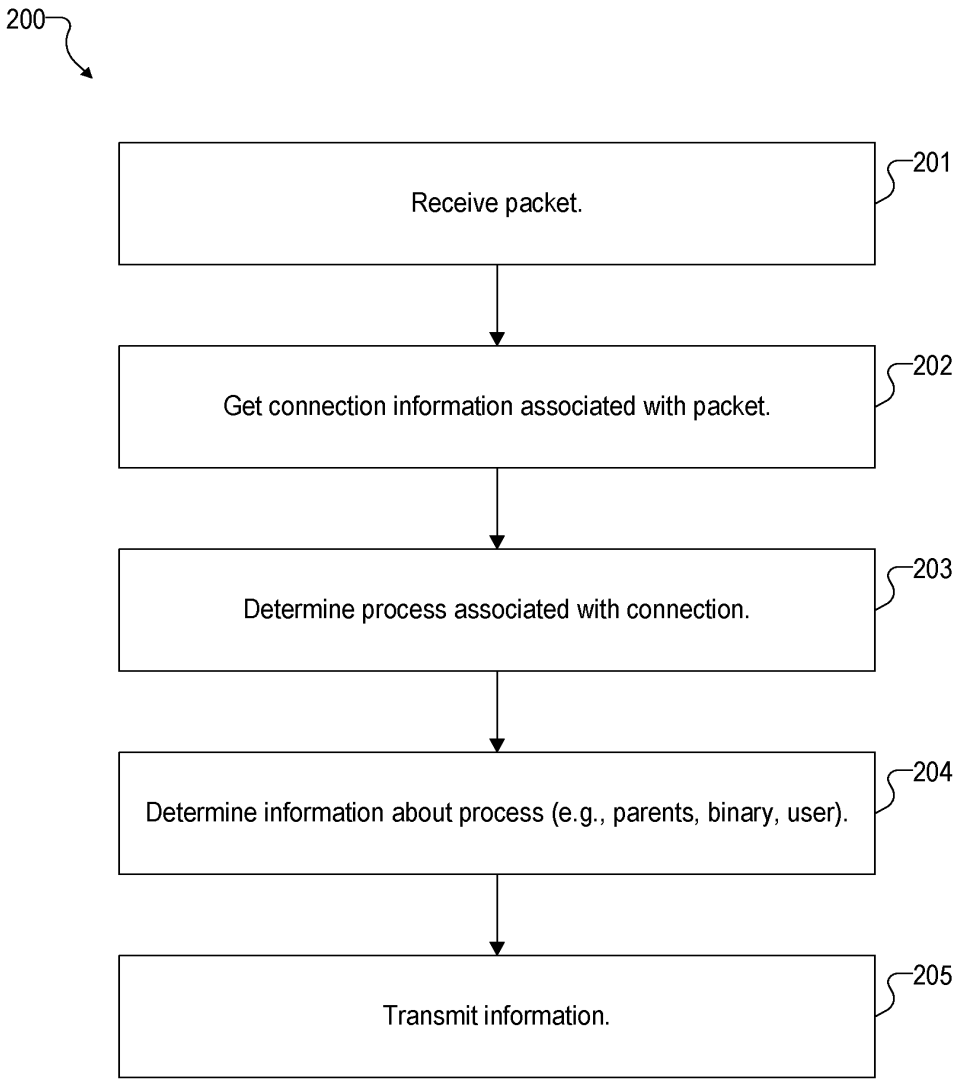

200
Receive packet.
201
Get connection information associated with packet.
202
Determine process associated with connection.
203
Determine information about process (e.g., parents, binary, user).
204
Transmit information.
205

Fig. 2A

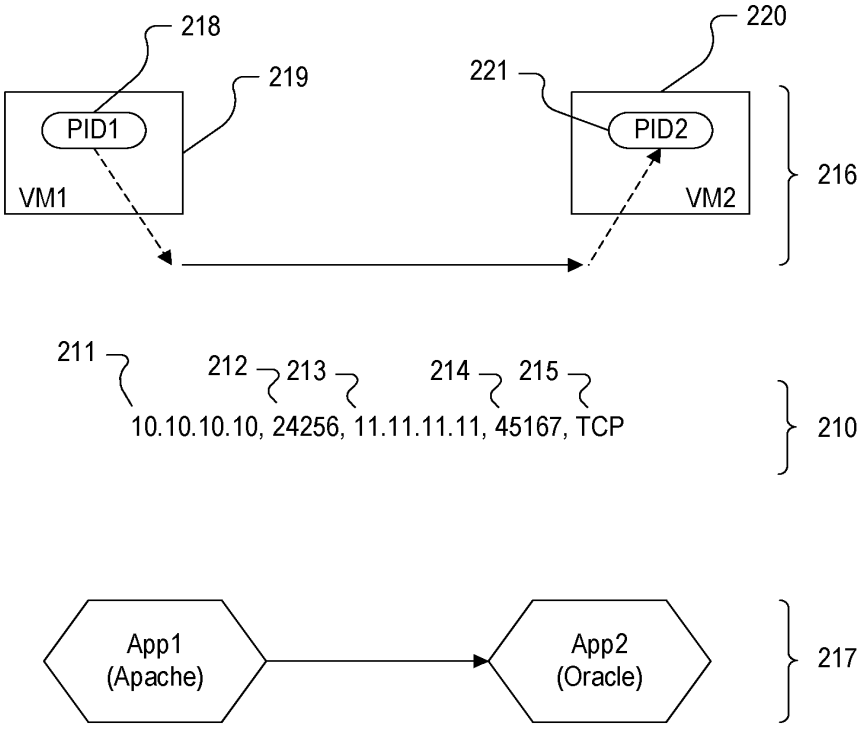

218
219
220
221
PID1
PID2
VM1
VM2
216
211
212
213
214
215
10.10.10.10, 24256, 11.11.11.11, 45167, TCP
210
App1
(Apache)
App2
(Oracle)
217

Fig. 2B

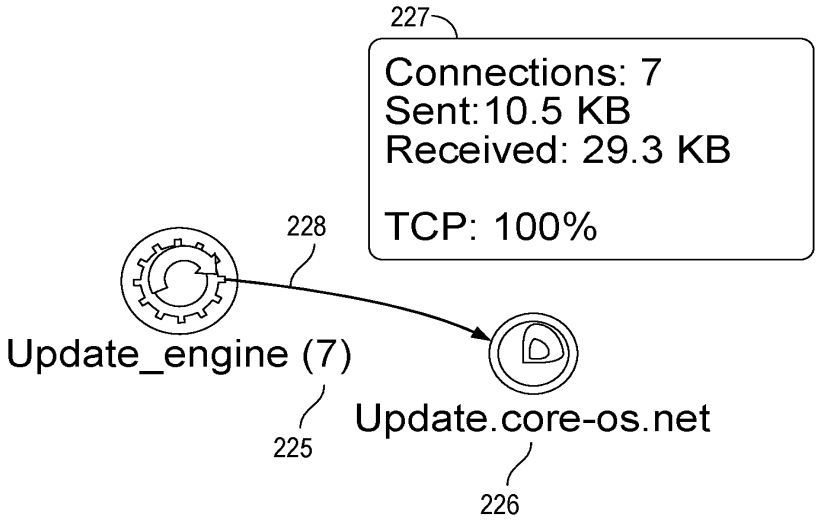

227
Connections: 7
Sent:10.5 KB
Received: 29.3 KB
TCP: 100%
228
Update_engine (7)
225
Update.core-os.net
226

Fig. 2C

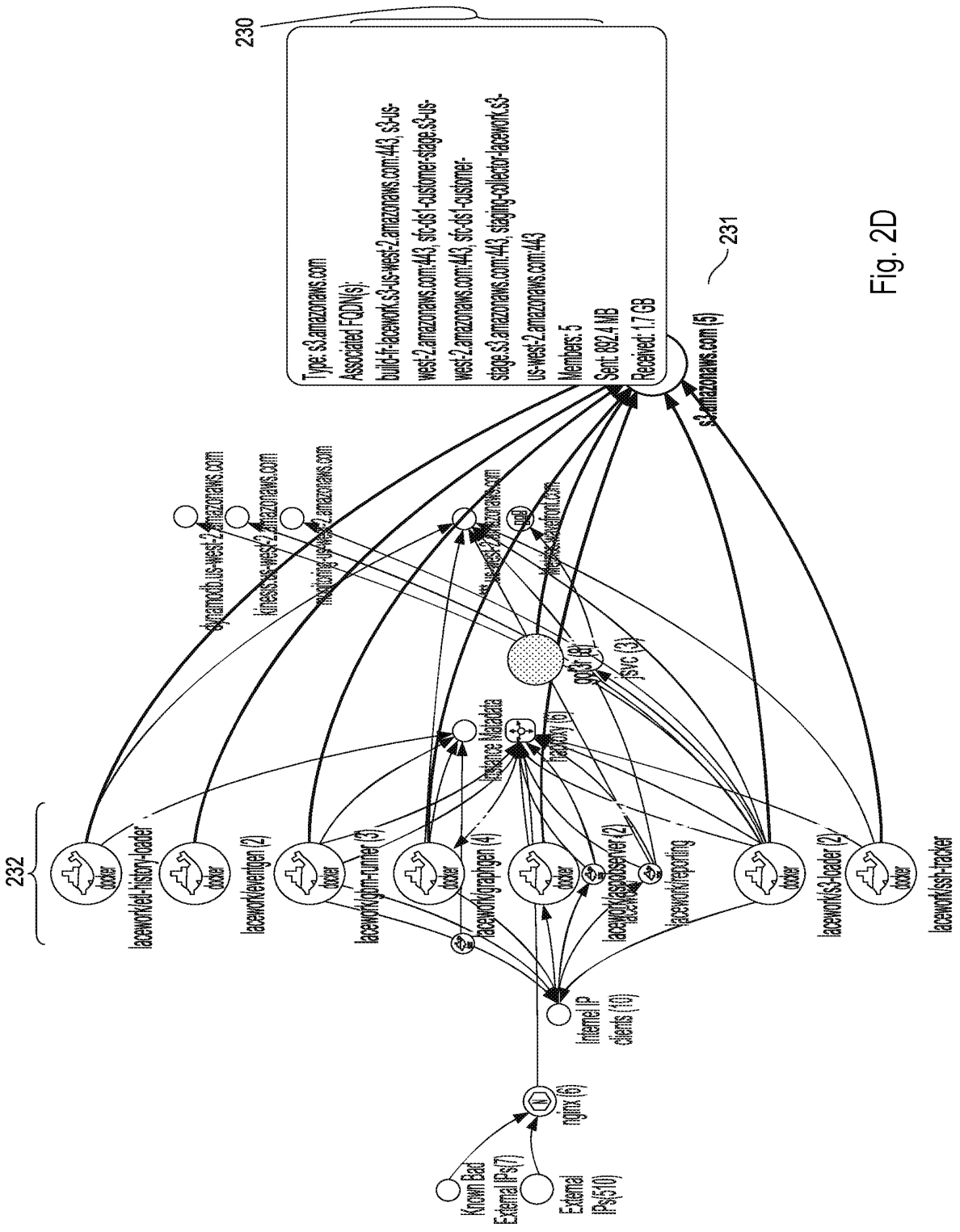

230
Type: s3.amazonaws.com
Associated FQDN(s):
build-fr-lacework.s3-us-west-2.amazonaws.com:443, s3-us-west-2.amazonaws.com:443, stc-ds1-customer-stage.s3-us-west-2.amazonaws.com:443, stc-ds1-customer-stage.s3.amazonaws.com:443, staging-collector-lacework.s3-us-west-2.amazonaws.com:443
Members: 5
Sent: 892.4 MB
Received: 1.7 GB
231
s3.amazonaws.com (5)
232
docker
lacework/ecs-task-history-loader
lacework/eventtugen (2)
lacework/qdm-runner (3)
lacework/graphtugen (4)
lacework/reporting
lacework/s3-loader (2)
lacework/ssh-tracker
dynamodb.us-west-2.amazonaws.com
kinesis.us-west-2.amazonaws.com
monitoring.us-west-2.amazonaws.com
sts.us-west-2.amazonaws.com
kinesis.us-west-2.amazonaws.com
cloudfront.com
instance Metadata
registry (5)
443 (8)
dns (3)
nginx (6)
Known Bad External IPs (7)
External IPs (510)
Internal IP clients (10)

Fig. 2D

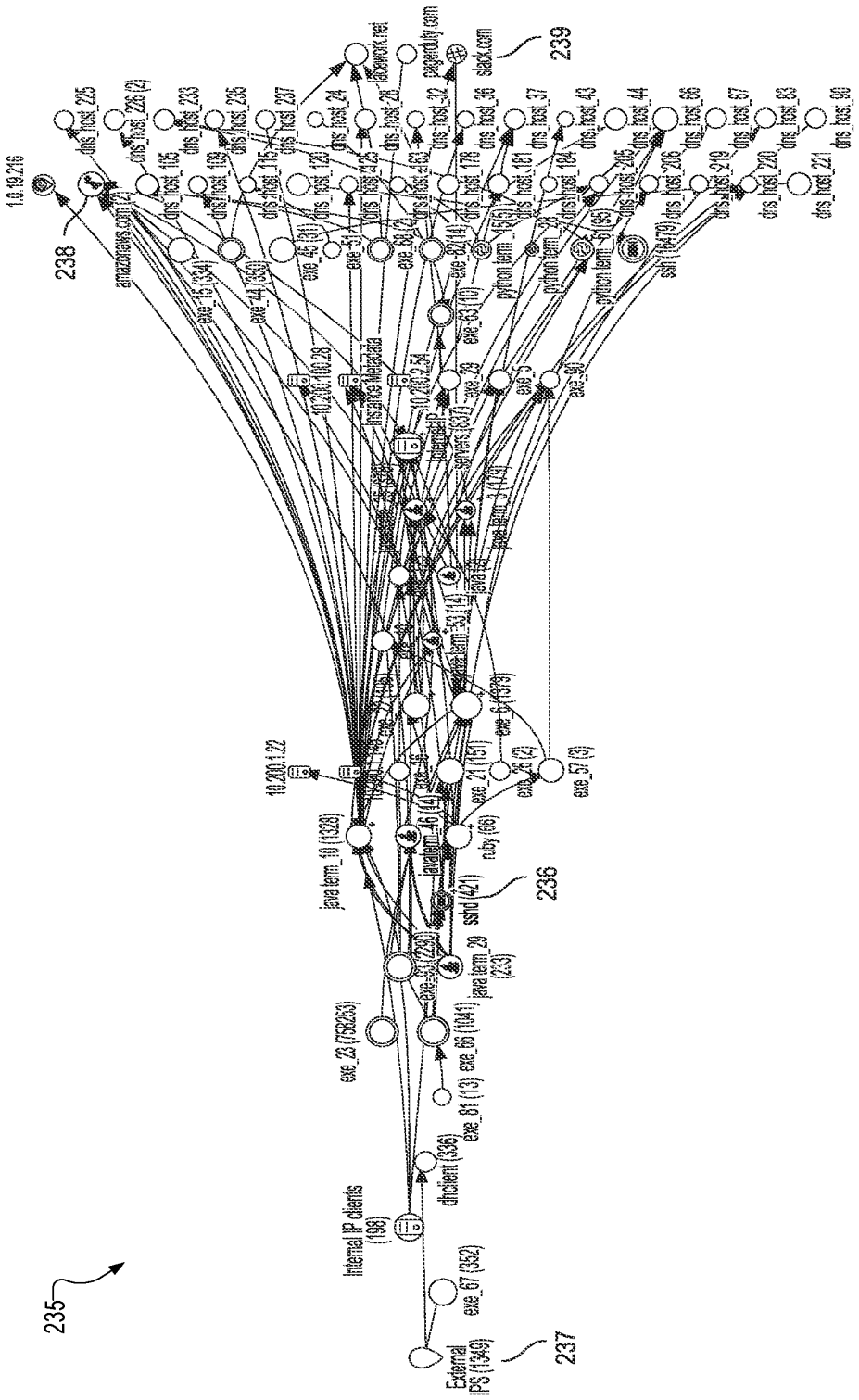

235
238
239
236
237
internal IP clients (196)
External IPS (1349)
dhclient (336)
sshd (421)
ruby (66)
java term_10 (1328)
java term_29 (233)
exe_67 (3521)
exe_23 (750253)
exe_66 (1041)
exe_61 (13)
exe_21 (157)
exe_26 (2)
exe_57 (3)
exe_64 (1078)
10.200.1.22
python term_51 (157)
ssh (164178)
slack.com
pagerduty.com
amazonaws.com (2)

Fig. 2E

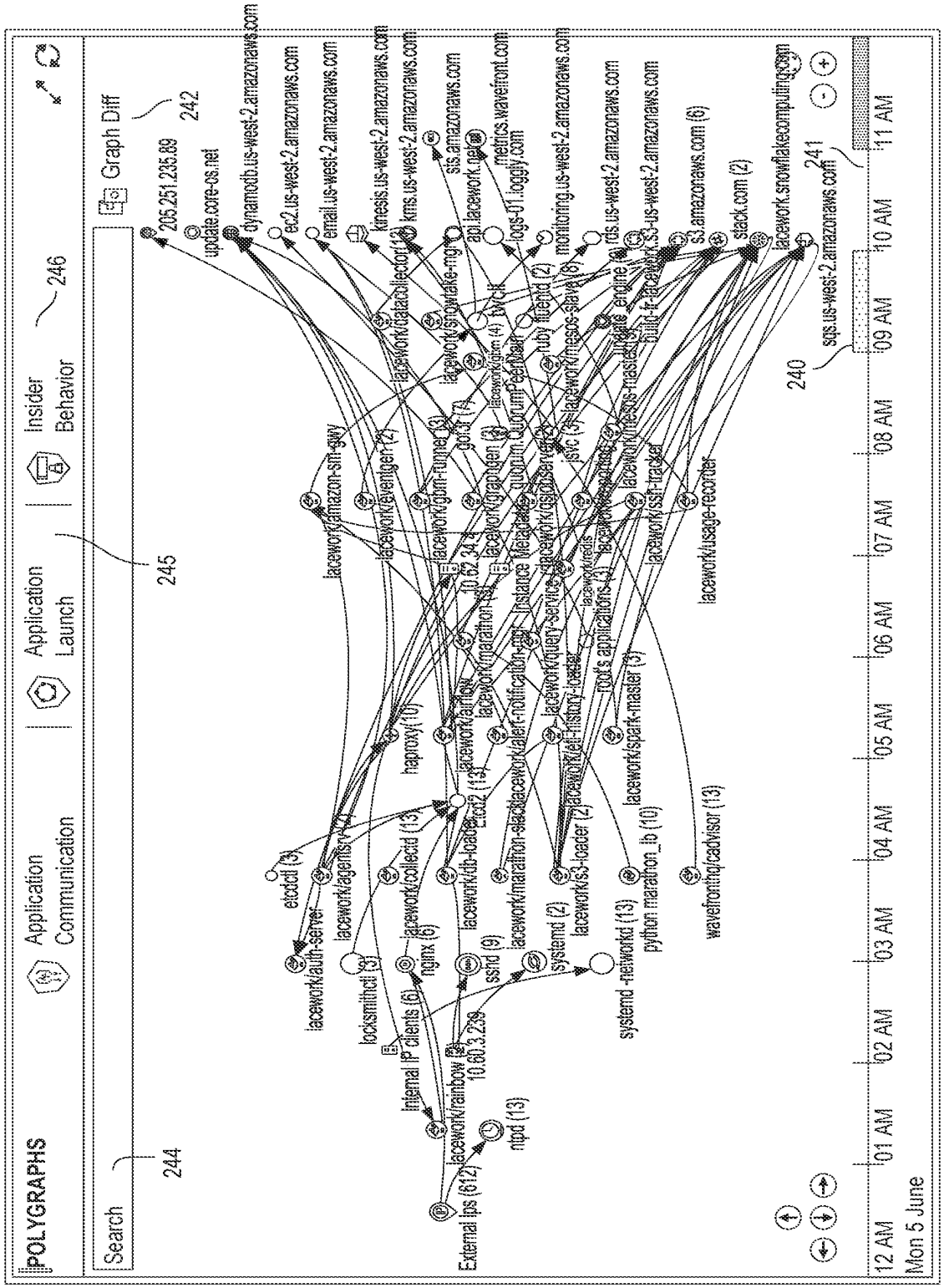

POLYGRAPHS
Application Communication
Application Launch
Insider Behavior
246
Graph Diff
242
Search
244
245
205.251.235.89
update.core-os.net
dynamodb.us-west-2.amazonaws.com
ec2.us-west-2.amazonaws.com
email.us-west-2.amazonaws.com
kinesis.us-west-2.amazonaws.com
kms.us-west-2.amazonaws.com
sts.amazonaws.com
api.lacework.net
metrics.wavefront.com
logs-01.loggly.com
monitoring.us-west-2.amazonaws.com
rds.us-west-2.amazonaws.com
s3.us-west-2.amazonaws.com
s3.amazonaws.com (6)
slack.com (2)
lacework.snowflakecomputing.com
sqs.us-west-2.amazonaws.com
241
240
lacework/amazon-sn-guy
lacework/kevenigen (12)
lacework/datacollector (10)
lacework/snowflake-mgr
lacework/cdm (4)
lacework/cdm-runner (13)
golib (7)
lacework/graphgen (4)
lacework/quorum-sidecar
ruby fluentd (2)
lacework/mesos-slave (6)
lacework/mesos-master (3)
lacework/spark-master (3)
lacework/usage-recorder
lacework/ssh-tracker
lacework/auth-server
lacework/agentsvr (4)
lacework/collectd (13)
haproxy (10)
lacework/marathon-lb
lacework/db-loader
etcd2 (11)
lacework/marathon-sec
lacework/alert-notification-mgr
lacework/query-service
lacework/osconfig
lacework/redis
lacework/alert-history-loader
lacework/s3-loader (2)
root's applications (3)
python marathon_lb (10)
wavefront/cadvisor (13)
etcdctl (3)
locksmithctl (3)
nginx (6)
sshd (9)
systemd (2)
systemd -networkd (13)
ntpd (13)
Internal IP clients (6)
External ips (612)
10.60.3.239
10.62.34.4
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM
12 AM
Mon 5 June

Fig. 2F

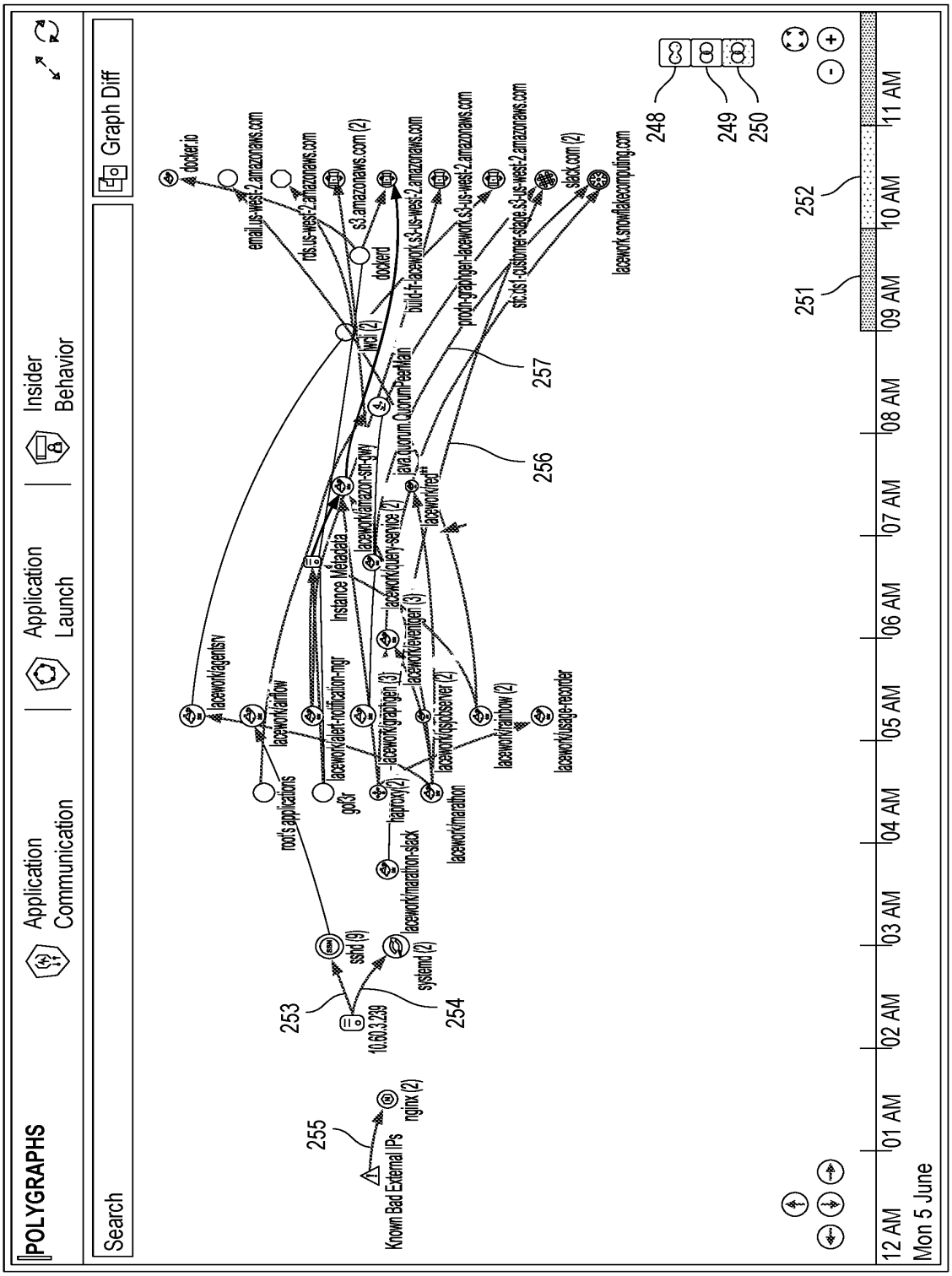

POLYGRAPHS
Application Communication
Application Launch
Insider Behavior
Search
Graph Diff
docker.io
email.us-west-2.amazonaws.com
rds.us-west-2.amazonaws.com
s3.amazonaws.com (2)
dockerd
build-tf-lacework.s3-us-west-2.amazonaws.com
prodn-graphgen-lacework.s3-us-west-2.amazonaws.com
stc.cbt-customer-stage.s3-us-west-2.amazonaws.com
slack.com (2)
lacework.snowflakecomputing.com
lacework/agentsrv
lacework/airflow
lacework/alert-notification-mgr
lacework/amazon-stir-gw
lacework/graphgen (3)
lacework/marathon
lacework/rainbow (2)
lacework/usage-recorder
root's applications
got3r
haproxy (2)
lacework/marathon-slack
lacework/qsglobserver (2)
lacework/rainbow (2)
Instance Metadata
lacework/query-service (2)
lacework/reg*
java.quorum.QuorumPeerMain
wcd (2)
sshd (9)
systemd (2)
10.60.3.239
Known Bad External IPs
nginx (2)
253
254
255
256
257
248
249
250
251
252
12 AM
Mon 5 June
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM

Fig. 2G

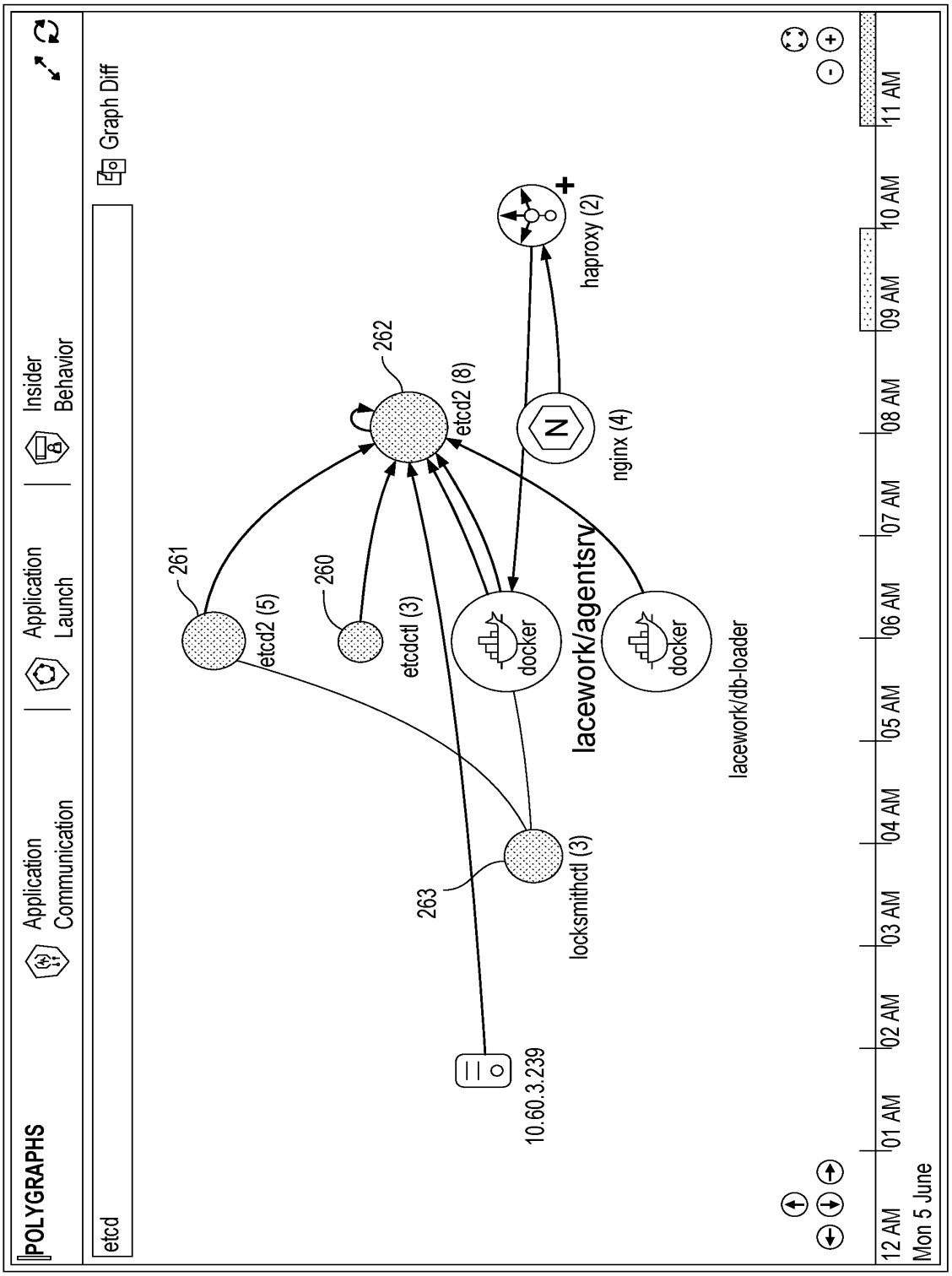

POLYGRAPHS
Application Communication
Application Launch
Insider Behavior
Graph Diff
etcd
261
etcd2 (5)
260
etcdctl (3)
262
etcd2 (8)
haproxy (2)
nginx (4)
docker
docker
lacework/agentsrv
lacework/db-loader
263
locksmithctl (3)
10.60.3.239
12 AM
Mon 5 June
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM

Fig. 2H

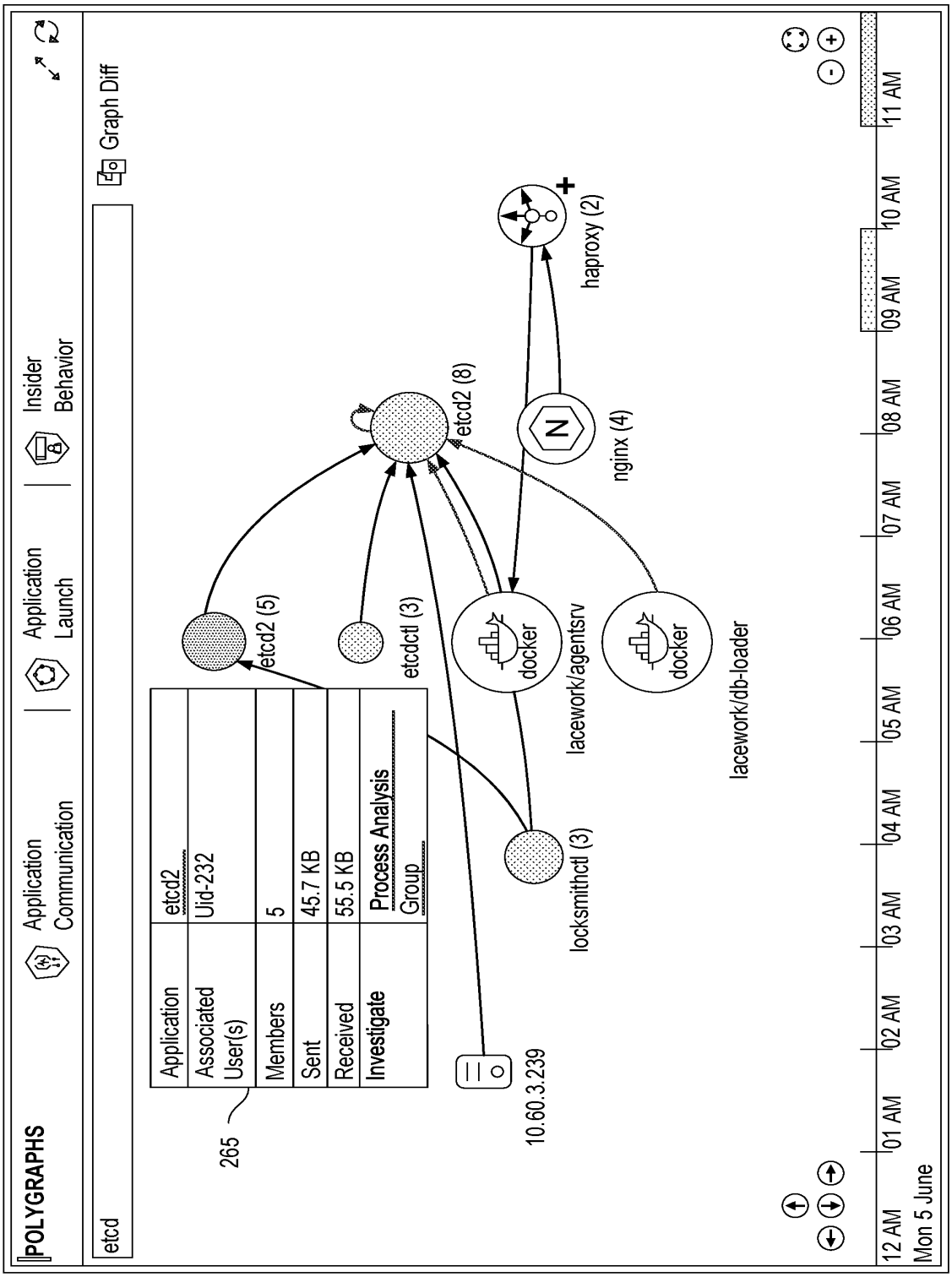

POLYGRAPHS
Application Communication
Application Launch
Insider Behavior
Graph Diff
etcd
Application
Associated User(s)
Members
Sent
Received
Investigate
etcd2
Uid-232
5
45.7 KB
55.5 KB
Process Analysis
Group
265
etcd2 (5)
etcdctl (3)
etcd2 (8)
haproxy (2)
nginx (4)
docker
docker
lacework/agentsrv
lacework/db-loader
locksmithctl (3)
10.60.3.239
12 AM
Mon 5 June
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM

Fig. 2I

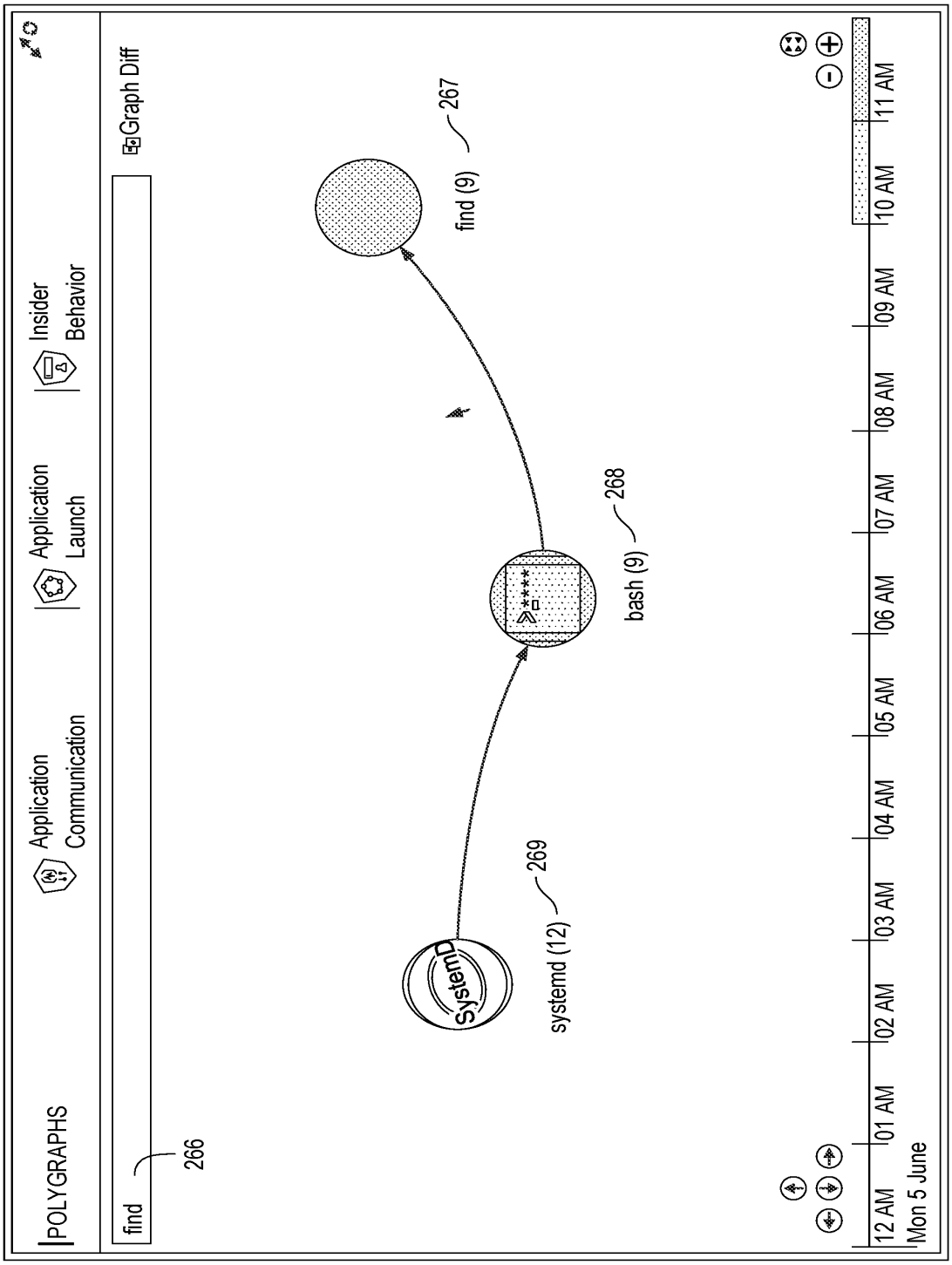

POLYGRAPHS
Application Communication
Application Launch
Insider Behavior
Graph Diff
find
266
267
find (9)
268
bash (9)
269
systemd (12)
12 AM
Mon 5 June
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM

Fig. 2J

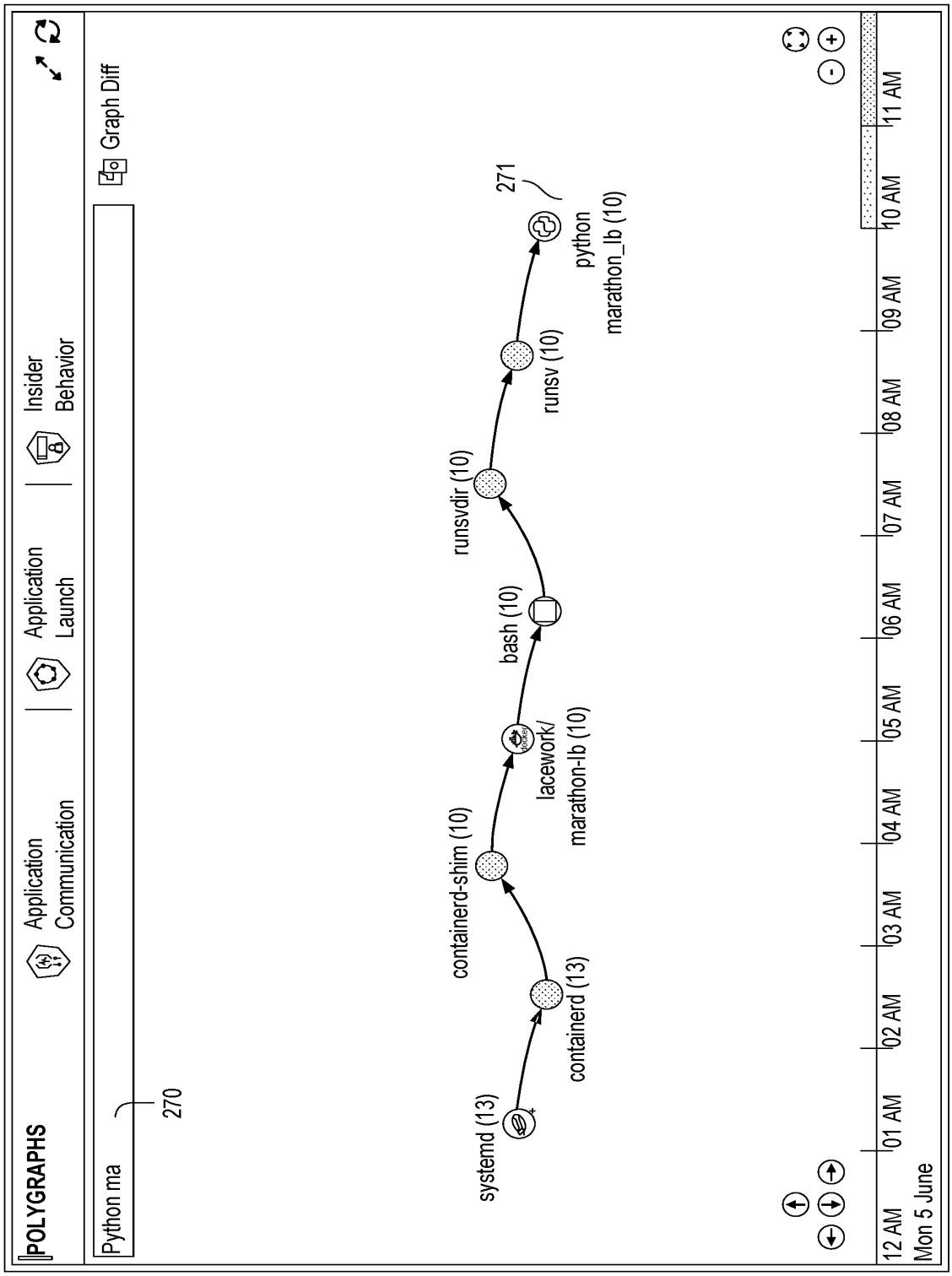

POLYGRAPHS
Application Communication
Application Launch
Insider Behavior
Graph Diff
Python ma
270
systemd (13)
containerd (13)
containerd-shim (10)
lacework/ marathon-lb (10)
bash (10)
runsvdir (10)
runsv (10)
271
python marathon_lb (10)
12 AM
Mon 5 June
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM

Fig. 2K

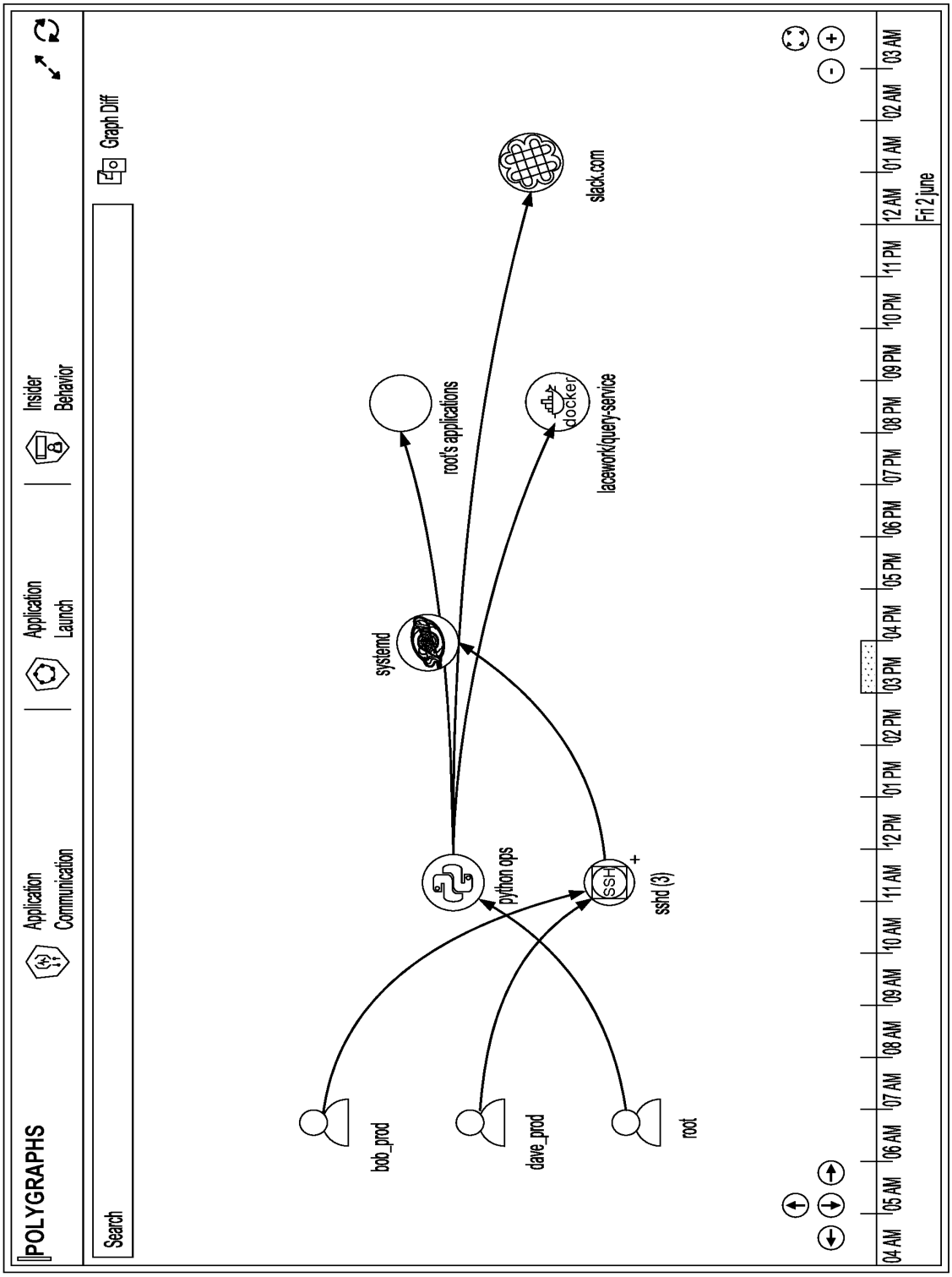

POLYGRAPHS
Application Communication
Application Launch
Insider Behavior
Graph Diff
Search
bob_prod
dave_prod
root
python ops
sshd (3)
systemd
root's applications
docker
lacework/query-service
slack.com
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM
12 PM
01 PM
02 PM
03 PM
04 PM
05 PM
06 PM
07 PM
08 PM
09 PM
10 PM
11 PM
12 AM
Fri 2 june
01 AM
02 AM
03 AM

Fig. 2L

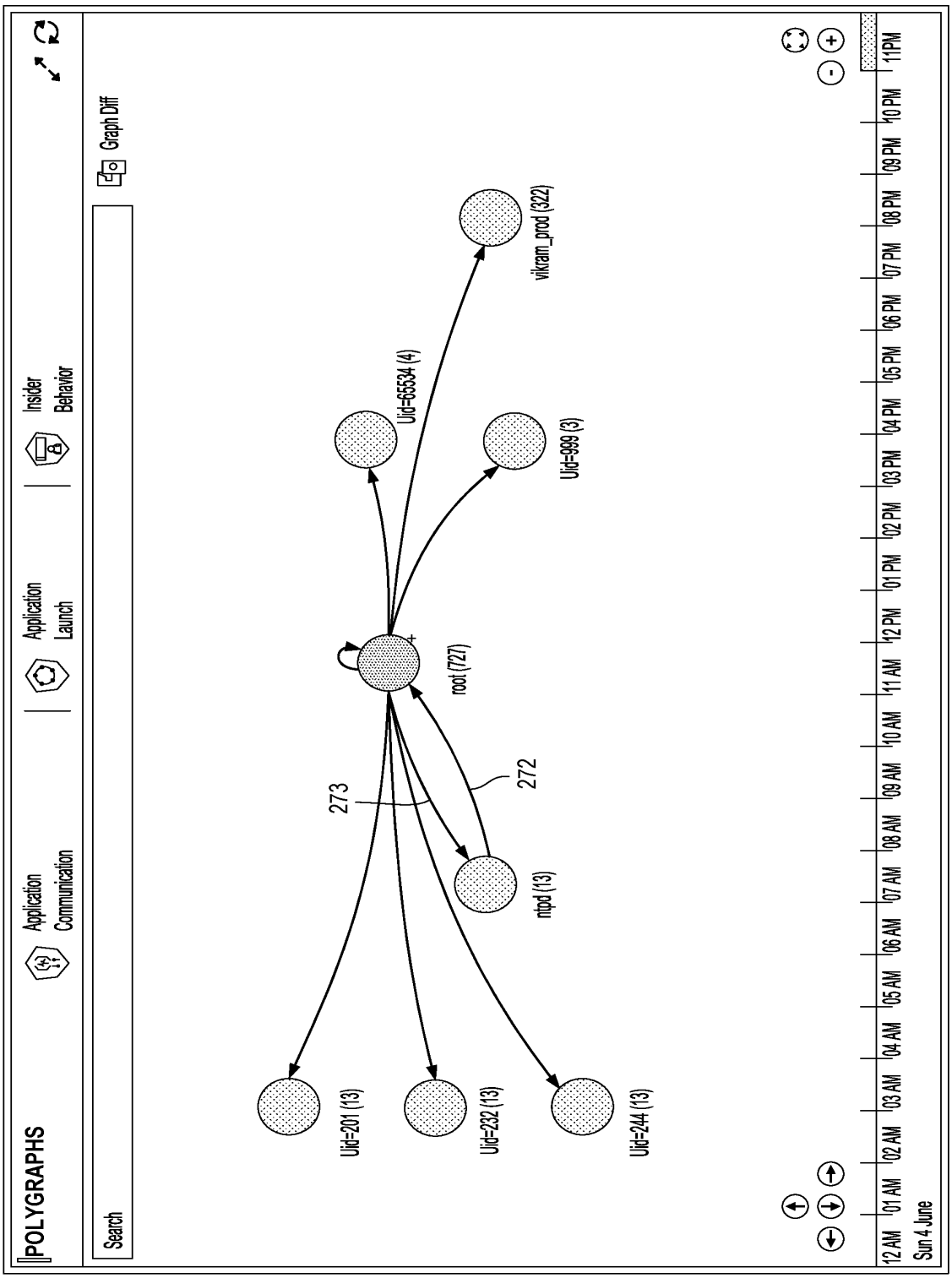

POLYGRAPHS
Application Communication
Application Launch
Insider Behavior
Graph Diff
Search
Uid=201 (13)
Uid=232 (13)
Uid=244 (13)
ntpd (13)
root (727)
Uid=65534 (4)
vikram_prod (322)
Uid=999 (3)
273
272
12 AM
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM
12 PM
01 PM
02 PM
03 PM
04 PM
05 PM
06 PM
07 PM
08 PM
09 PM
10 PM
11PM
Sun 4 June

Fig. 2M

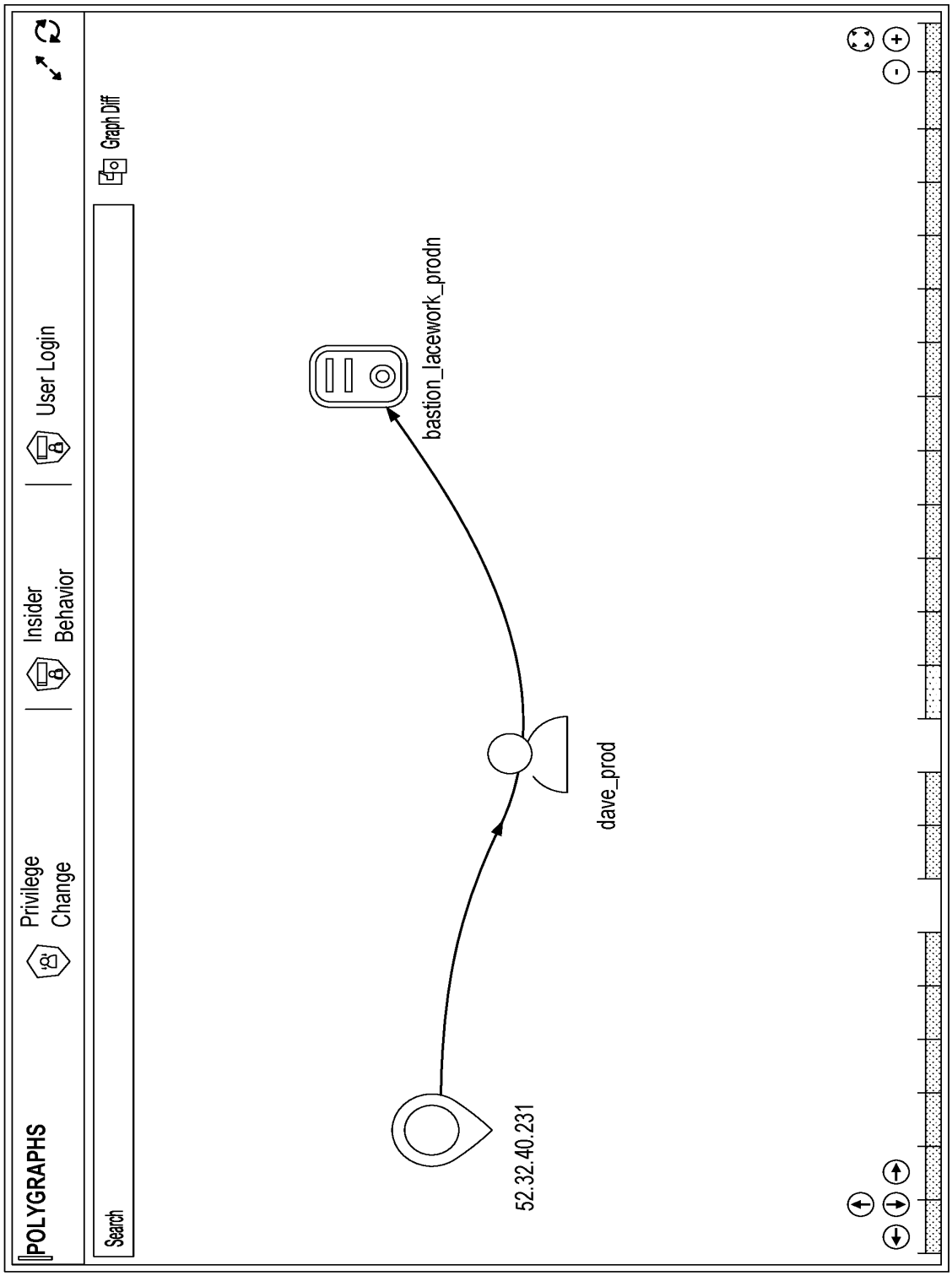

POLYGRAPHS
Privilege Change
Insider Behavior
User Login
Search
Graph Diff
bastion_lacework_prodn
dave_prod
52.32.40.231

Fig. 2N

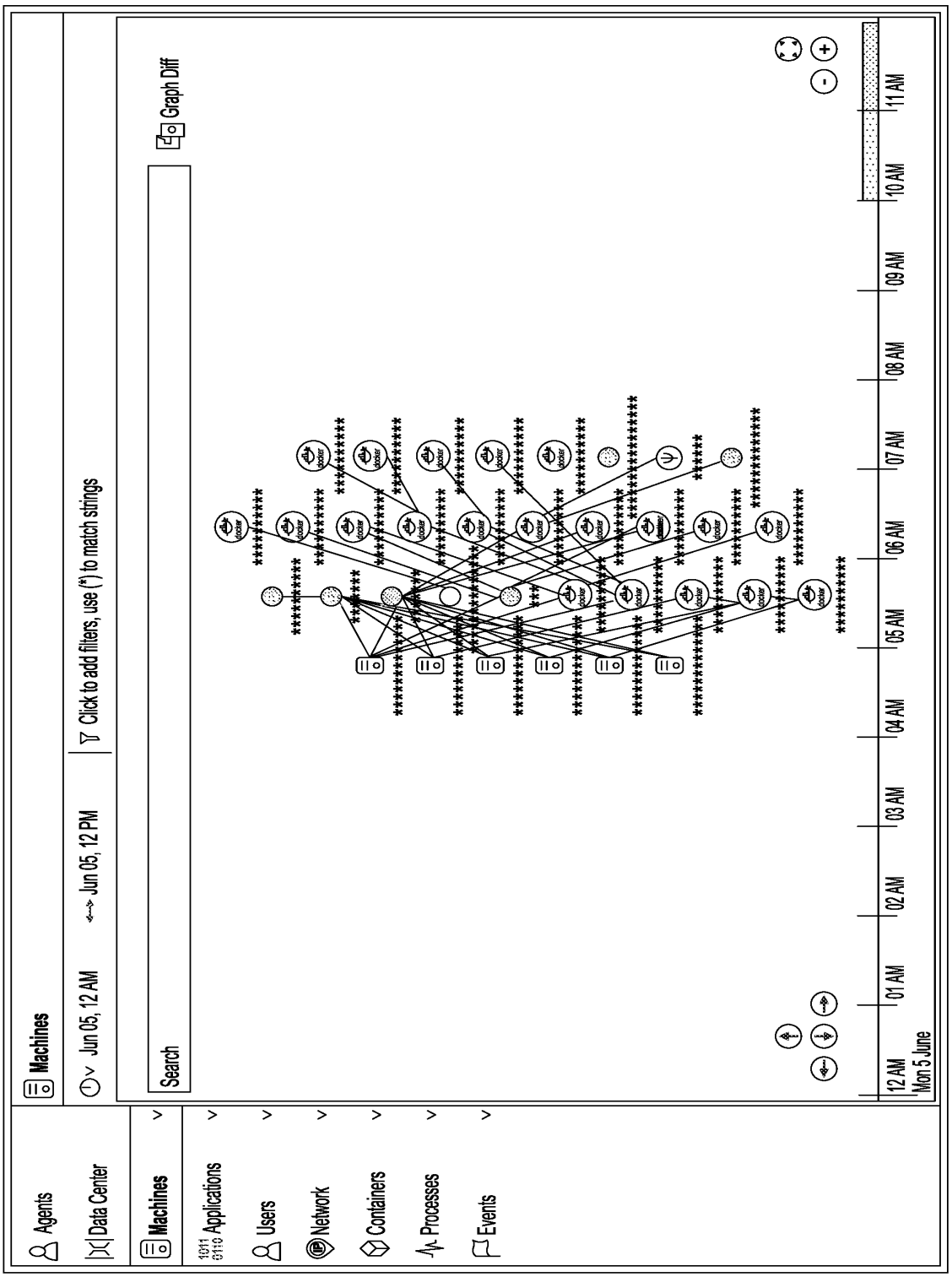

Agents
Data Center
Machines
Applications
Users
Network
Containers
Processes
Events
Machines
Jun 05, 12 AM
Jun 05, 12 PM
Click to add filters, use (*) to match strings
Graph Diff
Search
12 AM
Mon 5 June
01 AM
02 AM
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM

Fig. 20

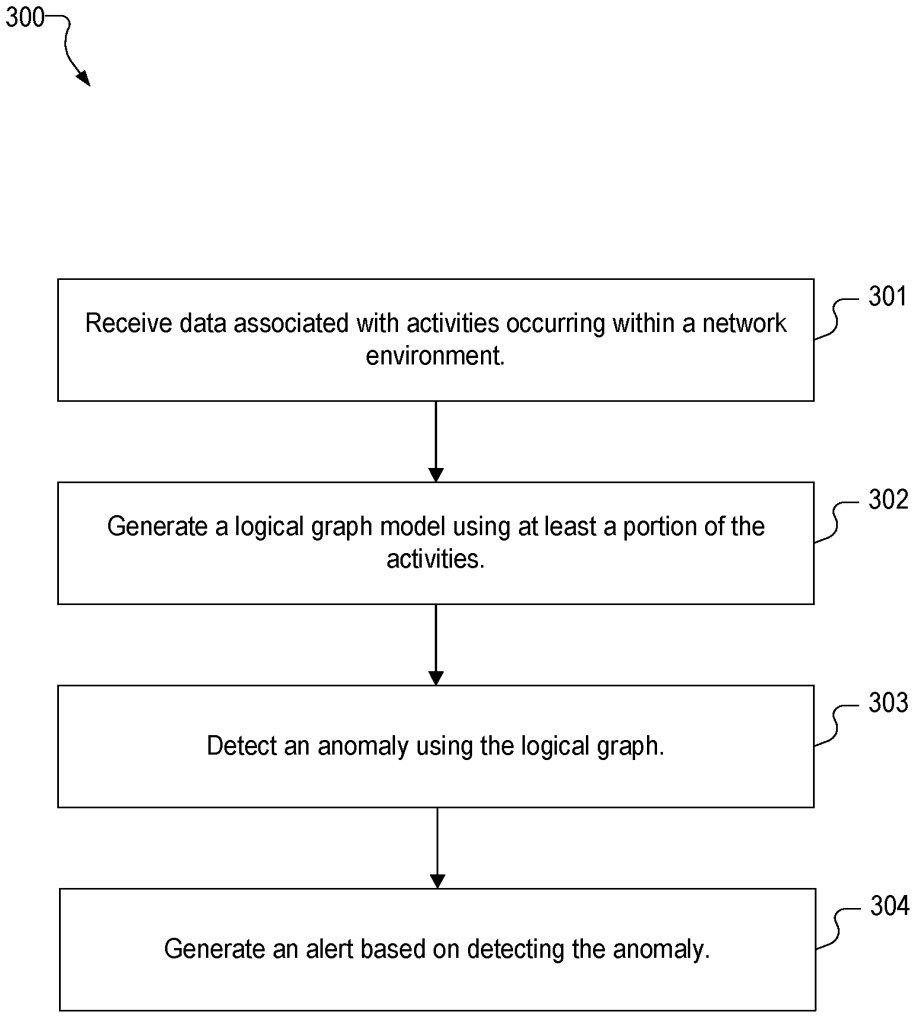

300
Receive data associated with activities occurring within a network environment.
301
Generate a logical graph model using at least a portion of the activities.
302
Detect an anomaly using the logical graph.
303
Generate an alert based on detecting the anomaly.
304

Fig. 3A

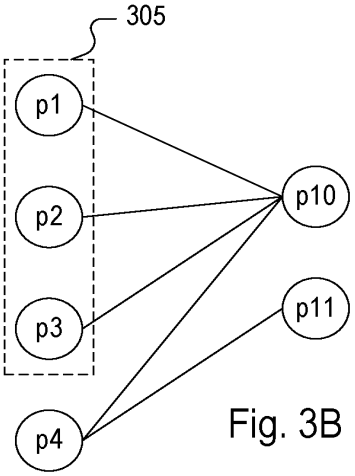


Fig. 3B

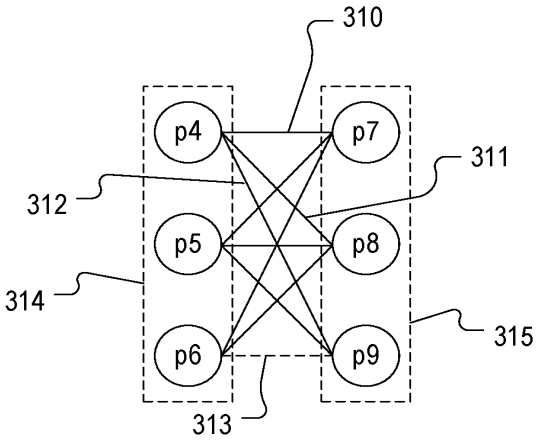


Fig. 3C

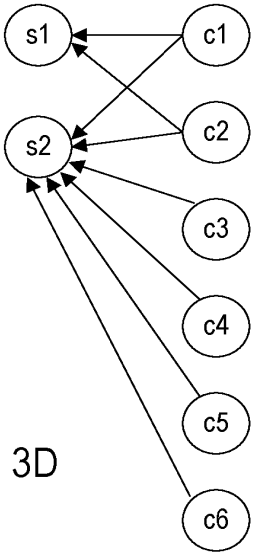


Fig. 3D

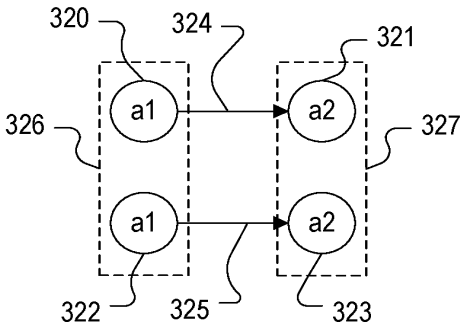


Fig. 3E

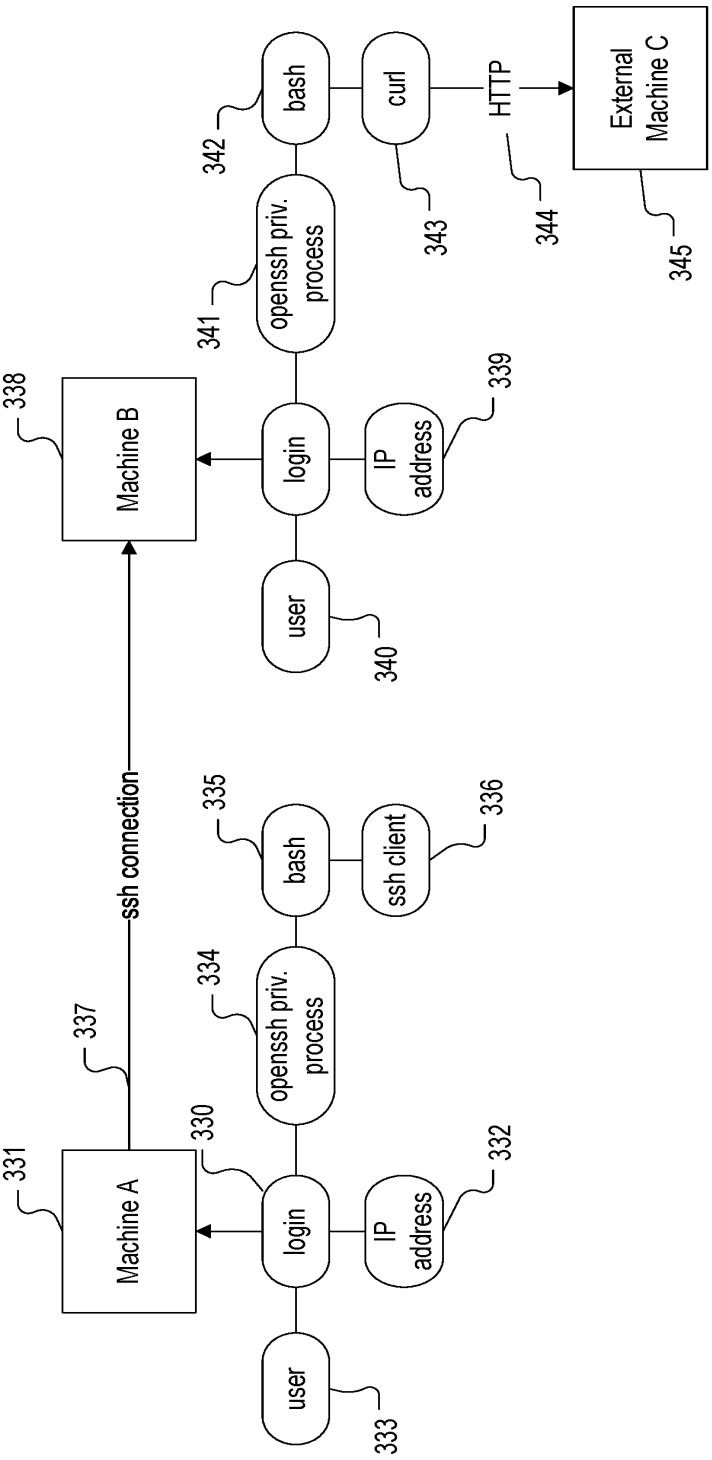

Machine A
331
Machine B
338
ssh connection
337
login
330
IP address
332
user
333
openssh priv. process
334
bash
335
ssh client
336
login
IP address
339
user
340
openssh priv. process
341
bash
342
curl
343
HTTP
344
External Machine C
345

Fig. 3F

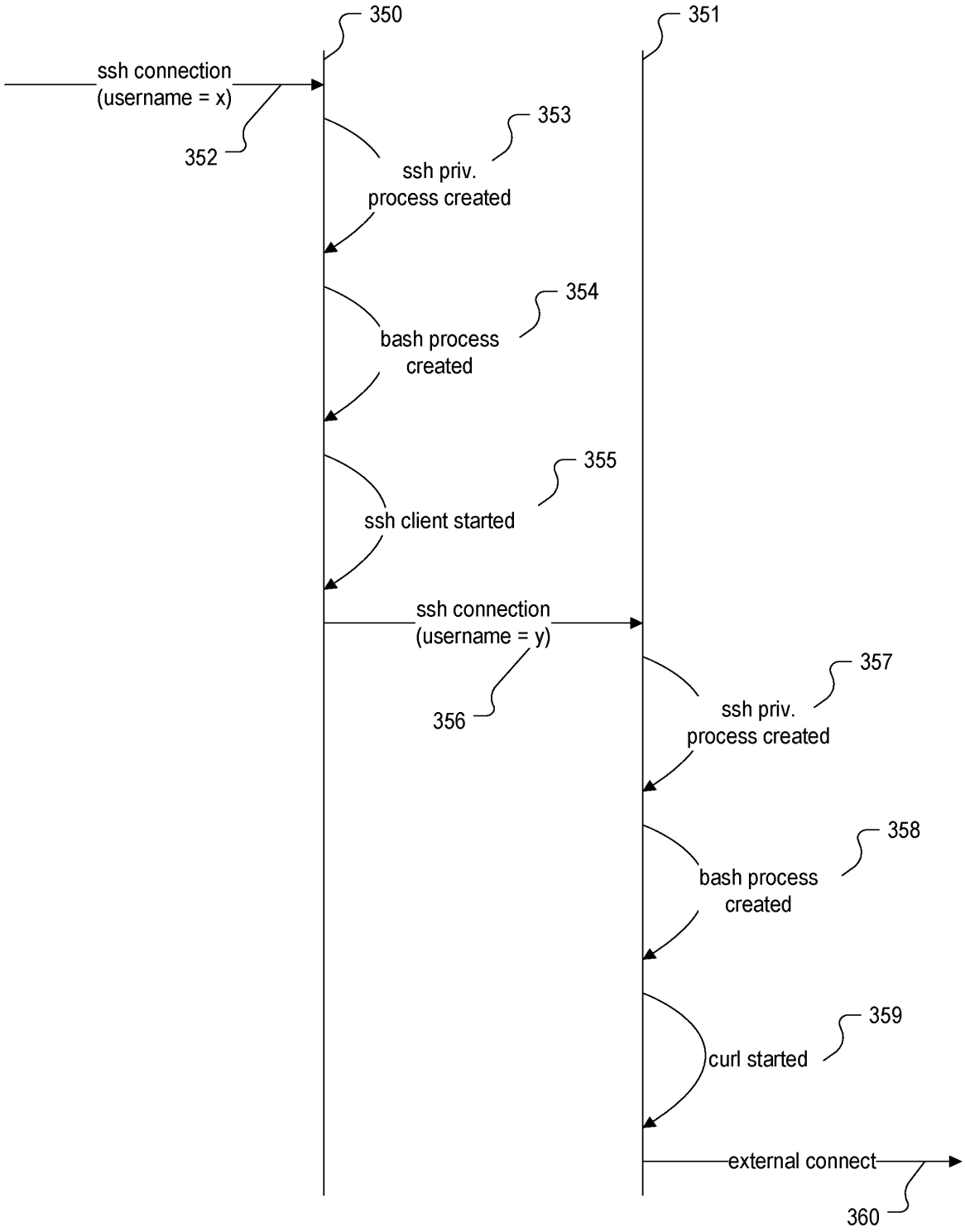

350
351
ssh connection
(username = x)
352
353
ssh priv.
process created
354
bash process
created
355
ssh client started
ssh connection
(username = y)
356
357
ssh priv.
process created
358
bash process
created
359
curl started
external connect
360

Fig. 3G

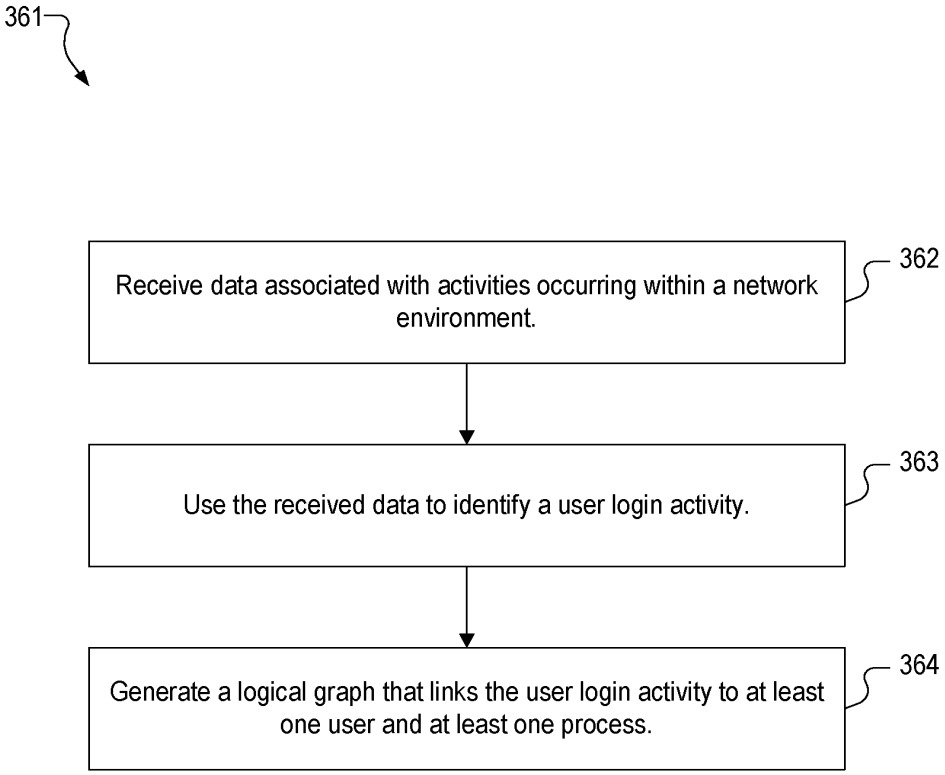

361
Receive data associated with activities occurring within a network environment.
362
Use the received data to identify a user login activity.
363
Generate a logical graph that links the user login activity to at least one user and at least one process.
364

Fig. 3H

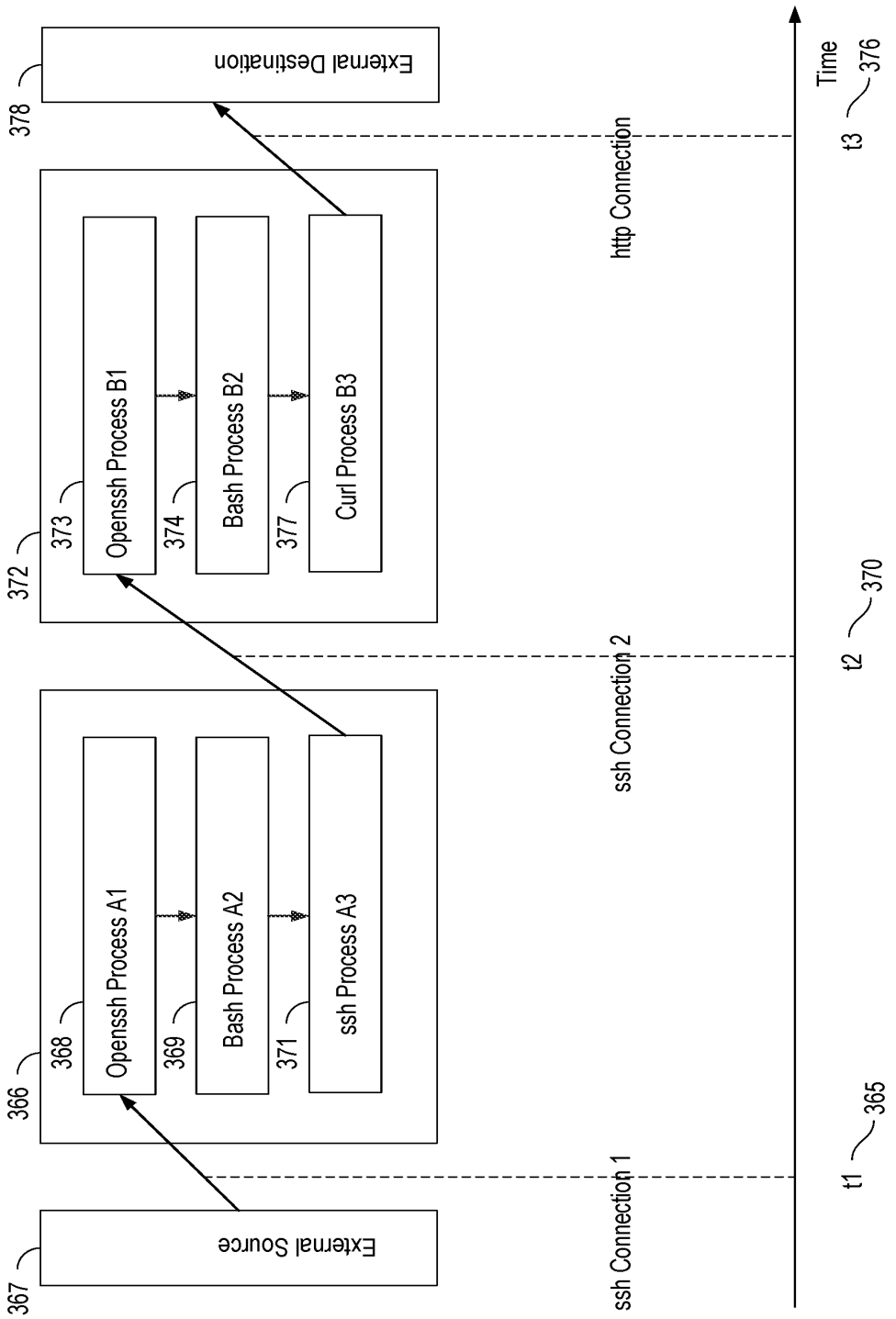

External Source
367
Openssh Process A1
368
Bash Process A2
369
ssh Process A3
371
366
Openssh Process B1
373
Bash Process B2
374
Curl Process B3
377
372
External Destination
378
ssh Connection 1
http Connection
ssh Connection 2
t1
365
t2
370
t3
Time
376

Fig. 3I

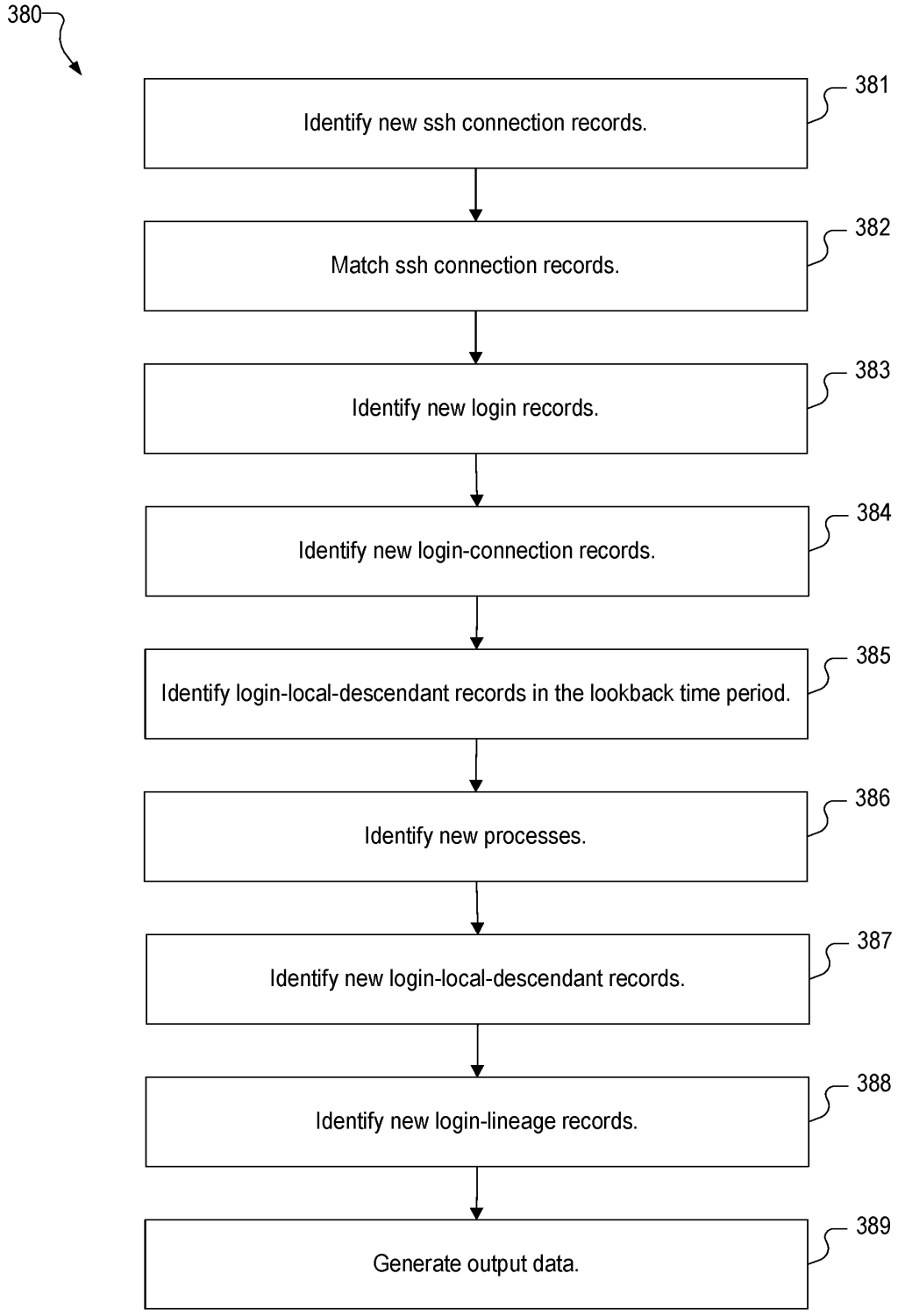

380
Identify new ssh connection records.
381
Match ssh connection records.
382
Identify new login records.
383
Identify new login-connection records.
384
Identify login-local-descendant records in the lookback time period.
385
Identify new processes.
386
Identify new login-local-descendant records.
387
Identify new login-lineage records.
388
Generate output data.
389

Fig. 3J

MID	start_time	PID_hash	src_IP_addr	src_port	dst_IP_addr	dst_port	prot	dir
A	t1	A1	1.1.1.10	10000	2.2.2.20	22	TCP	Incoming
A	t2	A3	2.2.2.20	10001	2.2.2.21	22	TCP	Outgoing
B	t2	B1	2.2.2.20	10001	2.2.2.21	22	TCP	Incoming

390

Fig. 3K

391

src_MID	src_PID_hash	dst_MID	dst_PID_hash	dst_start_time	src_IP_addr	src_port	dst_IP_addr	dst_port
null	null	A	A1	t1	1.1.1.10	10000	2.2.2.20	22
A	A3	B	B1	t2	2.2.2.20	10001	2.2.2.21	22

Fig. 3L

MID	login_time	sshd_PID_hash
A	t1	A1
B	t2	B1

Fig. 3M

MID	sshd_PID_hash	login_time	login_username	src_IP_addr	src_port	dst_IP_addr	dst_port
A	A1	t1	X	1.1.1.10	10000	2.2.2.20	22
B	B1	t2	Y	2.2.2.20	10001	2.2.2.21	22

Fig. 3N

MID	start_time	PID_hash	exe_path	parent_PID_hash
A	t1	A1	/usr/sbin/sshd	A0
A	t1	A2	/bin/bash	A1
A	t2	A3	/usr/bin/ssh	A2
B	t2	B1	/usr/sbin/sshd	B0
B	t2	B2	/bin/bash	B1
B	t3	B3	/usr/bin/curl	B2

Fig. 3O

MID	sshd_PID_hash	PID_hash
A	A1	A1
A	A1	A2
A	A1	A3
B	B1	B1
B	B1	B2
B	B1	B3

Fig. 3P

parent_MID	parent_sshd_PID_hash	child_MID	origin_sshd_PID_hash
A	A1	B	B1

Fig. 3Q

MID	sshd_PID_hash	parent_MID	parent_sshd_PID_hash	origin_MID	origin_sshd_PID_hash
A	A1	null	null	A	A1
B	B1	A	A1	A	A1

Fig. 3R

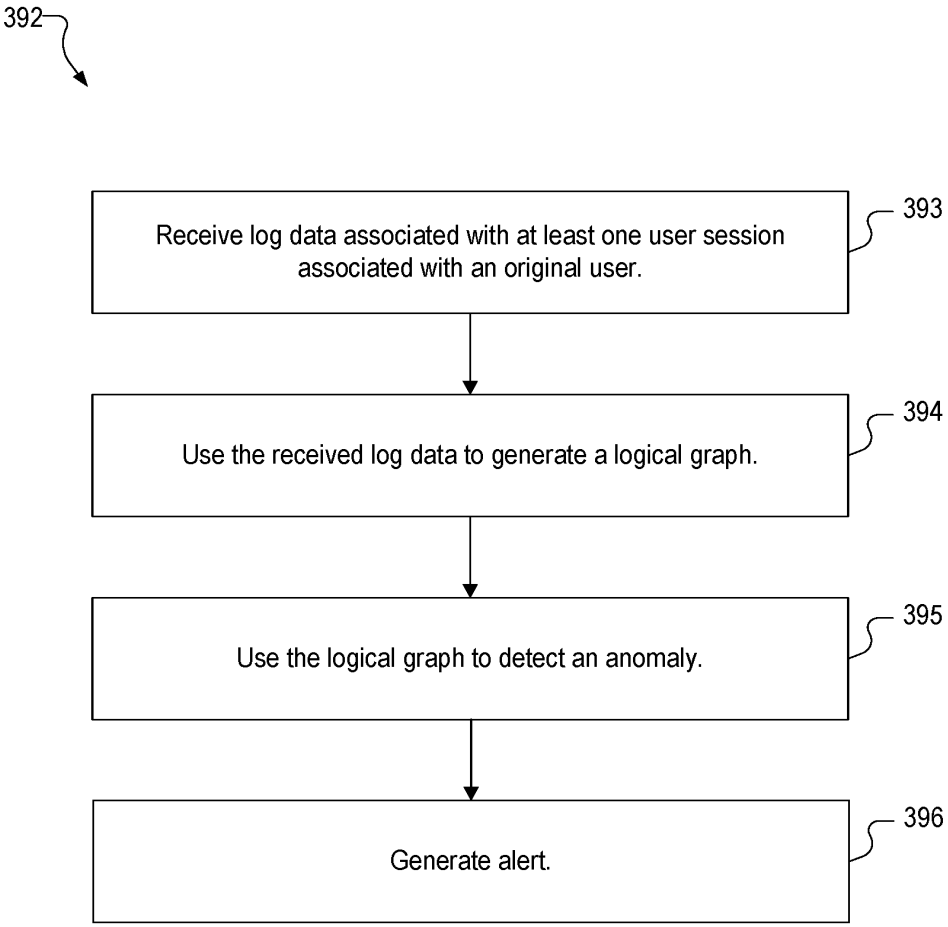

392
Receive log data associated with at least one user session associated with an original user.
393
Use the received log data to generate a logical graph.
394
Use the logical graph to detect an anomaly.
395
Generate alert.
396

Fig. 3S

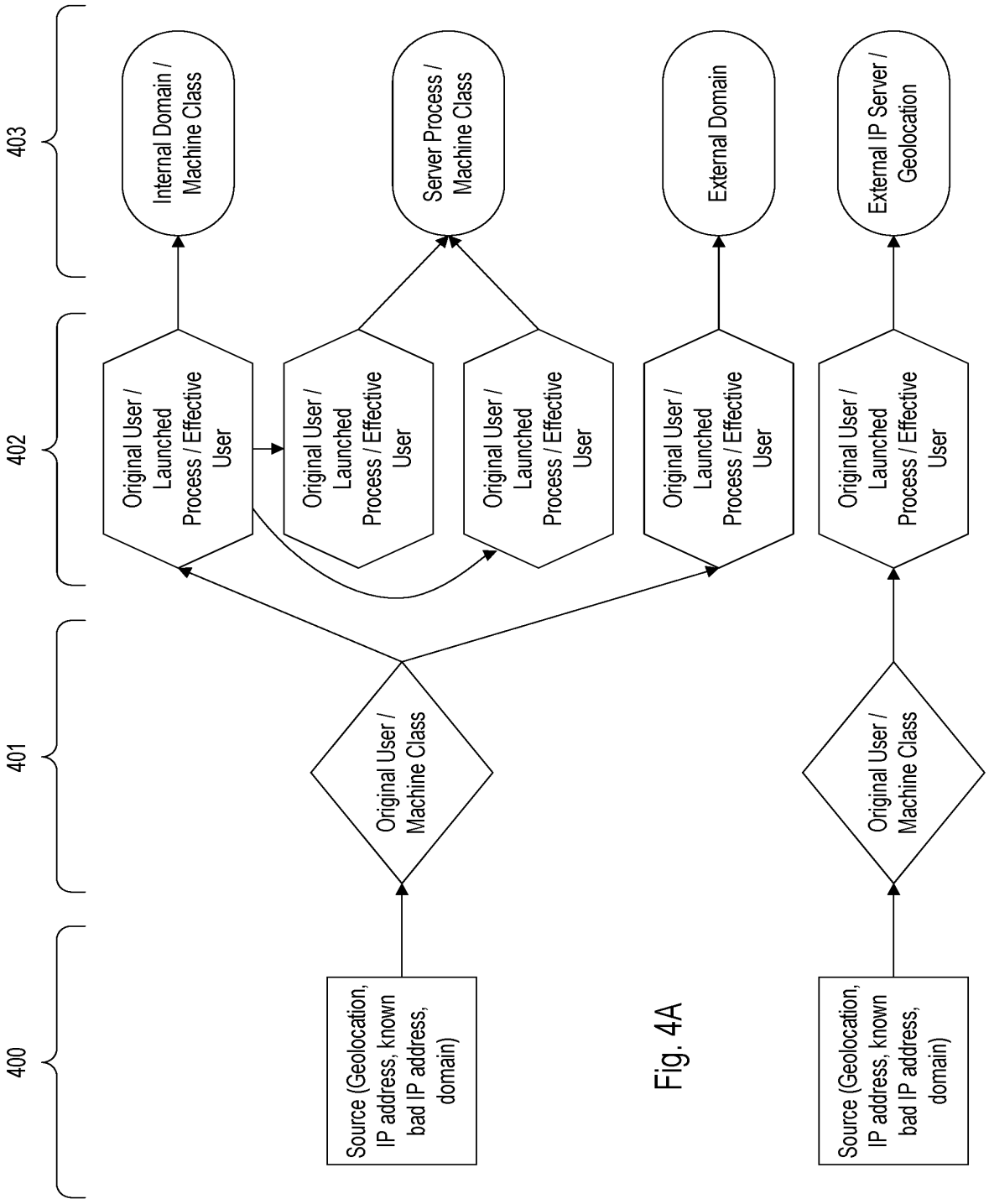

400
401
402
403
Source (Geolocation, IP address, known bad IP address, domain)
Original User / Machine Class
Original User / Launched Process / Effective User
Original User / Launched Process / Effective User
Original User / Launched Process / Effective User
Internal Domain / Machine Class
Server Process / Machine Class
Source (Geolocation, IP address, known bad IP address, domain)
Original User / Machine Class
Original User / Launched Process / Effective User
External Domain
Original User / Launched Process / Effective User
External IP Server / Geolocation

Fig. 4A

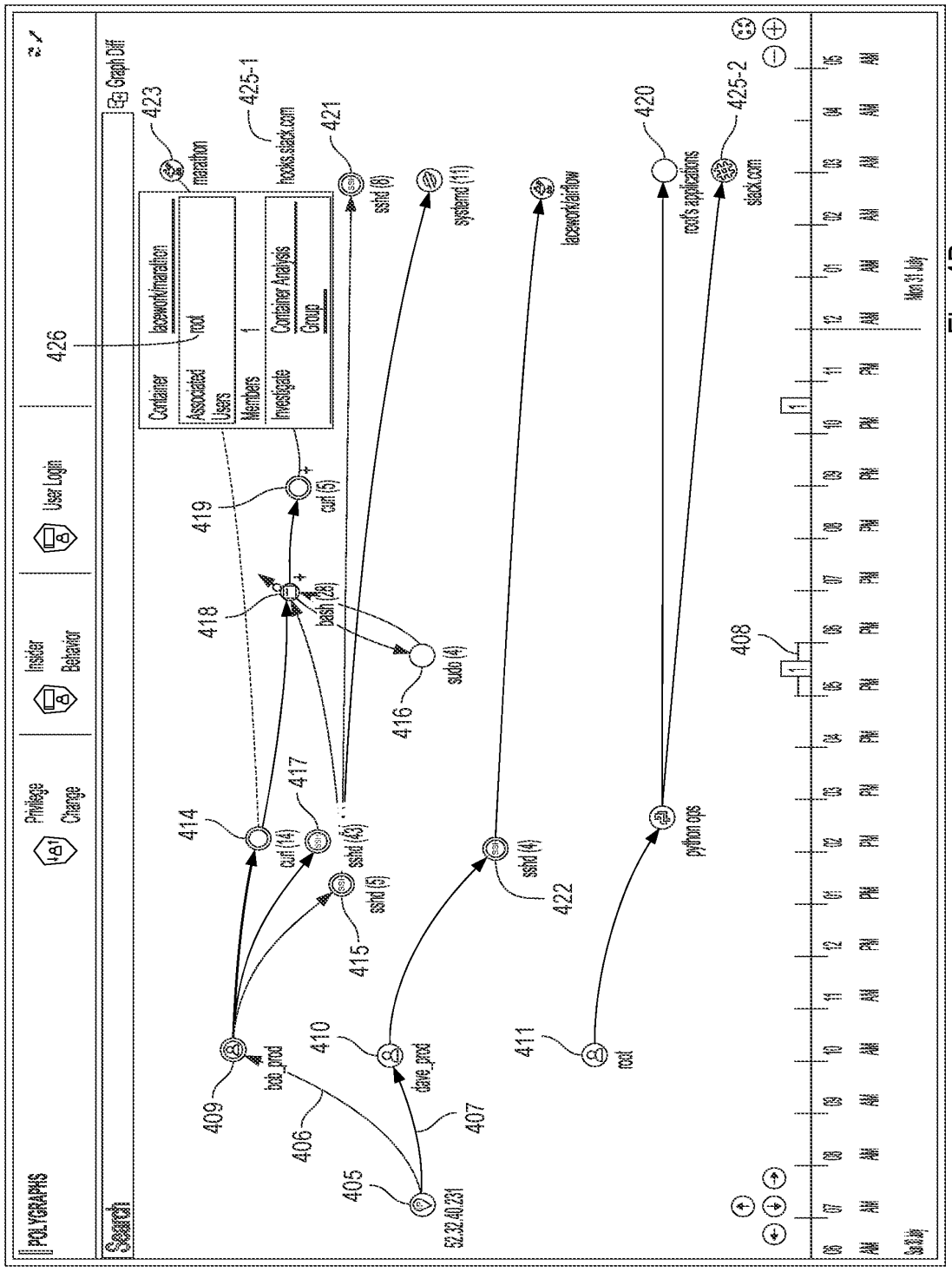

404
POLYGRAPHS
Search
Privilege Change
Insider Behavior
User Login
Graph Diff
426
423
marathon
425-1
hooks.slack.com
421
sshd (6)
Container
Associated Users
Members
Investigate
laceworkmarathon
root
1
Container Analysis
Group
419
curl (5)
418
bash (28)
systemd (11)
416
sudo (4)
laceworkdarthtow
420
root's applications
425-2
slack.com
408
414
curl (14)
417
sshd (43)
sshd (5)
415
sshd (4)
422
python ops
410
dave_prod
411
root
409
bob_prod
406
405
52.32.40.231
407
Mon 31 July
Tue 01 Aug

Fig. 4B

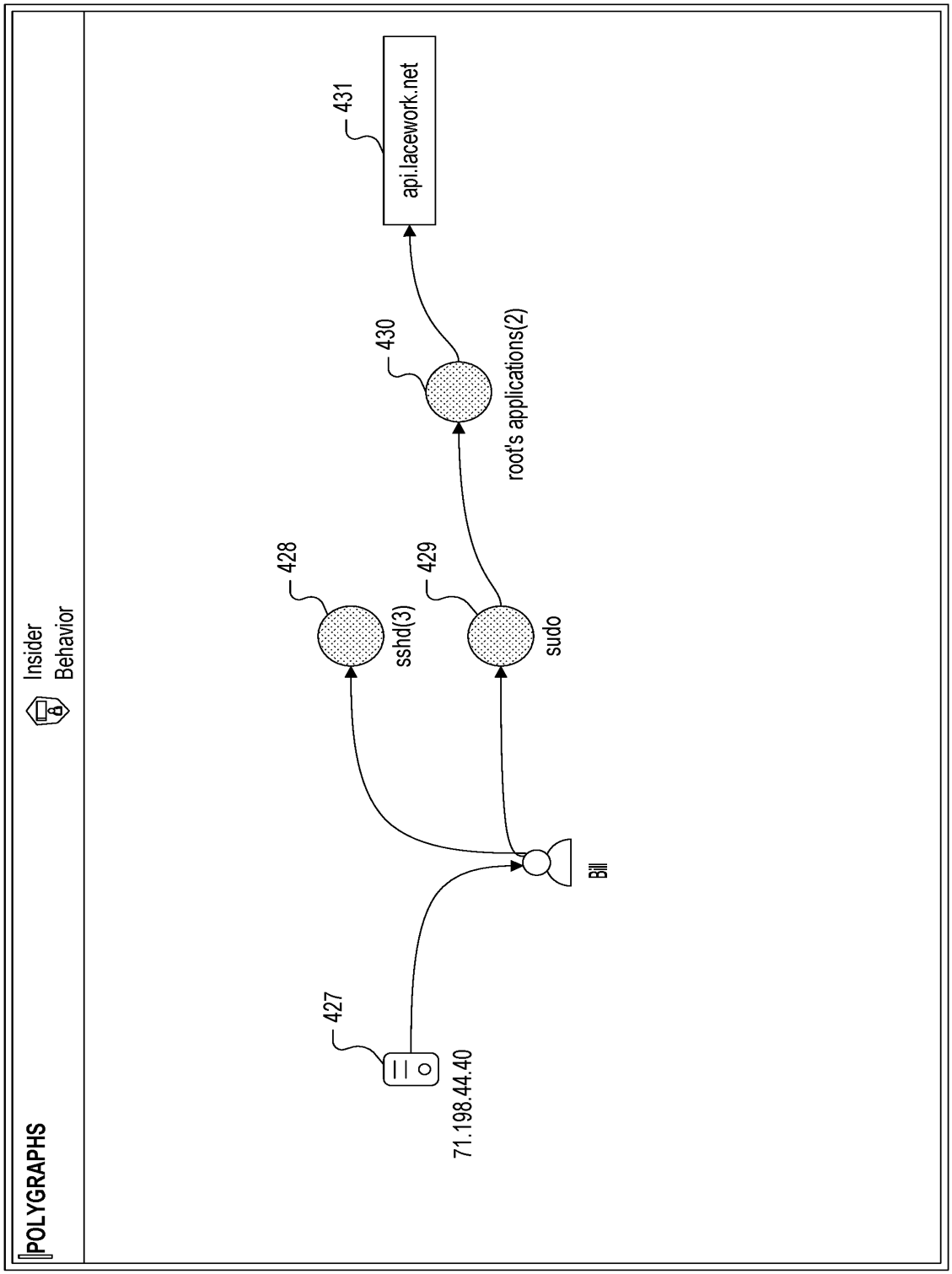

POLYGRAPHS
Insider Behavior
71.198.44.40
427
Bill
sudo
429
sshd(3)
428
root's applications(2)
430
api.lacework.net
431

Fig. 4C

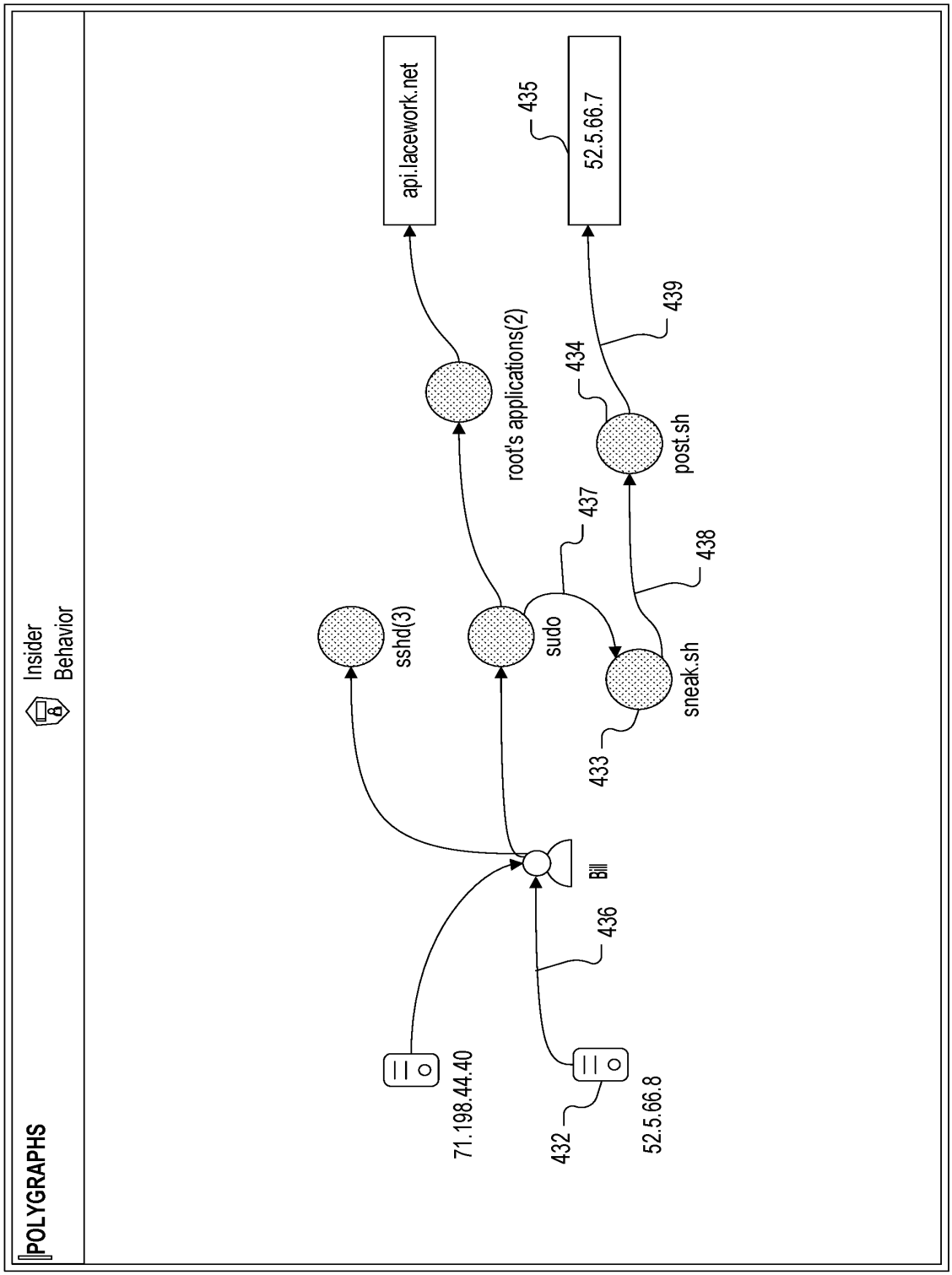

POLYGRAPHS
Insider Behavior
71.198.44.40
52.5.66.8
Bill
sshd(3)
sudo
root's applications(2)
sneak.sh
post.sh
api.lacework.net
52.5.66.7
432
433
434
435
436
437
438
439

Fig. 4D

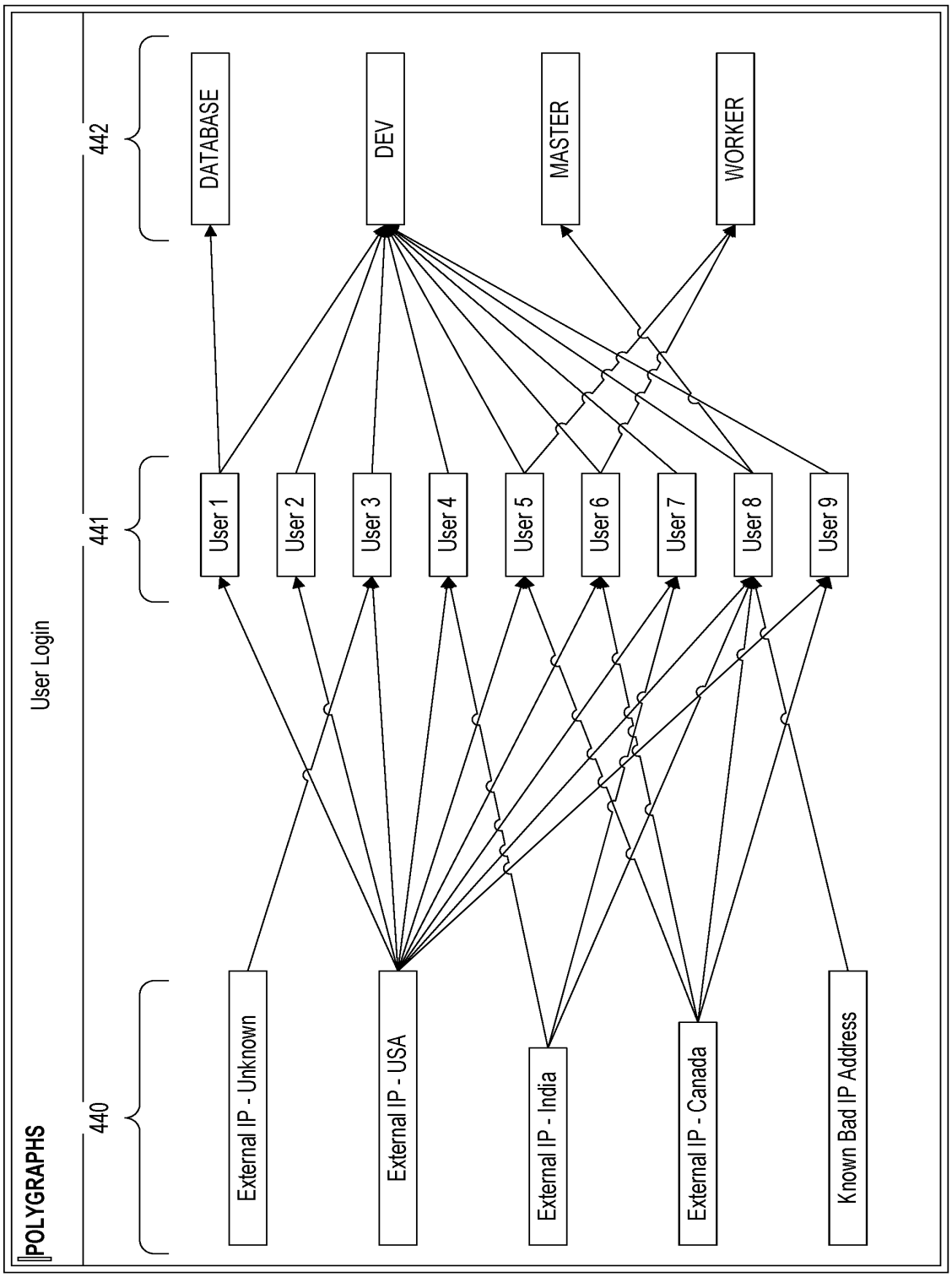

POLYGRAPHS
User Login
440
441
442
External IP - Unknown
External IP - USA
External IP - India
External IP - Canada
Known Bad IP Address
User 1
User 2
User 3
User 4
User 5
User 6
User 7
User 8
User 9
DATABASE
DEV
MASTER
WORKER

Fig. 4E

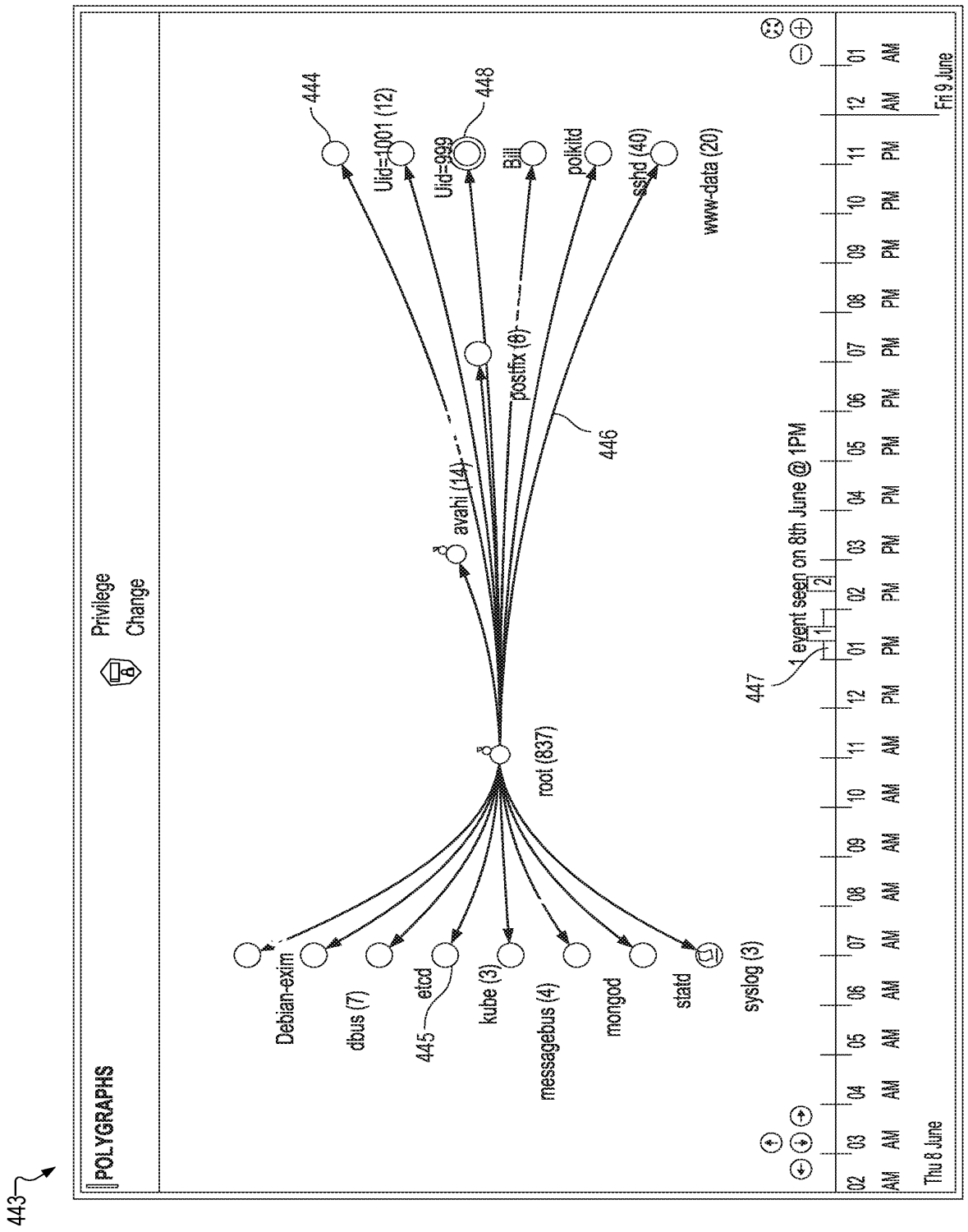

443
POLYGRAPHS
Privilege
Change
Debian-exim
dbus (7)
etcd
445
kube (3)
messagebus (4)
mongod
statd
syslog (3)
root (837)
avahi (14)
postfix (8)
446
www-data (20)
sshd (40)
polkitd
Bill
Uid=999
448
Uid=1001 (12)
444
447
1 event seen on 8th June @ 1PM
Thu 8 June
Fri 9 June

Fig. 4F

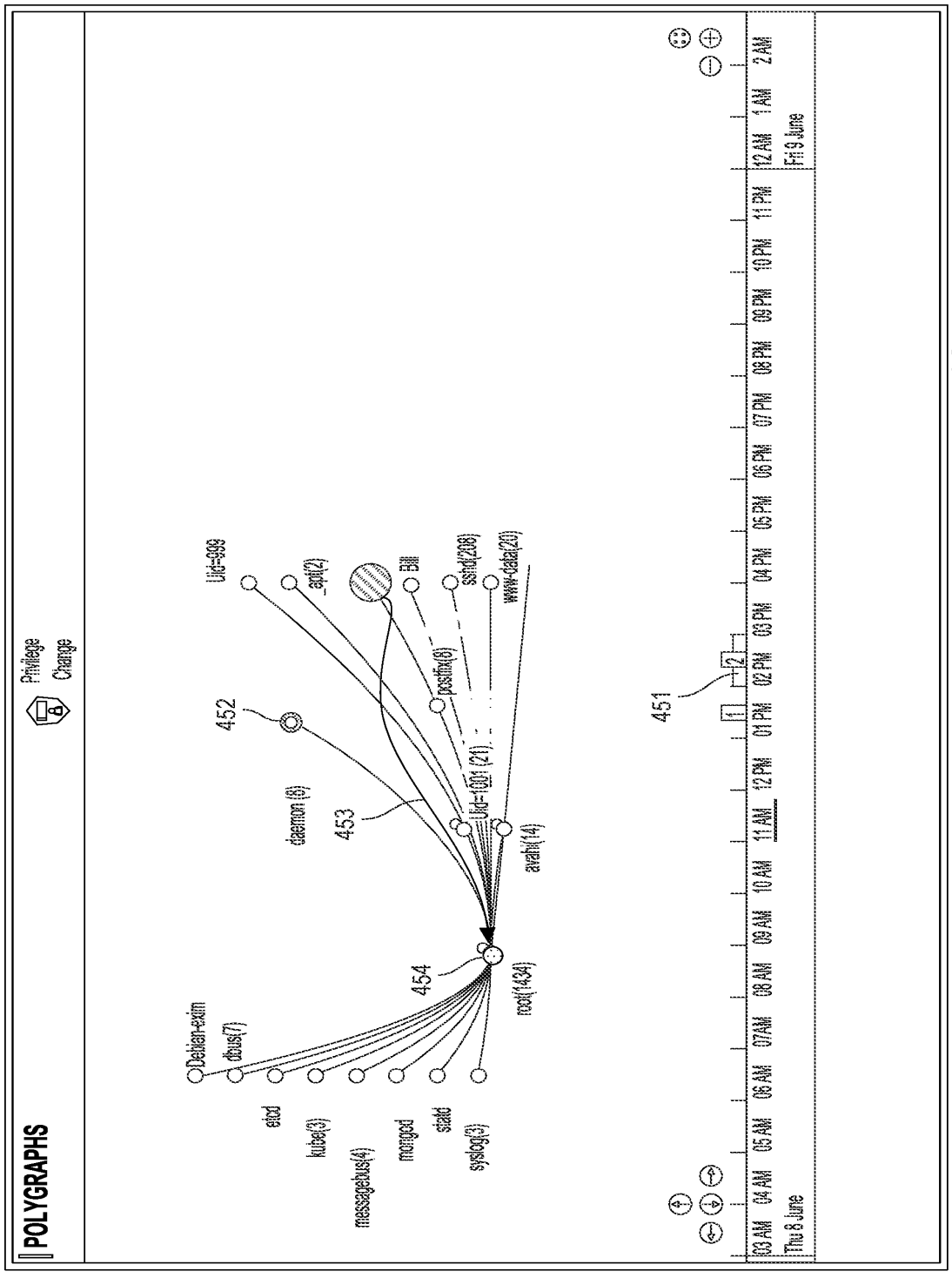

450
POLYGRAPHS
Privilege Change
Debian-exim
dbus(7)
etod
kube(3)
messagebus(4)
mongod
statd
syslog(3)
454
root(1434)
daemon (6)
453
452
Uid=999
_apt(2)
Bill
postfix(6)
Uid=1001 (21)
sshd(208)
www-data(20)
avahi(14)
451
03 AM
04 AM
05 AM
06 AM
07 AM
08 AM
09 AM
10 AM
11 AM
12 PM
01 PM
02 PM
03 PM
04 PM
05 PM
06 PM
07 PM
08 PM
09 PM
10 PM
11 PM
12 AM
1 AM
2 AM
Thu 8 June
Fri 9 June

Fig. 4G

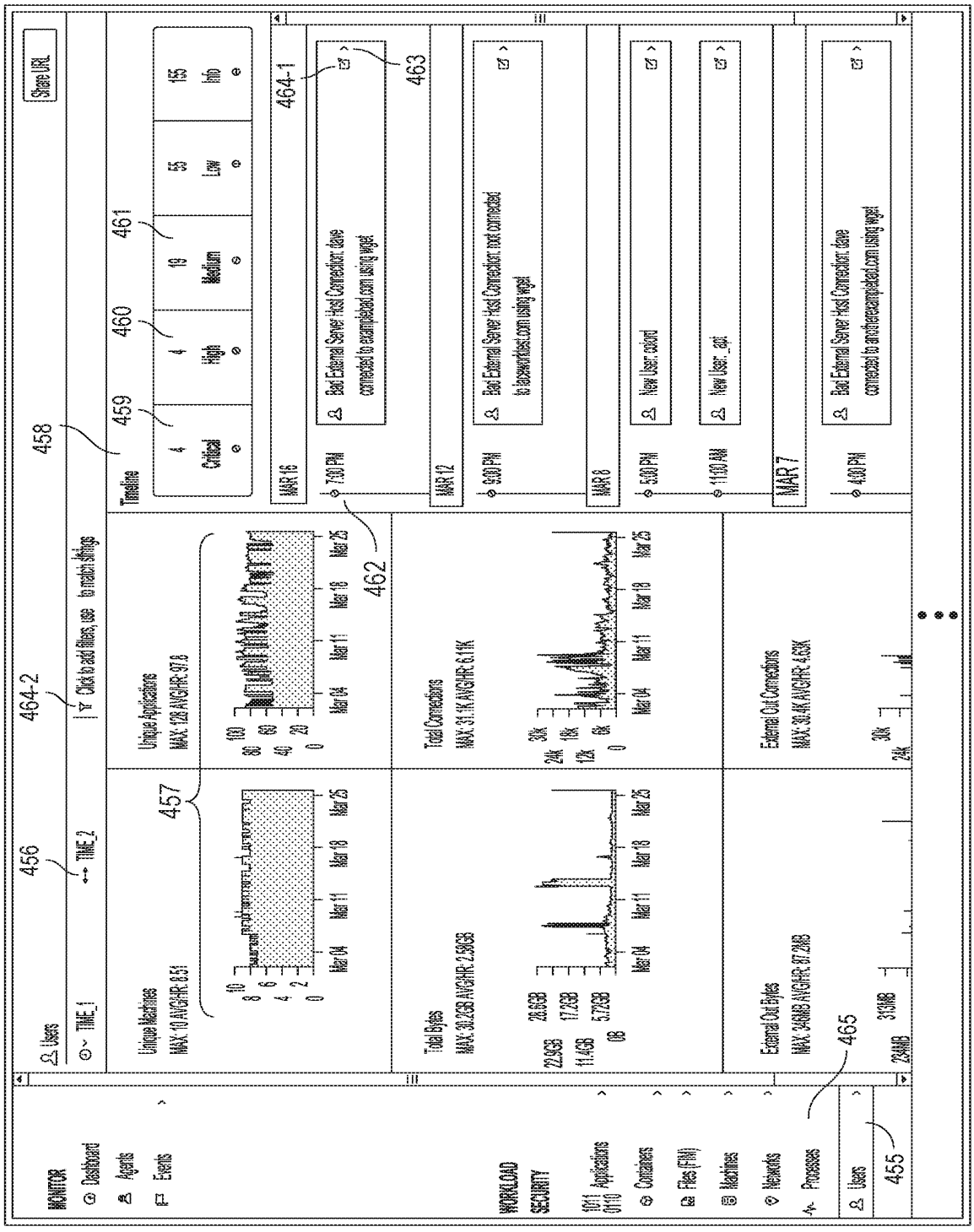

MONITOR
Dashboard
Agents
Events
WORKLOAD SECURITY
1911 Applications
0110
Containers
Files (FIM)
Machines
Networks
Processes
Users
455
456
TIME_1
TIME_2
457
458
Share URL
Users
Click to add filters, use to match Strings
464-2
Unique Machines
MAX: 10 AVG/HR: 0.51
Unique Applications
MAX: 128 AVG/HR: 97.6
462
Total Bytes
MAX: 38.2GB AVG/HR: 2.86GB
Total Connections
MAX: 31.1K AVG/HR: 6.11K
External Out Bytes
MAX: 24MB AVG/HR: 87.2MB
External Out Connections
MAX: 30.4K AVG/HR: 4.63K
465
Timeline
459
460
461
4 Critical
4 High
19 Medium
55 Low
155 Info
464-1
MAR 16
7:00 PM
Bad External Server Host Connection: done connected to examplebad.com using wget
463
MAR 12
9:00 PM
Bad External Server Host Connection: not connected to baseworldtest.com using wget
MAR 8
5:00 PM
New User: sdcrd
11:00 AM
New User: _cat
MAR 7
4:00 PM
Bad External Server Host Connection: done connected to anotherexampletest.com using wget

Fig. 4H

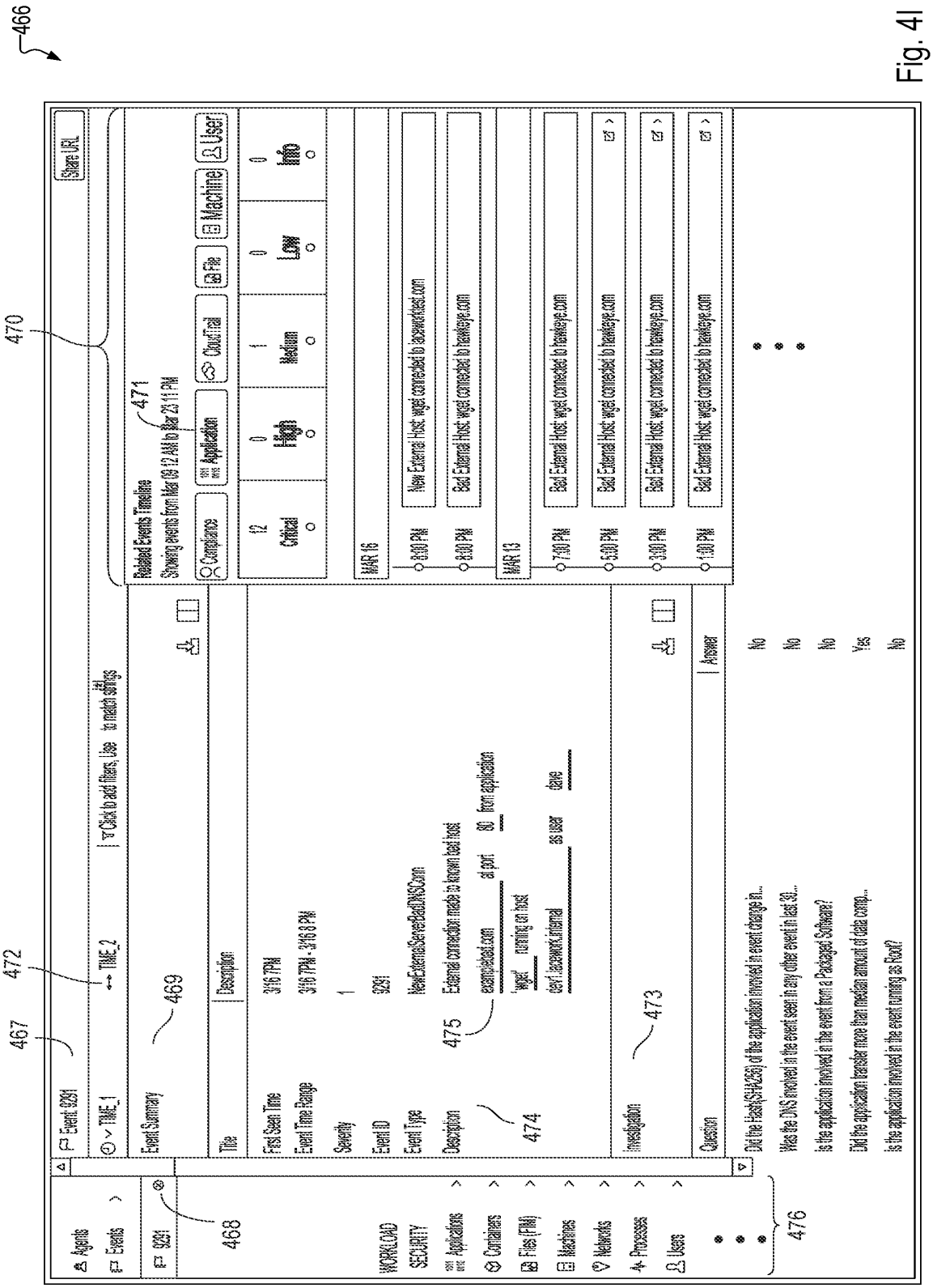

466
470
472
467
469
471
468
475
474
473
476
Agents
Events
9291
Event 9291
TIME_1
TIME_2
Click to add filters, Use to match settings
Share URL
Event Summary
Related Events Timeline
Showing events from Mar 09 12 AM to Mar 23 11 PM
Compliance
Application
CloudTrail
File
Machine
User
12 Critical
0 High
1 Medium
0 Low
0 Info
Title
Description
First Seen Time
Event Time Range
Severity
Event ID
Event Type
Description
3/16 7PM
3/16 7PM - 3/16 8 PM
1
9291
NewExternalServerBadDNSCom
External connection made to known bad host
examplebad.com at port 80 from application
'wget' running on host
doe\ Jacaranda.internal as user done
WORKLOAD
SECURITY
Applications
Containers
Files (FIM)
Machines
Networks
Processes
Users
MAR 16
8:00 PM
New External Host: wget connected to saxeworldtest.com
8:00 PM
Bad External Host: wget connected to hawkeye.com
MAR 13
7:00 PM
Bad External Host: wget connected to hawkeye.com
5:00 PM
Bad External Host: wget connected to hawkeye.com
3:00 PM
Bad External Host: wget connected to hawkeye.com
1:00 PM
Bad External Host: wget connected to hawkeye.com
Investigation
Question
Answer
Did the Hash(SHA256) of the application involved in event change in...
No
Was the DNS involved in the event seen in any other event in last 30...
No
Is the application involved in the event from a Privileged Software?
No
Did the application transfer more than median amount of data comp...
Yes
Is the application involved in the event running as Root?
No

Fig. 4I

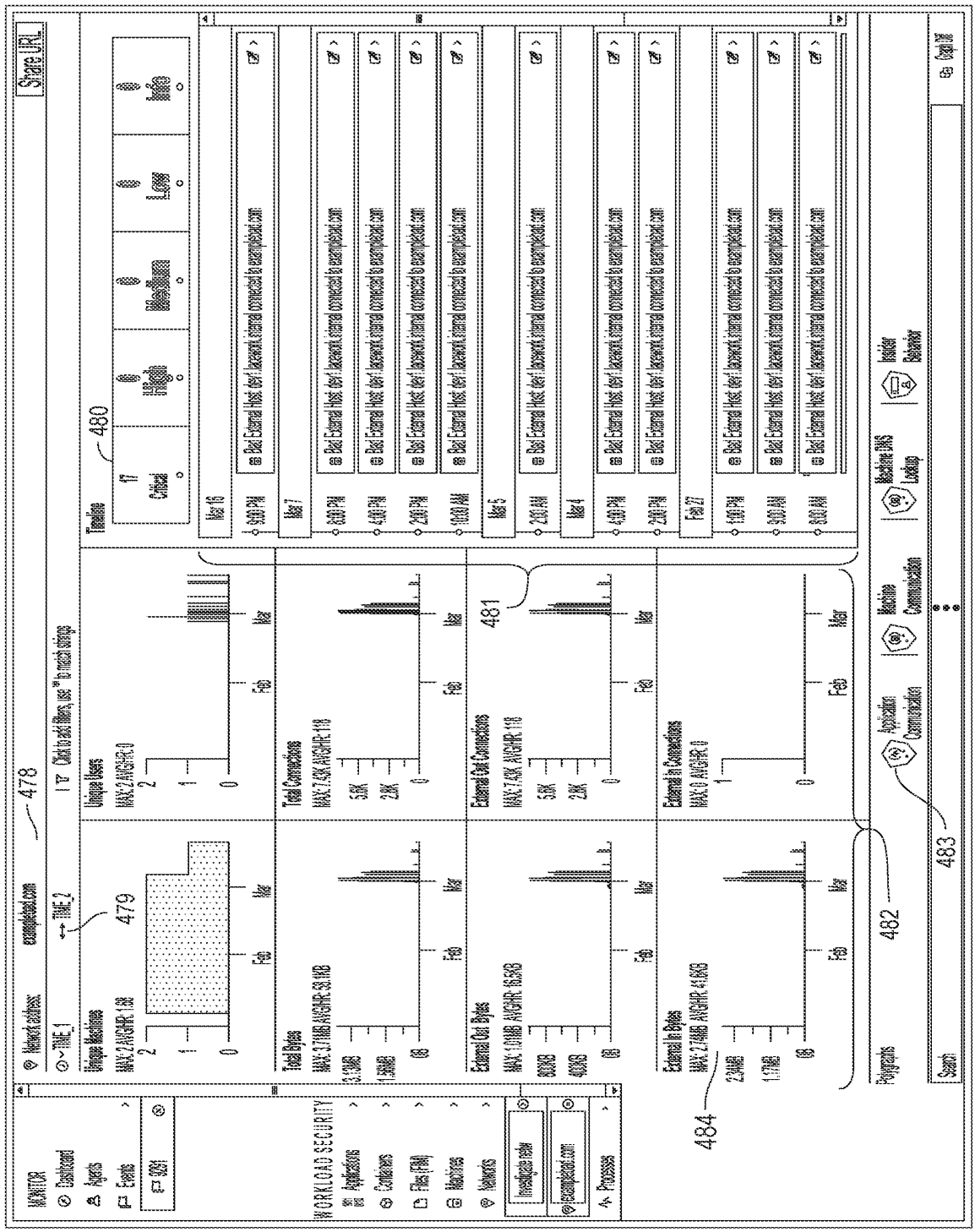

477
478
479
480
481
482
483
484
Share URL
MONITOR
Dashboard
Agents
Events
Network address
completed.com
TIME_1
TIME_2
Click to add filters, use * to match strings
Unique Machines
MAX: 2 AVG/HR: 1.08
Unique Users
MAX: 2 AVG/HR: 0
Timeline
17 Critical
0 High
0 Medium
0 Low
0 Info
Total Bytes
MAX: 3.71MB AVG/HR: 58.1KB
Total Connections
MAX: 7.5K AVG/HR: 118
External Out Bytes
MAX: 1.01MB AVG/HR: 16.53B
External Out Connections
MAX: 7.49K AVG/HR: 118
External In Bytes
MAX: 2.74MB AVG/HR: 41.6KB
External In Connections
MAX: 0 AVG/HR: 0
Bad External Host: dest: ascend.internal connected to examplebad.com
WORKLOAD SECURITY
Applications
Containers
Files (FIM)
Machines
Networks
Processes
Investigate new
examplebad.com
Polygraphs
Application Communication
Machine Communication
Machine DNS Lookup
Insider Behavior
Search
Feb
Mar

Fig. 4J

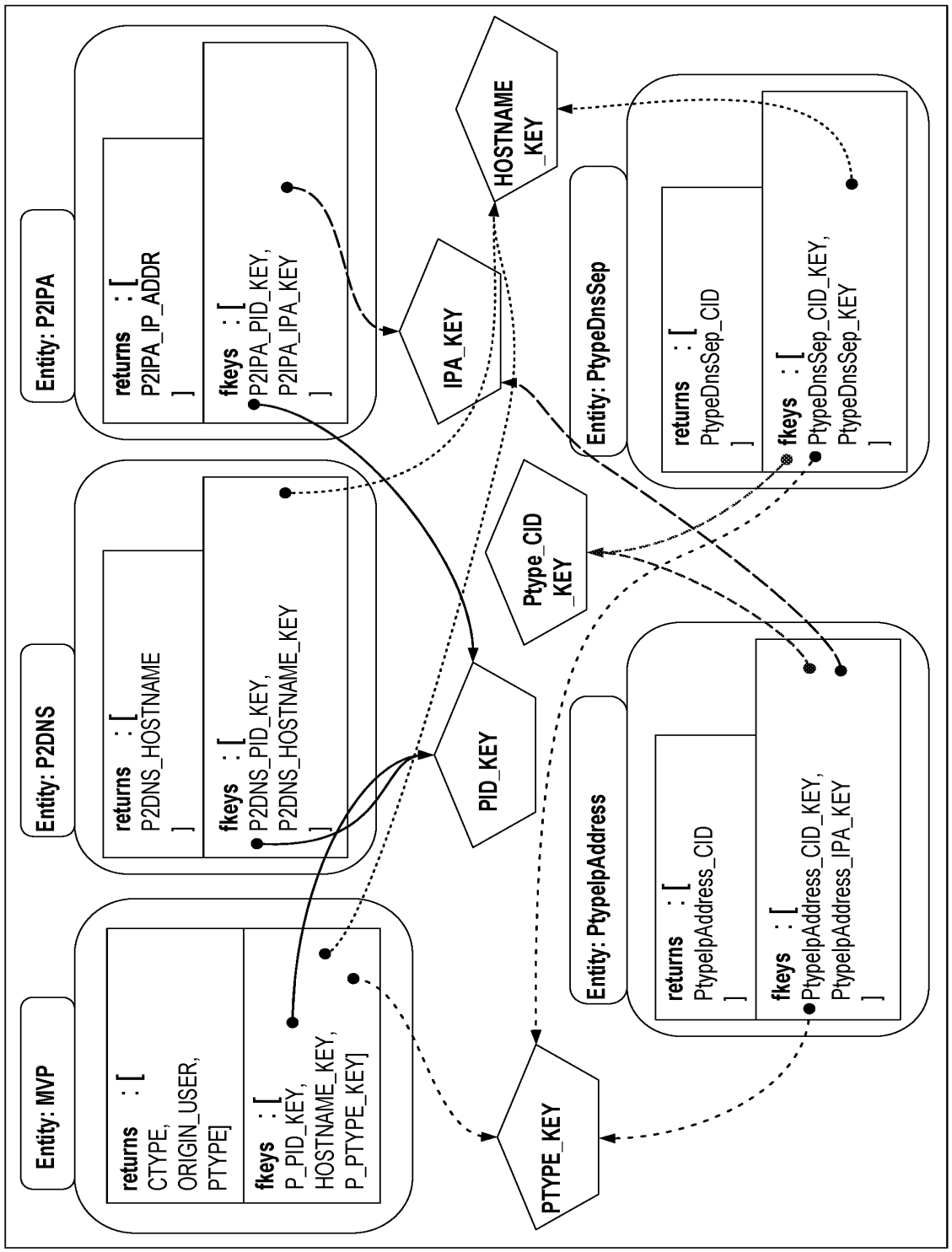

Entity: MVP
returns : [
CTYPE,
ORIGIN_USER,
PTYPE]
fkeys : [
P_PID_KEY,
HOSTNAME_KEY,
P_PTYPE_KEY]
Entity: P2DNS
returns : [
P2DNS_HOSTNAME
]
fkeys : [
P2DNS_PID_KEY,
P2DNS_HOSTNAME_KEY
]
Entity: P2IPA
returns : [
P2IPA_IP_ADDR
]
fkeys : [
P2IPA_PID_KEY,
P2IPA_IPA_KEY
]
Entity: PtypeIpAddress
returns : [
PtypeIpAddress_CID
]
fkeys : [
PtypeIpAddress_CID_KEY,
PtypeIpAddress_IPA_KEY
]
Entity: PtypeDnsSep
returns : [
PtypeDnsSep_CID
]
fkeys : [
PtypeDnsSep_CID_KEY,
PtypeDnsSep_KEY
]
PID_KEY
IPA_KEY
HOSTNAME_KEY
Ptype_CID_KEY
PTYPE_KEY

Fig. 4K

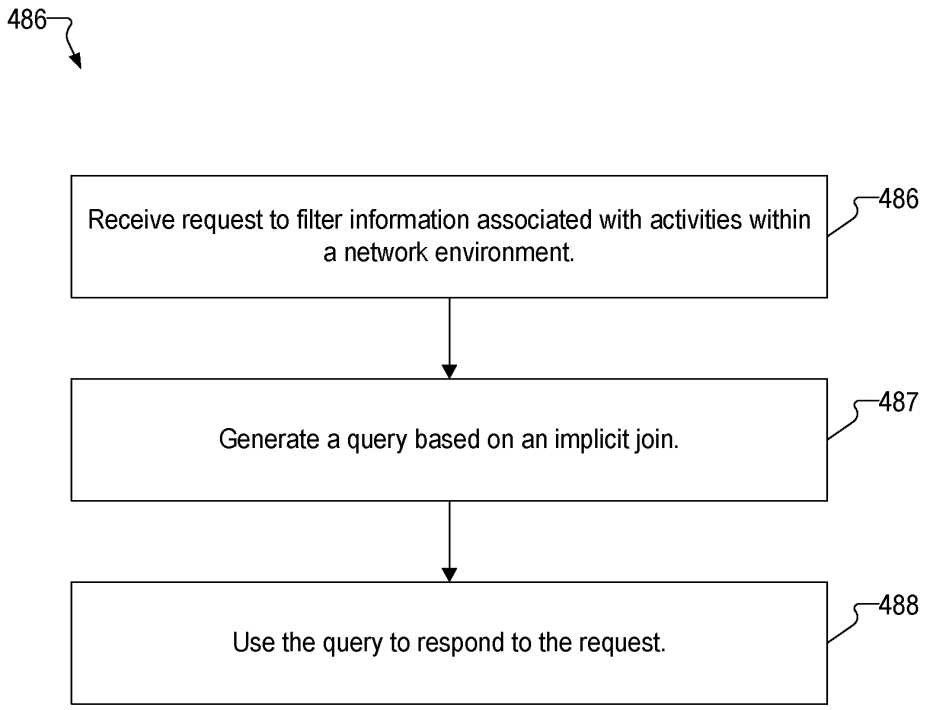
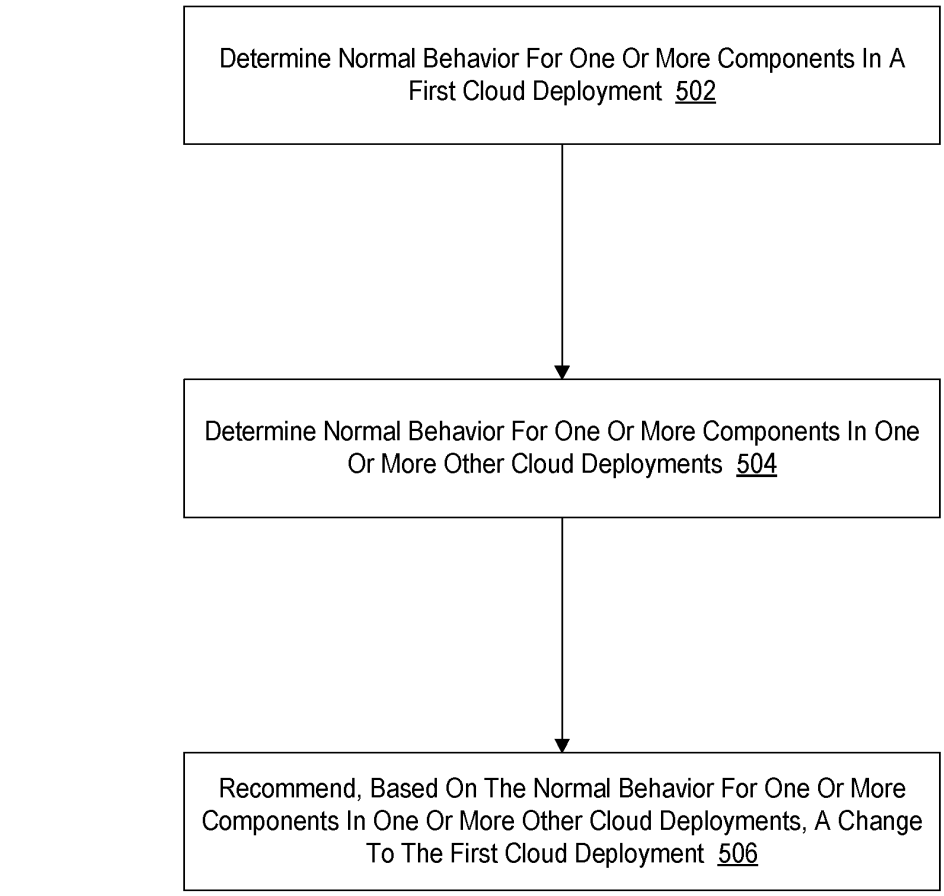

486
Receive request to filter information associated with activities within a network environment.
486
Generate a query based on an implicit join.
487
Use the query to respond to the request.
488

Fig. 4L


Determine Normal Behavior For One Or More Components In A First Cloud Deployment 502
Determine Normal Behavior For One Or More Components In One Or More Other Cloud Deployments 504
Recommend, Based On The Normal Behavior For One Or More Components In One Or More Other Cloud Deployments, A Change To The First Cloud Deployment 506

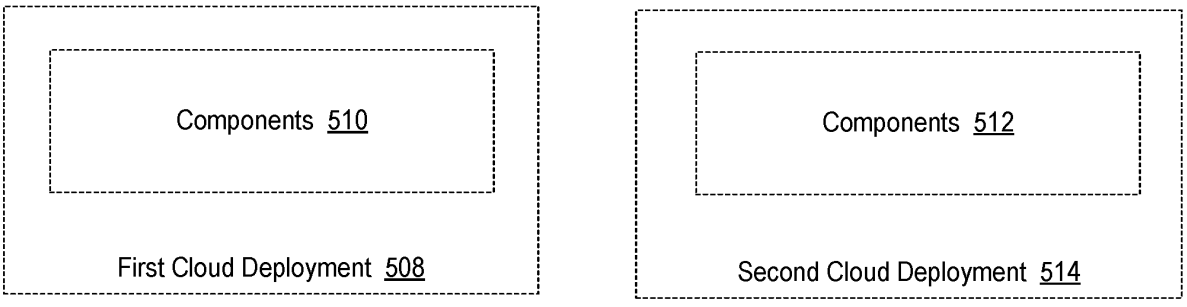

Components 510
First Cloud Deployment 508
Components 512
Second Cloud Deployment 514

Fig. 5

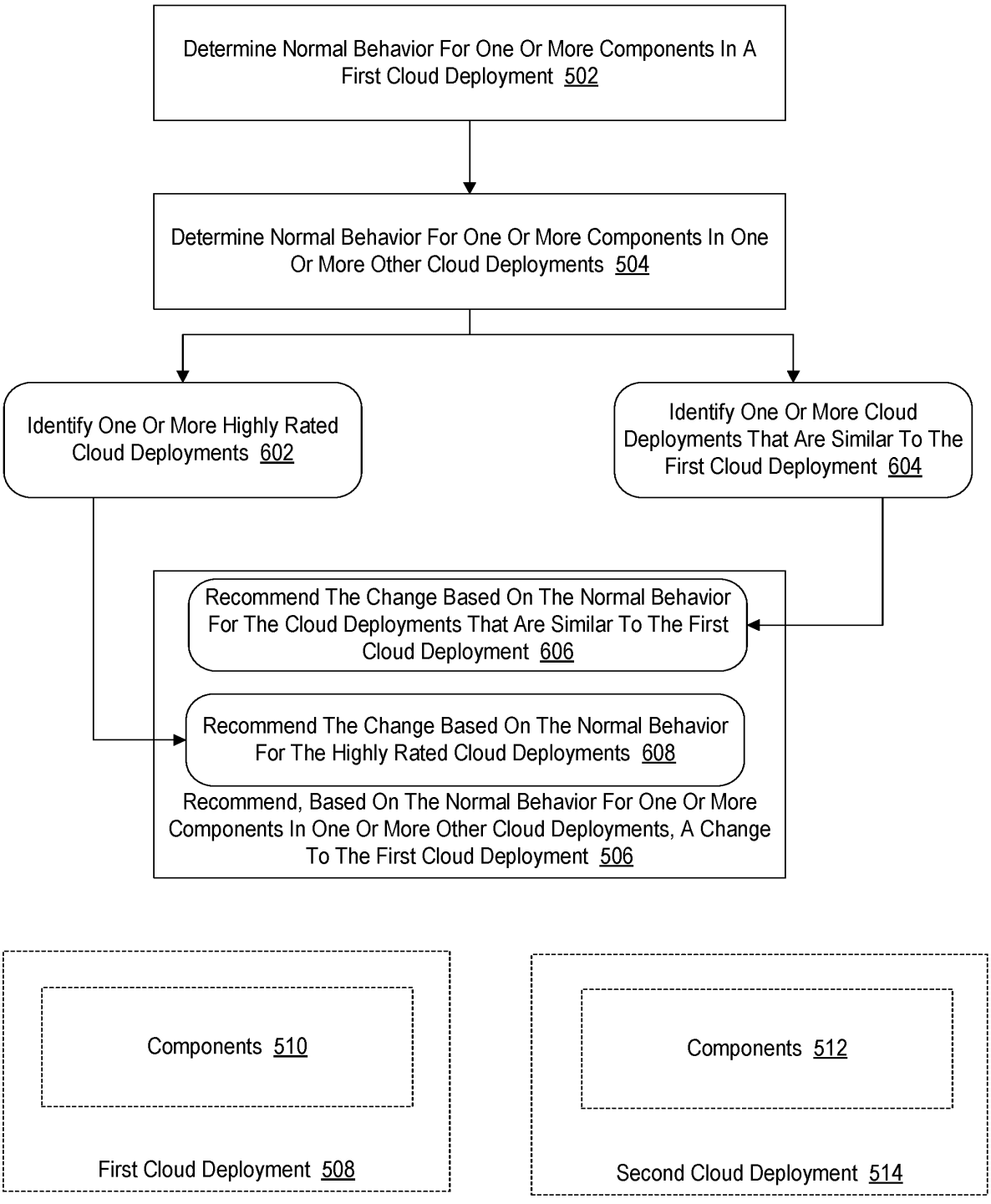

Determine Normal Behavior For One Or More Components In A First Cloud Deployment 502
Determine Normal Behavior For One Or More Components In One Or More Other Cloud Deployments 504
Identify One Or More Highly Rated Cloud Deployments 602
Identify One Or More Cloud Deployments That Are Similar To The First Cloud Deployment 604
Recommend The Change Based On The Normal Behavior For The Cloud Deployments That Are Similar To The First Cloud Deployment 606
Recommend The Change Based On The Normal Behavior For The Highly Rated Cloud Deployments 608
Recommend, Based On The Normal Behavior For One Or More Components In One Or More Other Cloud Deployments, A Change To The First Cloud Deployment 506
Components 510
First Cloud Deployment 508
Components 512
Second Cloud Deployment 514

Fig. 6

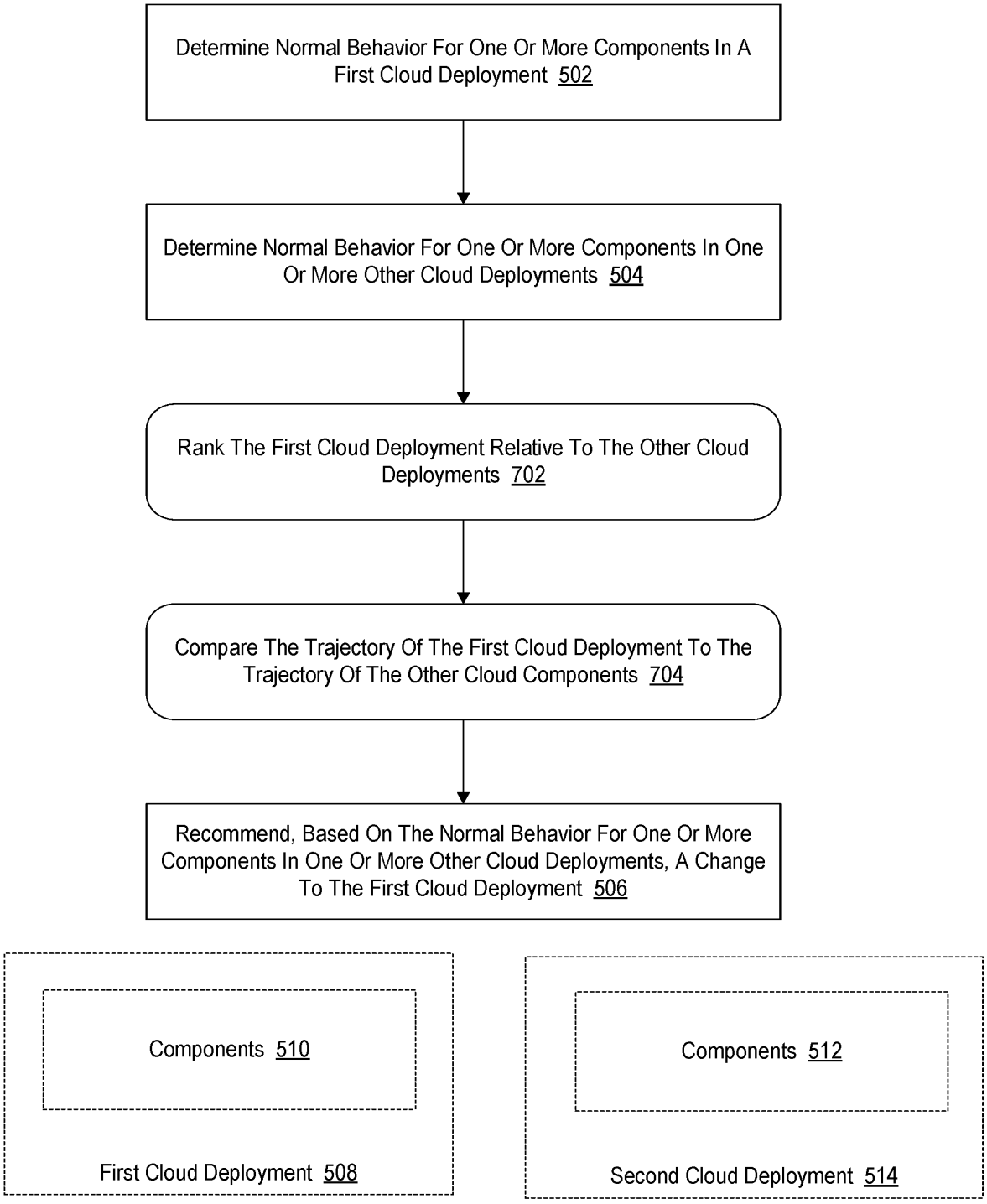

Determine Normal Behavior For One Or More Components In A First Cloud Deployment 502
Determine Normal Behavior For One Or More Components In One Or More Other Cloud Deployments 504
Rank The First Cloud Deployment Relative To The Other Cloud Deployments 702
Compare The Trajectory Of The First Cloud Deployment To The Trajectory Of The Other Cloud Components 704
Recommend, Based On The Normal Behavior For One Or More Components In One Or More Other Cloud Deployments, A Change To The First Cloud Deployment 506
Components 510
First Cloud Deployment 508
Components 512
Second Cloud Deployment 514

Fig. 5

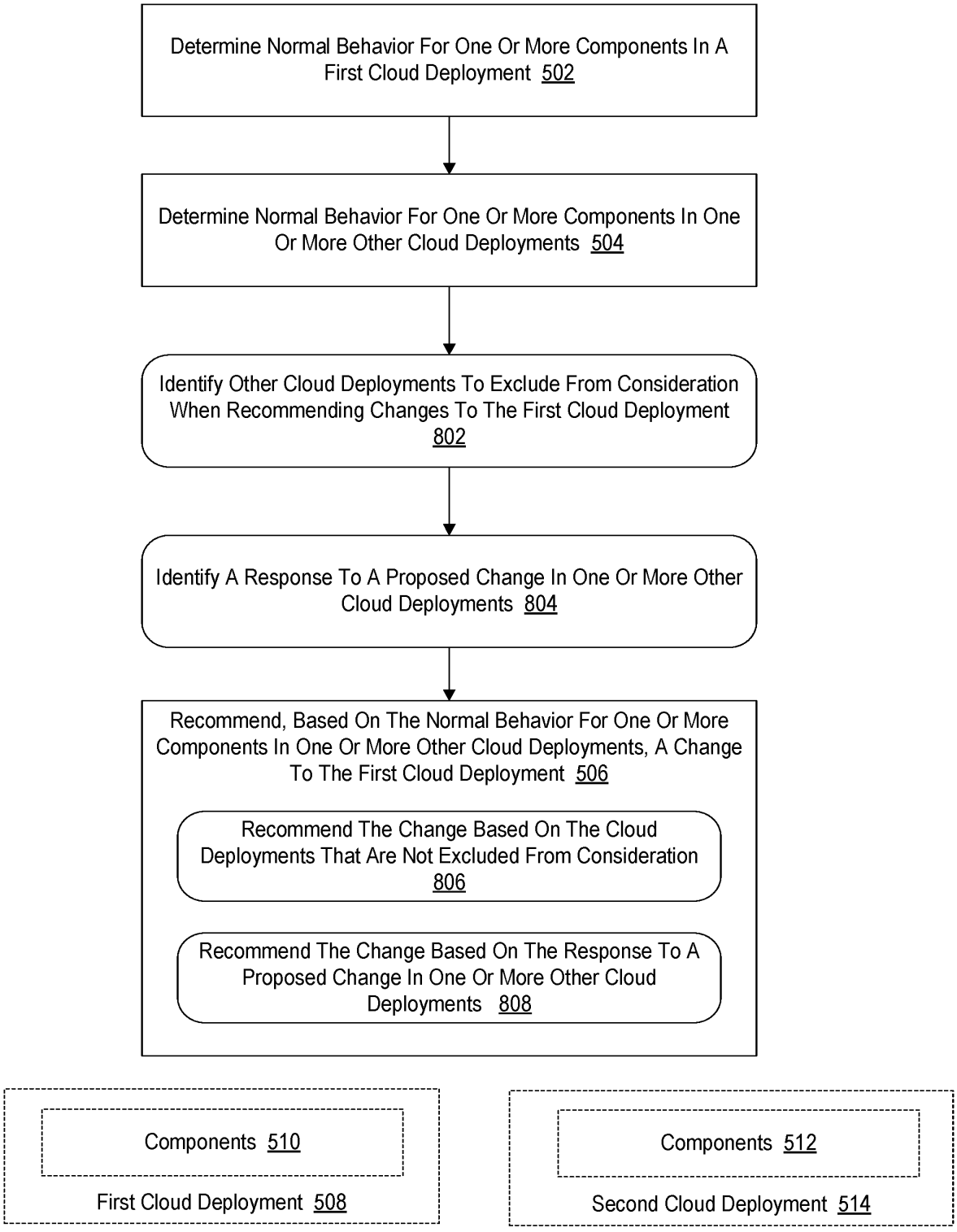

Determine Normal Behavior For One Or More Components In A First Cloud Deployment 502
Determine Normal Behavior For One Or More Components In One Or More Other Cloud Deployments 504
Identify Other Cloud Deployments To Exclude From Consideration When Recommending Changes To The First Cloud Deployment 802
Identify A Response To A Proposed Change In One Or More Other Cloud Deployments 804
Recommend, Based On The Normal Behavior For One Or More Components In One Or More Other Cloud Deployments, A Change To The First Cloud Deployment 506
Recommend The Change Based On The Cloud Deployments That Are Not Excluded From Consideration 806
Recommend The Change Based On The Response To A Proposed Change In One Or More Other Cloud Deployments 808
Components 510
First Cloud Deployment 508
Components 512
Second Cloud Deployment 514

Fig. 8

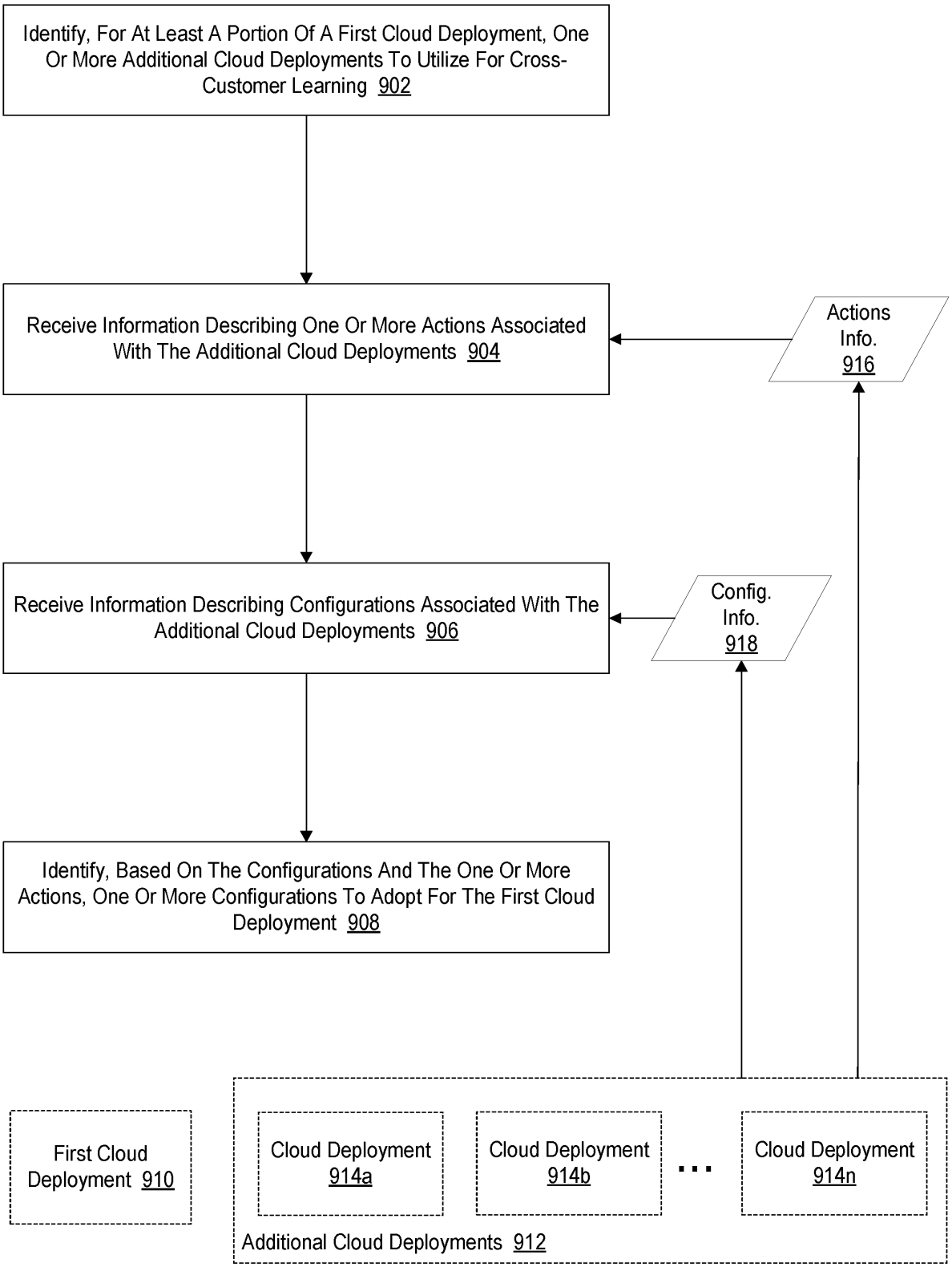

Identify, For At Least A Portion Of A First Cloud Deployment, One Or More Additional Cloud Deployments To Utilize For Cross-Customer Learning 902
Receive Information Describing One Or More Actions Associated With The Additional Cloud Deployments 904
Actions Info. 916
Receive Information Describing Configurations Associated With The Additional Cloud Deployments 906
Config. Info. 918
Identify, Based On The Configurations And The One Or More Actions, One Or More Configurations To Adopt For The First Cloud Deployment 908
First Cloud Deployment 910
Cloud Deployment 914a
Cloud Deployment 914b
...
Cloud Deployment 914n
Additional Cloud Deployments 912

Fig. 9

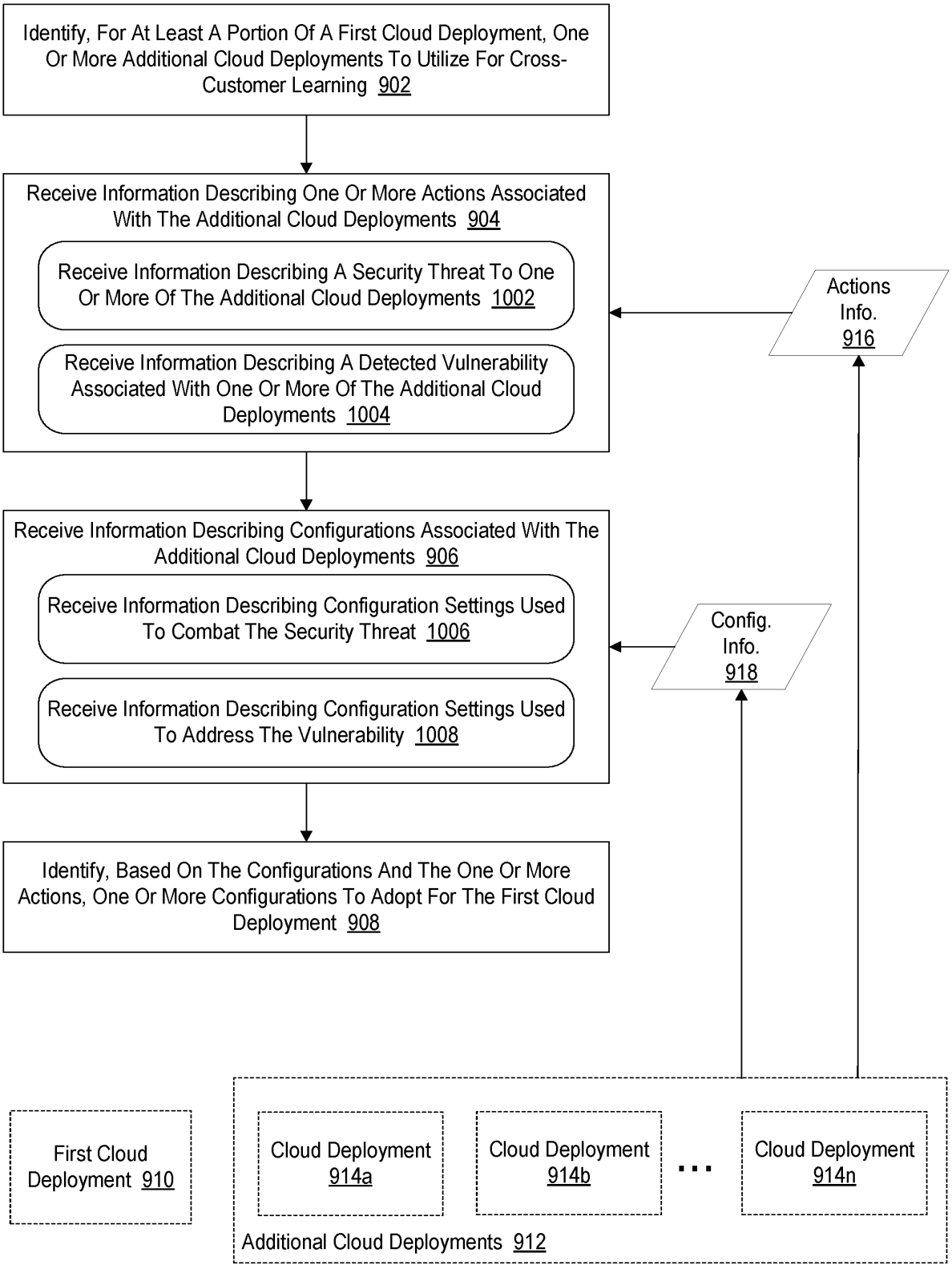

Identify, For At Least A Portion Of A First Cloud Deployment, One Or More Additional Cloud Deployments To Utilize For Cross-Customer Learning 902
Receive Information Describing One Or More Actions Associated With The Additional Cloud Deployments 904
Receive Information Describing A Security Threat To One Or More Of The Additional Cloud Deployments 1002
Receive Information Describing A Detected Vulnerability Associated With One Or More Of The Additional Cloud Deployments 1004
Actions Info. 916
Receive Information Describing Configurations Associated With The Additional Cloud Deployments 906
Receive Information Describing Configuration Settings Used To Combat The Security Threat 1006
Receive Information Describing Configuration Settings Used To Address The Vulnerability 1008
Config. Info. 918
Identify, Based On The Configurations And The One Or More Actions, One Or More Configurations To Adopt For The First Cloud Deployment 908
First Cloud Deployment 910
Cloud Deployment 914a
Cloud Deployment 914b
...
Cloud Deployment 914n
Additional Cloud Deployments 912

Fig. 10

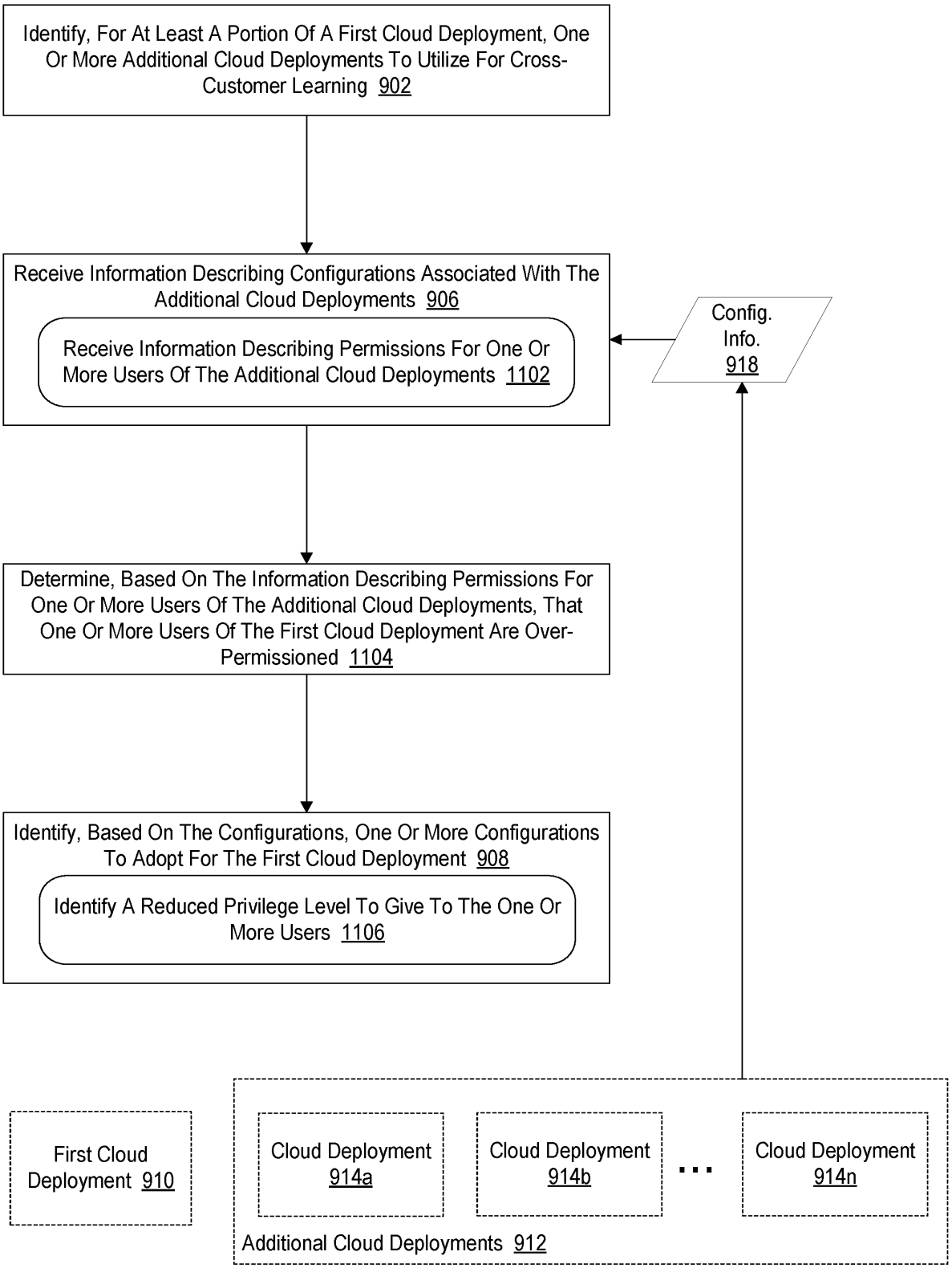

Identify, For At Least A Portion Of A First Cloud Deployment, One Or More Additional Cloud Deployments To Utilize For Cross-Customer Learning 902
Receive Information Describing Configurations Associated With The Additional Cloud Deployments 906
Receive Information Describing Permissions For One Or More Users Of The Additional Cloud Deployments 1102
Config. Info. 918
Determine, Based On The Information Describing Permissions For One Or More Users Of The Additional Cloud Deployments, That One Or More Users Of The First Cloud Deployment Are Over-Permissioned 1104
Identify, Based On The Configurations, One Or More Configurations To Adopt For The First Cloud Deployment 908
Identify A Reduced Privilege Level To Give To The One Or More Users 1106
First Cloud Deployment 910
Cloud Deployment 914a
Cloud Deployment 914b
...
Cloud Deployment 914n
Additional Cloud Deployments 912

Fig. 11

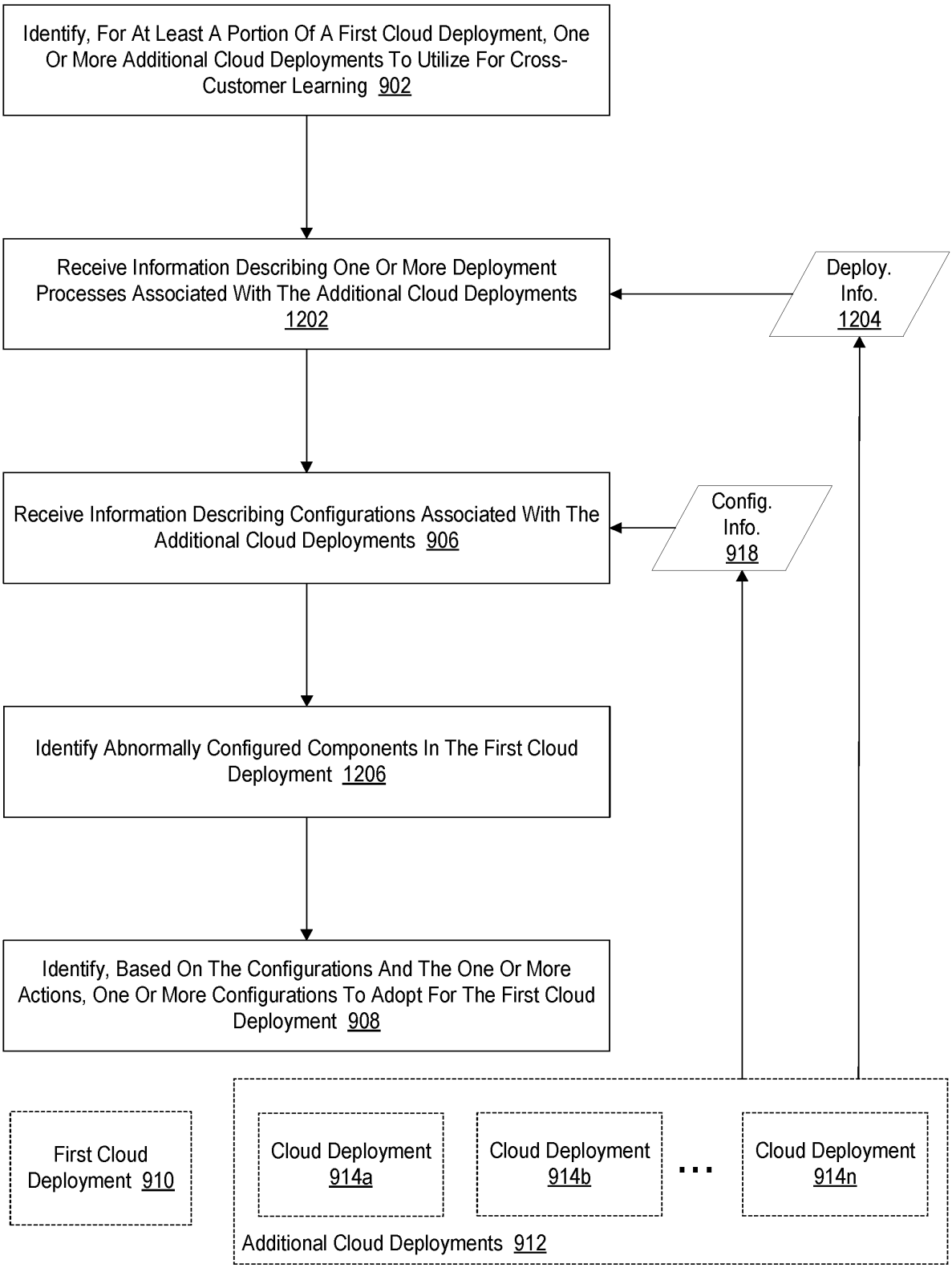

Identify, For At Least A Portion Of A First Cloud Deployment, One Or More Additional Cloud Deployments To Utilize For Cross-Customer Learning 902
Receive Information Describing One Or More Deployment Processes Associated With The Additional Cloud Deployments 1202
Deploy. Info. 1204
Receive Information Describing Configurations Associated With The Additional Cloud Deployments 906
Config. Info. 918
Identify Abnormally Configured Components In The First Cloud Deployment 1206
Identify, Based On The Configurations And The One Or More Actions, One Or More Configurations To Adopt For The First Cloud Deployment 908
First Cloud Deployment 910
Cloud Deployment 914a
Cloud Deployment 914b
...
Cloud Deployment 914n
Additional Cloud Deployments 912

Fig. 12

ENHANCING SECURITY OF A CLOUD DEPLOYMENT BASED ON LEARNINGS FROM OTHER CLOUD DEPLOYMENTS

BRIEF DESCRIPTION OF THE DRAWINGS

[0001] The accompanying drawings illustrate various embodiments and are a part of the specification. The illustrated embodiments are merely examples and do not limit the scope of the disclosure. Throughout the drawings, identical or similar reference numbers designate identical or similar elements.

[0002] Fig. 1A shows an illustrative configuration in which a data platform is configured to perform various operations with respect to a cloud environment that includes a plurality of compute assets.

[0003] Fig. 1B shows an illustrative implementation of the configuration of Fig. 1A.

[0004] Fig. 1C illustrates an example computing device.

[0005] Fig. 1D illustrates an example of an environment in which activities that occur within datacenters are modeled.

[0006] Fig. 2A illustrates an example of a process, used by an agent, to collect and report information about a client.

[0007] Fig. 2B illustrates a 5-tuple of data collected by an agent, physically and logically.

[0008] Fig. 2C illustrates a portion of a polygraph.

[0009] Fig. 2D illustrates a portion of a polygraph.

[0010] Fig. 2E illustrates an example of a communication polygraph.

[0011] Fig. 2F illustrates an example of a polygraph.

[0012] Fig. 2G illustrates an example of a polygraph as rendered in an interface.

[0013] Fig. 2H illustrates an example of a portion of a polygraph as rendered in an interface.

[0014] Fig. 2I illustrates an example of a portion of a polygraph as rendered in an interface.

[0015] Fig. 2J illustrates an example of a portion of a polygraph as rendered in an interface.

[0016] Fig. 2K illustrates an example of a portion of a polygraph as rendered in an interface.

[0017] Fig. 2L illustrates an example of an insider behavior graph as rendered in an interface.

[0018] Fig. 2M illustrates an example of a privilege change graph as rendered in an interface.

[0019] Fig. 2N illustrates an example of a user login graph as rendered in an interface.

[0020] Fig. 2O illustrates an example of a machine server graph as rendered in an interface.

[0021] Fig. 3A illustrates an example of a process for detecting anomalies in a network environment.

[0022] Fig. 3B depicts a set of example processes communicating with other processes.

[0023] Fig. 3C depicts a set of example processes communicating with other processes.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00549

[0024] Fig. 3D depicts a set of example processes communicating with other processes.

[0025] Fig. 3E depicts two pairs of clusters.

[0026] Fig. 3F is a representation of a user logging into a first machine, then into a second machine from the first machine, and then making an external connection.

[0027] Fig. 3G is an alternate representation of actions occurring in Fig. 3F.

[0028] Fig. 3H illustrates an example of a process for performing extended user tracking.

[0029] Fig. 3I is a representation of a user logging into a first machine, then into a second machine from the first machine, and then making an external connection.

[0030] Fig. 3J illustrates an example of a process for performing extended user tracking.

[0031] Fig. 3K illustrates example records.

[0032] Fig. 3L illustrates example output from performing an ssh connection match.

[0033] Fig. 3M illustrates example records.

[0034] Fig. 3N illustrates example records.

[0035] Fig. 3O illustrates example records.

[0036] Fig. 3P illustrates example records.

[0037] Fig. 3Q illustrates an adjacency relationship between two login sessions.

[0038] Fig. 3R illustrates example records.

[0039] Fig. 3S illustrates an example of a process for detecting anomalies.

[0040] Fig. 4A illustrates a representation of an embodiment of an insider behavior graph.

[0041] Fig. 4B illustrates an embodiment of a portion of an insider behavior graph.

[0042] Fig. 4C illustrates an embodiment of a portion of an insider behavior graph.

[0043] Fig. 4D illustrates an embodiment of a portion of an insider behavior graph.

[0044] Fig. 4E illustrates a representation of an embodiment of a user login graph.

[0045] Fig. 4F illustrates an example of a privilege change graph.

[0046] Fig. 4G illustrates an example of a privilege change graph.

[0047] Fig. 4H illustrates an example of a user interacting with a portion of an interface.

[0048] Fig. 4I illustrates an example of a dossier for an event.

[0049] Fig. 4J illustrates an example of a dossier for a domain.

[0050] Fig. 4K depicts an example of an Entity Join graph by FilterKey and FilterKey Group (implicit join).

[0051] Fig. 4L illustrates an example process for dynamically generating and executing a query.

[0052] Fig. 5 sets forth a flowchart illustrating an example method of improving developer efficiency and application quality in accordance with some embodiments.

[0053] Fig. 6 sets forth a flowchart illustrating an additional example method of improving developer efficiency and application quality in accordance with some embodiments.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00550

[0054] Fig. 7 sets forth a flowchart illustrating an additional example method of improving developer efficiency and application quality in accordance with some embodiments.

[0055] Fig. 8 sets forth a flowchart illustrating an additional example method of improving developer efficiency and application quality in accordance with some embodiments.

[0056] Fig. 9 sets forth a flowchart illustrating an example method of learning from similar cloud deployments in accordance with some embodiments of the present disclosure.

[0057] Fig. 10 sets forth a flowchart illustrating an additional example method of learning from similar cloud deployments in accordance with some embodiments of the present disclosure.

[0058] Fig. 11 sets forth a flowchart illustrating an additional example method of learning from similar cloud deployments in accordance with some embodiments of the present disclosure.

[0059] Fig. 12 sets forth a flowchart illustrating an additional example method of learning from similar cloud deployments in accordance with some embodiments of the present disclosure.

DETAILED DESCRIPTION

[0060] Various illustrative embodiments are described herein with reference to the accompanying drawings. It will, however, be evident that various modifications and changes may be made thereto, and additional embodiments may be implemented, without departing from the scope of the invention as set forth in the claims. For example, certain features of one embodiment described herein may be combined with or substituted for features of another embodiment described herein. The description and drawings are accordingly to be regarded in an illustrative rather than a restrictive sense.

[0061] Fig. 1A shows an illustrative configuration 10 in which a data platform 12 is configured to perform various operations with respect to a cloud environment 14 that includes a plurality of compute assets 16-1 through 16-N (collectively "compute assets 16). For example, data platform 12 may include data ingestion resources 18 configured to ingest data from cloud environment 14 into data platform 12, data processing resources 20 configured to perform data processing operations with respect to the data, user interface resources 22 configured to provide one or more external users and/or compute resources (e.g., computing device 24) with access to an output of data processing resources 20. Each of these resources are described in detail herein.

[0062] Cloud environment 14 may include any suitable network-based computing environment as may serve a particular application. For example, cloud environment 14 may be implemented by one or more compute resources provided and/or otherwise managed by one or more cloud service providers, such as Amazon Web Services (AWS), Google Cloud Platform (GCP),

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00551

Microsoft Azure, and/or any other cloud service provider configured to provide public and/or private access to network-based compute resources.

[0063] Compute assets 16 may include, but are not limited to, containers (e.g., container images, deployed and executing container instances, etc.), virtual machines, workloads, applications, processes, physical machines, compute nodes, clusters of compute nodes, software runtime environments (e.g., container runtime environments), and/or any other virtual and/or physical compute resource that may reside in and/or be executed by one or more computer resources in cloud environment 14. In some examples, one or more compute assets 16 may reside in one or more datacenters.

[0064] A compute asset 16 may be associated with (e.g., owned, deployed, or managed by) a particular entity, such as a customer or client of cloud environment 14 and/or data platform 12. Accordingly, for purposes of the discussion herein, cloud environment 14 may be used by one or more entities.

[0065] Data platform 12 may be configured to perform one or more data security monitoring and/or remediation services, compliance monitoring services, anomaly detection services, DevOps services, compute asset management services, and/or any other type of data analytics service as may serve a particular implementation. Data platform 12 may be managed or otherwise associated with any suitable data platform provider, such as a provider of any of the data analytics services described herein. The various resources included in data platform 12 may reside in the cloud and/or be located on-premises and be implemented by any suitable combination of physical and/or virtual compute resources, such as one or more computing devices, microservices, applications, etc.

[0066] Data ingestion resources 18 may be configured to ingest data from cloud environment 14 into data platform 12. This may be performed in various ways, some of which are described in detail herein. For example, as illustrated by arrow 26, data ingestion resources 18 may be configured to receive the data from one or more agents deployed within cloud environment 14, utilize an event streaming platform (e.g., Kafka) to obtain the data, and/or pull data (e.g., configuration data) from cloud environment 14. In some examples, data ingestion resources 18 may obtain the data using one or more agentless configurations.

[0067] The data ingested by data ingestion resources 18 from cloud environment 14 may include any type of data as may serve a particular implementation. For example, the data may include data representative of configuration information associated with compute assets 16, information about one or more processes running on compute assets 16, network activity information, information about events (creation events, modification events, communication events, user-initiated events, etc.) that occur with respect to compute assets 16, etc. In some examples, the

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00552

data may or may not include actual customer data processed or otherwise generated by compute assets 16.

[0068] As illustrated by arrow 28, data ingestion resources 18 may be configured to load the data ingested from cloud environment 14 into a data store 30. Data store 30 is illustrated in Fig. 1A as being separate from and communicatively coupled to data platform 12. However, in some alternative embodiments, data store 30 is included within data platform 12.

[0069] Data store 30 may be implemented by any suitable data warehouse, data lake, data mart, and/or other type of database structure as may serve a particular implementation. Such data stores may be proprietary or may be embodied as vendor provided products or services such as, for example, Snowflake, Google BigQuery, Druid, Amazon Redshift, IBM Db2, Dremio, Databricks Lakehouse Platform, Cloudera, Azure Synapse Analytics, and others.

[0070] Although the examples described herein largely relate to embodiments where data is collected from agents and ultimately stored in a data store such as those provided by Snowflake, in other embodiments data that is collected from agents and other sources may be stored in different ways. For example, data that is collected from agents and other sources may be stored in a data warehouse, data lake, data mart, and/or any other data store.

[0071] A data warehouse may be embodied as an analytic database (e.g., a relational database) that is created from two or more data sources. Such a data warehouse may be leveraged to store historical data, often on the scale of petabytes. Data warehouses may have compute and memory resources for running complicated queries and generating reports. Data warehouses may be the data sources for business intelligence ('BI') systems, machine learning applications, and/or other applications. By leveraging a data warehouse, data that has been copied into the data warehouse may be indexed for good analytic query performance, without affecting the write performance of a database (e.g., an Online Transaction Processing ('OLTP') database). Data warehouses also enable the joining of data from multiple sources for analysis. For example, a sales OLTP application probably has no need to know about the weather at various sales locations, but sales predictions could take advantage of that data. By adding historical weather data to a data warehouse, it would be possible to factor it into models of historical sales data.

[0072] Data lakes, which store files of data in their native format, may be considered as "schema on read" resources. As such, any application that reads data from the lake may impose its own types and relationships on the data. Data warehouses, on the other hand, are "schema on write," meaning that data types, indexes, and relationships are imposed on the data as it is stored in an enterprise data warehouse (EDW). "Schema on read" resources may be beneficial for data that may be used in several contexts and poses little risk of losing data. "Schema on write" resources may be beneficial for data that has a specific purpose, and good for data that must relate properly

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00553

to data from other sources. Such data stores may include data that is encrypted using homomorphic encryption, data encrypted using privacy-preserving encryption, smart contracts, non-fungible tokens, decentralized finance, and other techniques.

[0073] Data marts may contain data oriented towards a specific business line whereas data warehouses contain enterprise-wide data. Data marts may be dependent on a data warehouse, independent of the data warehouse (e.g., drawn from an operational database or external source), or a hybrid of the two. In embodiments described herein, different types of data stores (including combinations thereof) may be leveraged.

[0074] Data processing resources 20 may be configured to perform various data processing operations with respect to data ingested by data ingestion resources 18, including data ingested and stored in data store 30. For example, data processing resources 20 may be configured to perform one or more data security monitoring and/or remediation operations, compliance monitoring operations, anomaly detection operations, DevOps operations, compute asset management operations, and/or any other type of data analytics operation as may serve a particular implementation. Various examples of operations performed by data processing resources 20 are described herein.

[0075] As illustrated by arrow 32, data processing resources 20 may be configured to access data in data store 30 to perform the various operations described herein. In some examples, this may include performing one or more queries with respect to the data stored in data store 30. Such queries may be generated using any suitable query language.

[0076] In some examples, the queries provided by data processing resources 20 may be configured to direct data store 30 to perform one or more data analytics operations with respect to the data stored within data store 30. These data analytics operations may be with respect to data specific to a particular entity (e.g., data residing in one or more silos within data store 30 that are associated with a particular customer) and/or data associated with multiple entities. For example, data processing resources 20 may be configured to analyze data associated with a first entity and use the results of the analysis to perform one or more operations with respect to a second entity.

[0077] One or more operations performed by data processing resources 20 may be performed periodically according to a predetermined schedule. For example, one or more operations may be performed by processing resources 20 every hour or any other suitable time interval. Additionally or alternatively, one or more operations performed by data processing resources 20 may be performed in substantially real-time (or near real-time) as data is ingested into data platform 12. In this manner, the results of such operations (e.g., one or more detected anomalies in the data) may be provided to one or more external entities (e.g., computing device 24 and/or one or more users) in substantially real-time and/or in near real-time.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00554

[0078] User interface resources 22 may be configured to perform one or more user interface operations, examples of which are described herein. For example, user interface resources 22 may be configured to present one or more results of the data processing performed by data processing resources 20 to one or more external entities (e.g., computing device 24 and/or one or more users), as illustrated by arrow 34. As illustrated by arrow 36, user interface resources 22 may access data in data store 30 to perform the one or more user interface operations.

[0079] Fig. 1B illustrates an implementation of configuration 10 in which an agent 38 (e.g., agent 38-1 through agent 38-N) is installed on each of compute assets 16. As used herein, an agent may include a self-contained binary and/or other type of code or application that can be run on any appropriate platforms, including within containers and/or other virtual compute assets. Agents 38 may monitor the nodes on which they execute for a variety of different activities, including but not limited to, connection, process, user, machine, and file activities. In some examples, agents 38 can be executed in user space, and can use a variety of kernel modules (e.g., auditd, iptables, netfilter, pcap, etc.) to collect data. Agents can be implemented in any appropriate programming language, such as C or Golang, using applicable kernel APIs.

[0080] Agents 38 may be deployed in any suitable manner. For example, an agent 38 may be deployed as a containerized application or as part of a containerized application. As described herein, agents 38 may selectively report information to data platform 12 in varying amounts of detail and/or with variable frequency.

[0081] Also shown in Fig. 1B is a load balancer 40 configured to perform one or more load balancing operations with respect to data ingestion operations performed by data ingestion resources 18 and/or user interface operations performed by user interface resources 22. Load balancer 40 is shown to be included in data platform 12. However, load balancer 40 may alternatively be located external to data platform 12. Load balancer 40 may be implemented by any suitable microservice, application, and/or other computing resources. In some alternative examples, data platform 12 may not utilize a load balancer such as load balancer 40.

[0082] Also shown in Fig. 1B is long term storage 42 with which data ingestion resources may interface, as illustrated by arrow 44. Long term storage 42 may be implemented by any suitable type of storage resources, such as cloud-based storage (e.g., AWS S3, etc.) and/or on-premises storage and may be used by data ingestion resources 18 as part of the data ingestion process. Examples of this are described herein. In some examples, data platform 12 may not utilize long term storage 42.

[0083] The embodiments described herein can be implemented in numerous ways, including as a process; an apparatus; a system; a composition of matter; a computer program product embodied on a computer readable storage medium; and/or a processor, such as a processor configured to

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00555

execute instructions stored on and/or provided by a memory coupled to the processor. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. In general, the order of the steps of disclosed processes may be altered within the scope of the principles described herein. Unless stated otherwise, a component such as a processor or a memory described as being configured to perform a task may be implemented as a general component that is temporarily configured to perform the task at a given time or a specific component that is manufactured to perform the task. As used herein, the term 'processor' refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.

[0084] In some examples, a non-transitory computer-readable medium storing computer-readable instructions may be provided in accordance with the principles described herein. The instructions, when executed by a processor of a computing device, may direct the processor and/or computing device to perform one or more operations, including one or more of the operations described herein. Such instructions may be stored and/or transmitted using any of a variety of known computer-readable media.

[0085] A non-transitory computer-readable medium as referred to herein may include any non-transitory storage medium that participates in providing data (e.g., instructions) that may be read and/or executed by a computing device (e.g., by a processor of a computing device). For example, a non-transitory computer-readable medium may include, but is not limited to, any combination of non-volatile storage media and/or volatile storage media. Exemplary non-volatile storage media include, but are not limited to, read-only memory, flash memory, a solid-state drive, a magnetic storage device (e.g., a hard disk, a floppy disk, magnetic tape, etc.), ferroelectric random-access memory ("RAM"), and an optical disc (e.g., a compact disc, a digital video disc, a Blu-ray disc, etc.). Exemplary volatile storage media include, but are not limited to, RAM (e.g., dynamic RAM).

[0086] Fig. 1C illustrates an example computing device 50 that may be specifically configured to perform one or more of the processes described herein. Any of the systems, microservices, computing devices, and/or other components described herein may be implemented by computing device 50.

[0087] As shown in Fig. 1C, computing device 50 may include a communication interface 52, a processor 54, a storage device 56, and an input/output ("I/O") module 58 communicatively connected one to another via a communication infrastructure 60. While an exemplary computing device 50 is shown in Fig. 1C, the components illustrated in Fig. 1C are not intended to be limiting. Additional or alternative components may be used in other embodiments. Components of computing device 50 shown in Fig. 1C will now be described in additional detail.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00556

[0088] Communication interface 52 may be configured to communicate with one or more computing devices. Examples of communication interface 52 include, without limitation, a wired network interface (such as a network interface card), a wireless network interface (such as a wireless network interface card), a modem, an audio/video connection, and any other suitable interface.

[0089] Processor 54 generally represents any type or form of processing unit capable of processing data and/or interpreting, executing, and/or directing execution of one or more of the instructions, processes, and/or operations described herein. Processor 54 may perform operations by executing computer-executable instructions 62 (e.g., an application, software, code, and/or other executable data instance) stored in storage device 56.

[0090] Storage device 56 may include one or more data storage media, devices, or configurations and may employ any type, form, and combination of data storage media and/or device. For example, storage device 56 may include, but is not limited to, any combination of the non-volatile media and/or volatile media described herein. Electronic data, including data described herein, may be temporarily and/or permanently stored in storage device 56. For example, data representative of computer-executable instructions 62 configured to direct processor 54 to perform any of the operations described herein may be stored within storage device 56. In some examples, data may be arranged in one or more databases residing within storage device 56.

[0091] I/O module 58 may include one or more I/O modules configured to receive user input and provide user output. I/O module 58 may include any hardware, firmware, software, or combination thereof supportive of input and output capabilities. For example, I/O module 58 may include hardware and/or software for capturing user input, including, but not limited to, a keyboard or keypad, a touchscreen component (e.g., touchscreen display), a receiver (e.g., an RF or infrared receiver), motion sensors, and/or one or more input buttons.

[0092] I/O module 58 may include one or more devices for presenting output to a user, including, but not limited to, a graphics engine, a display (e.g., a display screen), one or more output drivers (e.g., display drivers), one or more audio speakers, and one or more audio drivers. In certain embodiments, I/O module 58 is configured to provide graphical data to a display for presentation to a user. The graphical data may be representative of one or more graphical user interfaces and/or any other graphical content as may serve a particular implementation.

[0093] Fig. 1D illustrates an example implementation 100 of configuration 10. As such, one or more components shown in Fig. 1D may implement one or more components shown in Fig. 1A and/or Fig. 1B. In particular, implementation 100 illustrates an environment in which activities that occur within datacenters are modeled using data platform 12. Using techniques described herein, a baseline of datacenter activity can be modeled, and deviations from that baseline can be

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00557

identified as anomalous. Anomaly detection can be beneficial in a security context, a compliance context, an asset management context, a DevOps context, and/or any other data analytics context as may serve a particular implementation.

[0094] Two example datacenters (104 and 106) are shown in Fig. 1D, and are associated with (e.g., belong to) entities named entity A and entity B, respectively. A datacenter may include dedicated equipment (e.g., owned and operated by entity A, or owned/leased by entity A and operated exclusively on entity A's behalf by a third party). A datacenter can also include cloud-based resources, such as infrastructure as a service (IaaS), platform as a service (PaaS), and/or software as a service (SaaS) elements. The techniques described herein can be used in conjunction with multiple types of datacenters, including ones wholly using dedicated equipment, ones that are entirely cloud-based, and ones that use a mixture of both dedicated equipment and cloud-based resources.

[0095] Both datacenter 104 and datacenter 106 include a plurality of nodes, depicted collectively as set of nodes 108 and set of nodes 110, respectively, in Fig. 1D. These nodes may implement compute assets 16. Installed on each of the nodes are in-server / in-virtual machine (VM) / embedded in IoT device agents (e.g., agent 112), which are configured to collect data and report it to data platform 12 for analysis. As described herein, agents may be small, self-contained binaries that can be run on any appropriate platforms, including virtualized ones (and, as applicable, within containers). Agents may monitor the nodes on which they execute for a variety of different activities, including: connection, process, user, machine, and file activities. Agents can be executed in user space, and can use a variety of kernel modules (e.g., auditd, iptables, netfilter, pcap, etc.) to collect data. Agents can be implemented in any appropriate programming language, such as C or Golang, using applicable kernel APIs.

[0096] As described herein, agents can selectively report information to data platform 12 in varying amounts of detail and/or with variable frequency. As is also described herein, the data collected by agents may be used by data platform 12 to create polygraphs, which are graphs of logical entities, connected by behaviors. In some embodiments, agents report information directly to data platform 12. In other embodiments, at least some agents provide information to a data aggregator, such as data aggregator 114, which in turn provides information to data platform 12. The functionality of a data aggregator can be implemented as a separate binary or other application (distinct from an agent binary), and can also be implemented by having an agent execute in an "aggregator mode" in which the designated aggregator node acts as a Layer 7 proxy for other agents that do not have access to data platform 12. Further, a chain of multiple aggregators can be used, if applicable (e.g., with agent 112 providing data to data aggregator 114, which in turn provides data to another aggregator (not pictured) which provides data to data

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00558

platform 12). An example way to implement an aggregator is through a program written in an appropriate language, such as C or Golang.

[0097] Use of an aggregator can be beneficial in sensitive environments (e.g., involving financial or medical transactions) where various nodes are subject to regulatory or other architectural requirements (e.g., prohibiting a given node from communicating with systems outside of datacenter 104). Use of an aggregator can also help to minimize security exposure more generally. As one example, by limiting communications with data platform 12 to data aggregator 114, individual nodes in nodes 108 need not make external network connections (e.g., via Internet 124), which can potentially expose them to compromise (e.g., by other external devices, such as device 118, operated by a criminal). Similarly, data platform 12 can provide updates, configuration information, etc., to data aggregator 114 (which in turn distributes them to nodes 108), rather than requiring nodes 108 to allow incoming connections from data platform 12 directly.

[0098] Another benefit of an aggregator model is that network congestion can be reduced (e.g., with a single connection being made at any given time between data aggregator 114 and data platform 12, rather than potentially many different connections being open between various of nodes 108 and data platform 12). Similarly, network consumption can also be reduced (e.g., with the aggregator applying compression techniques/bundling data received from multiple agents).

[0099] One example way that an agent (e.g., agent 112, installed on node 116) can provide information to data aggregator 114 is via a REST API, formatted using data serialization protocols such as Apache Avro. One example type of information sent by agent 112 to data aggregator 114 is status information. Status information may be sent by an agent periodically (e.g., once an hour or once any other predetermined amount of time). Alternatively, status information may be sent continuously or in response to occurrence of one or more events. The status information may include, but is not limited to, a. an amount of event backlog (in bytes) that has not yet been transmitted, b. configuration information, c. any data loss period for which data was dropped, d. a cumulative count of errors encountered since the agent started, e. version information for the agent binary, and/or f. cumulative statistics on data collection (e.g., number of network packets processed, new processes seen, etc.).

[00100] A second example type of information that may be sent by agent 112 to data aggregator 114 is event data (described in more detail herein), which may include a UTC timestamp for each event. As applicable, the agent can control the amount of data that it sends to the data aggregator in each call (e.g., a maximum of 10MB) by adjusting the amount of data sent to manage the conflicting goals of transmitting data as soon as possible, and maximizing throughput. Data can also be compressed or uncompressed by the agent (as applicable) prior to sending the data.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00559

[00101] Each data aggregator may run within a particular customer environment. A data aggregator (e.g., data aggregator 114) may facilitate data routing from many different agents (e.g., agents executing on nodes 108) to data platform 12. In various embodiments, data aggregator 114 may implement a SOCKS 5 caching proxy through which agents can connect to data platform 12. As applicable, data aggregator 114 can encrypt (or otherwise obfuscate) sensitive information prior to transmitting it to data platform 12, and can also distribute key material to agents which can encrypt the information (as applicable). Data aggregator 114 may include a local storage, to which agents can upload data (e.g., pcap packets). The storage may have a key-value interface. The local storage can also be omitted, and agents configured to upload data to a cloud storage or other storage area, as applicable. Data aggregator 114 can, in some embodiments, also cache locally and distribute software upgrades, patches, or configuration information (e.g., as received from data platform 12).

[00102] Various examples associated with agent data collection and reporting will now be described.

[00103] In the following example, suppose that a user (e.g., a network administrator) at entity A (hereinafter "user A") has decided to begin using the services of data platform 12. In some embodiments, user A may access a web frontend (e.g., web app 120) using a computer 126 and enrolls (on behalf of entity A) an account with data platform 12. After enrollment is complete, user A may be presented with a set of installers, pre-built and customized for the environment of entity A, that user A can download from data platform 12 and deploy on nodes 108. Examples of such installers include, but are not limited to, a Windows executable file, an iOS app, a Linux package (e.g., .deb or .rpm), a binary, or a container (e.g., a Docker container). When a user (e.g., a network administrator) at entity B (hereinafter "user B") also signs up for the services of data platform 12, user B may be similarly presented with a set of installers that are pre-built and customized for the environment of entity B.

[00104] User A deploys an appropriate installer on each of nodes 108 (e.g., with a Windows executable file deployed on a Windows-based platform or a Linux package deployed on a Linux platform, as applicable). As applicable, the agent can be deployed in a container. Agent deployment can also be performed using one or more appropriate automation tools, such as Chef, Puppet, Salt, and Ansible. Deployment can also be performed using managed/hosted container management/orchestration frameworks such as Kubernetes, Mesos, and/or Docker Swarm.

[00105] In various embodiments, the agent may be installed in the user space (i.e., is not a kernel module), and the same binary is executed on each node of the same type (e.g., all Windows-based platforms have the same Windows-based binary installed on them). An illustrative function of an agent, such as agent 112, is to collect data (e.g., associated with node 116) and report it

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00560

(e.g., to data aggregator 114). Other tasks that can be performed by agents include data configuration and upgrading.

[00106] One approach to collecting data as described herein is to collect virtually all information available about a node (and, e.g., the processes running on it). Alternatively, the agent may monitor for network connections, and then begin collecting information about processes associated with the network connections, using the presence of a network packet associated with a process as a trigger for collecting additional information about the process. As an example, if a user of node 116 executes an application, such as a calculator application, which does not typically interact with the network, no information about use of that application may be collected by agent 112 and/or sent to data aggregator 114. If, however, the user of node 116 executes an ssh command (e.g., to ssh from node 116 to node 122), agent 112 may collect information about the process and provide associated information to data aggregator 114. In various embodiments, the agent may always collect/report information about certain events, such as privilege escalation, irrespective of whether the event is associated with network activity.

[00107] An approach to collecting information (e.g., by an agent) is as follows, and described in conjunction with process 200 depicted in Fig. 2A. An agent (e.g., agent 112) monitors its node (e.g., node 116) for network activity. One example way that agent 112 can monitor node 116 for network activity is by using a network packet capture tool (e.g., listening using libpcap). As packets are received (201), the agent obtains and maintains (e.g., in an in-memory cache) connection information associated with the network activity (202). Examples of such information include DNS query/response, TCP, UDP, and IP information.

[00108] The agent may also determine a process associated with the network connection (203). One example approach is for the agent to use a kernel network diagnostic API (e.g., netlink_diag) to obtain inode/process information from the kernel. Another example approach is for the agent to scan using netstat (e.g., on /proc/net/tcp, /proc/net/tcp6, /proc/net/udp, and /proc/net/udp6) to obtain sockets and relate them to processes. Information such as socket state (e.g., whether a socket is connected, listening, etc.) can also be collected by the agent.

[00109] One way an agent can obtain a mapping between a given inode and a process identifier is to scan within the /proc/pid directory. For each of the processes currently running, the agent examines each of their file descriptors. If a file descriptor is a match for the inode, the agent can determine that the process associated with the file descriptor owns the inode. Once a mapping is determined between an inode and a process identifier, the mapping is cached. As additional packets are received for the connection, the cached process information is used (rather than a new search being performed).

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00561

[00110] In some cases, exhaustively scanning for an inode match across every file descriptor may not be feasible (e.g., due to CPU limitations). In various embodiments, searching through file descriptors is accordingly optimized. User filtering is one example of such an optimization. A given socket is owned by a user. Any processes associated with the socket will be owned by the same user as the socket. When matching an inode (identified as relating to a given socket) against processes, the agent can filter through the processes and only examine the file descriptors of processes sharing the same user owner as the socket. In various embodiments, processes owned by root are always searched against (e.g., even when user filtering is employed).

[00111] Another example of an optimization is to prioritize searching the file descriptors of certain processes over others. One such prioritization is to search through the subdirectories of /proc/ starting with the youngest process. One approximation of such a sort order is to search through /proc/ in reverse order (e.g., examining highest numbered processes first). Higher numbered processes are more likely to be newer (i.e., not long-standing processes), and thus more likely to be associated with new connections (i.e., ones for which inode-process mappings are not already cached). In some cases, the most recently created process may not have the highest process identifier (e.g., due to the kernel wrapping through process identifiers).

[00112] Another example prioritization is to query the kernel for an identification of the most recently created process and to search in a backward order through the directories in /proc/ (e.g., starting at the most recently created process and working backwards, then wrapping to the highest value (e.g., 32768) and continuing to work backward from there). An alternate approach is for the agent to keep track of the newest process that it has reported information on (e.g., to data aggregator 114), and begin its search of /proc/ in a forward order starting from the PID of that process.

[00113] Another example prioritization is to maintain, for each user actively using node 116, a list of the five (or any other number) most recently active processes. Those processes are more likely than other processes (less active, or passive) on node 116 to be involved with new connections, and can thus be searched first. For many processes, lower valued file descriptors tend to correspond to non-sockets (e.g., stdin, stdout, stderr). Yet another optimization is to preferentially search higher valued file descriptors (e.g., across processes) over lower valued file descriptors (that are less likely to yield matches).

[00114] In some cases, while attempting to locate a process identifier for a given inode, an agent may encounter a socket that does not correspond to the inode being matched against and is not already cached. The identity of that socket (and its corresponding inode) can be cached, once discovered, thus removing a future need to search for that pair.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00562

[00115] In some cases, a connection may terminate before the agent is able to determine its associated process (e.g., due to a very short-lived connection, due to a backlog in agent processing, etc.). One approach to addressing such a situation is to asynchronously collect information about the connection using the audit kernel API, which streams information to user space. The information collected from the audit API (which can include PID/inode information) can be matched by the agent against pcap/inode information. In some embodiments, the audit API is always used, for all connections. However, due to CPU utilization considerations, use of the audit API can also be reserved for short/otherwise problematic connections (and/or omitted, as applicable).

[00116] Once the agent has determined which process is associated with the network connection (203), the agent can then collect additional information associated with the process (204). As will be described in more detail below, some of the collected information may include attributes of the process (e.g., a process parent hierarchy, and an identification of a binary associated with the process). As will also be described in more detail below, other of the collected information is derived (e.g., session summarization data and hash values).

[00117] The collected information is then transmitted (205), e.g., by an agent (e.g., agent 112) to a data aggregator (e.g., data aggregator 114), which in turn provides the information to data platform 12. In some embodiments, all information collected by an agent may be transmitted (e.g., to a data aggregator and/or to data platform 12). In other embodiments, the amount of data transmitted may be minimized (e.g., for efficiency reasons), using various techniques.

[00118] One approach to minimizing the amount of data flowing from agents (such as agents installed on nodes 108) to data platform 12 is to use a technique of implicit references with unique keys. The keys can be explicitly used by data platform 12 to extract/derive relationships, as necessary, in a data set at a later time, without impacting performance.

[00119] As previously mentioned, some data collected about a process is constant and does not change over the lifetime of the process (e.g., attributes), and some data changes (e.g., statistical information and other variable information). Constant data can be transmitted (210) once, when the agent first becomes aware of the process. And, if any changes to the constant data are detected (e.g., a process changes its parent), a refreshed version of the data can be transmitted (210) as applicable.

[00120] In some examples, an agent may collect variable data (e.g., data that may change over the lifetime of the process). In some examples, variable data can be transmitted (210) at periodic (or other) intervals. Alternatively, variable data may be transmitted in substantially real time as it is collected. In some examples, the variable data may indicate a thread count for a process, a total virtual memory used by the process, the total resident memory used by the process, the total time

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00563

spent by the process executing in user space, and/or the total time spent by the process executing in kernel space. In some examples, the data may include a hash that may be used within data platform 12 to join process creation time attributes with runtime attributes to construct a full dataset.

[00121] Below are additional examples of data that an agent, such as agent 112, can collect and provide to data platform 12.

[00122] 1. User Data

[00123] Core User Data: user name, UID (user ID), primary group, other groups, home directory.

[00124] Failed Login Data: IP address, hostname, username, count.

[00125] User Login Data: user name, hostname, IP address, start time, TTY (terminal), UID (user ID), GID (group ID), process, end time.

[00126] 2. Machine Data

[00127] Dropped Packet Data: source IP address, destination IP address, destination port, protocol, count.

[00128] Machine Data: hostname, domain name, architecture, kernel, kernel release, kernel version, OS, OS version, OS description, CPU, memory, model number, number of cores, last boot time, last boot reason, tags (e.g., Cloud provider tags such as AWS, GCP, or Azure tags), default router, interface name, interface hardware address, interface IP address and mask, promiscuous mode.

[00129] 3. Network Data

[00130] Network Connection Data: source IP address, destination IP address, source port, destination port, protocol, start time, end time, incoming and outgoing bytes, source process, destination process, direction of connection, histograms of packet length, inter packet delay, session lengths, etc.

[00131] Listening Ports in Server: source IP address, port number, protocol, process.

[00132] Dropped Packet Data: source IP address, destination IP address, destination port, protocol, count.

[00133] Arp Data: source hardware address, source IP address, destination hardware address, destination IP address.

[00134] DNS Data: source IP address, response code, response string, question (request), packet length, final answer (response).

[00135] 4. Application Data

[00136] Package Data: exe path, package name, architecture, version, package path, checksums (MD5, SHA-1, SHA-256), size, owner, owner ID.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00564

[00137] Application Data: command line, PID (process ID), start time, UID (user ID), EUID (effective UID), PPID (parent process ID), PGID (process group ID), SID (session ID), exe path, username, container ID.

[00138] 5. Container Data

[00139] Container Image Data: image creation time, parent ID, author, container type, repo, (AWS) tags, size, virtual size, image version.

[00140] Container Data: container start time, container type, container name, container ID, network mode, privileged, PID mode, IP addresses, listening ports, volume map, process ID.

[00141] 6. File Data

[00142] File path, file data hash, symbolic links, file creation data, file change data, file metadata, file mode.

[00143] As mentioned above, an agent, such as agent 112, can be deployed in a container (e.g., a Docker container), and can also be used to collect information about containers. Collection about a container can be performed by an agent irrespective of whether the agent is itself deployed in a container or not (as the agent can be deployed in a container running in a privileged mode that allows for monitoring).

[00144] Agents can discover containers (e.g., for monitoring) by listening for container create events (e.g., provided by Docker), and can also perform periodic ordered discovery scans to determine whether containers are running on a node. When a container is discovered, the agent can obtain attributes of the container, e.g., using standard Docker API calls (e.g., to obtain IP addresses associated with the container, whether there's a server running inside, what port it is listening on, associated PIDs, etc.). Information such as the parent process that started the container can also be collected, as can information about the image (which comes from the Docker repository).

[00145] In various embodiments, agents may use namespaces to determine whether a process is associated with a container. Namespaces are a feature of the Linux kernel that can be used to isolate resources of a collection of processes. Examples of namespaces include process ID (PID) namespaces, network namespaces, and user namespaces. Given a process, the agent can perform a fast lookup to determine whether the process is part of the namespace the container claims to be its namespace.

[00146] As mentioned, agents can be configured to report certain types of information (e.g., attribute information) once, when the agent first becomes aware of a process. In various embodiments, such static information is not reported again (or is reported once a day, every twelve hours, etc.), unless it changes (e.g., a process changes its parent, changes its owner, or a SHA-1 of the binary associated with the process changes).

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00565

[00147] In contrast to static/attribute information, certain types of data change constantly (e.g., network-related data). In various embodiments, agents are configured to report a list of current connections every minute (or other appropriate time interval). In that connection list will be connections that started in that minute interval, connections that ended in that minute interval, and connections that were ongoing throughout the minute interval (e.g., a one minute slice of a one hour connection).

[00148] In various embodiments, agents are configured to collect/compute statistical information about connections (e.g., at the one minute level of granularity and or at any other time interval). Examples of such information include, for the time interval, the number of bytes transferred, and in which direction. Another example of information collected by an agent about a connection is the length of time between packets. For connections that span multiple time intervals (e.g., a seven minute connection), statistics may be calculated for each minute of the connection. Such statistical information (for all connections) can be reported (e.g., to a data aggregator) once a minute.

[00149] In various embodiments, agents are also configured to maintain histogram data for a given network connection, and provide the histogram data (e.g., in the Apache Avro data exchange format) under the Connection event type data. Examples of such histograms include: 1. a packet length histogram (packet_len_hist), which characterizes network packet distribution; 2. a session length histogram (session_len_hist), which characterizes a network session length; 3. a session time histogram (session_time_hist), which characterizes a network session time; and 4. a session switch time histogram (session_switch_time_hist), which characterizes network session switch time (i.e., incoming->outgoing and vice versa). For example, histogram data may include one or more of the following fields: 1. count, which provides a count of the elements in the sampling; 2. sum, which provides a sum of elements in the sampling; 3. max, which provides the highest value element in the sampling; 4. std_dev, which provides the standard deviation of elements in the sampling; and 5. buckets, which provides a discrete sample bucket distribution of sampling data (if applicable).

[00150] For some protocols (e.g., HTTP), typically, a connection is opened, a string is sent, a string is received, and the connection is closed. For other protocols (e.g., NFS), both sides of the connection engage in a constant chatter. Histograms allow data platform 12 to model application behavior (e.g., using machine learning techniques), for establishing baselines, and for detecting deviations. As one example, suppose that a given HTTP server typically sends/receives 1,000 bytes (in each direction) whenever a connection is made with it. If a connection generates 500 bytes of traffic, or 2,000 bytes of traffic, such connections would be considered within the typical

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00566

usage pattern of the server. Suppose, however, that a connection is made that results in 10G of traffic. Such a connection is anomalous and can be flagged accordingly.

[00151] Returning to Fig. 1D, as previously mentioned, data aggregator 114 may be configured to provide information (e.g., collected from nodes 108 by agents) to data platform 12. Data aggregator 128 may be similarly configured to provide information to data platform 12. As shown in Fig. 1D, both aggregator 114 and aggregator 128 may connect to a load balancer 130, which accepts connections from aggregators (and/or as applicable, agents), as well as other devices, such as computer 126 (e.g., when it communicates with web app 120), and supports fair balancing. In various embodiments, load balancer 130 is a reverse proxy that load balances accepted connections internally to various microservices (described in more detail below), allowing for services provided by data platform 12 to scale up as more agents are added to the environment and/or as more entities subscribe to services provided by data platform 12. Example ways to implement load balancer 130 include, but are not limited to, using HaProxy, using nginx, and using elastic load balancing (ELB) services made available by Amazon.

[00152] Agent service 132 is a microservice that is responsible for accepting data collected from agents (e.g., provided by aggregator 114). In various embodiments, agent service 132 uses a standard secure protocol, such as HTTPS to communicate with aggregators (and as applicable agents), and receives data in an appropriate format such as Apache Avro. When agent service 132 receives an incoming connection, it can perform a variety of checks, such as to see whether the data is being provided by a current customer, and whether the data is being provided in an appropriate format. If the data is not appropriately formatted (and/or is not provided by a current customer), it may be rejected.

[00153] If the data is appropriately formatted, agent service 132 may facilitate copying the received data to a streaming data stable storage using a streaming service (e.g., Amazon Kinesis and/or any other suitable streaming service. Once the ingesting into the streaming service is complete, service 132 may send an acknowledgement to the data provider (e.g., data aggregator 114). If the agent does not receive such an acknowledgement, it is configured to retry sending the data to data platform 12. One way to implement agent service 132 is as a REST API server framework (e.g., Java DropWizard), configured to communicate with Kinesis (e.g., using a Kinesis library).

[00154] In various embodiments, data platform 12 uses one or more streams (e.g., Kinesis streams) for all incoming customer data (e.g., including data provided by data aggregator 114 and data aggregator 128), and the data is sharded based on the node (also referred to herein as a "machine") that originated the data (e.g., node 116 vs. node 122), with each node having a

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00567

globally unique identifier within data platform 12. Multiple instances of agent service 132 can write to multiple shards.

[00155] Kinesis is a streaming service with a limited period (e.g., 1-7 days). To persist data longer than a day, the data may be copied to long term storage 42 (e.g., S3). Data loader 136 is a microservice that is responsible for picking up data from a data stream (e.g., a Kinesis stream) and persisting it in long term storage 42. In one example embodiment, files collected by data loader 136 from the Kinesis stream are placed into one or more buckets, and segmented using a combination of a customer identifier and time slice. Given a particular time segment, and a given customer identifier, the corresponding file (stored in long term storage) contains five minutes (or another appropriate time slice) of data collected at that specific customer from all of the customer's nodes. Data loader 136 can be implemented in any appropriate programming language, such as Java or C, and can be configured to use a Kinesis library to interface with Kinesis. In various embodiments, data loader 136 uses the Amazon Simple Queue Service (SQS) (e.g., to alert DB loader 140 that there is work for it to do).

[00156] DB loader 140 is a microservice that is responsible for loading data into an appropriate data store 30, such as SnowflakeDB or Amazon Redshift, using individual per-customer databases. In particular, DB loader 140 is configured to periodically load data into a set of raw tables from files created by data loader 136 as per above. DB loader 140 manages throughput, errors, etc., to make sure that data is loaded consistently and continuously. Further, DB loader 140 can read incoming data and load into data store 30 data that is not already present in tables of data store 30 (also referred to herein as a database). DB loader 140 can be implemented in any appropriate programming language, such as Java or C, and an SQL framework such as jOOQ (e.g., to manage SQLs for insertion of data), and SQL/JDBC libraries. In some examples, DB loader 140 may use Amazon S3 and Amazon Simple Queue Service (SQS) to manage files being transferred to and from data store 30.

[00157] Customer data included in data store 30 can be augmented with data from additional data sources, such as AWS CloudTrail and/or other types of external tracking services. To this end, data platform may include a tracking service analyzer 144, which is another microservice. Tracking service analyzer 144 may pull data from an external tracking service (e.g., Amazon CloudTrail) for each applicable customer account, as soon as the data is available. Tracking service analyzer 144 may normalize the tracking data as applicable, so that it can be inserted into data store 30 for later querying/analysis. Tracking service analyzer 144 can be written in any appropriate programming language, such as Java or C. Tracking service analyzer 144 also makes use of SQL/JDBC libraries to interact with data store 30 to insert/query data.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00568

[00158] As described herein, data platform 12 can model activities that occur within datacenters, such as datacenters 104 and 106. The model may be stable over time, and differences, even subtle ones (e.g., between a current state of the datacenter and the model) can be surfaced. The ability to surface such anomalies can be particularly beneficial in datacenter environments where rogue employees and/or external attackers may operate slowly (e.g., over a period of months), hoping that the elastic nature of typical resource use (e.g., virtualized servers) will help conceal their nefarious activities.

[00159] Using techniques described herein, data platform 12 can automatically discover entities (which may implement compute assets 16) deployed in a given datacenter. Examples of entities include workloads, applications, processes, machines, virtual machines, containers, files, IP addresses, domain names, and users. The entities may be grouped together logically (into analysis groups) based on behaviors, and temporal behavior baselines can be established. In particular, using techniques described herein, periodic graphs can be constructed (also referred to herein as polygraphs), in which the nodes are applicable logical entities, and the edges represent behavioral relationships between the logical entities in the graph. Baselines can be created for every node and edge.

[00160] Communication (e.g., between applications/nodes) is one example of a behavior. A model of communications between processes is an example of a behavioral model. As another example, the launching of applications is another example of a behavior that can be modeled. The baselines may be periodically updated (e.g., hourly) for every entity. Additionally or alternatively, the baselines may be continuously updated in substantially real-time as data is collected by agents. Deviations from the expected normal behavior can then be detected and automatically reported (e.g., as anomalies or threats detected). Such deviations may be due to a desired change, a misconfiguration, or malicious activity. As applicable, data platform 12 can score the detected deviations (e.g., based on severity and threat posed). Additional examples of analysis groups include models of machine communications, models of privilege changes, and models of insider behaviors (monitoring the interactive behavior of human users as they operate within the datacenter).

[00161] Two example types of information collected by agents are network level information and process level information. As previously mentioned, agents may collect information about every connection involving their respective nodes. And, for each connection, information about both the server and the client may be collected (e.g., using the connection-to-process identification techniques described above). DNS queries and responses may also be collected. The DNS query information can be used in logical entity graphing (e.g., collapsing many different IP addresses to a single service – e.g., s3.amazon.com). Examples of process level information collected by

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00569

agents include attributes (user ID, effective user ID, and command line). Information such as what user/application is responsible for launching a given process and the binary being executed (and its SHA-256 values) may also be provided by agents.

[00162] The dataset collected by agents across a datacenter can be very large, and many resources (e.g., virtual machines, IP addresses, etc.) are recycled very quickly. For example, an IP address and port number used at a first point in time by a first process on a first virtual machine may very rapidly be used (e.g., an hour later) by a different process/virtual machine.

[00163] A dataset (and elements within it) can be considered at both a physical level, and a logical level, as illustrated in Fig. 2B. In particular, Fig. 2B illustrates an example 5-tuple of data 210 collected by an agent, represented physically (216) and logically (217). The 5-tuple includes a source address 211, a source port 212, a destination address 213, a destination port 214, and a protocol 215. In some cases, port numbers (e.g., 212, 214) may be indicative of the nature of a connection (e.g., with certain port usage standardized). However, in many cases, and in particular in datacenters, port usage is ephemeral. For example, a Docker container can listen on an ephemeral port, which is unrelated to the service it will run. When another Docker container starts (for the same service), the port may well be different. Similarly, particularly in a virtualized environment, IP addresses may be recycled frequently (and are thus also potentially ephemeral) or could be NATed, which makes identification difficult.

[00164] A physical representation of the 5-tuple is depicted in region 216. A process 218 (executing on machine 219) has opened a connection to machine 220. In particular, process 218 is in communication with process 221. Information such as the number of packets exchanged between the two machines over the respective ports can be recorded.

[00165] As previously mentioned, in a datacenter environment, portions of the 5-tuple may change – potentially frequently – but still be associated with the same behavior. Namely, one application (e.g., Apache) may frequently be in communication with another application (e.g., Oracle), using ephemeral datacenter resources. Further, either/both of Apache and Oracle may be multi-homed. This can lead to potentially thousands of 5-tuples (or more) that all correspond to Apache communicating with Oracle within a datacenter. For example, Apache could be executed on a single machine, and could also be executed across fifty machines, which are variously spun up and down (with different IP addresses each time). An alternate representation of the 5-tuple of data 210 is depicted in region 217, and is logical. The logical representation of the 5-tuple aggregates the 5-tuple (along with other connections between Apache and Oracle having other 5-tuples) as logically representing the same connection. By aggregating data from raw physical connection information into logical connection information, using techniques described herein, a size reduction of six orders of magnitude in the data set can be achieved.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00570

[00166] Fig. 2C depicts a portion of a logical polygraph. Suppose a datacenter has seven instances of the application update_engine 225, executing as seven different processes on seven different machines, having seven different IP addresses, and using seven different ports. The instances of update_engine variously communicate with update.core-os.net 226, which may have a single IP address or many IP addresses itself, over the one hour time period represented in the polygraph. In the example shown in Fig. 2C, update_engine is a client, connecting to the server update.core-os.net, as indicated by arrow 228.

[00167] Behaviors of the seven processes are clustered together, into a single summary. As indicated in region 227, statistical information about the connections is also maintained (e.g., number of connections, histogram information, etc.). A polygraph such as is depicted in Fig. 2C can be used to establish a baseline of behavior (e.g., at the one-hour level), allowing for the future detection of deviations from that baseline. As one example, suppose that statistically an update_engine instance transmits data at 11 bytes per second. If an instance were instead to transmit data at 1000 bytes per second, such behavior would represent a deviation from the baseline and could be flagged accordingly. Similarly, changes that are within the baseline (e.g., an eighth instance of update_engine appears, but otherwise behaves as the other instances; or one of the seven instances disappears) are not flagged as anomalous. Further, datacenter events, such as failover, autobalancing, and A-B refresh are unlikely to trigger false alarms in a polygraph, as at the logical level, the behaviors remain the same.

[00168] In various embodiments, polygraph data is maintained for every application in a datacenter, and such polygraph data can be combined to make a single datacenter view across all such applications. Fig. 2D illustrates a portion of a polygraph for a service that evidences more complex behaviors than are depicted in Fig. 2C. In particular, Fig. 2D illustrates the behaviors of S3 as a service (as used by a particular customer datacenter). Clients within the datacenter variously connect to the S3 service using one of five fully qualified domains (listed in region 230). Contact with any of the domains is aggregated as contact with S3 (as indicated in region 231). Depicted in region 232 are various containers which (as clients) connect with S3. Other containers (which do not connect with S3) are not included. As with the polygraph portion depicted in Fig. 2C, statistical information about the connections is known and summarized, such as the number of bytes transferred, histogram information, etc.

[00169] Fig. 2E illustrates a communication polygraph for a datacenter. In particular, the polygraph indicates a one hour summary of approximately 500 virtual machines, which collectively run one million processes, and make 100 million connections in that hour. As illustrated in Fig. 2E, a polygraph represents a drastic reduction in size (e.g., from tracking information on 100 million connections in an hour, to a few hundred nodes and a few hundred

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00571

edges). Further, as a datacenter scales up (e.g., from using 10 virtual machines to 100 virtual machines as the datacenter uses more workers to support existing applications), the polygraph for the datacenter will tend to stay the same size (with the 100 virtual machines clustering into the same nodes that the 10 virtual machines previously clustered into). As new applications are added into the datacenter, the polygraph may automatically scale to include behaviors involving those applications.

[00170] In the particular polygraph shown in Fig. 2E, nodes generally correspond to workers, and edges correspond to communications the workers engage in (with connection activity being the behavior modeled in polygraph 235). Another example polygraph could model other behavior, such as application launching. The communications graphed in Fig. 2E include traffic entering the datacenter, traffic exiting the datacenter, and traffic that stays wholly within the datacenter (e.g., traffic between workers). One example of a node included in polygraph 235 is the sshd application, depicted as node 236. As indicated in Fig. 2E, 421 instances of sshd were executing during the one hour time period of data represented in polygraph 235. As indicated in region 237, nodes within the datacenter communicated with a total of 1349 IP addresses outside of the datacenter (and not otherwise accounted for, e.g., as belonging to a service such as Amazon AWS 238 or Slack 239).

[00171] In the following examples, suppose that user B, an administrator of datacenter 106, is interacting with data platform 12 to view visualizations of polygraphs in a web browser (e.g., as served to user B via web app 120). One type of polygraph user B can view is an application-communication polygraph, which indicates, for a given one hour window (or any other suitable time interval), which applications communicated with which other applications. Another type of polygraph user B can view is an application launch polygraph. User B can also view graphs related to user behavior, such as an insider behavior graph which tracks user connections (e.g., to internal and external applications, including chains of such behavior), a privilege change graph which tracks how privileges change between processes, and a user login graph, which tracks which (logical) machines a user logs into.

[00172] Fig. 2F illustrates an example of an application-communication polygraph for a datacenter (e.g., datacenter 106) for the one hour period of 9am-10am on June 5. The time slice currently being viewed is indicated in region 240. If user B clicks his mouse in region 241, user B will be shown a representation of the application-communication polygraph as generated for the following hour (10am-11am on June 5).

[00173] Fig. 2G depicts what is shown in user B's browser after he has clicked on region 241, and has further clicked on region 242. The selection in region 242 turns on and off the ability to compare two time intervals to one another. User B can select from a variety of options when

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00572

comparing the 9am-10am and 10am-11am time intervals. By clicking region 248, user B will be shown the union of both graphs (i.e., any connections that were present in either time interval). By clicking region 249, user B will be shown the intersection of both graphs (i.e., only those connections that were present in both time intervals).

[00174] As shown in Fig. 2G, user B has elected to click on region 250, which depicts connections that are only present in the 9am-10am polygraph in a first color 251, and depicts connections that are only present in the 10am-11am polygraph in a second color 252. Connections present in both polygraphs are omitted from display. As one example, in the 9am-10am polygraph (corresponding to connections made during the 9am-10am time period at datacenter 106), a connection was made by a server to sshd (253) and also to systemd (254). Both of those connections ended prior to 10am and are thus depicted in the first color. As another example, in the 10am-11am polygraph (corresponding to connections made during the 10am-11am time period at datacenter 106), a connection was made from a known bad external IP to nginx (255). The connection was not present during the 9am-10am time slice and thus is depicted in the second color. As yet another example, two different connections were made to a Slack service between 9am and 11am. However, the first was made by a first client during the 9am-10am time slice (256) and the second was made by a different client during the 10am-11am slice (257), and so the two connections are depicted respectively in the first and second colors and blue.

[00175] Returning to the polygraph depicted in Fig. 2F, suppose user B enters "etcd" into the search box located in region 244. User B will then be presented with the interface illustrated in Fig. 2H. As shown in Fig. 2H, three applications containing the term "etcd" were engaged in communications during the 9am-10am window. One application is etcdctl, a command line client for etcd. As shown in Fig. 2H, a total of three different etcdctl processes were executed during the 9am-10am window, and were clustered together (260). Fig. 2H also depicts two different clusters that are both named etcd2. The first cluster includes (for the 9am-10am window) five members (261) and the second cluster includes (for the same window) eight members (262). The reason for these two distinct clusters is that the two groups of applications behave differently (e.g., they exhibit two distinct sets of communication patterns). Specifically, the instances of etcd2 in cluster 261 only communicate with locksmithctl (263) and other etcd2 instances (in both clusters 261 and 262). The instances of etcd2 in cluster 262 communicate with additional entities, such as etcdctl and Docker containers. As desired, user B can click on one of the clusters (e.g., cluster 261) and be presented with summary information about the applications included in the cluster, as is shown in Fig. 2I (e.g., in region 265). User B can also double click on a given

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00573

cluster (e.g., cluster 261) to see details on each of the individual members of the cluster broken out.

[00176] Suppose user B now clicks on region 245 of the interface shown in Fig. 2F. User B will then be shown an application launch polygraph. Launching an application is another example of a behavior. The launch polygraph models how applications are launched by other applications. Fig. 2J illustrates an example of a portion of a launch polygraph. In particular, user B has typed "find" into region 266, to see how the "find" application is being launched. As shown in Fig. 2J, in the launch polygraph for the 10am-11am time period, find applications (267) are always launched by bash (268), which is in turn always launched by systemd (269). If find is launched by a different application, this would be anomalous behavior.

[00177] Fig. 2K illustrates another example of a portion of an application launch polygraph. In Fig. 2K, user B has searched (270) for "python ma" to see how "python marathon_lb" (271) is launched. As shown in Fig. 2K, in each case (during the one hour time slice of 10am-11am), python marathon_lb is launched as a result of a chain of the same seven applications each time. If python marathon_lb is ever launched in a different manner, this indicates anomalous behavior. The behavior could be indicative of malicious activities, but could also be due to other reasons, such as a misconfiguration, a performance-related issue, and/or a failure, etc.

[00178] Suppose user B now clicks on region 246 of the interface shown in Fig. 2F. User B will then be shown an insider behavior graph. The insider behavior graph tracks information about behaviors such as processes started by a user interactively using protocols such as ssh or telnet, and any processes started by those processes. As one example, suppose an administrator logs into a first virtual machine in datacenter 106 (e.g., using sshd via an external connection he makes from a hotel), using a first set of credentials (e.g., first.last@example.com and an appropriate password). From the first virtual machine, the administrator connects to a second virtual machine (e.g., using the same credentials), then uses the sudo command to change identities to those of another user, and then launches a program. graphs built by data platform 12 can be used to associate the administrator with each of his actions, including launching the program using the identity of another user.

[00179] Fig. 2L illustrates an example of a portion of an insider behavior graph. In particular, in Fig. 2L, user B is viewing a graph that corresponds to the time slice of 3pm-4pm on June 1. Fig. 2L illustrates the internal/external applications that users connected to during the one hour time slice. If a user typically communicates with particular applications, that information will become part of a baseline. If the user deviates from his baseline behavior (e.g., using new applications, or changing privilege in anomalous ways), such anomalies can be surfaced.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00574

[00180] Fig. 2M illustrates an example of a portion of a privilege change graph, which identifies how privileges are changed between processes. Typically, when a user launches a process (e.g., "ls"), the process inherits the same privileges that the user has. And, while a process can have fewer privileges than the user (i.e., go down in privilege), it is rare (and generally undesirable) for a user to escalate in privilege. Information included in the privilege change graph can be determined by examining the parent of each running process, and determining whether there is a match in privilege between the parent and the child. If the privileges are different, a privilege change has occurred (whether a change up or a change down). The application ntpd is one rare example of a scenario in which a process escalates (272) to root, and then returns back (273). The sudo command is another example (e.g., used by an administrator to temporarily have a higher privilege). As with the other examples, ntpd's privilege change actions, and the legitimate actions of various administrators (e.g., using sudo) will be incorporated into a baseline model by data platform 12. When deviations occur, such as where a new application that is not ntpd escalates privilege, or where an individual that has not previously/does not routinely use sudo does so, such behaviors can be identified as anomalous.

[00181] Fig. 2N illustrates an example of a portion of a user login graph, which identifies which users log into which logical nodes. Physical nodes (whether bare metal or virtualized) are clustered into a logical machine cluster, for example, using yet another graph, a machine-server graph, an example of which is shown in Fig. 2O. For each machine, a determination is made as to what type of machine it is, based on what kind(s) of workflows it runs. As one example, some machines run as master nodes (having a typical set of workflows they run, as master nodes) and can thus be clustered as master nodes. Worker nodes are different from master nodes, for example, because they run Docker containers, and frequently change as containers move around. Worker nodes can similarly be clustered.

[00182] As previously mentioned, the polygraph depicted in Fig. 2E corresponds to activities in a datacenter in which, in a given hour, approximately 500 virtual machines collectively run one million processes, and make 100 million connections in that hour. The polygraph represents a drastic reduction in size (e.g., from tracking information on 100 million connections in an hour, to a few hundred nodes and a few hundred edges). Using techniques described herein, such a polygraph can be constructed (e.g., using commercially available computing infrastructure) in less than an hour (e.g., within a few minutes). Thus, ongoing hourly snapshots of a datacenter can be created within a two hour moving window (i.e., collecting data for the time period 8am-9am, while also generating a snapshot for the time previous time period 7am-8am). The following describes various example infrastructure that can be used in polygraph construction, and also describes various techniques that can be used to construct polygraphs.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00575

[00183] Returning to Fig. 1D, embodiments of data platform 12 may be built using any suitable infrastructure as a service (IaaS) (e.g., AWS). For example, data platform 12 can use Simple Storage Service (S3) for data storage, Key Management Service (KMS) for managing secrets, Simple Queue Service (SQS) for managing messaging between applications, Simple Email Service (SES) for sending emails, and Route 53 for managing DNS. Other infrastructure tools can also be used. Examples include: orchestration tools (e.g., Kubernetes or Mesos/Marathon), service discovery tools (e.g., Mesos-DNS), service load balancing tools (e.g., marathon-LB), container tools (e.g., Docker or rkt), log/metric tools (e.g., collectd, fluentd, kibana, etc.), big data processing systems (e.g., Spark, Hadoop, AWS Redshift, Snowflake etc.), and distributed key value stores (e.g., Apache Zookeeper or etcd2).

[00184] As previously mentioned, in various embodiments, data platform 12 may make use of a collection of microservices. Each microservice can have multiple instances, and may be configured to recover from failure, scale, and distribute work amongst various such instances, as applicable. For example, microservices are auto-balancing for new instances, and can distribute workload if new instances are started or existing instances are terminated. In various embodiments, microservices may be deployed as self-contained Docker containers. A Mesos-Marathon or Spark framework can be used to deploy the microservices (e.g., with Marathon monitoring and restarting failed instances of microservices as needed). The service etcd2 can be used by microservice instances to discover how many peer instances are running, and used for calculating a hash-based scheme for workload distribution. Microservices may be configured to publish various health/status metrics to either an SQS queue, or etcd2, as applicable. In some examples, Amazon DynamoDB can be used for state management.

[00185] Additional information on various microservices used in embodiments of data platform 12 is provided below.

[00186] Graph generator 146 is a microservice that may be responsible for generating raw behavior graphs on a per customer basis periodically (e.g., once an hour). In particular, graph generator 146 may generate graphs of entities (as the nodes in the graph) and activities between entities (as the edges). In various embodiments, graph generator 146 also performs other functions, such as aggregation, enrichment (e.g., geolocation and threat), reverse DNS resolution, TF-IDF based command line analysis for command type extraction, parent process tracking, etc.

[00187] Graph generator 146 may perform joins on data collected by the agents, so that both sides of a behavior are linked. For example, suppose a first process on a first virtual machine (e.g., having a first IP address) communicates with a second process on a second virtual machine (e.g., having a second IP address). Respective agents on the first and second virtual machines may each report information on their view of the communication (e.g., the PID of their respective

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00576

processes, the amount of data exchanged and in which direction, etc.). When graph generator performs a join on the data provided by both agents, the graph will include a node for each of the processes, and an edge indicating communication between them (as well as other information, such as the directionality of the communication – i.e., which process acted as the server and which as the client in the communication).

[00188] In some cases, connections are process to process (e.g., from a process on one virtual machine within the cloud environment associated with entity A to another process on a virtual machine within the cloud environment associated with entity A). In other cases, a process may be in communication with a node (e.g., outside of entity A) which does not have an agent deployed upon it. As one example, a node within entity A might be in communication with node 172, outside of entity A. In such a scenario, communications with node 172 are modeled (e.g., by graph generator 146) using the IP address of node 172. Similarly, where a node within entity A does not have an agent deployed upon it, the IP address of the node can be used by graph generator in modeling.

[00189] Graphs created by graph generator 146 may be written to data store 30 and cached for further processing. A graph may be a summary of all activity that happened in a particular time interval. As each graph corresponds to a distinct period of time, different rows can be aggregated to find summary information over a larger timestamp. In some examples, picking two different graphs from two different timestamps can be used to compare different periods. If necessary, the graph generator can parallelize its workload (e.g., where its backlog cannot otherwise be handled within a particular time period, such as an hour, or if is required to process a graph spanning a long time period).

[00190] Graph generator 146 can be implemented in any appropriate programming language, such as Java or C, and machine learning libraries, such as Spark's MLLib. Example ways that graph generator computations can be implemented include using SQL or Map-R, using Spark or Hadoop.

[00191] SSH tracker 148 is a microservice that may be responsible for following ssh connections and process parent hierarchies to determine trails of user ssh activity. Identified ssh trails are placed by the SSH tracker 148 into data store 30 and cached for further processing.

[00192] SSH tracker 148 can be implemented in any appropriate programming language, such as Java or C, and machine libraries, such as Spark's MLLib. Example ways that SSH tracker computations can be implemented include using SQL or Map-R, using Spark or Hadoop.

[00193] Threat aggregator 150 is a microservice that may be responsible for obtaining third party threat information from various applicable sources, and making it available to other micro-services. Examples of such information include reverse DNS information, GeoIP information,

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00577

lists of known bad domains/IP addresses, lists of known bad files etc. As applicable, the threat information is normalized before insertion into data store 30. Threat aggregator 150 can be implemented in any appropriate programming language, such as Java or C, using SQL/JDBC libraries to interact with data store 30 (e.g., for insertions and queries).

[00194] Scheduler 152 is a microservice that may act as a scheduler and that may run arbitrary jobs organized as a directed graph. In some examples, scheduler 152 ensures that all jobs for all customers are able to run during at a given time interval (e.g., every hour). Scheduler 152 may handle errors and retrying for failed jobs, track dependencies, manage appropriate resource levels, and/or scale jobs as needed. Scheduler 152 can be implemented in any appropriate programming language, such as Java or C. A variety of components can also be used, such as open source scheduler frameworks (e.g., Airflow), or AWS services (e.g., the AWS Data pipeline) which can be used for managing schedules.

[00195] Graph Behavior Modeler (GBM) 154 is a microservice that may compute polygraphs. In particular, GBM 154 can be used to find clusters of nodes in a graph that should be considered similar based on some set of their properties and relationships to other nodes. As described herein, the clusters and their relationships can be used to provide visibility into a datacenter environment without requiring user specified labels. GBM 154 may track such clusters over time persistently, allowing for changes to be detected and alerts to be generated.

[00196] GBM 154 may take as input a raw graph (e.g., as generated by graph generator 146). Nodes are actors of a behavior, and edges are the behavior relationship itself. For example, in the case of communication, example actors include processes, which communicate with other processes. The GBM 154 clusters the raw graph based on behaviors of actors and produces a summary (the polygraph). The polygraph summarizes behavior at a datacenter level. The GBM also produces "observations" that represent changes detected in the datacenter. Such observations may be based on differences in cumulative behavior (e.g., the baseline) of the datacenter with its current behavior. The GBM 154 can be implemented in any appropriate programming language, such as Java, C, or Golang, using appropriate libraries (as applicable) to handle distributed graph computations (handling large amounts of data analysis in a short amount of time). Apache Spark is another example tool that can be used to compute polygraphs. The GBM can also take feedback from users and adjust the model according to that feedback. For example, if a given user is interested in relearning behavior for a particular entity, the GBM can be instructed to "forget" the implicated part of the polygraph.

[00197] GBM runner 156 is a microservice that may be responsible for interfacing with GBM 154 and providing GBM 154 with raw graphs (e.g., using a query language, such as SQL, to push any computations it can to data store 30). GBM runner 156 may also insert polygraph output

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00578

from GBM 154 to data store 30. GBM runner 156 can be implemented in any appropriate programming language, such as Java or C, using SQL/JDBC libraries to interact with data store 30 to insert and query data.

[00198] Alert generator 158 is a microservice that may be responsible for generating alerts. Alert generator 158 may examine observations (e.g., produced by GBM 154) in aggregate, deduplicate them, and score them. Alerts may be generated for observations with a score exceeding a threshold. Alert generator 158 may also compute (or retrieves, as applicable) data that a customer (e.g., user A or user B) might need when reviewing the alert. Examples of events that can be detected by data platform 12 (and alerted on by alert generator 158) include, but are not limited to the following:

[00199] new user: This event may be created the first time a user (e.g., of node 116) is first observed by an agent within a datacenter.

[00200] user launched new binary: This event may be generated when an interactive user launches an application for the first time.

[00201] new privilege escalation: This event may be generated when user privileges are escalated and a new application is run.

[00202] new application or container: This event may be generated when an application or container is seen for the first time.

[00203] new external connection: This event may be generated when a connection to an external IP/domain is made from a new application.

[00204] new external host or IP: This event may be generated when a new external host or IP is involved in a connection with a datacenter.

[00205] new internal connection: This event may be generated when a connection between internal-only applications is seen for the first time.

[00206] new external client: This event may be generated when a new external connection is seen for an application which typically does not have external connections.

[00207] new parent: This event may be generated when an application is launched by a different parent.

[00208] connection to known bad IP/domain: Data platform 12 maintains (or can otherwise access) one or more reputation feeds. If an environment makes a connection to a known bad IP or domain, an event will be generated.

[00209] login from a known bad IP/domain: An event may be generated when a successful connection to a datacenter from a known bad IP is observed by data platform 12.

[00210] Alert generator 158 can be implemented in any appropriate programming language, such as Java or C, using SQL/JDBC libraries to interact with data store 30 to insert and query data. In

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00579

various embodiments, alert generator 158 also uses one or more machine learning libraries, such as Spark's MLLib (e.g., to compute scoring of various observations). Alert generator 158 can also take feedback from users about which kinds of events are of interest and which to suppress.

[00211] QsJobServer 160 is a microservice that may look at all the data produced by data platform 12 for an hour, and compile a materialized view (MV) out of the data to make queries faster. The MV helps make sure that the queries customers most frequently run, and data that they search for, can be easily queried and answered. QsJobServer 160 may also precompute and cache a variety of different metrics so that they can quickly be provided as answers at query time. QsJobServer 160 can be implemented using any appropriate programming language, such as Java or C, using SQL/JDBC libraries. In some examples, QsJobServer 160 is able to compute an MV efficiently at scale, where there could be a large number of joins. An SQL engine, such as Oracle, can be used to efficiently execute the SQL, as applicable.

[00212] Alert notifier 162 is a microservice that may take alerts produced by alert generator 158 and send them to customers' integrated Security Information and Event Management (SIEM) products (e.g., Splunk, Slack, etc.). Alert notifier 162 can be implemented using any appropriate programming language, such as Java or C. Alert notifier 162 can be configured to use an email service (e.g., AWS SES or pagerduty) to send emails. Alert notifier 162 may also provide templating support (e.g., Velocity or Moustache) to manage templates and structured notifications to SIEM products.

[00213] Reporting module 164 is a microservice that may be responsible for creating reports out of customer data (e.g., daily summaries of events, etc.) and providing those reports to customers (e.g., via email). Reporting module 164 can be implemented using any appropriate programming language, such as Java or C. Reporting module 164 can be configured to use an email service (e.g., AWS SES or pagerduty) to send emails. Reporting module 164 may also provide templating support (e.g., Velocity or Moustache) to manage templates (e.g., for constructing HTML-based email).

[00214] Web app 120 is a microservice that provides a user interface to data collected and processed on data platform 12. Web app 120 may provide login, authentication, query, data visualization, etc. features. Web app 120 may, in some embodiments, include both client and server elements. Example ways the server elements can be implemented are using Java DropWizard or Node.Js to serve business logic, and a combination of JSON/HTTP to manage the service. Example ways the client elements can be implemented are using frameworks such as React, Angular, or Backbone. JSON, jQuery, and JavaScript libraries (e.g., underscore) can also be used.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00580

[00215] Query service 166 is a microservice that may manage all database access for web app 120. Query service 166 abstracts out data obtained from data store 30 and provides a JSON-based REST API service to web app 120. Query service 166 may generate SQL queries for the REST APIs that it receives at run time. Query service 166 can be implemented using any appropriate programming language, such as Java or C and SQL/JDBC libraries, or an SQL framework such as jOOQ. Query service 166 can internally make use of a variety of types of databases, including a relational database engine 168 (e.g., AWS Aurora) and/or data store 30 to manage data for clients. Examples of tables that query service 166 manages are OLTP tables and data warehousing tables.

[00216] Cache 170 may be implemented by Redis and/or any other service that provides a key-value store. Data platform 12 can use cache 170 to keep information for frontend services about users. Examples of such information include valid tokens for a customer, valid cookies of customers, the last time a customer tried to login, etc.

[00217] Fig. 3A illustrates an example of a process for detecting anomalies in a network environment. In various embodiments, process 300 is performed by data platform 12. The process begins at 301 when data associated with activities occurring in a network environment (such as entity A's datacenter) is received. One example of such data that can be received at 301 is agent-collected data described above (e.g., in conjunction with process 200).

[00218] At 302, a logical graph model is generated, using at least a portion of the monitored activities. A variety of approaches can be used to generate such logical graph models, and a variety of logical graphs can be generated (whether using the same, or different approaches). The following is one example of how data received at 301 can be used to generate and maintain a model.

[00219] During bootstrap, data platform 12 creates an aggregate graph of physical connections (also referred to herein as an aggregated physical graph) by matching connections that occurred in the first hour into communication pairs. Clustering is then performed on the communication pairs. Examples of such clustering, described in more detail below, include performing Matching Neighbor clustering and similarity (e.g., SimRank) clustering. Additional processing can also be performed (and is described in more detail below), such as by splitting clusters based on application type, and annotating nodes with DNS query information. The resulting graph (also referred to herein as a base graph or common graph) can be used to generate a variety of models, where a subset of node and edge types (described in more detail below) and their properties are considered in a given model. One example of a model is a UID to UID model (also referred to herein as a Uid2Uid model) which clusters together processes that share a username and show similar privilege change behavior. Another example of a model is a CType model, which clusters

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00581

together processes that share command line similarity. Yet another example of a model is a PType model, which clusters together processes that share behaviors over time.

[00220] Each hour (or any other predetermined time interval) after bootstrap, a new snapshot is taken (i.e., data collected about a datacenter in the last hour is processed) and information from the new snapshot is merged with existing data to create and (as additional data is collected/processed) maintain a cumulative graph. The cumulative graph (also referred to herein as a cumulative PType graph and a polygraph) is a running model of how processes behave over time. Nodes in the cumulative graph are PType nodes, and provide information such as a list of all active processes and PIDs in the last hour, the number of historic total processes, the average number of active processes per hour, the application type of the process (e.g., the CType of the PType), and historic CType information/frequency. Edges in the cumulative graph can represent connectivity and provide information such as connectivity frequency. The edges can be weighted (e.g., based on number of connections, number of bytes exchanged, etc.). Edges in the cumulative graph (and snapshots) can also represent transitions.

[00221] One approach to merging a snapshot of the activity of the last hour into a cumulative graph is as follows. An aggregate graph of physical connections is made for the connections included in the snapshot (as was previously done for the original snapshot used during bootstrap). And, clustering/splitting is similarly performed on the snapshot's aggregate graph. Next, PType clusters in the snapshot's graph are compared against PType clusters in the cumulative graph to identify commonality.

[00222] One approach to determining commonality is, for any two nodes that are members of a given CmdType (described in more detail below), comparing internal neighbors and calculating a set membership Jaccard distance. The pairs of nodes are then ordered by decreasing similarity (i.e., with the most similar sets first). For nodes with a threshold amount of commonality (e.g., at least 66% members in common), any new nodes (i.e., appearing in the snapshot's graph but not the cumulative graph) are assigned the same PType identifier as is assigned to the corresponding node in the cumulative graph. For each node that is not classified (i.e., has not been assigned a PType identifier), a network signature is generated (i.e., indicative of the kinds of network connections the node makes, who the node communicates with, etc.). The following processing is then performed until convergence. If a match of the network signature is found in the cumulative graph, the unclassified node is assigned the PType identifier of the corresponding node in the cumulative graph. Any nodes which remain unclassified after convergence are new PTypes and are assigned new identifiers and added to the cumulative graph as new. As applicable, the detection of a new PType can be used to generate an alert. If the new PType has a new CmdType, a severity of the alert can be increased. If any surviving nodes (i.e., present in both the

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00582

cumulative graph and the snapshot graph) change PTypes, such change is noted as a transition, and an alert can be generated. Further, if a surviving node changes PType and also changes CmdType, a severity of the alert can be increased.

[00223] Changes to the cumulative graph (e.g., a new PType or a new edge between two PTypes) can be used (e.g., at 303) to detect anomalies (described in more detail below). Two example kinds of anomalies that can be detected by data platform 12 include security anomalies (e.g., a user or process behaving in an unexpected manner) and devops/root cause anomalies (e.g., network congestion, application failure, etc.). Detected anomalies can be recorded and surfaced (e.g., to administrators, auditors, etc.), such as through alerts which are generated at 304 based on anomaly detection.

[00224] Additional detail regarding processing performed, by various components depicted in Fig. 1D (whether performed individually or in combination), in conjunction with model/polygraph construction (e.g., as performed at 302) are provided below.

[00225] As explained above, an aggregated physical graph can be generated on a per customer basis periodically (e.g., once an hour) from raw physical graph information, by matching connections (e.g., between two processes on two virtual machines). In various embodiments, a deterministic fixed approach is used to cluster nodes in the aggregated physical graph (e.g., representing processes and their communications). As one example, Matching Neighbors Clustering (MNC) can be performed on the aggregated physical graph to determine which entities exhibit identical behavior and cluster such entities together.

[00226] Fig. 3B depicts a set of example processes (p1, p2, p3, and p4) communicating with other processes (p10 and p11). Fig. 3B is a graphical representation of a small portion of an aggregated physical graph showing (for a given time period, such as an hour) which processes in a datacenter communicate with which other processes. Using MNC, processes p1, p2, and p3 will be clustered together (305), as they exhibit identical behavior (they communicate with p10 and only p10). Process p4, which communicates with both p10 and p11, will be clustered separately.

[00227] In MNC, only those processes exhibiting identical (communication) behavior will be clustered. In various embodiments, an alternate clustering approach can also/instead be used, which uses a similarity measure (e.g., constrained by a threshold value, such as a 60% similarity) to cluster items. In some embodiments, the output of MNC is used as input to SimRank, in other embodiments, MNC is omitted.

[00228] Fig. 3C depicts a set of example processes (p4, p5, p6) communicating with other processes (p7, p8, p9). As illustrated, most of nodes p4, p5, and p6 communicate with most of nodes p7, p8, and p9 (as indicated in Fig. 3C with solid connection lines). As one example, process p4 communicates with process p7 (310), process p8 (311), and process p9 (312). An

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00583

exception is process p6, which communicates with processes p7 and p8, but does not communicate with process p9 (as indicated by dashed line 313). If MNC were applied to the nodes depicted in Fig. 3C, nodes p4 and p5 would be clustered (and node p6 would not be included in their cluster).

[00229] One approach to similarity clustering is to use SimRank. In an embodiment of the SimRank approach, for a given node v in a directed graph, $I(v)$ and $O(v)$ denote the respective set of in-neighbors and out-neighbors of v. Individual in-neighbors are denoted as $I_i(v)$, for $1 \leq i \leq |I(v)|$, and individual out-neighbors are denoted as $O_i(v)$, for $1 \leq i \leq |O(v)|$. The similarity between two objects a and b can be denoted by $s(a,b) \in [1,0]$. A recursive equation (hereinafter "the SimRank equation") can be written for $s(a,b)$, where, if a=b, then $s(a,b)$ is defined as 1, otherwise, $s(a,b)=\frac{C}{|I(a)||I(b)|}\sum_{i=1}^{|I(a)|}\sum_{j=1}^{|I(b)|} s(I_i(a), I_j(b))$ where C is a constant between 0 and 1. One example value for the decay factor C is 0.8 (and a fixed number of iterations such as five). Another example value for the decay factor C is 0.6 (and/or a different number of iterations). In the event that a or b has no in-neighbors, similarity is set to $s(a,b)=0$, so the summation is defined to be 0 when $I(a)=\emptyset$ or $I(b)=\emptyset$.

[00230] The SimRank equations for a graph G can be solved by iteration to a fixed point. Suppose n is the number of nodes in G. For each iteration k, n^2 entries $s_k(*,*)$ are kept, where $s_k(a,b)$ gives the score between a and b on iteration k. Successive computations of $s_{k+1}(*,*)$ are made based on $s_k(*,*)$. Starting with $s_0(*,*)$, where each $s_0(a,b)$ is a lower bound on the actual SimRank score $s(a,b)$: $s_0(a,b) = \begin{cases} 1, \text{if } a = b, \\ 0, \text{if } a \neq b. \end{cases}$

[00231] The SimRank equation can be used to compute $s_{k+1}(a,b)$ from $s_k(*,*)$ with $s_{k+1}(a,b) = \frac{C}{|I(a)||I(b)|}\sum_{i=1}^{|I(a)|}\sum_{j=1}^{|I(b)|} s_k(I_i(a), I_j(b))$ for $a \neq b$, and $s_{k+1}(a,b)=1$ for $a=b$. On each iteration k+1, the similarity of (a,b) is updated using the similarity scores of the neighbors of (a,b) from the previous iteration k according to the SimRank equation. The values $s_k(*,*)$ are nondecreasing as k increases.

[00232] Returning to Fig. 3C, while MNC would cluster nodes p4 and p5 together (and not include node p6 in their cluster), application of SimRank would cluster nodes p4-p6 into one cluster (314) and also cluster nodes p7-p9 into another cluster (315).

[00233] Fig. 3D depicts a set of processes, and in particular server processes s1 and s2, and client processes c1, c2, c3, c4, c5, and c6. Suppose only nodes s1, s2, c1, and c2 are present in the graph depicted in Fig. 3D (and the other nodes depicted are omitted from consideration). Using MNC, nodes s1 and s2 would be clustered together, as would nodes c1 and c2. Performing SimRank clustering as described above would also result in those two clusters (s1 and s2, and c1 and c2). As previously mentioned, in MNC, identical behavior is required. Thus, if node c3 were

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00584

now also present in the graph, MNC would not include c3 in a cluster with c2 and c1 because node c3 only communicates with node s2 and not node s1. In contrast, a SimRank clustering of a graph that includes nodes s1, s2, c1, c2, and c3 would result (based, e.g., on an applicable selected decay value and number of iterations) in a first cluster comprising nodes s1 and s2, and a second cluster of c1, c2, and c3. As an increasing number of nodes which communicate with server process s2, and do not also communicate with server process s1, are included in the graph (e.g., as c4, c5, and c6 are added), under SimRank, nodes s1 and s2 will become decreasingly similar (i.e., their intersection is reduced).

[00234] In various embodiments, SimRank is modified (from what is described above) to accommodate differences between the asymmetry of client and server connections. As one example, SimRank can be modified to use different thresholds for client communications (e.g., an 80% match among nodes c1-c6) and for server communications (e.g., a 60% match among nodes s1 and s2). Such modification can also help achieve convergence in situations such as where a server process dies on one node and restarts on another node.

[00235] The application of MNC/SimRank to an aggregated physical graph results in a smaller graph, in which processes which are determined to be sufficiently similar are clustered together. Typically, clusters generated as output of MNC will be underinclusive. For example, for the nodes depicted in Fig. 3C, process p6 will not be included in a cluster with processes p4 and p5, despite substantial similarity in their communication behaviors. The application of SimRank (e.g., to the output of MNC) helps mitigate the underinclusiveness of MNC, but can result in overly inclusive clusters. As one example, suppose (returning to the nodes depicted in Fig. 3B) that as a result of applying SimRank to the depicted nodes, nodes p1-p4 are all included in a single cluster. Both MNC and SimRank operate agnostically of which application a given process belongs to. Suppose processes p1-p3 each correspond to a first application (e.g., an update engine), and process p4 corresponds to a second application (e.g., sshd). Further suppose process p10 corresponds to contact with AWS. Clustering all four of the processes together (e.g., as a result of SimRank) could be problematic, particularly in a security context (e.g., where granular information useful in detecting threats would be lost).

[00236] As previously mentioned, data platform 12 may maintain a mapping between processes and the applications to which they belong. In various embodiments, the output of SimRank (e.g., SimRank clusters) is split based on the applications to which cluster members belong (such a split is also referred to herein as a "CmdType split"). If all cluster members share a common application, the cluster remains. If different cluster members originate from different applications, the cluster members are split along application-type (CmdType) lines. Using the nodes depicted in Fig. 3D as an example, suppose that nodes c1, c2, c3, and c5 all share "update

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00585

engine" as the type of application to which they belong (sharing a CmdType). Suppose that node c4 belongs to "ssh," and suppose that node c6 belongs to "bash." As a result of SimRank, all six nodes (c1-c6) might be clustered into a single cluster. After a CmdType split is performed on the cluster, however, the single cluster will be broken into three clusters (c1, c2, c3, c5; c4; and c6). Specifically, the resulting clusters comprise processes associated with the same type of application, which exhibit similar behaviors (e.g., communication behaviors). Each of the three clusters resulting from the CmdType split represents, respectively, a node (also referred to herein as a PType) of a particular CmdType. Each PType is given a persistent identifier and stored persistently as a cumulative graph.

[00237] A variety of approaches can be used to determine a CmdType for a given process. As one example, for some applications (e.g., sshd), a one-to-one mapping exists between the CmdType and the application/binary name. Thus, processes corresponding to the execution of sshd will be classified using a CmdType of sshd. In various embodiments, a list of common application/binary names (e.g., sshd, apache, etc.) is maintained by data platform 12 and manually curated as applicable. Other types of applications (e.g., Java, Python, and Ruby) are multi-homed, meaning that several very different applications may all execute using the binary name, "java." For these types of applications, information such as command line / execution path information can be used in determining a CmdType. In particular, the subapplication can be used as the CmdType of the application, and/or term frequency analysis (e.g., TF/IDF) can be used on command line information to group, for example, any marathon related applications together (e.g., as a python.marathon CmdType) and separately from other Python applications (e.g., as a python.airflow CmdType).

[00238] In various embodiments, machine learning techniques are used to determine a CmdType. The CmdType model is constrained such that the execution path for each CmdType is unique. One example approach to making a CmdType model is a random forest based approach. An initial CmdType model is bootstrapped using process parameters (e.g., available within one minute of process startup) obtained using one hour of information for a given customer (e.g., entity A). Examples of such parameters include the command line of the process, the command line of the process's parent(s) (if applicable), the uptime of the process, UID/EUID and any change information, TTY and any change information, listening ports, and children (if any). Another approach is to perform term frequency clustering over command line information to convert command lines into cluster identifiers.

[00239] The random forest model can be used (e.g., in subsequent hours) to predict a CmdType for a process (e.g., based on features of the process). If a match is found, the process can be assigned the matching CmdType. If a match is not found, a comparison between features of the

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00586

process and its nearest CmdType (e.g., as determined using a Levenstein distance) can be performed. The existing CmdType can be expanded to include the process, or, as applicable, a new CmdType can be created (and other actions taken, such as generating an alert). Another approach to handling processes which do not match an existing CmdType is to designate such processes as unclassified, and once an hour, create a new random forest seeded with process information from a sampling of classified processes (e.g., 10 or 100 processes per CmdType) and the new processes. If a given new process winds up in an existing set, the process is given the corresponding CmdType. If a new cluster is created, a new CmdType can be created.

[00240] Conceptually, a polygraph represents the smallest possible graph of clusters that preserve a set of rules (e.g., in which nodes included in the cluster must share a CmdType and behavior). As a result of performing MNC, SimRank, and cluster splitting (e.g., CmdType splitting) many processes are clustered together based on commonality of behavior (e.g., communication behavior) and commonality of application type. Such clustering represents a significant reduction in graph size (e.g., compared to the original raw physical graph). Nonetheless, further clustering can be performed (e.g., by iterating on the graph data using the GBM to achieve such a polygraph). As more information within the graph is correlated, more nodes can be clustered together, reducing the size of the graph, until convergence is reached and no further clustering is possible.

[00241] Fig. 3E depicts two pairs of clusters. In particular, cluster 320 represents a set of client processes sharing the same CmdType ("a1"), communicating (collectively) with a server process having a CmdType ("a2"). Cluster 322 also represents a set of client processes having a CmdType a1 communicating with a server process having a CmdType a2. The nodes in clusters 320 and 322 (and similarly nodes in 321 and 323) remain separately clustered (as depicted) after MNC/SimRank/CmdType splitting – isolated islands. One reason this could occur is where server process 321 corresponds to processes executing on a first machine (having an IP address of 1.1.1.1). The machine fails and a new server process 323 starts, on a second machine (having an IP address of 2.2.2.2) and takes over for process 321.

[00242] Communications between a cluster of nodes (e.g., nodes of cluster 320) and the first IP address can be considered different behavior from communications between the same set of nodes and the second IP address, and thus communications 324 and 325 will not be combined by MNC/SimRank in various embodiments. Nonetheless, it could be desirable for nodes of clusters 320/322 to be combined (into cluster 326), and for nodes of clusters 321/323 to be combined (into cluster 327), as representing (collectively) communications between a1 and a2. One task that can be performed by data platform 12 is to use DNS query information to map IP addresses to logical entities. As will be described in more detail below, GBM 154 can make use of the DNS

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00587

query information to determine that graph nodes of cluster 320 and graph nodes of cluster 322 both made DNS queries for "appserverabc.example.com," which first resolved to 1.1.1.1 and then to 2.2.2.2, and to combine nodes 320/322 and 321/323 together into a single pair of nodes (326 communicating with 327).

[00243] In various embodiments, GBM 154 operates in a batch manner in which it receives as input the nodes and edges of a graph for a particular time period along with its previous state, and generates as output clustered nodes, cluster membership edges, cluster-to-cluster edges, events, and its next state.

[00244] GBM 154 may not try to consider all types of entities and their relationships that may be available in a conceptual common graph all at once. Instead, GBM uses a concept of models where a subset of node and edge types and their properties are considered in a given model. Such an approach is helpful for scalability, and also to help preserve detailed information (of particular importance in a security context) – as clustering entities in a more complex and larger graph could result in less useful results. In particular, such an approach allows for different types of relationships between entities to be preserved/more easily analyzed.

[00245] While GBM 154 can be used with different models corresponding to different subgraphs, core abstractions remain the same across types of models.

[00246] For example, each node type in a GBM model is considered to belong to a class. The class can be thought of as a way for the GBM to split nodes based on the criteria it uses for the model. The class for a node is represented as a string whose value is derived from the node's key and properties depending on the GBM Model. Note that different GBM models may create different class values for the same node. For each node type in a given GBM model, GBM 154 can generate clusters of nodes for that type. A GBM generated cluster for a given member node type cannot span more than one class for that node type. GBM 154 generates edges between clusters that have the same types as the edges between source and destination cluster node types.

[00247] Additionally or alternatively, the processes described herein as being used for a particular model can be used (can be the same) across models, and different models can also be configured with different settings.

[00248] Additionally or alternatively, the node types and the edge types may correspond to existing types in the common graph node and edge tables but this is not necessary. Even when there is a correspondence, the properties provided to GBM 154 are not limited to the properties that are stored in the corresponding graph table entries. They can be enriched with additional information before being passed to GBM 154.

[00249] Logically, the input for a GBM model can be characterized in a manner that is similar to other graphs. Edge triplets can be expressed, for example, as an array of source node type, edge

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00588

type, and destination node type. And, each node type is associated with node properties, and each edge type is associated with edge properties. Other edge triplets can also be used (and/or edge triplets can be extended) in accordance with various embodiments.

[00250] Note that the physical input to the GBM model need not (and does not, in various embodiments) conform to the logical input. For example, the edges in the PtypeConn model correspond to edges between Matching Neighbors (MN) clusters, where each process node has an MN cluster identifier property. In the User ID to User ID model (also referred to herein as the Uid2Uid model), edges are not explicitly provided separately from nodes (as the euid array in the node properties serves the same purpose). In both cases, however, the physical information provides the applicable information necessary for the logical input.

[00251] The state input for a particular GBM model can be stored in a file, a database, or other appropriate storage. The state file (from a previous run) is provided, along with graph data, except for when the first run for a given model is performed, or the model is reset. In some cases, no data may be available for a particular model in a given time period, and GBM may not be run for that time period. As data becomes available at a future time, GBM can run using the latest state file as input.

[00252] GBM 154 outputs cluster nodes, cluster membership edges, and inter-cluster relationship edges that are stored (in some embodiments) in the graph node tables: node_c, node_cm, and node_icr, respectively. The type names of nodes and edges may conform to the following rules:

[00253] * A given node type can be used in multiple different GBM models. The type names of the cluster nodes generated by two such models for that node type will be different. For instance, process type nodes will appear in both PtypeConn and Uid2Uid models, but their cluster nodes will have different type names.

[00254] * The membership edge type name is "MemberOf."

[00255] * The edge type names for cluster-to-cluster edges will be the same as the edge type names in the underlying node-to-node edges in the input.

[00256] The following are example events GBM 154 can generate: new class, new cluster, new edge from class to class, split class (the notion that GBM 154 considers all nodes of a given type and class to be in the same cluster initially and if GBM 154 splits them into multiple clusters, it is splitting a class), new edge from cluster and class, new edge between cluster and cluster, and/or new edge from class to cluster.

[00257] One underlying node or edge in the logical input can cause multiple types of events to be generated. Conversely, one event can correspond to multiple nodes or edges in the input. Not every model generates every event type.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00589

[00258] Additional information regarding examples of data structures/models that can be used in conjunction with models used by data platform 12 is now provided.

[00259] In some examples, a PTypeConn Model clusters nodes of the same class that have similar connectivity relationships. For example, if two processes had similar incoming neighbors of the same class and outgoing neighbors of the same class, they could be clustered.

[00260] The node input to the PTypeConn model for a given time period includes non-interactive (i.e., not associated with tty) process nodes that had connections in the time period and the base graph nodes of other types (IP Service Endpoint (IPSep) comprising an IP address and a port), DNS Service Endpoint (DNSSep) and IPAddress) that have been involved in those connections. The base relationship is the connectivity relationship for the following type triplets:

[00261] * Process, ConnectedTo, Process

[00262] * Process, ConnectedTo, IP Service Endpoint (IPSep)

[00263] * Process, ConnectedTo, DNS Service Endpoint (DNSSep)

[00264] * IPAddress, ConnectedTo, ProcessProcess, DNS, ConnectedTo, Process

[00265] The edge inputs to this model are the ConnectedTo edges from the MN cluster, instead of individual node-to-node ConnectedTo edges from the base graph. The membership edges created by this model refer to the base graph node type provided in the input.

[00266] Class Values:

[00267] The class values of nodes are determined as follows depending on the node type (e.g., Process nodes, IPSep nodes, DNSSep nodes, and IP Address nodes).

[00268] Process nodes:

[00269] if exe_path contains java then "java <cmdline_term_1> ..."

[00270] else if exe_path contains python then "python <cmdline_term_1> ..."

[00271] else "last_part_of_exe_path"

[00272] IPSep nodes:

[00273] if IP_internal then "IntIPS"

[00274] else if severity = 0 then "<IP_addr>:<protocol>:<port>"

[00275] else "<IP_addr>:<port>_BadIP"

[00276] DNSSep nodes:

[00277] if IP_internal = 1 then "<hostname>"

[00278] else if severity = 0 then "<hostname>:<protocol>:port"

[00279] else "<hostname>:<port>_BadIP"

[00280] IPAddress nodes (will appear only on client side):

[00281] if IP_internal = 1 then "IPIntC"

[00282] else if severity = 0 then "ExtIPC"

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00590

[00283] else "ExtBadIPC"

[00284] Events:

[00285] A new class event in this model for a process node is equivalent to seeing a new CType being involved in a connection for the first time. Note that this does not mean the CType was not seen before. It is possible that it was previously seen but did not make a connection at that time.

[00286] A new class event in this model for an IPSep node with IP_internal = 0 is equivalent to seeing a connection to a new external IP address for the first time.

[00287] A new class event in this model for a DNSSep node is equivalent to seeing a connection to a new domain for the first time.

[00288] A new class event in this model for an IPAddress node with IP_internal = 0 and severity = 0 is equivalent to seeing a connection from any external IP address for the first time.

[00289] A new class event in this model for an IPAddress node with IP_internal = 0 and severity > 0 is equivalent to seeing a connection from any bad external IP address for the first time.

[00290] A new class to class to edge from a class for a process node to a class for a process node is equivalent to seeing a communication from the source CType making a connection to the destination CType for the first time.

[00291] A new class to class to edge from a class for a process node to a class for a DNSSep node is equivalent to seeing a communication from the source CType making a connection to the destination domain name for the first time.

[00292] An IntPConn Model may be similar to the PtypeConn Model, except that connection edges between parent/child processes and connections between processes where both sides are not interactive are filtered out.

[00293] A Uid2Uid Model may cluster processes with the same username that show similar privilege change behavior. For instance, if two processes with the same username had similar effective user values, launched processes with similar usernames, and were launched by processes with similar usernames, then they could be clustered.

[00294] An edge between a source cluster and destination cluster generated by this model means that all of the processes in the source cluster had a privilege change relationship to at least one process in the destination cluster.

[00295] The node input to this model for a given time period includes process nodes that are running in that period. The value of a class of process nodes is "<username>".

[00296] The base relationship that is used for clustering is privilege change, either by the process changing its effective user ID, or by launching a child process which runs with a different user.

[00297] The physical input for this model includes process nodes (only), with the caveat that the complete ancestor hierarchy of process nodes active (i.e., running) for a given time period is

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00591

provided as input even if an ancestor is not active in that time period. Note that effective user IDs of a process are represented as an array in the process node properties, and launch relationships are available from ppid_hash fields in the properties as well.

[00298] A new class event in this model is equivalent to seeing a user for the first time.

[00299] A new class to class edge event is equivalent to seeing the source user making a privilege change to the destination user for the first time.

[00300] A Ct2Ct Model may cluster processes with the same CType that show similar launch behavior. For instance, if two processes with the same CType have launched processes with similar CTypes, then they could be clustered.

[00301] The node input to this model for a given time period includes process nodes that are running in that period. The value class of process nodes is CType (similar to how it is created for the PtypeConn Model).

[00302] The base relationship that is used for clustering is a parent process with a given CType launching a child process with another given destination CType.

[00303] The physical input for this model includes process nodes (only) with the caveat that the complete ancestor hierarchy active process nodes (i.e., that are running) for a given time period is provided as input even if an ancestor is not active in that time period. Note that launch relationships are available from ppid_hash fields in the process node properties.

[00304] An edge between a source cluster and destination cluster generated by this model means that all of the processes in the source cluster launched at least one process in the destination cluster.

[00305] A new class event in this model is equivalent to seeing a CType for the first time. Note that the same type of event will be generated by the PtypeConn Model as well.

[00306] A new class to class edge event is equivalent to seeing the source CType launching the destination CType for the first time.

[00307] An MTypeConn Model may cluster nodes of the same class that have similar connectivity relationships. For example, if two machines had similar incoming neighbors of the same class and outgoing neighbors of the same class, they could be clustered.

[00308] A new class event in this model will be generated for external IP addresses or (as applicable) domain names seen for the first time. Note that a new class to class to edge Machine, class to class for an IPSep or DNSName node will also be generated at the same time.

[00309] The membership edges generated by this model will refer to Machine, IPAddress, DNSName, and IPSep nodes in the base graph. Though the nodes provided to this model are IPAddress nodes instead of IPSep nodes, the membership edges it generates will refer to IPSep type nodes. Alternatively, the base graph can generate edges between Machine and IPSep node

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00592

types. Note that the Machine to IPAddress edges have tcp_dst_ports/udp_dst_ports properties that can be used for this purpose.

[00310] The node input to this model for a given time period includes machine nodes that had connections in the time period and the base graph nodes of other types (IPAddress and DNSName) that were involved in those connections.

[00311] The base relationship is the connectivity relationship for the following type triplets:

[00312] * Machine, ConnectedTo, Machine

[00313] * Machine, ConnectedTo, IPAddress

[00314] * Machine, ConnectedTo, DNSName

[00315] * IPAddress, ConnectedTo, Machine, DNS, ConnectedTo, Machine

[00316] The edge inputs to this model are the corresponding ConnectedTo edges in the base graph.

[00317] Class Values:

[00318] Machine:

[00319] The class value for all Machine nodes is "Machine."

[00320] The machine_terms property in the Machine nodes is used, in various embodiments, for labeling machines that are clustered together. If a majority of the machines clustered together share a term in the machine_terms, that term can be used for labeling the cluster.

[00321] IPSep:

[00322] The class value for IPSep nodes is determined as follows:

[00323] if IP_internal then "IntIPS"

[00324] else

[00325] if severity = 0 then "<ip_addr>:<protocol>:<port>"

[00326] else "<IP_addr_BadIP>"

[00327] IPAddress:

[00328] The class value for IpAddress nodes is determined as follows:

[00329] if IP_internal then "IntIPC"

[00330] else

[00331] if severity = 0 then "ExtIPC"

[00332] else "ExtBadIPC"

[00333] DNSName:

[00334] The class value for DNSName nodes is determined as follows:

[00335] if severity = 0 then "<hostname>"

[00336] else then "<hostname>_BadIP"

[00337] An example structure for a New Class Event is now described.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00593

[00338] The key field for this event type looks as follows (using the PtypeConn model as an example):

[00339] {

[00340] "node": {

[00341] "class": {

[00342] "cid": "httpd"

[00343] },

[00344] "key": {

[00345] "cid": "29654"

[00346] },

[00347] "type": "PtypeConn"

[00348] }

[00349] }

[00350] It contains the class value and also the ID of the cluster where that class value is observed. Multiple clusters can be observed with the same value in a given time period. It contains the class value and also the ID of the cluster where that class value is observed. Multiple clusters can be observed with the same value in a given time period. Accordingly, in some embodiments, GBM 154 generates multiple events of this type for the same class value.

[00351] The properties field looks as follows:

[00352] {

[00353] "set_size": 5

[00354] }

[00355] The set_size indicates the size of the cluster referenced in the keys field.

[00356] Conditions:

[00357] For a given model and time period, multiple NewClass events can be generated if there is more than one cluster in that class. NewNode events will not be generated separately in this case.

[00358] Example New Class to Class Edge Event structure:

[00359] The key field for this event type looks as follows (using the PtypeConn model as an example):

[00360] "edge": {

[00361] "dst_node": {

[00362] "class": {

[00363] "cid": "java war"

[00364] },

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00594

[00365] "key": {

[00366] "cid": "27635"

[00367] },

[00368] "type": "PtypeConn"

[00369] },

[00370] "src_node": {

[00371] "class": {

[00372] "cid": "IntIPC"

[00373] },

[00374] "key": {

[00375] "cid": "20881"

[00376] },

[00377] "type": "PtypeConn"

[00378] },

[00379] "type": "ConnectedTo"

[00380] }

[00381] }

[00382] The key field contains source and destination class values and also source and destination cluster identifiers (i.e., the src/dst_node:key.cid represents the src/dst cluster identifier).

[00383] In a given time period for a given model, an event of this type could involve multiple edges between different cluster pairs that have the same source and destination class values. GBM 154 can generate multiple events in this case with different source and destination cluster identifiers.

[00384] The props fields look as follows for this event type:

[00385] {

[00386] "dst_set_size": 2,

[00387] "src_set_size": 1

[00388] }

[00389] The source and destination sizes represent the sizes of the clusters given in the keys field.

[00390] Conditions:

[00391] For a given model and time period, multiple NewClassToClass events can be generated if there are more than one pair of clusters in that class pair. NewNodeToNode events are not generated separately in this case.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00595

[00392] Combining Events at the Class Level: for a given model and time period, the following example types of events can represent multiple changes in the underlying GBM cluster level graph in terms of multiple new clusters or multiple new edges between clusters:

[00393] * NewClass

[00394] * NewEdgeClassToClass

[00395] * NewEdgeNodeToClass

[00396] * NewEdgeClassToNode

[00397] Multiple NewClass events with the same model and class can be output if there are multiple clusters in that new class.

[00398] Multiple NewEdgeClassToClass events with the same model and class pair can be output if there are multiple new cluster edges within that class pair.

[00399] Multiple NewEdgeNodeToClass events with the same model and destination class can be output if there are multiple new edges from the source cluster to the destination clusters in that destination class (the first time seeing this class as a destination cluster class for the source cluster).

[00400] Multiple NewEdgeClassToNode events with the same model and source class can be output if there are multiple new edges from source clusters to the destination clusters in that source class (the first time seeing this class as a source cluster class for the destination cluster).

[00401] These events may be combined at the class level and treated as a single event when it is desirable to view changes at the class level, e.g., when one wants to know when there is a new CType.

[00402] In some examples, different models may have partial overlap in the types of nodes they use from the base graph. Therefore, they can generate NewClass type events for the same class. NewClass events can also be combined across models when it is desirable to view changes at the class level.

[00403] Using techniques herein, actions can be associated with processes and (e.g., by associating processes with users) actions can thus also be associated with extended user sessions. Such information can be used to track user behavior correctly, even where a malicious user attempts to hide his trail by changing user identities (e.g., through lateral movement). Extended user session tracking can also be useful in operational use cases without malicious intent, e.g., where users make original logins with distinct usernames (e.g., “charlie” or “dave”) but then perform actions under a common username (e.g., “admin” or “support”). One such example is where multiple users with administrator privileges exist, and they need to gain superuser privilege to perform a particular type of maintenance. It may be desirable to know which operations are performed (as the superuser) by which original user when debugging issues. In the

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00596

following examples describing extended user session tracking, reference is generally made to using the secure shell (ssh) protocol as implemented by openssh (on the server side) as the mechanism for logins. However, extended user session tracking is not limited to the ssh protocol or a particular limitation and the techniques described herein can be extended to other login mechanisms.

[00404] On any given machine, there will be a process that listens for and accepts ssh connections on a given port. This process can run the openssh server program running in daemon mode or it could be running another program (e.g., initd on a Linux system). In either case, a new process running openssh will be created for every new ssh login session and this process can be used to identify an ssh session on that machine. This process is called the "privileged" process in openssh.

[00405] After authentication of the ssh session, when an ssh client requests a shell or any other program to be run under that ssh session, a new process that runs that program will be created under (i.e., as a child of) the associated privileged process. If an ssh client requests port forwarding to be performed, the connections will be associated with the privileged process.

[00406] In modern operating systems such as Linux and Windows, each process has a parent process (except for the very first process) and when a new process is created the parent process is known. By tracking the parent-child hierarchy of processes, one can determine if a particular process is a descendant of a privileged openssh process and thus if it is associated with an ssh login session.

[00407] For user session tracking across machines (or on a single machine with multiple logins) in a distributed environment, it is established when two login sessions have a parent-child relationship. After that, the "original" login session, if any, for any given login session can be determined by following the parent relationship recursively.

[00408] Fig. 3F is a representation of a user logging into a first machine and then into a second machine from the first machine, as well as information associated with such actions. In the example of Fig. 3F, a user, Charlie, logs into Machine A (331) from a first IP address (332). As part of the login process, he provides a username (333). Once connected to Machine A, an openssh privileged process (334) is created to handle the connection for the user, and a terminal session is created and a bash process (335) is created as a child. Charlie launches an ssh client (336) from the shell, and uses it to connect (337) to Machine B (338). As with the connection he makes to Machine A, Charlie's connection to Machine B will have an associated incoming IP address (339), in this case, the IP address of Machine A. And, as part of the login process with Machine B, Charlie will provide a username (340) which need not be the same as username 333. An openssh privileged process (341) is created to handle the connection, and a terminal session

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00597

and child bash process (342) will be created. From the command line of Machine B, Charlie launches a curl command (343), which opens an HTTP connection (2028) to an external Machine C (345).

[00409] Fig. 3G is an alternate representation of actions occurring in Fig. 3F, where events occurring on Machine A are indicated along line 350, and events occurring on Machine B are indicated along line 351. As shown in Fig. 3G, an incoming ssh connection is received at Machine A (352). Charlie logs in (as user "x") and an ssh privileged process is created to handle Charlie's connection (353). A terminal session is created and a bash process is created (354) as a child of process 353. Charlie wants to ssh to Machine B, and so executes an ssh client on Machine A (355), providing credentials (as user "y") at 356. Charlie logs into Machine B, and an ssh privileged process is created to handle Charlie's connection (357). A terminal session is created and a bash process is created (358) as a child of process 357. Charlie then executes curl (359) to download content from an external domain (via connection 360).

[00410] The external domain could be a malicious domain, or it could be benign. Suppose the external domain is malicious (and, e.g., Charlie has malicious intent). It would be advantageous (e.g., for security reasons) to be able to trace the contact with the external domain back to Machine A, and then back to Charlie's IP address. Using techniques described herein (e.g., by correlating process information collected by various agents), such tracking of Charlie's activities back to his original login (330) can be accomplished. In particular, an extended user session can be tracked that associates Charlie's ssh processes together with a single original login and thus original user.

[00411] As described herein, software agents (such as agent 112) may run on machines (such as a machine that implements one of nodes 116) and detect new connections, processes, and/or logins. As also previously explained, such agents send associated records to data platform 12 which includes one or more datastores (e.g., data store 30) for persistently storing such data. Such data can be modeled using logical tables, also persisted in datastores (e.g., in a relational database that provides an SQL interface), allowing for querying of the data. Other datastores such as graph oriented databases and/or hybrid schemes can also be used.

[00412] The following identifiers are commonly used in the tables:

[00413] * MID

[00414] * PID_hash

[00415] An ssh login session can be identified uniquely by an (MID, PID_hash) tuple. The MID is a machine identifier that is unique to each machine, whether physical or virtual, across time and space. Operating systems use numbers called process identifiers (PIDs) to identify processes running at a given time. Over time processes may die and new processes may be started on a

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00598

machine or the machine itself may restart. The PID is not necessarily unique across time in that the same PID value can be reused for different processes at different times. In order to track process descendants across time, one should therefore account for time as well. In order to be able to identify a process on a machine uniquely across time, another number called a PID_hash is generated for the process. In various embodiments, the PID_hash is generated using a collision-resistant hash function that takes the PID, start time, and (in various embodiments, as applicable) other properties of a process.

[00416] Input data collected by agents comprises the input data model and is represented by the following logical tables:

[00417] * connections

[00418] * processes

[00419] * logins

[00420] A connections table may maintain records of TCP/IP connections observed on each machine. Example columns included in a connections table are as follows:

Column Name	Description
MID	Identifier of the machine that the connection was observed on.
start_time	Connection start time.
PID_hash	Identifier of the process that was associated with the connection.
src_IP_addr	Source IP address (the connection was initiated from this IP address).
src_port	Source port.
dst_IP_addr	Destination IP address (the connection was made to this IP address).
dst_port	Destination port.
Prot	Protocol (TCP or UDP).
Dir	Direction of the connection (incoming or outgoing) with respect to this machine.

[00421] The source fields (IP address and port) correspond to the side from which the connection was initiated. On the destination side, the agent associates an ssh connection with the privileged ssh process that is created for that connection.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00599

[00422] For each connection in the system, there will be two records in the table, assuming that the machines on both sides of the connection capture the connection. These records can be matched based on equality of the tuple (src_IP_addr, src_port, dst_IP_addr, dst_port, Prot) and proximity of the start_time fields (e.g., with a one minute upper threshold between the start_time fields).

[00423] A processes table maintains records of processes observed on each machine. It may have the following columns:

Column Name	Description
MID	Identifier of the machine that the process was observed on.
PID_hash	Identifier of the process.
start_time	Start time of the process.
exe_path	The executable path of the process.
PPID_hash	Identifier of the parent process.

[00424] A logins table may maintain records of logins to machines. It may have the following columns:

Column Name	Description
MID	Identifier of the machine that the login was observed on.
sshd_PID_hash	Identifier of the sshd privileged process associated with login.
login_time	Time of login.
login_username	Username used in login.

[00425] Output data generated by session tracking is represented with the following logical tables:

[00426] * login-local-descendant

[00427] * login-connection

[00428] * login-lineage

[00429] Using data in these tables, it is possible to determine descendant processes of a given ssh login session across the environment (i.e., spanning machines). Conversely, given a process, it is

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00600

possible to determine if it is an ssh login descendant as well as the original ssh login session for it if so.

[00430] A login-local-descendant table maintains the local (i.e., on the same machine) descendant processes of each ssh login session. It may have the following columns:

Column Name	Description
MID	Identifier of the machine that the login was observed on.
sshd_PID_hash	Identifier of the sshd privileged process associated with login.
login_time	Time of login.
login_username	Username used in login.

[00431] A login-connections table may maintain the connections associated with ssh logins. It may have the following columns:

Column Name	Description
MID	Identifier of the machine that the process was observed on.
sshd_PID_hash	Identifier of the sshd privileged process associated with the login.
login_time	Time of login.
login_username	The username used in the login.
src_IP_addr	Source IP address (connection was initiated from this IP address).
src_port	Source port.
dst_IP_addr	Destination IP address (connection was made to this IP address).
dst_port	Destination port.

[00432] A login-lineage table may maintain the lineage of ssh login sessions. It may have the following columns:

Column Name	Description
MID	Identifier of the machine that the ssh login was observed on.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00601

sshd_PID_hash	Identifier of the sshd privileged process associated with the login.
parent_MID	Identifier of the machine that the parent ssh login was observed on.
parent_sshd_PID_hash	Identifier of the sshd privileged process associated with the parent login.
origin_MID	Identifier of the machine that the origin ssh login was observed on.
origin_sshd_PID_hash	Identifier of the sshd privileged process associated with the origin login.

[00433] The parent_MID and parent_sshd_PID_hash columns can be null if there is no parent ssh login. In that case, the (MID, sshd_PID_hash) tuple will be the same as the (origin_MID, origin_sshd_PID_hash) tuple.

[00434] Fig. 3H illustrates an example of a process for performing extended user tracking. In various embodiments, process 361 is performed by data platform 12. The process begins at 362 when data associated with activities occurring in a network environment (such as entity A's datacenter) is received. One example of such data that can be received at 362 is agent-collected data described above (e.g., in conjunction with process 200). At 363, the received network activity is used to identify user login activity. And, at 364, a logical graph that links the user login activity to at least one user and at least one process is generated (or updated, as applicable). Additional detail regarding process 361, and in particular, portions 363 and 364 of process 361 are described in more detail below (e.g., in conjunction with discussion of Fig. 3J).

[00435] Fig. 3I depicts a representation of a user logging into a first machine, then into a second machine from the first machine, and then making an external connection. The scenario depicted in Fig. 3I is used to describe an example of processing that can be performed on data collected by agents to generate extended user session tracking information. Fig. 3I is an alternate depiction of the information shown in Figs. 3F and 3G.

[00436] At time t1 (365), a first ssh connection is made to Machine A (366) from an external source (367) by a user having a username of "X." In the following example, suppose the external source has an IP address of 1.1.1.10 and uses source port 10000 to connect to Machine A (which has an IP address of 2.2.2.20 and a destination port 22). External source 367 is considered an external source because its IP address is outside of the environment being monitored (e.g., is a node outside of entity A's datacenter, connecting to a node inside of entity A's datacenter).

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00602

[00437] A first ssh login session LS1 is created on machine A for user X. The privileged openssh process for this login is A1 (368). Under the login session LS1, the user creates a bash shell process with PID_hash A2 (369).

[00438] At time t2 (370), inside the bash shell process A2, the user runs an ssh program under a new process A3 (371) to log in to machine B (372) with a different username ("Y"). In particular, an ssh connection is made from source IP address 2.2.2.20 and source port 10001 (Machine A's source information) to destination IP address 2.2.2.21 and destination port 22 (Machine B's destination information).

[00439] A second ssh login session LS2 is created on machine B for user Y. The privileged openssh process for this login is B1 (373). Under the login session LS2, the user creates a bash shell process with PID_hash B2 (374).

[00440] At time t3 (376), inside the bash shell process B2, the user runs a curl command under a new process B3 (377) to download a file from an external destination (378). In particular, an HTTPS connection is made from source IP address 2.2.2.21 and source port 10002 (Machine B's source information) to external destination IP address 3.3.3.30 and destination port 443 (the external destination's information).

[00441] Using techniques described herein, it is possible to determine the original user who initiated the connection to external destination 378, which in this example is a user having the username X on machine A (where the extended user session can be determined to start with ssh login session LS1).

[00442] Based on local descendant tracking, the following determinations can be on machine A and B without yet having performed additional processing (described in more detail below):

[00443] * A3 is a descendant of A1 and thus associated with LS1.

[00444] * The connection to the external domain from machine B is initiated by B3.

[00445] * B3 is a descendant of B1 and is thus associated with LS2.

[00446] * Connection to the external domain is thus associated with LS2.

[00447] An association between A3 and LS2 can be established based on the fact that LS2 was created based on an ssh connection initiated from A3. Accordingly, it can be determined that LS2 is a child of LS1.

[00448] To determine the user responsible for making the connection to the external destination (e.g., if it were a known bad destination), first, the process that made the connection would be traced, i.e., from B3 to LS2. Then LS2 would be traced to LS1 (i.e., LS1 is the origin login session for LS2). Thus the user for this connection is the user for LS1, i.e., X. As represented in Fig. 3I, one can visualize the tracing by following the links (in the reverse direction of arrows) from external destination 378 to A1 (368).

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00603

[00449] In the example scenario, it is assumed that both ssh connections occur in the same analysis period. However, the approaches described herein will also work for connections and processes that are created in different time periods.

[00450] Fig. 3J illustrates an example of a process for performing extended user tracking. In various embodiments, process 380 is performed periodically (e.g., once an hour in a batch fashion) by ssh tracker 148 to generate new output data. In general, batch processing allows for efficient analysis of large volumes of data. However, the approach can be adapted, as applicable, to process input data on a record-by-record fashion while maintaining the same logical data processing flow. As applicable the results of a given portion of process 380 are stored for use in a subsequent portion.

[00451] The process begins at 381 when new ssh connection records are identified. In particular, new ssh connections started during the current time period are identified by querying the connections table. The query uses filters on the start_time and dst_port columns. The values of the range filter on the start_time column are based on the current time period. The dst_port column is checked against ssh listening port(s). By default, the ssh listening port number is 22. However, as this could vary across environments, the port(s) that openssh servers are listening to in the environment can be determined by data collection agents dynamically and used as the filter value for the dst_port as applicable. In the scenario depicted in Fig. 3I, the query result will generate the records shown in Fig. 3K. Note that for the connection between machine A and B, the two machines are likely to report start_time values that are not exactly the same but close enough to be considered matching (e.g., within one minute or another appropriate amount of time). In the above table, they are shown to be the same for simplicity.

[00452] At 382, ssh connection records reported from source and destination sides of the same connection are matched. The ssh connection records (e.g., returned from the query at 381) are matched based on the following criteria:

[00453] * The five tuples (src_IP, dst_IP, IP_prot, src_port, dst_port) of the connection records must match.

[00454] * The delta between the start times of the connections must be within a limit that would account for the worst case clock difference expected between two machines in the environment and typical connection setup latency.

[00455] * If there are multiple matches possible, then the match with the smallest time delta is chosen.

[00456] Note that record 390 from machine A for the incoming connection from the external source cannot be matched with another record as there is an agent only on the destination side for

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00604

this connection. Example output of portion 382 of process 380 is shown in Fig. 3L. The values in the dst_PID_hash column (391) are that of the sshd privileged process associated with ssh logins.

[00457] At 383, new logins during the current time period are identified by querying the logins table. The query uses a range filter on the login_time column with values based on the current time period. In the example depicted in Fig. 3I, the query result will generate the records depicted in Fig. 3M.

[00458] At 384, matched ssh connection records created at 382 and new login records created at 383 are joined to create new records that will eventually be stored in the login-connection table. The join condition is that dst_MID of the matched connection record is equal to the MID of the login record and the dst_PID_hash of the matched connection record is equal to the sshd_PID_hash of the login record. In the example depicted in Fig. 3I, the processing performed at 384 will generate the records depicted in Fig. 3N.

[00459] At 385, login-local-descendant records in the lookback time period are identified. It is possible that a process that is created in a previous time period makes an ssh connection in the current analysis batch period. Although not depicted in the example illustrated in Fig. 3I, consider a case where bash process A2 does not create ssh process A3 right away but instead that the ssh connection A3 later makes to machine B is processed in a subsequent time period than the one where A2 was processed. While processing this subsequent time period in which processes A3 and B1 are seen, knowledge of A2 would be useful in establishing that B1 is associated with A3 (via ssh connection) which is associated with A2 (via process parentage) which in turn would be useful in establishing that the parent of the second ssh login is the first ssh login. The time period for which look back is performed can be limited to reduce the amount of historical data that is considered. However, this is not a requirement (and the amount of look back can be determined, e.g., based on available processing resources). The login local descendants in the lookback time period can be identified by querying the login-local-descendant table. The query uses a range filter on the login_time column where the range is from start_time_of_current_period - lookback_time to start_time_of_current_period. (No records as a result of performing 385 on the scenario depicted in Fig. 3I are obtained, as only a single time period is applicable in the example scenario.)

[00460] At 386, new processes that are started in the current time period are identified by querying the processes table. The query uses a range filter on the start_time column with values based on the current time period. In the example depicted in Fig. 3I, the processing performed at 386 will generate the records depicted in Fig. 3O.

[00461] At 387, new login-local-descendant records are identified. The purpose is to determine whether any of the new processes in the current time period are descendants of an ssh login

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00605

process and if so to create records that will be stored in the login-local-descendant table for them. In order to do so, the parent-child relationships between the processes are recursively followed. Either a top down or bottom up approach can be used. In a top down approach, the ssh local descendants in the lookback period identified at 385, along with new ssh login processes in the current period identified at 384 are considered as possible ancestors for the new processes in the current period identified at 386.

[00462] Conceptually, the recursive approach can be considered to include multiple sub-steps where new processes that are identified to be ssh local descendants in the current sub-step are considered as ancestors for the next step. In the example scenario depicted in Fig. 3I, the following descendancy relationships will be established in two sub-steps:

[00463] Sub-step 1:

[00464] Process A2 is a local descendant of LS1 (i.e., MID = A, sshd_PID_hash = A1) because it is a child of process A1 which is the login process for LS1.

[00465] Process B2 is a local descendant of LS2 (i.e., MID = B, sshd_PID_hash = B1) because it is a child of process B1 which is the login process for LS2.

[00466] Sub-step 2:

[00467] Process A3 is a local descendant of LS1 because it is a child of process A2 which is associated to LS1 in sub-step 1.

[00468] Process B3 is a local descendant of LS2 because it is a child of process B1 which is associated to LS2 in sub-step 1.

[00469] Implementation portion 387 can use a datastore that supports recursive query capabilities, or, queries can be constructed to process multiple conceptual sub-steps at once. In the example depicted in Fig. 3I, the processing performed at 387 will generate the records depicted in Fig. 3P. Note that the ssh privileged processes associated with the logins are also included as they are part of the login session.

[00470] At 388, the lineage of new ssh logins created in the current time period is determined by associating their ssh connections to source processes that may be descendants of other ssh logins (which may have been created in the current period or previous time periods). In order to do so, first an attempt is made to join the new ssh login connections in the current period (identified at 384) with the combination of the login local descendants in the lookback period (identified at 385) and the login local descendants in the current time period (identified at 386). This will create adjacency relationships between child and parent logins. In the example depicted in Fig. 3I, the second ssh login connection will be associated with process A3 and an adjacency relationship between the two login sessions will be created (as illustrated in Fig. 3Q).

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00606

[00471] Next, the adjacency relationships are used to find the original login sessions. While not shown in the sample scenario, there could be multiple ssh logins in a chain in the current time period, in which case a recursive approach (as in 387) could be used. At the conclusion of portion 388, the login lineage records depicted in Fig. 3R will be generated.

[00472] Finally, at 389, output data is generated. In particular, the new login-connection, login-local-descendant, and login-lineage records generated at 384, 387, and 388 are inserted into their respective output tables (e.g., in a transaction manner).

[00473] An alternate approach to matching TCP connections between machines running an agent is for the client to generate a connection GUID and send it in the connection request (e.g., the SYN packet) it sends and for the server to extract the GUID from the request. If two connection records from two machines have the same GUID, they are for the same connection. Both the client and server will store the GUID (if it exists) in the connection records they maintain and report. On the client side, the agent can configure the network stack (e.g., using IP tables functionality on Linux) to intercept an outgoing TCP SYN packet and modify it to add the generated GUID as a TCP option. On the server side, the agent already extracts TCP SYN packets and thus can look for this option and extract the GUID if it exists.

[00474] Example graph-based user tracking and threat detection embodiments associated with data platform 12 will now be described. Administrators and other users of network environments (e.g., entity A's datacenter 104) often change roles to perform tasks. As one example, suppose that at the start of a workday, an administrator (hereinafter "Joe Smith") logs in to a console, using an individualized account (e.g., username=joe.smith). Joe performs various tasks as himself (e.g., answering emails, generating status reports, writing code, etc.). For other tasks (e.g., performing updates), Joe may require different/additional permission than his individual account has (e.g., root privileges). One way Joe can gain access to such permissions is by using sudo, which will allow Joe to run a single command with root privileges. Another way Joe can gain access to such permissions is by su or otherwise logging into a shell as root. After gaining root privileges, another thing that Joe can do is switch identities. As one example, to perform administrative tasks, Joe may use "su help" or "su database-admin" to become (respectively) the help user or the database-admin user on a system. He may also connect from one machine to another, potentially changing identities along the way (e.g., logging in as joe.smith at a first console, and connecting to a database server as database-admin). When he's completed various administrative tasks, Joe can relinquish his root privileges by closing out of any additional shells created, reverting back to a shell created for user joe.smith.

[00475] While there are many legitimate reasons for Joe to change his identity throughout the day, such changes may also correspond to nefarious activity. Joe himself may be nefarious, or

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00607

Joe's account (joe.smith) may have been compromised by a third party (whether an "outsider" outside of entity A's network, or an "insider"). Using techniques described herein, the behavior of users of the environment can be tracked (including across multiple accounts and/or multiple machines) and modeled (e.g., using various graphs described herein). Such models can be used to generate alerts (e.g., to anomalous user behavior). Such models can also be used forensically, e.g., helping an investigator visualize various aspects of a network and activities that have occurred, and to attribute particular types of actions (e.g., network connections or file accesses) to specific users.

[00476] In a typical day in a datacenter, a user (e.g., Joe Smith) will log in, run various processes, and (optionally) log out. The user will typically log in from the same set of IP addresses, from IP addresses within the same geographical area (e.g., city or country), or from historically known IP addresses/geographical areas (i.e., ones the user has previously/occasionally used). A deviation from the user's typical (or historical) behavior indicates a change in login behavior. However, it does not necessarily mean that a breach has occurred. Once logged into a datacenter, a user may take a variety of actions. As a first example, a user might execute a binary/script. Such binary/script might communicate with other nodes in the datacenter, or outside of the datacenter, and transfer data to the user (e.g., executing "curl" to obtain data from a service external to the datacenter). As a second example, the user can similarly transfer data (e.g., out of the datacenter), such as by using POST. As a third example, a user might change privilege (one or more times), at which point the user can send/receive data as per above. As a fourth example, a user might connect to a different machine within the datacenter (one or more times), at which point the user can send/receive data as per the above.

[00477] In various embodiments, the above information associated with user behavior is broken into four tiers. The tiers represent example types of information that data platform 12 can use in modeling user behavior:

[00478] 1. The user's entry point (e.g., domains, IP addresses, and/or geolocation information such as country/city) from which a user logs in.

[00479] 2. The login user and machine class.

[00480] 3. Binaries, executables, processes, etc. a user launches.

[00481] 4. Internal servers with which the user (or any of the user's processes, child processes, etc.) communicates, and external contacts (e.g., domains, IP addresses, and/or geolocation information such as country/city) with which the user communicates (i.e., transfers data).

[00482] In the event of a security breach, being able to concretely answer questions about such information can be very important. And, collectively, such information is useful in providing an end-to-end path (e.g., for performing investigations).

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00608

[00483] In the following example, suppose a user ("UserA") logs into a machine ("Machine01") from a first IP address ("IP01"). Machine01 is inside a datacenter. UserA then launches a script ("runnable.sh") on Machine01. From Machine01, UserA next logs into a second machine ("Machine02") via ssh, also as UserA, also within the datacenter. On Machine02, UserA again launches a script ("new_runnable.sh"). On Machine02, UserA then changes privilege, becoming root on Machine02. From Machine02, UserA (now as root) logs into a third machine ("Machine03") in the datacenter via ssh, as root on Machine03. As root on Machine03, the user executes a script ("collect_data.sh") on Machine03. The script internally communicates (as root) to a MySQL-based service internal to the datacenter, and downloads data from the MySQL-based service. Finally, as root on Machine03, the user externally communicates with a server outside the datacenter ("External01"), using a POST command. To summarize what has occurred, in this example, the source/entry point is IP01. Data is transferred to an external server External01. The machine performing the transfer to External01 is Machine03. The user transferring the data is "root" (on Machine03), while the actual user (hiding behind root) is UserA.

[00484] In the above scenario, the "original user" (ultimately responsible for transmitting data to External01) is UserA, who logged in from IP01. Each of the processes ultimately started by UserA, whether started at the command line (tty) such as "runnable.sh" or started after an ssh connection such as "new_runnable.sh," and whether as UserA, or as a subsequent identity, are all examples of child processes which can be arranged into a process hierarchy.

[00485] As previously mentioned, machines can be clustered together logically into machine clusters. One approach to clustering is to classify machines based on information such as the types of services they provide/binaries they have installed upon them/processes they execute. Machines sharing a given machine class (as they share common binaries/services/etc.) will behave similarly to one another. Each machine in a datacenter can be assigned to a machine cluster, and each machine cluster can be assigned an identifier (also referred to herein as a machine class). One or more tags can also be assigned to a given machine class (e.g., database_servers_west or prod_web_frontend). One approach to assigning a tag to a machine class is to apply term frequency analysis (e.g., TF/IDF) to the applications run by a given machine class, selecting as tags those most unique to the class. Data platform 12 can use behavioral baselines taken for a class of machines to identify deviations from the baseline (e.g., by a particular machine in the class).

[00486] Fig. 3S illustrates an example of a process for detecting anomalies. In various embodiments, process 392 is performed by data platform 12. As explained above, a given session will have an original user. And, each action taken by the original user can be tied back to the original user, despite privilege changes and/or lateral movement throughout a datacenter. Process

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00609

392 begins at 393 when log data associated with a user session (and thus an original user) is received. At 394, a logical graph is generated, using at least a portion of the collected data. When an anomaly is detected (395), it can be recorded, and as applicable, an alert is generated (396). The following are examples of graphs that can be generated (e.g., at 394), with corresponding examples of anomalies that can be detected (e.g., at 395) and alerted upon (e.g., at 396).

[00487] Fig. 4A illustrates a representation of an embodiment of an insider behavior graph. In the example of Fig. 4A, each node in the graph can be: (1) a cluster of users; (2) a cluster of launched processes; (3) a cluster of processes/servers running on a machine class; (4) a cluster of external IP addresses (of incoming clients); or (5) a cluster of external servers based on DNS/IP/etc. As depicted in Fig. 4A, graph data is vertically tiered into four tiers. Tier 0 (400) corresponds to entry point information (e.g., domains, IP addresses, and/or geolocation information) associated with a client entering the datacenter from an external entry point. Entry points are clustered together based on such information. Tier 1 (401) corresponds to a user on a machine class, with a given user on a given machine class represented as a node. Tier 2 (402) corresponds to launched processes, child processes, and/or interactive processes. Processes for a given user and having similar connectivity (e.g., sharing the processes they launch and the machines with which they communicate) are grouped into nodes. Finally, Tier 3 (403) corresponds to the services/servers/domains/IP addresses with which processes communicate. A relationship between the tiers can be stated as follows: Tier 0 nodes log in to tier 1 nodes. Tier 1 nodes launch tier 2 nodes. Tier 2 nodes connect to tier 3 nodes.

[00488] The inclusion of an original user in both Tier 1 and Tier 2 allows for horizontal tiering. Such horizontal tiering ensures that there is no overlap between any two users in Tier 1 and Tier 2. Such lack of overlap provides for faster searching of an end-to-end path (e.g., one starting with a Tier 0 node and terminating at a Tier 3 node). Horizontal tiering also helps in establishing baseline insider behavior. For example, by building an hourly insider behavior graph, new edges/changes in edges between nodes in Tier 1 and Tier 2 can be identified. Any such changes correspond to a change associated with the original user. And, any such changes can be surfaced as anomalous and alerts can be generated.

[00489] As explained above, Tier 1 corresponds to a user (e.g., user "U") logging into a machine having a particular machine class (e.g., machine class "M"). Tier 2 is a cluster of processes having command line similarity (e.g., CType "C"), having an original user "U," and running as a particular effective user (e.g., user "U1"). The value of U1 may be the same as U (e.g., joe.smith in both cases), or the value of U1 may be different (e.g., U=joe.smith and U1=root). Thus, while an edge may be present from a Tier 1 node to a Tier 2 node, the effective user in the Tier 2 node

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00610

may or may not match the original user (while the original user in the Tier 2 node will match the original user in the Tier 1 node).

[00490] A change from a user U into a user U1 can take place in a variety of ways. Examples include where U becomes U1 on the same machine (e.g., via su), and also where U sshes to other machine(s). In both situations, U can perform multiple changes, and can combine approaches. For example, U can become U1 on a first machine, ssh to a second machine (as U1), become U2 on the second machine, and ssh to a third machine (whether as user U2 or user U3). In various embodiments, the complexity of how user U ultimately becomes U3 (or U5, etc.) is hidden from a viewer of an insider behavior graph, and only an original user (e.g., U) and the effective user of a given node (e.g., U5) are depicted. As applicable (e.g., if desired by a viewer of the insider behavior graph), additional detail about the path (e.g., an end-to-end path of edges from user U to user U5) can be surfaced (e.g., via user interactions with nodes).

[00491] Fig. 4B illustrates an example of a portion of an insider behavior graph (e.g., as rendered in a web browser). In the example shown, node 405 (the external IP address, 52.32.40.231) is an example of a Tier 0 node, and represents an entry point into a datacenter. As indicated by directional arrows 406 and 407, two users, "bob_prod" and "dave_prod," both made use of the source IP 52.32.40.231 when logging in between 5pm and 6pm on Sunday July 30 (408). Nodes 409 and 410 are examples of Tier 1 nodes, having bob_prod and dave_prod as associated respective original users. As previously mentioned, Tier 1 nodes correspond to a combination of a user and a machine class. In the example depicted in Fig. 4B, the machine class associated with nodes 409 and 410 is hidden from view to simplify visualization, but can be surfaced to a viewer of interface 404 (e.g., when the user clicks on node 409 or 410).

[00492] Nodes 414-423 are examples of Tier 2 nodes – processes that are launched by users in Tier 1 and their child, grandchild, etc. processes. Note that also depicted in Fig. 4B is a Tier 1 node 411 that corresponds to a user, "root," that logged in to a machine cluster from within the datacenter (i.e., has an entry point within the datacenter). Nodes 425-1 and 425-2 are examples of Tier 3 nodes – internal/external IP addresses, servers, etc., with which Tier 2 nodes communicate.

[00493] In the example shown in Fig. 4B, a viewer of interface 404 has clicked on node 423. As indicated in region 426, the user running the marathon container is "root." However, by following the directional arrows in the graph backwards from node 423 (i.e. from right to left), the viewer can determine that the original user, responsible for node 423, is "bob_prod," who logged into the datacenter from IP 52.32.40.231.

[00494] The following are examples of changes that can be tracked using an insider behavior graph model:

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00611

[00495] * A user logs in from a new IP address.

[00496] * A user logs in from a geolocation not previously used by that user.

[00497] * A user logs into a new machine class.

[00498] * A user launches a process not previously used by that user.

[00499] * A user connects to an internal server to which the user has not previously connected.

[00500] * An original user communicates with an external server (or external server known to be malicious) with which that user has not previously communicated.

[00501] * A user communicates with an external server which has a geolocation not previously used by that user.

[00502] Such changes can be surfaced as alerts, e.g., to help an administrator determine when/what anomalous behavior occurs within a datacenter. Further, the behavior graph model can be used (e.g., during forensic analysis) to answer questions helpful during an investigation. Examples of such questions include:

[00503] * Was there any new login activity (Tier 0) in the timeframe being investigated? As one example, has a user logged in from an IP address with unknown geolocation information? Similarly, has a user started communicating externally with a new Tier 3 node (e.g., one with unknown geolocation information).

[00504] * Has there been any suspicious login activity (Tier 0) in the timeframe being investigated? As one example, has a user logged in from an IP address that corresponds to a known bad IP address as maintained by Threat aggregator 150? Similarly, has there been any suspicious Tier 3 activity?

[00505] * Were any anomalous connections made within the datacenter during the timeframe being investigated? As one example, suppose a given user ("Frank") typically enters a datacenter from a particular IP address (or range of IP addresses), and then connects to a first machine type (e.g., bastion), and then to a second machine type (e.g., database_prod). If Frank has directly connected to database_prod (instead of first going through bastion) during the timeframe, this can be surfaced using the insider graph.

[00506] * Who is (the original user) responsible for running a particular process?

[00507] An example of an insider behavior graph being used in an investigation is depicted in Figs. 4C and 4D. Fig. 4C depicts a baseline of behavior for a user, "Bill." As shown in Fig. 4C, Bill typically logs into a datacenter from the IP address, 71.198.44.40 (427). He typically makes use of ssh (428), and sudo (429), makes use of a set of typical applications (430) and connects (as root) with the external service, api.lacework.net (431).

[00508] Suppose Bill's credentials are compromised by a nefarious outsider ("Eve"). Fig. 4D depicts an embodiment of how the graph depicted in Fig. 4C would appear once Eve begins

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00612

exfiltrating data from the datacenter. Eve logs into the datacenter (using Bill's credentials) from 52.5.66.8 (432). As Bill, Eve escalates her privilege to root (e.g., via su), and then becomes a different user, Alex (e.g., via su alex). As Alex, Eve executes a script, "sneak.sh" (433), which launches another script, "post.sh" (434), which contacts external server 435 which has an IP address of 52.5.66.7, and transmits data to it. Edges 436-439 each represent changes in Bill's behavior. As previously mentioned, such changes can be detected as anomalies and associated alerts can be generated. As a first example, Bill logging in from an IP address he has not previously logged in from (436) can generate an alert. As a second example, while Bill does typically make use of sudo (429), he has not previously executed sneak.sh (433) or post.sh (434) and the execution of those scripts can generate alerts as well. As a third example, Bill has not previously communicated with server 435, and an alert can be generated when he does so (439). Considered individually, each of edges 436-439 may indicate nefarious behavior, or may be benign. As an example of a benign edge, suppose Bill begins working from a home office two days a week. The first time he logs in from his home office (i.e., from an IP address that is not 71.198.44.40), an alert can be generated that he has logged in from a new location. Over time, however, as Bill continues to log in from his home office but otherwise engages in typical activities, Bill's graph will evolve to include logins from both 71.198.44.40 and his home office as baseline behavior. Similarly, if Bill begins using a new tool in his job, an alert can be generated the first time he executes the tool, but over time will become part of his baseline.

[00509] In some cases, a single edge can indicate a serious threat. For example, if server 432 (or 435) is included in a known bad IP listing, edge 436 (or 439) indicates compromise. An alert that includes an appropriate severity level (e.g., "threat level high") can be generated. In other cases, a combination of edges could indicate a threat (where a single edge might otherwise result in a lesser warning). In the example shown in Fig. 4D, the presence of multiple new edges is indicative of a serious threat. Of note, even though "sneak.sh" and "post.sh" were executed by Alex, because data platform 12 also keeps track of an original user, the compromise of user B's account will be discovered.

[00510] Fig. 4E illustrates a representation of an embodiment of a user login graph. In the example of Fig. 4E, tier 0 (440) clusters source IP addresses as belonging to a particular country (including an "unknown" country) or as a known bad IP. Tier 1 (441) clusters user logins, and tier 2 (442) clusters type of machine class into which a user is logging in. The user login graph tracks the typical login behavior of users. By interacting with a representation of the graph, answers to questions such as the following can be obtained:

[00511] * Where is a user logging in from?

[00512] * Have any users logged in from a known bad address?

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00613

[00513] * Have any non-developer users accessed development machines?

[00514] * Which machines does a particular user access?

[00515] Examples of alerts that can be generated using the user login graph include:

[00516] * A user logs in from a known bad IP address.

[00517] * A user logs in from a new country for the first time.

[00518] * A new user logs into the datacenter for the first time.

[00519] * A user accesses a machine class that the user has not previously accessed.

[00520] One way to track privilege changes in a datacenter is by monitoring a process hierarchy of processes. To help filter out noisy commands/processes such as "su –u," the hierarchy of processes can be constrained to those associated with network activity. In a *nix system, each process has two identifiers assigned to it, a process identifier (PID) and a parent process identifier (PPID). When such a system starts, the initial process is assigned a PID 0. Each user process has a corresponding parent process.

[00521] Using techniques described herein, a graph can be constructed (also referred to herein as a privilege change graph) which models privilege changes. In particular, a graph can be constructed which identifies where a process P1 launches a process P2, where P1 and P2 each have an associated user U1 and U2, with U1 being an original user, and U2 being an effective user. In the graph, each node is a cluster of processes (sharing a CType) executed by a particular (original) user. As all the processes in the cluster belong to the same user, a label that can be used for the cluster is the user's username. An edge in the graph, from a first node to a second node, indicates that a user of the first node changed its privilege to the user of the second node.

[00522] Fig. 4F illustrates an example of a privilege change graph. In the example shown in Fig. 4F, each node (e.g., nodes 444 and 445) represents a user. Privilege changes are indicated by edges, such as edge 446.

[00523] As with other graphs, anomalies in graph 443 can be used to generate alerts. Three examples of such alerts are as follows:

[00524] * New user entering the datacenter. Any time a new user enters the datacenter and runs a process, the graph will show a new node, with a new CType. This indicates a new user has been detected within the datacenter. Fig. 4F is a representation of an example of an interface that depicts such an alert. Specifically, as indicated in region 447, an alert for the time period 1pm-2pm on June 8 was generated. The alert identifies that a new user, Bill (448) executed a process.

[00525] *Privilege change. As explained above, a new edge, from a first node (user A) to a second node (user B) indicates that user A has changed privilege to user B.

[00526] * Privilege escalation. Privilege escalation is a particular case of privilege change, in which the first user becomes root.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00614

[00527] An example of an anomalous privilege change and an example of an anomalous privilege escalation are each depicted in graph 450 of Fig. 4G. In particular, as indicated in region 451, two alerts for the time period 2pm-3pm on June 8 were generated (corresponding to the detection of the two anomalous events). In region 452, root has changed privilege to the user "daemon," which root has not previously done. This anomaly is indicated to the user by highlighting the daemon node (e.g., outlining it in a particular color, e.g., red). As indicated by edge 453, Bill has escalated his privilege to the user root (which can similarly be highlighted in region 454). This action by Bill represents a privilege escalation.

[00528] An Extensible query interface for dynamic data compositions and filter applications will now be described.

[00529] As described herein, datacenters are highly dynamic environments. And, different customers of data platform 12 (e.g., entity A vs. entity B) may have different/disparate needs/requirements of data platform 12, e.g., due to having different types of assets, different applications, etc. Further, as time progresses, new software tools will be developed, new types of anomalous behavior will be possible (and should be detectable), etc. In various embodiments, data platform 12 makes use of predefined relational schema (including by having different predefined relational schema for different customers). However, the complexity and cost of maintaining/updating such predefined relational schema can rapidly become problematic – particularly where the schema includes a mix of relational, nested, and hierarchical (graph) datasets. In other embodiments, the data models and filtering applications used by data platform 12 are extensible. As will be described in more detail below, in various embodiments, data platform 12 supports dynamic query generation by automatic discovery of join relations via static or dynamic filtering key specifications among composable data sets. This allows a user of data platform 12 to be agnostic to modifications made to existing data sets as well as creation of new data sets. The extensible query interface also provides a declarative and configurable specification for optimizing internal data generation and derivations.

[00530] As will also be described in more detail below, data platform 12 is configured to dynamically translate user interactions (e.g., received via web app 120) into SQL queries (and without the user needing to know how to write queries). Such queries can then be performed (e.g., by query service 166) against any compatible backend (e.g., data store 30).

[00531] Fig. 4H illustrates an example of a user interacting with a portion of an interface. When a user visits data platform 12 (e.g., via web app 120 using a browser), data is extracted from data store 30 as needed (e.g., by query service 166), to provide the user with information, such as the visualizations depicted variously herein). As the user continues to interact with such visualizations (e.g., clicking on graph nodes, entering text into search boxes, navigating between

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00615

tabs (e.g., tab 455 vs. 465)), such interactions act as triggers that cause query service 166 to continue to obtain information from data store 30 as needed (and as described in more detail below).

[00532] In the example shown in Fig. 4H, user A is viewing a dashboard that provides various information about entity A users (455), during the time period March 2 at midnight – March 25 at 7pm (which she selected by interacting with region 456). Various statistical information is presented to user A in region 457. Region 458 presents a timeline of events that occurred during the selected time period. User A has opted to list only the critical, high, and medium events during the time period by clicking on the associated boxes (459-461). A total of 55 low severity, and 155 info-only events also occurred during the time period. Each time user A interacts with an element in Fig. 4H (e.g., clicks on box 461, clicks on link 464-1, or clicks on tab 465), her actions are translated/formalized into filters on the data set and used to dynamically generate SQL queries. The SQL queries are generated transparently to user A (and also to a designer of the user interface shown in Fig. 4H).

[00533] User A notes in the timeline (462) that a user, Dave, connected to a known bad server (examplebad.com) using wget, an event that has a critical severity level. User A can click on region 463 to expand details about the event inline (which will display, for example, the text "External connection made to known bad host examplebad.com at port 80 from application 'wget' running on host dev1.lacework.internal as user dave") directly below line 462. User A can also click on link 464-1, which will take her to a dossier for the event (depicted in Fig. 4I). As will be described in more detail below, a dossier is a template for a collection of visualizations.

[00534] As shown in interface 466, the event of Dave using wget to contact examplebad.com on March 16 was assigned an event ID of 9291 by data platform 12 (467). For convenience to user A, the event is also added to her dashboard in region 476 as a bookmark (468). A summary of the event is depicted in region 469. By interacting with boxes shown in region 470, user A can see a timeline of related events. In this case, user A has indicated that she would like to see other events involving the wget application (by clicking box 471). Events of critical and medium security involving wget occurred during the one hour window selected in region 472.

[00535] Region 473 automatically provides user A with answers to questions that may be helpful to have answers to while investigating event 9291. If user A clicks on any of the links in the event description (474), she will be taken to a corresponding dossier for the link. As one example, suppose user A clicks on link 475. She will then be presented with interface 477 shown in Fig. 4J.

[00536] Interface 477 is an embodiment of a dossier for a domain. In this example, the domain is "examplebad.com," as shown in region 478. Suppose user A would like to track down more

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00616

information about interactions entity A resources have made with examplebad.com between January 1 and March 20. She selects the appropriate time period in region 479 and information in the other portions of interface 477 automatically update to provide various information corresponding to the selected time frame. As one example, user A can see that contact was made with examplebad.com a total of 17 times during the time period (480), as well as a list of each contact (481). Various statistical information is also included in the dossier for the time period (482). If she scrolls down in interface 477, user A will be able to view various polygraphs associated with examplebad.com, such as an application-communication polygraph (483).

[00537] Data stored in data store 30 can be internally organized as an activity graph. In the activity graph, nodes are also referred to as Entities. Activities generated by Entities are modeled as directional edges between nodes. Thus, each edge is an activity between two Entities. One example of an Activity is a "login" Activity, in which a user Entity logs into a machine Entity (with a directed edge from the user to the machine). A second example of an Activity is a "launch" Activity, in which a parent process launches a child process (with a directed edge from the parent to the child). A third example of an Activity is a "DNS query" Activity, in which either a process or a machine performs a query (with a directed edge from the requestor to the answer, e.g., an edge from a process to www.example.com). A fourth example of an Activity is a network "connected to" Activity, in which processes, IP addresses, and listen ports can connect to each other (with a directed edge from the initiator to the server).

[00538] As will be described in more detail below, query service 166 provides either relational views or graph views on top of data stored in data store 30. Typically, a user will want to see data filtered using the activity graph. For example, if an entity was not involved in an activity in a given time period, that entity should be filtered out of query results. Thus, a request to show "all machines" in a given time frame will be interpreted as "show distinct machines that were active" during the time frame.

[00539] Query service 166 relies on three main data model elements: fields, entities, and filters. As used herein, a field is a collection of values with the same type (logical and physical). A field can be represented in a variety of ways, including: 1. a column of relations (table/view), 2. a return field from another entity, 3. an SQL aggregation (e.g., COUNT, SUM, etc.), 4. an SQL expression with the references of other fields specified, and 5. a nested field of a JSON object. As viewed by query service 166, an entity is a collection of fields that describe a data set. The data set can be composed in a variety of ways, including: 1. a relational table, 2. a parameterized SQL statement, 3. DynamicSQL created by a Java function, and 4. join/project/aggregate/subclass of other entities. Some fields are common for all entities. One example of such a field is a "first observed" timestamp (when first use of the entity was detected). A second example of such a

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00617

field is the entity classification type (e.g., one of: 1. Machine (on which an agent is installed), 2. Process, 3. Binary, 4. UID, 5. IP, 6. DNS Information, 7. ListenPort, and 8. PType). A third example of such a field is a "last observed" timestamp.

[00540] A filter is an operator that: 1. takes an entity and field values as inputs, 2. a valid SQL expression with specific reference(s) of entity fields, or 3. is a conjunct/disjunct of filters. As will be described in more detail below, filters can be used to filter data in various ways, and limit data returned by query service 166 without changing the associated data set.

[00541] As mentioned above, a dossier is a template for a collection of visualizations. Each visualization (e.g., the box including chart 484) has a corresponding card, which identifies particular target information needed (e.g., from data store 30) to generate the visualization. In various embodiments, data platform 12 maintains a global set of dossiers/cards. Users of data platform 12 such as user A can build their own dashboard interfaces using preexisting dossiers/cards as components, and/or they can make use of a default dashboard (which incorporates various of such dossiers/cards).

[00542] A JSON file can be used to store multiple cards (e.g., as part of a query service catalog). A particular card is represented by a single JSON object with a unique name as a field name.

[00543] Each card may be described by the following named fields:

[00544] TYPE: the type of the card. Example values include:

[00545] * Entity (the default type)

[00546] * SQL

[00547] * Filters

[00548] * DynamicSQL

[00549] * graphFilter

[00550] * graph

[00551] * Function

[00552] * Template

[00553] PARAMETERS: a JSON array object that contains an array of parameter objects with the following fields:

[00554] * name (the name of the parameter)

[00555] * required (a Boolean flag indicating whether the parameter is required or not)

[00556] * default (a default value of the parameter)

[00557] * props (a generic JSON object for properties of the parameter. Possible values are: "utype" (a user defined type), and "scope" (an optional property to configure a namespace of the parameter))

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00618

[00558] * value (a value for the parameter - non-null to override the default value defined in nested source entities)

[00559] SOURCES: a JSON array object explicitly specifying references of input entities. Each source reference has the following attributes:

[00560] * name (the card/entity name or fully-qualified Table name)

[00561] * type (required for base Table entity)

[00562] * alias (an alias to access this source entity in other fields (e.g., returns, filters, groups, etc))

[00563] RETURNS: a required JSON array object of a return field object. A return field object can be described by the following attributes:

[00564] * field (a valid field name from a source entity)

[00565] * expr (a valid SQL scalar expression. References to input fields of source entities are specified in the format of #{Entity.Field}. Parameters can also be used in the expression in the format of ${ParameterName})

[00566] * type (the type of field, which is required for return fields specified by expr. It is also required for all return fields of an Entity with an SQL type)

[00567] * alias (the unique alias for return field)

[00568] * aggr (possible aggregations are: COUNT, COUNT_DISTINCT, DISTINCT, MAX, MIN, AVG, SUM, FIRST_VALUE, LAST_VALUE)

[00569] * case (JSON array object represents conditional expressions “when” and “expr”)

[00570] * fieldsFrom, and, except (specification for projections from a source entity with excluded fields)

[00571] * props (general JSON object for properties of the return field. Possible properties include: “filterGroup,” “title,” “format,” and “utype”)

[00572] PROPS: generic JSON objects for other entity properties

[00573] SQL: a JSON array of string literals for SQL statements. Each string literal can contain parameterized expressions ${ParameterName} and/or composable entity by #{EntityName}

[00574] GRAPH: required for graph entity. Has the following required fields:

[00575] * source (including “type,” “props,” and “keys”)

[00576] * target (including “type,” “props,” and “keys”)

[00577] * edge (including “type” and “props”)

[00578] JOINS: a JSON array of join operators. Possible fields for a join operator include:

[00579] * type (possible join types include: “loj” - Left Outer Join, “join” - Inner Join, “in” - Semi Join, “implicit” - Implicit Join)

[00580] * left (a left hand side field of join)

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00619

[00581] * right (a right hand side field of join)

[00582] * keys (key columns for multi-way joins)

[00583] * order (a join order of multi-way joins)

[00584] FKEYS: a JSON array of FilterKey(s). The fields for a FilterKey are:

[00585] * type (type of FilterKey)

[00586] * fieldRefs (reference(s) to return fields of an entity defined in the sources field)

[00587] * alias (an alias of the FilterKey, used in implicit join specification)

[00588] FILTERS: a JSON array of filters (conjunct). Possible fields for a filter include:

[00589] * type (types of filters, including: “eq” - equivalent to SQL =, “ne” - equivalent to SQL <>, “ge” - equivalent to SQL >=, “gt” - equivalent to SQL >, “le” - equivalent to SQL <=, “lt” - equivalent to SQL <, “like” - equivalent to SQL LIKE, “not_like” - equivalent to SQL NOT LIKE, “rlike” - equivalent to SQL RLIKE (Snowflake specific), “not_rlike” - equivalent to SQL NOT RLIKE (Snowflake specific), “in” - equivalent to SQL IN, “not_in” - equivalent to SQL NOT IN)

[00590] * expr (generic SQL expression)

[00591] * field (field name)

[00592] * value (single value)

[00593] * values (for both IN and NOT IN)

[00594] ORDERS: a JSON array of ORDER BY for returning fields. Possible attributes for the ORDER BY clause include:

[00595] * field (field ordinal index (1 based) or field alias)

[00596] * order (asc/desc, default is ascending order)

[00597] GROUPS: a JSON array of GROUP BY for returning fields. Field attributes are:

[00598] * field (ordinal index (1 based) or alias from the return fields)

[00599] LIMIT: a limit for the number of records to be returned

[00600] OFFSET: an offset of starting position of returned data. Used in combination with limit for pagination.

[00601] Suppose customers of data platform 12 (e.g., entity A and entity B) request new data transformations or a new aggregation of data from an existing data set (as well as a corresponding visualization for the newly defined data set). As mentioned above, the data models and filtering applications used by data platform 12 are extensible. Thus, two example scenarios of extensibility are (1) extending the filter data set, and (2) extending a FilterKey in the filter data set.

[00602] Data platform 12 includes a query service catalog that enumerates cards available to users of data platform 12. New cards can be included for use in data platform 12 by being added

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00620

to the query service catalog (e.g., by an operator of data platform 12). For reusability and maintainability, a single external-facing card (e.g., available for use in a dossier) can be composed of multiple (nested) internal cards. Each newly added card (whether external or internal) will also have associated FilterKey(s) defined. A user interface (UI) developer can then develop a visualization for the new data set in one or more dossier templates. The same external card can be used in multiple dossier templates, and a given external card can be used multiple times in the same dossier (e.g., after customization). Examples of external card customization include customization via parameters, ordering, and/or various mappings of external data fields (columns).

[00603] As mentioned above, a second extensibility scenario is one in which a FilterKey in the filter data set is extended (i.e., existing template functions are used to define a new data set). As also mentioned above, data sets used by data platform 12 are composable/reusable/extensible, irrespective of whether the data sets are relational or graph data sets. One example data set is the User Tracking polygraph, which is generated as a graph data set (comprising nodes and edges). Like other polygraphs, User Tracking is an external data set that can be visualized both as a graph (via the nodes and edges) and can also be used as a filter data set for other cards, via the cluster identifier (CID) field.

[00604] As mentioned above, as users such as user A navigate through/interact with interfaces provided by data platform 12 (e.g., as shown in Fig. 4H), such interactions trigger query service 166 to generate and perform queries against data store 30. Dynamic composition of filter datasets can be implemented using FilterKeys and FilterKey Types. A FilterKey can be defined as a list of columns and/or fields in a nested structure (e.g., JSON). Instances of the same FilterKey Type can be formed as an Implicit Join Group. The same instance of a FilterKey can participate in different Implicit Join Groups. A list of relationships among all possible Implicit Join Groups is represented as a Join graph for the entire search space to create a final data filter set by traversing edges and producing Join Path(s).

[00605] Each card (e.g., as stored in the query service catalog and used in a dossier) can be introspected by a /card/describe/CardID REST request.

[00606] At runtime (e.g., whenever it receives a request from web app 120), query service 166 parses the list of implicit joins and creates a Join graph to manifest relationships of FilterKeys among Entities. A Join graph (an example of which is depicted in Fig. 4K) comprises a list of Join Link(s). A Join Link represents each implicit join group by the same FilterKey type. A Join Link maintains a reverse map (Entity-to-FilterKey) of FilterKeys and their Entities. As previously mentioned, Entities can have more than one FilterKey defined. The reverse map guarantees one FilterKey per Entity can be used for each JoinLink. Each JoinLink also maintains

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00621

a list of entities for the priority order of joins. Each JoinLink is also responsible for creating and adding directional edge(s) to graphs. An edge represents a possible join between two Entities.
[00607] At runtime, each Implicit Join uses the Join graph to find all possible join paths. The search of possible join paths starts with the outer FilterKey of an implicit join. One approach is to use a shortest path approach, with breadth first traversal and subject to the following criteria:
[00608] * Use the priority order list of Join Links for all entities in the same implicit join group.
[00609] * Stop when a node (Entity) is reached which has local filter(s).
[00610] * Include all join paths at the same level (depth).
[00611] * Exclude join paths based on the predefined rules (path of edges).
[00612] Fig. 4L illustrates an example of a process for dynamically generating and executing a query. In various embodiments, process 485 is performed by data platform 12. The process begins at 486 when a request is received to filter information associated with activities within a network environment. One example of such a request occurs in response to user A clicking on tab 465. Another example of such a request occurs in response to user A clicking on link 464-1. Yet another example of such a request occurs in response to user A clicking on link 464-2 and selecting (e.g., from a dropdown) an option to filter (e.g., include, exclude) based on specific criteria that she provides (e.g., an IP address, a username, a range of criteria, etc.).
[00613] At 487, a query is generated based on an implicit join. One example of processing that can be performed at 487 is as follows. As explained above, one way dynamic composition of filter datasets can be implemented is by using FilterKeys and FilterKey Types. And, instances of the same FilterKey Type can be formed as an Implicit Join Group. A Join graph for the entire search space can be constructed from a list of all relationships among all possible Join Groups. And, a final data filter set can be created by traversing edges and producing one or more Join Paths. Finally, the shortest path in the join paths is used to generate an SQL query string.
[00614] One approach to generating an SQL query string is to use a query building library (authored in an appropriate language such as Java). For example, a common interface "sqlGen" may be used in conjunction with process 485 is as follows. First, a card/entity is composed by a list of input cards/entities, where each input card recursively is composed by its own list of input cards. This nested structure can be visualized as a tree of query blocks(SELECT) in standard SQL constructs. SQL generation can be performed as the traversal of the tree from root to leaf entities (top-down), calling the sqlGen of each entity. Each entity can be treated as a subclass of the Java class(Entity). An implicit join filter (EntityFilter) is implemented as a subclass of Entity, similar to the right hand side of a SQL semi-join operator. Unlike the static SQL semi-join construct, it is conditionally and recursively generated even if it is specified in the input sources of the JSON specification. Another recursive interface can also be used in conjunction with

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00622

process 485, preSQLGen, which is primarily the entry point for EntityFilter to run a search and generate nested implicit join filters. During preSQLGen recursive invocations, the applicability of implicit join filters is examined and pushed down to its input subquery list. Another top-down traversal, pullUpCachable, can be used to pull up common sub-query blocks, including those dynamically generated by preSQLGen, such that SELECT statements of those cacheable blocks are generated only once at top-level WITH clauses. A recursive interface, sqlWith, is used to generate nested subqueries inside WITH clauses. The recursive calls of a sqlWith function can generate nested WITH clauses as well. An sqlFrom function can be used to generate SQL FROM clauses by referencing those subquery blocks in the WITH clauses. It also produces INNER/OUTER join operators based on the joins in the specification. Another recursive interface, sqlWhere, can be used to generate conjuncts and disjuncts of local predicates and semi-join predicates based on implicit join transformations. Further, sqlProject, sqlGroupBy, sqlOrderBy, and sqlLimitOffset can respectively be used to translate the corresponding directives in JSON spec to SQL SELECT list, GROUP BY, ORDER BY, and LIMIT/OFFSET clauses.

[00615] Returning to process 485, at 488, the query (generated at 487) is used to respond to the request. As one example of the processing performed at 488, the generated query is used to query data store 30 and provide (e.g., to web app 120) fact data formatted in accordance with a schema (e.g., as associated with a card associated with the request received at 486).

[00616] Although the examples described herein largely relate to embodiments where data is collected from agents and ultimately stored in a data store such as those provided by Snowflake, in other embodiments data that is collected from agents and other sources may be stored in different ways. For example, data that is collected from agents and other sources may be stored in a data warehouse, data lake, data mart, and/or any other data store.

[00617] A data warehouse may be embodied as an analytic database (e.g., a relational database) that is created from two or more data sources. Such a data warehouse may be leveraged to store historical data, often on the scale of petabytes. Data warehouses may have compute and memory resources for running complicated queries and generating reports. Data warehouses may be the data sources for business intelligence ('BI') systems, machine learning applications, and/or other applications. By leveraging a data warehouse, data that has been copied into the data warehouse may be indexed for good analytic query performance, without affecting the write performance of a database (e.g., an Online Transaction Processing ('OLTP') database). Data warehouses also enable the joining of data from multiple sources for analysis. For example, a sales OLTP application probably has no need to know about the weather at various sales locations, but sales predictions could take advantage of that data. By adding historical weather data to a data warehouse, it would be possible to factor it into models of historical sales data.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00623

[00618] Data lakes, which store files of data in their native format, may be considered as "schema on read" resources. As such, any application that reads data from the lake may impose its own types and relationships on the data. Data warehouses, on the other hand, are "schema on write," meaning that data types, indexes, and relationships are imposed on the data as it is stored in the EDW. "Schema on read" resources may be beneficial for data that may be used in several contexts and poses little risk of losing data. "Schema on write" resources may be beneficial for data that has a specific purpose, and good for data that must relate properly to data from other sources. Such data stores may include data that is encrypted using homomorphic encryption, data encrypted using privacy-preserving encryption, smart contracts, non-fungible tokens, decentralized finance, and other techniques.

[00619] Data marts may contain data oriented towards a specific business line whereas data warehouses contain enterprise-wide data. Data marts may be dependent on a data warehouse, independent of the data warehouse (e.g., drawn from an operational database or external source), or a hybrid of the two. In embodiments described herein, different types of data stores (including combinations thereof) may be leveraged. Such data stores may be proprietary or may be embodied as vendor provided products or services such as, for example, Google BigQuery, Druid, Amazon Redshift, IBM Db2, Dremio, Databricks Lakehouse Platform, Cloudera, Azure Synapse Analytics, and others.

[00620] The deployments (e.g., a customer's cloud deployment) that are analyzed, monitored, evaluated, or otherwise observed by the systems described herein (e.g., systems that include components such as the platform 12 of Fig. 1D, the data collection agents described herein, and/or other components) may be provisioned, deployed, and/or managed using infrastructure as code ('IaC'). IaC involves the managing and/or provisioning of infrastructure through code instead of through manual processes. With IaC, configuration files may be created that include infrastructure specifications. IaC can be beneficial as configurations may be edited and distributed, while also ensuring that environments are provisioned in a consistent manner. IaC approaches may be enabled in a variety of ways including, for example, using IaC software tools such as Terraform by HashiCorp. Through the usage of such tools, users may define and provide data center infrastructure using JavaScript Object Notation ('JSON'), YAML, proprietary formats, or some other format. In some embodiments, the configuration files may be used to emulate a cloud deployment for the purposes of analyzing the emulated cloud deployment using the systems described herein. Likewise, the configuration files themselves may be used as inputs to the systems described herein, such that the configuration files may be inspected to identify vulnerabilities, misconfigurations, violations of regulatory requirements, or other issues. In fact, configuration files for multiple cloud deployments may even be used by the systems described

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00624

herein to identify best practices, to identify configuration files that deviate from typical configuration files, to identify configuration files with similarities to deployments that have been determined to be deficient in some way, or the configuration files may be leveraged in some other ways to detect vulnerabilities, misconfigurations, violations of regulatory requirements, or other issues prior to deploying an infrastructure that is described in the configuration files. In some embodiments the techniques described herein may be used in multi-cloud, multi-tenant, cross-cloud, cross-tenant, cross-user, industry cloud, digital platform, and other scenarios depending on specific need or situation.

[00621] In some embodiments, the deployments that are analyzed, monitored, evaluated, or otherwise observed by the systems described herein (e.g., systems that include components such as the platform 12 of Fig. 1D, the data collection agents described herein, and/or other components) may be monitored to determine the extent to which a particular component has experienced "drift" relative to its associated IaC configuration. Discrepancies between how cloud resources were defined in an IaC configuration file and how they are currently configured in runtime may be identified and remediation workflows may be initiated to generate an alert, reconfigure the deployment, or take some other action. Such discrepancies may occur for a variety of reasons. Such discrepancies may occur, for example, due to maintenance operations being performed, due to incident response tasks being carried out, or for some other reason. Readers will appreciate that while IaC helps avoid initial misconfigurations of a deployment by codifying and enforcing resource creation, resource configuration, security policies, and so on, the systems described herein may prevent unwanted drift from occurring during runtime and after a deployment has been created in accordance with an IaC configuration.

[00622] In some embodiments, the deployments (e.g., a customer's cloud deployment) that are analyzed, monitored, evaluated, or otherwise observed by the systems described herein (e.g., systems that include components such as the platform 12 of Fig. 1D, the data collection agents described herein, and/or other components) may also be provisioned, deployed, and/or managed using security as code ('SaC'). SaC extends IaC concepts by defining cybersecurity policies and/or standards programmatically, so that the policies and/or standards can be referenced automatically in the configuration scripts used to provision cloud deployments. Stated differently, SaC can automate policy implementation and cloud deployments may even be compared with the policies to prevent "drift." For example, if a policy is created where all personally identifiable information ('PII') or personal health information ('PHI') must be encrypted when it is stored, that policy is translated into a process that is automatically launched whenever a developer submits code, and code that violates the policy may be automatically rejected.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00625

[00623] In some embodiments, SaC may be implemented by initially classifying workloads (e.g., by sensitivity, by criticality, by deployment model, by segment). Policies that can be instantiated as code may subsequently be designed. For example, compute-related policies may be designed, access-related policies may be designed, application-related policies may be designed, network-related policies may be designed, data-related policies may be designed, and so on. Security as code may then be instantiated through architecture and automation, as successful implementation of SaC can benefit from making key architectural-design decisions and executing the right automation capabilities. Next, operating model protections may be built and supported. For example, an operating model may "shift left" to maximize self-service and achieve full-life-cycle security automation (e.g., by standardizing common development toolchains, CI/CD pipelines, and the like). In such an example, security policies and access controls may be part of the pipeline, automatic code review and bug/defect detection may be performed, automated build processes may be performed, vulnerability scanning may be performed, checks against a risk-control framework may be made, and other tasks may be performed all before deploying an infrastructure or components thereof.

[00624] The systems described herein may be useful in analyzing, monitoring, evaluating, or otherwise observing a GitOps environment. In a GitOps environment, Git may be viewed as the one and only source of truth. As such, GitOps may require that the desired state of infrastructure (e.g., a customer's cloud deployment) be stored in version control such that the entire audit trail of changes to such infrastructure can be viewed or audited. In a GitOps environment, all changes to infrastructure are embodied as fully traceable commits that are associated with committer information, commit IDs, time stamps, and/or other information. In such an embodiment, both an application and the infrastructure (e.g., a customer's cloud deployment) that supports the execution of the application are therefore versioned artifacts and can be audited using the gold standards of software development and delivery. Readers will appreciate that while the systems described herein are described as analyzing, monitoring, evaluating, or otherwise observing a GitOps environment, in other embodiments other source control mechanisms may be utilized for creating infrastructure, making changes to infrastructure, and so on. In these embodiments, the systems described herein may similarly be used for analyzing, monitoring, evaluating, or otherwise observing such environments.

[00625] As described in other portions of the present disclosure, the systems described herein may be used to analyze, monitor, evaluate, or otherwise observe a customer's cloud deployment. While securing traditional datacenters requires managing and securing an IP-based perimeter with networks and firewalls, hardware security modules ('HSMs'), security information and event management ('SIEM') technologies, and other physical access restrictions, such solutions

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00626

are not particularly useful when applied to cloud deployments. As such, the systems described herein may be configured to interact with and even monitor other solutions that are appropriate for cloud deployments such as, for example, "zero trust" solutions.

[00626] A zero trust security model (a.k.a., zero trust architecture) describes an approach to the design and implementation of IT systems. A primary concept behind zero trust is that devices should not be trusted by default, even if they are connected to a managed corporate network such as the corporate LAN and even if they were previously verified. Zero trust security models help prevent successful breaches by eliminating the concept of trust from an organization's network architecture. Zero trust security models can include multiple forms of authentication and authorization (e.g., machine authentication and authorization, human/user authentication and authorization) and can also be used to control multiple types of accesses or interactions (e.g., machine-to-machine access, human-to-machine access).

[00627] In some embodiments, the systems described herein may be configured to interact with zero trust solutions in a variety of ways. For example, agents that collect input data for the systems described herein (or other components of such systems) may be configured to access various machines, applications, data sources, or other entity through a zero trust solution, especially where local instances of the systems described herein are deployed at edge locations. Likewise, given that zero trust solutions may be part of a customer's cloud deployment, the zero trust solution itself may be monitored to identify vulnerabilities, anomalies, and so on. For example, network traffic to and from the zero trust solution may be analyzed, the zero trust solution may be monitored to detect unusual interactions, log files generated by the zero trust solution may be gathered and analyzed, and so on.

[00628] In some embodiments, the systems described herein may leverage various tools and mechanisms in the process of performing its primary tasks (e.g., monitoring a cloud deployment). For example, Linux eBPF is mechanism for writing code to be executed in the Linux kernel space. Through the usage of eBPF, user mode processes can hook into specific trace points in the kernel and access data structures and other information. For example, eBPF may be used to gather information that enables the systems described herein to attribute the utilization of networking resources or network traffic to specific processes. This may be useful in analyzing the behavior of a particular process, which may be important for observability/SIEM.

[00629] The systems described may be configured to collect security event logs (or any other type of log or similar record of activity) and telemetry in real time for threat detection, for analyzing compliance requirements, or for other purposes. In such embodiments, the systems described herein may analyze telemetry in real time (or near real time), as well as historical telemetry, to detect attacks or other activities of interest. The attacks or activities of interest may

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00627

be analyzed to determine their potential severity and impact on an organization. In fact, the attacks or activities of interest may be reported, and relevant events, logs, or other information may be stored for subsequent examination.

[00630] In one embodiment, systems described herein may be configured to collect security event logs (or any other type of log or similar record of activity) and telemetry in real time to provide customers with a SIEM or SIEM-like solution. SIEM technology aggregates event data produced by security devices, network infrastructure, systems, applications, or other source. Centralizing all of the data that may be generated by a cloud deployment may be challenging for a traditional SIEM, however, as each component in a cloud deployment may generate log data or other forms of machine data, such that the collective amount of data that can be used to monitor the cloud deployment can grow to be quite large. A traditional SIEM architecture, where data is centralized and aggregated, can quickly result in large amounts of data that may be expensive to store, process, retain, and so on. As such, SIEM technologies may frequently be implemented such that silos are created to separate the data.

[00631] In some embodiments of the present disclosure, data that is ingested by the systems described herein may be stored in a cloud-based data warehouse such as those provided by Snowflake and others. Given that companies like Snowflake offer data analytics and other services to operate on data that is stored in their data warehouses, in some embodiments one or more of the components of the systems described herein may be deployed in or near Snowflake as part of a secure data lake architecture (a.k.a., a security data lake architecture, a security data lake/warehouse). In such an embodiment, components of the systems described herein may be deployed in or near Snowflake to collect data, transform data, analyze data for the purposes of detecting threats or vulnerabilities, initiate remediation workflows, generate alerts, or perform any of the other functions that can be performed by the systems described herein. In such embodiments, data may be received from a variety of sources (e.g., EDR or EDR-like tools that handle endpoint data, cloud access security broker ('CASB') or CASB-like tools that handle data describing interactions with cloud applications, Identity and Access Management ('IAM') or IAM-like tools, and many others), normalized for storage in a data warehouse, and such normalized data may be used by the systems described herein. In fact, the systems described herein may actually implement the data sources (e.g., an EDR tool, a CASB tool, an IAM tool) described above.

[00632] In some embodiments one data source that is ingested by the systems described herein is log data, although other forms of data such as network telemetry data (flows and packets) and/or many other forms of data may also be utilized. In some embodiments, event data can be combined with contextual information about users, assets, threats, vulnerabilities, and so on, for

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00628

the purposes of scoring, prioritization and expediting investigations. In some embodiments, input data may be normalized, so that events, data, contextual information, or other information from disparate sources can be analyzed more efficiently for specific purposes (e.g., network security event monitoring, user activity monitoring, compliance reporting). The embodiments described here offer real-time analysis of events for security monitoring, advanced analysis of user and entity behaviors, querying and long-range analytics for historical analysis, other support for incident investigation and management, reporting (for compliance requirements, for example), and other functionality.

[00633] In some embodiments, the systems described herein may be part of an application performance monitoring ('APM') solution. APM software and tools enable the observation of application behavior, observation of its infrastructure dependencies, observation of users and business key performance indicators ('KPIs') throughout the application's life cycle, and more. The applications being observed may be developed internally, as packaged applications, as software as a service ('SaaS'), or embodied in some other ways. In such embodiments, the systems described herein may provide one or more of the following capabilities:

[00634] The ability to operate as an analytics platform that ingests, analyzes, and builds context from traces, metrics, logs, and other sources.

[00635] Automated discovery and mapping of an application and its infrastructure components.

[00636] Observation of an application's complete transactional behavior, including interactions over a data communications network.

[00637] Monitoring of applications running on mobile (native and browser) and desktop devices.

[00638] Identification of probable root causes of an application's performance problems and their impact on business outcomes.

[00639] Integration capabilities with automation and service management tools.

[00640] Analysis of business KPIs and user journeys (for example, login to check-out).

[00641] Domain-agnostic analytics capabilities for integrating data from third-party sources.

[00642] Endpoint monitoring to understand the user experience and its impact on business outcomes.

[00643] Support for virtual desktop infrastructure ('VDI') monitoring.

[00644] In embodiments where the systems described herein are used for APM, some components of the system may be modified, other components may be added, some components may be removed, and other components may remain the same. In such an example, similar mechanisms as described elsewhere in this disclosure may be used to collect information from the applications, network resources used by the application, and so on. The graph based

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00629

modelling techniques may also be leveraged to perform some of the functions mentioned above, or other functions as needed.

[00645] In some embodiments, the systems described herein may be part of a solution for developing and/or managing artificial intelligence ('AI') or machine learning ('ML') applications. For example, the systems described herein may be part of an AutoML tool that automate the tasks associated with developing and deploying ML models. In such an example, the systems described herein may perform various functions as part of an AutoML tool such as, for example, monitoring the performance of a series of processes, microservices, and so on that are used to collectively form the AutoML tool. In other embodiments, the systems described herein may perform other functions as part of an AutoML tool or may be used to monitor, analyze, or otherwise observe an environment that the AutoML tool is deployed within.

[00646] In some embodiments, the systems described herein may be used to manage, analyze, or otherwise observe deployments that include other forms of AI/ML tools. For example, the systems described herein may manage, analyze, or otherwise observe deployments that include AI services. AI services are, like other resources in an as-a-service model, ready-made models and AI applications that are consumable as services and made available through APIs. In such an example, rather than using their own data to build and train models for common activities, organizations may access pre-trained models that accomplish specific tasks. Whether an organization needs natural language processing ('NLP'), automatic speech recognition ('ASR'), image recognition, or some other capability, AI services simply plug-and-play into an application through an API. Likewise, the systems described herein may be used to manage, analyze, or otherwise observe deployments that include other forms of AI/ML tools such as Amazon Sagemaker (or other cloud machine-learning platform that enables developers to create, train, and deploy ML models) and related services such as Data Wrangler (a service to accelerate data prep for ML) and Pipelines (a CI/CD service for ML).

[00647] In some embodiments, the systems described herein may be used to manage, analyze, or otherwise observe deployments that include various data services. For example, data services may include secure data sharing services, data marketplace services, private data exchanges services, and others. Secure data sharing services can allow access to live data from its original location, where those who are granted access to the data simply reference the data in a controlled and secure manner, without latency or contention from concurrent users. Because changes to data are made to a single version, data remains up-to-date for all consumers, which ensures data models are always using the latest version of such data. Data marketplace services operate as a single location to access live, ready-to-query data (or data that is otherwise ready for some other use). A data marketplace can even include a "feature stores," which can allow data scientists to

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00630

repurpose existing work. For example, once a data scientist has converted raw data into a metric (e.g., costs of goods sold), this universal metric can be found quickly and used by other data scientists for quick analysis against that data.

[00648] In some embodiments, the systems described herein may be used to manage, analyze, or otherwise observe deployments that include distributed training engines or similar mechanisms such as, for example, such as tools built on Dask. Dask is an open source library for parallel computing that is written in Python. Dask is designed to enable data scientists to improve model accuracy faster, as Dask enables data scientists can do everything in Python end-to-end, which means that they no longer need to convert their code to execute in environments like Apache Spark. The result is reduced complexity and increased efficiency. The systems described herein may also be used to manage, analyze, or otherwise observe deployments that include technologies such as RAPIDS (an open source Python framework which is built on top of Dask). RAPIDS optimizes compute time and speed by providing data pipelines and executing data science code entirely on graphics processing units (GPUs) rather than CPUs. Multi-cluster, shared data architecture, DataFrames, Java user-defined functions (UDF) are supported to enable trained models to run within a data warehouse.

[00649] In some embodiments, the systems described herein may be leveraged for the specific use case of detecting and/or remediating ransomware attacks and/or other malicious action taken with respect to data, systems, and/or other resources associated with one or more entities. Ransomware is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to such data unless a ransom is paid. In such embodiments, ransomware attacks may be carried out in a manner such that patterns (e.g., specific process-to-process communications, specific data access patterns, unusual amounts of encryption/re-encryption activities) emerge, where the systems described herein may monitor for such patterns. Alternatively, ransomware attacks may involve behavior that deviates from normal behavior of a cloud deployment that is not experiencing a ransomware attack, such that the mere presence of unusual activity may trigger the systems described herein to generate alerts or take some other action, even without explicit knowledge that the unusual activity is associated with a ransomware attack.

[00650] In some embodiments, the systems described herein may be configured to enforce such policies as part of an effort to thwart ransomware attacks. For example, particular network sharing protocols (e.g., Common Internet File System ('CIFS'), Network File System ('NFS')) may be avoided when implementing storage for backup data, policies that protect backup systems may be implemented and enforced to ensure that usable backups are always available, multifactor authentication for particular accounts may be utilized and accounts may be configured with the

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00631

minimum privilege required to function, isolated recovery environments may be created and isolation may be monitored and enforced to ensure the integrity of the recovery environment, and so on. As described in the present disclosure, the systems described herein may be configured to explicitly enforce such policies or may be configured to detect unusual activity that represents a violation of such policies, such that the mere presence of unusual activity may trigger the systems described herein to generate alerts or take some other action, even without explicit knowledge that the unusual activity is associated with a violation of a particular policy.

[00651] Readers will appreciate that ransomware attacks are often deployed as part of a larger attack that may involve, for example:

[00652] Penetration of the network through means such as, for example, stolen credentials and remote access malware.

[00653] Stealing of credentials for critical system accounts, including subverting critical administrative accounts that control systems such as backup, Active Directory ('AD'), DNS, storage admin consoles, and/or other key systems.

[00654] Attacks on a backup administration console to turn off or modify backup jobs, change retention policies, or even provide a roadmap to where sensitive application data is stored.

[00655] Data theft attacks.

[00656] As a result of the many aspects that are part of a ransomware attack, embodiments of the present disclosure may be configured as follows:

[00657] The systems may include one or more components that detect malicious activity based on the behavior of a process.

[00658] The systems may include one or more components that store indicator of compromise ('IOC') or indicator of attack ('IOA') data for retrospective analysis.

[00659] The systems may include one or more components that detect and block fileless malware attacks.

[00660] The systems may include one or more components that remove malware automatically when detected.

[00661] The systems may include a cloud-based, SaaS-style, multitenant infrastructure.

[00662] The systems may include one or more components that identify changes made by malware and provide the recommended remediation steps or a rollback capability.

[00663] The systems may include one or more components that detect various application vulnerabilities and memory exploit techniques.

[00664] The systems may include one or more components that continue to collect suspicious event data even when a managed endpoint is outside of an organization's network.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00632

[00665] The systems may include one or more components that perform static, on-demand malware detection scans of folders, drives, devices, or other entities.

[00666] The systems may include data loss prevention (DLP) functionality.

[00667] In some embodiments, the systems described herein may manage, analyze, or otherwise observe deployments that include deception technologies. Deception technologies allow for the use of decoys that may be generated based on scans of true network areas and data. Such decoys may be deployed as mock networks running on the same infrastructure as the real networks, but when an intruder attempts to enter the real network, they are directed to the false network and security is immediately notified. Such technologies may be useful for detecting and stopping various types of cyber threats such as, for example, Advanced Persistent Threats ('APTs'), malware, ransomware, credential dumping, lateral movement and malicious insiders. To continue to outsmart increasingly sophisticated attackers, these solutions may continuously deploy, support, refresh and respond to deception alerts.

[00668] In some embodiments, the systems described herein may manage, analyze, or otherwise observe deployments that include various authentication technologies, such as multi-factor authentication and role-based authentication. In fact, the authentication technologies may be included in the set of resources that are managed, analyzed, or otherwise observed as interactions with the authentication technologies may be monitored. Likewise, log files or other information retained by the authentication technologies may be gathered by one or more agents and used as input to the systems described herein.

[00669] In some embodiments, the systems described herein may be leveraged for the specific use case of detecting supply chain attacks. More specifically, the systems described herein may be used to monitor a deployment that includes software components, virtualized hardware components, and other components of an organization's supply chain such that interactions with an outside partner or provider with access to an organization's systems and data can be monitored. In such embodiments, supply chain attacks may be carried out in a manner such that patterns (e.g., specific interactions between internal and external systems) emerge, where the systems described herein may monitor for such patterns. Alternatively, supply chain attacks may involve behavior that deviates from normal behavior of a cloud deployment that is not experiencing a supply chain attack, such that the mere presence of unusual activity may trigger the systems described herein to generate alerts or take some other action, even without explicit knowledge that the unusual activity is associated with a supply chain attack.

[00670] In some embodiments, the systems described herein may be leveraged for other specific use cases such as, for example, detecting the presence of (or preventing infiltration from) cryptocurrency miners (e.g., bitcoin miners), token miners, hashing activity, non-fungible token

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00633

activity, other viruses, other malware, and so on. As described in the present disclosure, the systems described herein may monitor for such threats using known patterns or by detecting unusual activity, such that the mere presence of unusual activity may trigger the systems described herein to generate alerts or take some other action, even without explicit knowledge that the unusual activity is associated with a particular type of threat, intrusion, vulnerability, and so on.

[00671] The systems described herein may also be leveraged for endpoint protection, such the systems described herein form all of or part of an endpoint protection platform. In such an embodiment, agents, sensors, or similar mechanisms may be deployed on or near managed endpoints such as computers, servers, virtualized hardware, internet of things ('IotT') devices, mobile devices, phones, tablets, watches, other personal digital devices, storage devices, thumb drives, secure data storage cards, or some other entity. In such an example, the endpoint protection platform may provide functionality such as:

[00672] Prevention and protection against security threats including malware that uses file-based and fileless exploits.

[00673] The ability to apply control (allow/block) to access of software, scripts, processes, microservices, and so on.

[00674] The ability to detect and prevent threats using behavioral analysis of device activity, application activity, user activity, and/or other data.

[00675] The ability for facilities to investigate incidents further and/or obtain guidance for remediation when exploits evade protection controls.

[00676] The ability to collect and report on inventory, configuration and policy management of the endpoints.

[00677] The ability to manage and report on operating system security control status for the monitored endpoints.

[00678] The ability to scan systems for vulnerabilities and report/manage the installation of security patches.

[00679] The ability to report on internet, network and/or application activity to derive additional indications of potentially malicious activity.

[00680] Example embodiments are described in which policy enforcement, threat detection, or some other function is carried out by the systems described herein by detecting unusual activity, such that the mere presence of unusual activity may trigger the systems described herein to generate alerts or take some other action, even without explicit knowledge that the unusual activity is associated with a particular type of threat, intrusion, vulnerability, and so on. Although these examples are largely described in terms of identifying unusual activity, in these examples

the systems described herein may be configured to learn what constitutes 'normal activity' – where 'normal activity' is activity observed, modeled, or otherwise identified in the absence of a particular type of threat, intrusion, vulnerability, and so on. As such, detecting 'unusual activity' may alternatively be viewed as detecting a deviation from 'normal activity' such that 'unusual activity' does not need to be identified and sought out. Instead, deviations from 'normal activity' may be assumed to be 'unusual activity'.

[00681] Readers will appreciate that while specific examples of the functionality that the systems described herein can provide are included in the present disclosure, such examples are not to be interpreted as limitations as to the functionality that the systems described herein can provide. Other functionality may be provided by the systems described herein, all of which are within the scope of the present disclosure. For the purposes of illustration and not as a limitation, additional examples can include governance, risk, and compliance ('GRC'), threat detection and incident response, identity and access management, network and infrastructure security, data protection and privacy, identity and access management ('IAM'), and many others.

[00682] In order to provide the functionality described above, the systems described herein or the deployments that are monitored by such systems may implement a variety of techniques. For example, the systems described herein or the deployments that are monitored by such systems may tag data and logs to provide meaning or context, persistent monitoring techniques may be used to monitor a deployment at all times and in real time, custom alerts may be generated based on rules, tags, and/or known baselines from one or more polygraphs, and so on.

[00683] Although examples are described above where data may be collected from one or more agents, in some embodiments other methods and mechanisms for obtaining data may be utilized. For example, some embodiments may utilize agentless deployments where no agent (or similar mechanism) is deployed on one or more customer devices, deployed within a customer's cloud deployment, or deployed at another location that is external to the data platform. In such embodiments, the data platform may acquire data through one or more APIs such as the APIs that are available through various cloud services. For example, one or more APIs that enable a user to access data captured by Amazon CloudTrail may be utilized by the data platform to obtain data from a customer's cloud deployment without the use of an agent that is deployed on the customer's resources. In some embodiments, agents may be deployed as part of a data acquisition service or tool that does not utilize a customer's resources or environment. In some embodiments, agents (deployed on a customer's resources or elsewhere) and mechanisms in the data platform that can be used to obtain data from through one or more APIs such as the APIs that are available through various cloud services may be utilized. In some embodiments, one or more cloud services themselves may be configured to push data to some entity (deployed

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00635

anywhere), which may or may not be an agent. In some embodiments, other data acquisition techniques may be utilized, including combinations and variations of the techniques described above, each of which is within the scope of the present disclosure.

[00684] Readers will appreciate that while specific examples of the cloud deployments that may be monitored, analyzed, or otherwise observed by the systems described herein have been provided, such examples are not to be interpreted as limitations as to the types of deployments that may be monitored, analyzed, or otherwise observed by the systems described herein. Other deployments may be monitored, analyzed, or otherwise observed by the systems described herein, all of which are within the scope of the present disclosure. For the purposes of illustration and not as a limitation, additional examples can include multi-cloud deployments, on-premises environments, hybrid cloud environments, sovereign cloud environments, heterogeneous environments, DevOps environments, DevSecOps environments, GitOps environments, quantum computing environments, data fabrics, composable applications, composable networks, decentralized applications, and many others.

[00685] Readers will appreciate that while specific examples of the types of data that may be collected, transformed, stored, and/or analyzed by the systems described herein have been provided, such examples are not to be interpreted as limitations as to the types of data that may be collected, transformed, stored, and/or analyzed by the systems described herein. Other types of data can include, for example, data collected from different tools (e.g., DevOps tools, DevSecOps, GitOps tools), different forms of network data (e.g., routing data, network translation data, message payload data, Wi-Fi data, Bluetooth data, personal area networking data, payment device data, near field communication data, metadata describing interactions carried out over a network, and many others), data describing processes executing in a container, lambda, EC2 instance, virtual machine, or other execution environment), information describing the execution environment itself, and many other types of data.

[00686] In some embodiments, one or more of the components described above may be deployed using a secure access service edge ('SASE') model or similar model. In a SASE model, the services, functionality, or components described above may be deployed at edge devices (or relatively close to such edge device) such as a user's laptop, tablet, smartphone, or other device. In such a way, network security controls may be delivered on such edge devices. SASE capabilities may be delivered as a service based upon the identity of the entity, real-time context, enterprise security/compliance policies and continuous assessment of risk/trust throughout the sessions, where the identity of entities can be associated with people, groups of people, devices, applications, services, IoT systems or edge computing locations, and so on. In these embodiments, one or more of the components described above may be deployed at or near the

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00636

edge devices, and the edge devices may even include local applications that are configured to utilize one or more of the components described above where the components are not deployed on the edge devices themselves.

[00687] For further explanation, Fig. 5 sets forth a flowchart illustrating an example method of configuring cloud deployments based on learnings obtained by monitoring other cloud deployments in accordance with some embodiments of the present disclosure. The cloud deployments 508, 514 may be similar to the cloud deployments described above, where a particular cloud deployment can include a variety of components 510, 512 such as one or more applications, one or more data sources, networking resources, processing resources, and other resources. Such components 510, 512 may, in some embodiments, be deployed in the cloud deployments 508, 514 using one or more as-a-service models where software, infrastructure, platforms, databases, and other components as delivered as services. Configuring cloud deployments 508, 514 based on learnings obtained by monitoring other cloud deployments may be carried out using the systems described above. As such, one or more of the steps depicted in Fig. 5 may be performed by the systems described above.

[00688] The example method depicted in Figure 5 includes determining 502 normal behavior for one or more components 510 in a first cloud deployment 508. Determining 502 normal behavior for one or more components 510 in a first cloud deployment 508 may be carried out, for example, as described in greater detail above (at times described as identifying 'normal activity') by the systems described above (also referred to herein as a 'data platform').

[00689] The example method depicted in Figure 5 also includes determining 504 normal behavior for one or more components 512 in one or more other cloud deployments 514. Determining 504 normal behavior for one or more components 512 in one or more other cloud deployments 514 may also be carried out, for example, as described in greater detail above (at times described as identifying 'normal activity') by the systems described above.

[00690] In some embodiments, a customer-specific data platform may be used to analyze, monitor, or otherwise observe a particular customer's cloud deployment (or some other deployment). Within such a cloud deployment, various clusters may exist. For example, a collection of microservices may form a cluster by virtue of those microservices communicating only (or mostly) with each other. Likewise, one or more cloud computing instances (e.g., one or more EC2 instances) and a database may form a cluster by virtue of the EC2 instances accessing the database as the only source of data utilized by the EC2 instances. Using the techniques and mechanisms described above, such clusters may be identified. Although clusters may be identified and characteristics associated with the cluster may be learned, limited insights may be gained if only a particular customer's cloud deployment is analyzed, monitored, or otherwise

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00637

observed. In accordance with embodiments of the present disclosure, cross-customer analysis may be leveraged to gain deeper insights than would be gained if only a single customer's cloud deployment is analyzed, monitored, or otherwise observed.

[00691] In some embodiments, cross-customer analysis may be carried out by gathering information related to cloud deployments (or some other deployments) for multiple customers and comparing such information. Using the example described above, information describing clusters identified in a first customer's cloud deployment may be compared to information describing clusters identified in a second customer's cloud deployment for the purposes of identifying similar or identical clusters in each customer's cloud deployment.

[00692] Consider an example in which each customer's deployment included a web server that was deployed in one or more EC2 instances. In such an example, a particular cluster that represents the web server may be identified in each customer's deployment. For example, a first cluster in the first customer's deployment may represent a first web server and a second cluster in the second customer's deployment may represent a second web server. Because the first cluster and the second cluster would have similar characteristics (e.g., each cluster receives data communications using HTTP or HTTPS or any other suitable communication protocol, each cluster communicates with a web browser, each cluster requires similar computing resources, and so on), the first cluster and the second cluster may be identified as being identical clusters by comparing the characteristics of each cluster that each cluster. This process may be repeated across the cloud deployments for many customers such that a collection of 'web server' clusters (in this example) may be identified.

[00693] Readers will appreciate that although the example described above relates to an embodiment where a collection of 'web server' clusters are identified in different customer's cloud deployments, identifying the nature or type (e.g., a web server) of the clusters is not required. In fact, by comparing the characteristics of different clusters to each other, similar or identical clusters may be identified even if the exact nature/type of those clusters is not known. For example, a comparison of the characteristics of multiple clusters may only reveal that the clusters are identical, even if such a comparison does not reveal that clusters are 'web server' clusters. Multiple clusters that have been identified as being identical (or sufficiently similar as measured by a threshold) will be referred to throughout the remainder of this document as a "cluster set," where the clusters that are members of the cluster set may be deployed across multiple customer's cloud deployments.

[00694] In some embodiments, information describing each member of the cluster set may be utilized to identify distributions across the cluster set. Distributions may be identified for traditional resource consumption metrics such as, for example, CPU usage, memory usage,

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00638

network bandwidth usage, and others. A distribution may reveal, for example, that all members of the cluster set utilize between 10-60 Mb/s of network bandwidth, with the vast majority of members of the cluster set utilize between 45-60 Mb/s of network bandwidth. Readers will appreciate that distributions may also be identified for other quantifiable characteristics of each cluster. Such quantifiable characteristics can include, for example, the failure rate of a cluster or particular components thereof, an identification of communication protocols used by a cluster or particular components thereof, an identification of the types of communications endpoints that a cluster or particular components thereof communicate with (e.g., endpoints that reside on the public internet v. endpoints that are in a private network), characteristics that can be classified by a binary value (e.g., does any component in the cluster perform privileged operations), information describing the various privileges that are given to a particular cluster, and many more.

[00695] In some embodiments, the distributions may be used to identify 'normal' behavior for a particular cluster. Consider an example in which the cluster set is identified, where each member of the cluster set represents a payroll system deployed in a particular customer's cloud deployment. In such an example, a distribution may be identified which indicates that all members of the cluster communicate with (and has privileged access to) the same set of cloud services, including: 1) a cloud database service (e.g., Amazon Aurora, Microsoft Azure SQL Database, Amazon Relational Database Service, Google Cloud SQL, Amazon DynamoDB), 2) a vendor provided SaaS offering that provides bill payment services, and 3) a vendor provided SaaS offering that provides accounting services. In such an example, by looking at each member of the cluster set and identifying that each member communicates with the same set of cloud services, a baseline may be established that identifies 'normal' behavior for each member of the cluster set, at least with respect to the specific characteristic (i.e., what cloud services are utilized by members) that the distribution is based on. As such, if monitoring a particular cluster revealed that some member of the cluster set accessed a source code repository cloud service (e.g., GitHub Enterprise on AWS), this sort of access would be outside of the typical distribution for this cluster set and could serve as the basis for raising an alert, denying access to the service, or initiating some other alerting/remediation workflow. Readers will appreciate that many distributions may be created for each cluster set, where each distribution is based on one or more characteristics of the members of the cluster set.

[00696] The example method depicted in Figure 5 also includes recommending 506, based on the normal behavior for one or more components 512 in one or more other cloud deployments 514, a change to the first cloud deployment 508. Recommending 506 a change to the first cloud deployment 508 may be carried out, for example, in response to determining that the normal

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00639

behavior in one or more other cloud deployments 514 differs from the normal behavior for one or more components 510 in a first cloud deployment 508. In such an example, changes to the first cloud deployment 508 may be recommended that (if implemented) would cause the first cloud deployment 508 to be more similar to the other cloud deployments 514. For example, if the normal behavior in one or more other cloud deployments 514 indicates that all computing resources (e.g., virtual machines, container, serverless computing resources) communicate with each other using a particular secure data communications protocol and the normal behavior for one or more components 510 in a first cloud deployment 508 is for computing resources to communicate using some other data communications protocol, a change may be recommended that involves reconfiguring the computing resources to communicate using the particular secure data communications protocol.

[00697] Readers will appreciate that in some embodiments the mere fact that normal behavior in a first cloud deployment 508 deviates from normal behavior in one or more other cloud deployments 514 may be sufficient rationale for recommending 506 a change to the first cloud deployment 508. That is, a departure from normality and standard practices alone may result in recommending 506 a change to the first cloud deployment 508. In other embodiments, recommending 506 a change to the first cloud deployment 508 may only occur where the normal behavior in one or more other cloud deployments 514 is determined to be superior to the normal behavior in the first cloud deployment 508. For example, recommending 506 a change to the first cloud deployment 508 may only be carried where the normal behavior in one or more other cloud deployments 514 is representative of a stronger security posture than the normal behavior in the first cloud deployment 508.

[00698] Consider an example in which a particular threat was detected (in part by detecting a deviation from normal behavior for one or more components 512) in a particular customer's cloud deployment 514, where the threat turned out to be a ransomware attack, which may in some embodiments include an encryption component and/or a data theft or leakage component. In such an example, if an identical (or sufficiently similar, following a general recognized pattern or 'fingerprint') threat is detected in the first customer's cloud deployment 508 (in part by detecting a similar deviation from deviation from normal behavior for one or more components 510), information describing the remedial actions (e.g., disabling encryption, increasing the frequency of backups, locking down a backup system, blocking transmission of data externally, etc.) that were taken by the particular customer 514 may even recommended 506 as changes to be made to the first cloud deployment 508. Furthermore, if many customers had experienced the same attack and the data platform could determine with sufficient certainty that the first cloud

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00640

deployment 508 was experiencing the same attack, workflows may be automatically initiated to carry out various remedial actions.

[00699] For further explanation, Fig. 6 sets forth a flowchart illustrating an additional example method of configuring cloud deployments based on learnings obtained by monitoring other cloud deployments in accordance with some embodiments of the present disclosure. The example depicted in Fig. 6 is similar to the example depicted in Fig. 5, as the example depicted in Fig. 6 also includes determining 502 normal behavior for one or more components 510 in a first cloud deployment 508, determining 504 normal behavior for one or more components 512 in one or more other cloud deployments 514, and recommending 506 a change to the first cloud deployment 508 based on the normal behavior for one or more components 512 in one or more other cloud deployments 514.

[00700] In some embodiments, customers (and their corresponding deployments) may be modeled into logical groups such that cross customer learning could be carried out only across customers in the same logical group, or other customers in the same logical group may be given a greater weighting for the purposes of cross customer learning. For example, a logical group may be tied to a customer's business function (e.g., the customer is a financial company, the customer is a health care company, the customer is a services company, the customer has inventory to manage, the customer sells to retail customers, and so on). Likewise, a logical group may be tied to a customer's cloud deployment (e.g., the deployment uses a particular combination of resources, the deployment uses a particular set of cloud-services, the deployment utilizes availability zones and regions in a particular way, and so on). In such an example, a particular customer may be associated with multiple logical groups and cross customer learning for the particular customer may only involve other customers that are in the same (or sufficiently similar) logical groups. As such, the particular customer's resources (e.g., people, cloud deployment) may only be included in cluster sets with resources associated with other customers that are in the same (or sufficiently similar) logical groups.

[00701] To that end, the example method depicted in Fig. 6 also includes identifying 604, from the other cloud deployments, cloud deployments that are similar to the first cloud deployment 508. Identifying 604 cloud deployments that are similar to the first cloud deployment 508 may be carried out, for example, by taking an inventory of the various components in each cloud deployment 508, 514 and identifying cloud deployments that have similar components, portions of the cloud deployment that have similar deployments, and so on. Alternatively, identifying 604 cloud deployments that are similar to the first cloud deployment 508 may be carried out, for example, by identifying cloud deployments that are associated with customers in the same industry as the customer associated with the first cloud deployment 508, by identifying cloud

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00641

deployments that are associated with a similar intended functionality as the first cloud deployment 508 (e.g., both cloud deployment are intended to provide an online store for an online retailer), and so on. In the examples in the preceding sentence, it may be assumed that two cloud deployments should be relatively similar even without inspecting the cloud deployments themselves. In such examples, similarity may be judged based on the application of rules, policies, heuristics, or similar mechanism. Alternatively, similarity may be detected via machine learning techniques as where information describing the activity of various components in many cloud deployments are fed as input to one or more machine learning models which subsequently identifies clusters across various cloud deployments that are similar.

[00702] In the example depicted in Fig. 6, recommending 506 the change to the first cloud deployment 508 may be based on the normal behavior for the cloud deployments that are similar to the first cloud deployment. Recommending 606 the change to the first cloud deployment 508 based on the normal behavior for the cloud deployments that are similar to the first cloud deployment 508 may be carried out, for example, by ignoring normal behavior for dissimilar cloud deployments and only taking into consideration those cloud deployments that have been identified 604 as being sufficiently similar to the first cloud deployment 508.

[00703] The example method depicted in Fig. 6 also includes identifying 602, from the other cloud deployments, one or more highly rated cloud deployments. A cloud deployment may be identified 602 as being 'highly rated' in the sense that fewer than a threshold number of vulnerabilities have been detected in the cloud deployment over some period of time, fewer than a threshold number of outages (or less than a threshold amount of downtime) has been detected in the cloud deployment over some period of time, fewer than a threshold number of regulatory violations (or attempted violations) have been detected in the cloud deployment over some period of time, or identified 602 based on some other standard. In fact, comparisons may be relative (rather than comparing some quantifiable aspect of the other deployments operation) such that, for example, the 15% of cloud deployments with the fewest detected vulnerabilities over some period of time as identified 602 as being 'highly rated'. In other embodiments, identifying 602 one or more highly rated cloud deployments may be carried out through the use of machine learning techniques where information describing the activity of various components in many cloud deployments are fed as input to one or more machine learning models which subsequently identifies deployments that have the best performance against a combination of one or more metrics (e.g., vulnerabilities, availability, cost). In such a way, the best-of-breed cloud deployments may be identified 602.

[00704] In the example depicted in Fig. 6, recommending 506 the change to the first cloud deployment 508 may be based on the normal behavior for the highly rated cloud deployments.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00642

Recommending 608 the change to the first cloud deployment 508 based on the normal behavior for the highly rated cloud deployments may be carried out, for example, by ignoring normal behavior for cloud deployments that are not highly rated and only taking into consideration those cloud deployments are highly rated.

[00705] Readers will appreciate that although the example in Fig. 6 is depicted where identifying 604 cloud deployments that are similar to the first cloud deployment 508 and identifying 602 one or more highly rated cloud deployments are alternatives to each other, in other embodiments both steps may be performed. In such embodiments, recommending 506 the change to the first cloud deployment 508 may be based on the normal behavior of other cloud deployments that are both highly rated and similar to the first cloud deployment 508.

[00706] For further explanation, Fig. 7 sets forth a flowchart illustrating an additional example method of configuring cloud deployments based on learnings obtained by monitoring other cloud deployments in accordance with some embodiments of the present disclosure. The example depicted in Fig. 7 is similar to the examples depicted in Fig. 5 and Fig. 6, as the example depicted in Fig. 7 also includes determining 502 normal behavior for one or more components 510 in a first cloud deployment 508, determining 504 normal behavior for one or more components 512 in one or more other cloud deployments 514, and recommending 506 a change to the first cloud deployment 508 based on the normal behavior for one or more components 512 in one or more other cloud deployments 514.

[00707] The example method depicted in Fig. 7 also includes ranking 702 the first cloud deployment 508 relative to the other cloud deployments 514. Ranking 702 the first cloud deployment 508 relative to the other cloud deployments 514 may be carried out, for example, by identifying how well the cloud deployment 508 compares to other cloud deployments 514 with respect to one or more metrics. For example, cloud deployments may be ranked based on a weighted combination of multiple metrics (e.g., reliability, cost, regulatory compliance) such that the best-of-breed deployments may be identified. In such an example, the ranking of the first cloud deployment 508 relative to the other cloud deployments 514 may be presented to an administrator or other user associated with the first cloud deployment 508 for analysis by the administrator or other user.

[00708] The example method depicted in Fig. 7 also includes comparing 704 the trajectory of the first cloud deployment 508 to the trajectory of the other cloud deployments 514. The trajectory of a particular cloud deployment 508, 514 may be determined, for example, by evaluating the particular cloud deployment's 508, 514 performance over time as measured by one or more metrics. For example, the performance of each cloud deployment may be periodically scored based on a weighted combination of multiple metrics (e.g., reliability, cost, regulatory

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00643

compliance). In such an example, the trajectory for a particular cloud deployment may be determined by determining the extent to which the score associated with a particular cloud deployment is changing over time. For example, if the first cloud deployment's 508 scoring is improving over time while the other cloud deployments' 514 scores are remaining the same over time, the trajectory of the first cloud deployment 508 may be determined to be better than the trajectory of the other cloud deployments 514 (in embodiments where a higher score is considered to be better).

[00709] Readers will appreciate that ranking 702 the first cloud deployment 508 relative to the other cloud deployments 514 and comparing 704 the trajectory of the first cloud deployment 508 to the trajectory of the other cloud deployments 514 are just two examples of the sort of analytics that can be performed by comparing the performance of multiple cloud deployments 508, 514. Readers will appreciate that other analytics may also be put in place due to the availability of information describing the performance of multiple cloud deployments 508, 514.

[00710] For further explanation, Fig. 8 sets forth a flowchart illustrating an additional example method of configuring cloud deployments based on learnings obtained by monitoring other cloud deployments in accordance with some embodiments of the present disclosure. The example depicted in Fig. 8 is similar to the examples depicted in Figs. 5-7, as the example depicted in Fig. 8 also includes determining 502 normal behavior for one or more components 510 in a first cloud deployment 508, determining 504 normal behavior for one or more components 512 in one or more other cloud deployments 514, and recommending 506 a change to the first cloud deployment 508 based on the normal behavior for one or more components 512 in one or more other cloud deployments 514.

[00711] The example method depicted in Fig. 8 also includes identifying 802 other cloud deployments 514 to exclude from consideration when recommending changes to the first cloud deployment 508. Readers will appreciate that other cloud deployments 514 may be excluded from consideration when recommending changes to the first cloud deployment 508 for a variety of reasons. For example, another cloud deployment 514 may be so dissimilar to the first cloud deployment 508 that there may be very little to learn that is relevant to the first cloud deployment 508, another cloud deployment 514 may be deficient for a variety of reasons such that there may be very little high quality takeaways from evaluating the other cloud deployment 514 that are relevant to the first cloud deployment 508, another cloud deployment 514 may be a relatively recent deployment such that any takeaways from evaluating the other cloud deployment 514 may not be reliable and proven over time, or for some other reason. In such an example, identifying 802 other cloud deployments 514 to exclude from consideration when recommending changes to the first cloud deployment 508 may be carried out by filtering the set of other cloud deployments

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00644

514 according to some criteria, or carried out in some other way. In the example depicted in Fig. 8, recommending 506 the change to the first cloud deployment 508 may therefore include recommending 806 changes based on the other cloud deployments 514 that are not excluded from consideration.

[00712] The example method depicted in Fig. 8 also includes identifying 804 a response to a recommended change in one or more other cloud deployments 514. Identifying 804 a response to a recommended change in one or more other cloud deployments 514 may be carried out, for example, by tracking the status of a recommended change that was recommended for another cloud deployment 514 to determine whether the recommended change was actually implemented. Consider an example in which a recommendation was made to have another cloud deployment 514 switch from using a first IaaS offering to a second IaaS offering in response to detecting some condition in the cloud deployment 514. In such an example, identifying 804 a response to a recommended change in one or more other cloud deployments 514 may be carried out by determining whether the recommended change was actually implemented and a switch was made to utilize the second IaaS offering as part of the cloud deployment 514. Readers will appreciate that by repeatedly identifying 804 responses to recommended changes in one or more other cloud deployments 514 can be used by the systems described above as an indication as to the systems described above are making useful recommendations. For example, if identifying 804 a response to a recommended change in one or more other cloud deployments 514 reveals that a very small percentage of administrators actually implement the recommended change, this may indicate that the recommend change is not particularly valuable and may be used as feedback in determining whether to make the recommended change if the condition that triggered the recommendation is encountered again. Alternatively, if identifying 804 a response to a recommended change in one or more other cloud deployments 514 reveals that a very large percentage of administrators actually implement the recommended change, this may indicate that the recommend change is valuable and may be used as feedback in determining whether to make the recommended change if the condition that triggered the recommendation is encountered again. In such a way, the response from other customers may be used to drive recommendations that are made regarding the first cloud deployment 508.

[00713] In the example depicted in Fig. 8, recommending 506 the change to the first cloud deployment 508 recommending 808 the change to the first cloud deployment 508 based on the response to the recommended change in one or more other cloud deployments 514. Recommending 808 the change to the first cloud deployment 508 based on the response to the recommended change in one or more other cloud deployments 514 may be carried out, for

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00645

example, only if a predetermined percentage of previous recipients of similar recommendations have actually implemented the recommended change, as described above.

[00714] Readers will appreciate that while the examples described in the preceding two paragraphs relate to an example in which the response to a recommended change in one or more other cloud deployments 514 is expressed in terms of whether the recommended change was or was not implemented, in other embodiments the response to a recommended change in one or more other cloud deployments 514 may be measured in other ways. For example, a response to a recommended change in one or more other cloud deployments 514 may represent whether the recommended change did or did not resolve the condition that caused the recommendation to be generated in the first place. In other embodiments, the response to a recommended change in one or more other cloud deployments 514 may be measured or determined using different criteria.

[00715] Although some of the figures described above depict only a single other cloud deployment 514, a single other cloud deployment 514 is included for ease of illustration but in no way represents a limitation of the embodiments described herein. In fact, most embodiments will include multiple other cloud deployments 514 that may be monitored and learned from.

[00716] Readers will appreciate that while many of the embodiments described above relate to embodiments where cross-customer learnings are used to generate recommendations for changes to the first cloud deployment 508, in other embodiments the cross-customer learning may be used to initiate, based on the normal behavior for the one or more other cloud deployments, a change to the first cloud deployment. Initiating such changes may be carried out, for example, by initiating one or more remediation workflows that implement the changes. As was the case with recommendations, initiating a change to the first cloud environment may be based on the normal behavior for similar cloud deployments, based on the normal behavior for the highly rated cloud deployments, based on the cloud deployments to exclude from consideration when recommending changes to the first cloud deployment, and so on.

[00717] For further explanation, Fig. 9 sets forth a flowchart illustrating an example method of learning from similar cloud deployments in accordance with some embodiments of the present disclosure. The example method depicted in Fig. 9 may be carried out by the systems described above (also referred to as a 'data platform' above). As such, the systems described above may include computer program instructions executing on computer hardware, virtualized hardware, or some other execution environment (e.g., one or more containers, one or more serverless compute instances), where the computer program instructions carry out the steps described in Fig. 9 when the computer program instructions are executed.

[00718] The example depicted in Fig. 9 includes a plurality of cloud deployments, including a first cloud deployment 910 and one or more additional cloud deployments 912, which in this

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00646

illustration includes three cloud deployments 914a, 914b, 914n, although more or fewer cloud deployments may be included in the set of additional cloud deployments 912 in other embodiments. Such cloud deployments may be embodied as described above and may include a variety of components such as, for example, software applications, storage resources, computing resources, networking resources, and other resources. In each cloud deployment, each of the resources may be delivered as services provided by a public cloud, private cloud, hybrid cloud, and so on.

[00719] The example method depicted in Fig. 9 includes identifying 902, for at least a portion of a first cloud deployment 910, one or more additional cloud deployments 912 to utilize for cross-customer learning. Cross-customer learning, as the phrase is used here, can generally be described as the process of learning about the cloud deployments of different customers, different organizations, or some other entity for the benefit of tailoring another entity's cloud deployment. For example, the cloud deployments of Customer A, Customer B, Customer C, Customer D, and Customer F may be evaluated and the information gathered about their deployments may be leveraged to help shape the cloud deployment of Customer F. In such an example, lessons learned by other customers may be used to help guide a particular customer's design, deployment, and management of their cloud deployments, which may be particularly useful for organizations that are pivoting to the cloud from on-premises based deployments.

[00720] Identifying 902 one or more additional cloud deployments 912 to utilize for cross-customer learning may be carried out, for example, by identifying cloud deployments for other customers that are in similar industries as the customer associated with the first cloud deployment 910, by identifying highly rated (as described above) cloud deployments, by identifying cloud deployments (or portions thereof) that are similar to the first cloud deployment 910 (or some portion thereof), or in some other way. In some embodiments, identifying 902 one or more additional cloud deployments 912 to utilize for cross-customer learning may be carried out using machine learning techniques as one or more machine learning models may be used to identify cloud deployments that are similar to the first cloud deployment 910, to identify best-of-breed cloud deployments, and so on. In such a way, identifying 902 one or more additional cloud deployments 912 to utilize for cross-customer learning may result in a subset of curated, relevant, and/or exemplary cloud deployments being utilized for cross-customer learning rather than using the entire set of available cloud deployments being utilized for cross-customer learning (although some embodiments could utilize all cloud deployments for cross-customer learning).

[00721] The example method depicted in Fig. 9 also includes receiving 904 information 916 describing one or more actions associated with the additional cloud deployments 912. The one or more actions associated with the additional cloud deployments 912 may be embodied as actions

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00647

taken by components within the additional cloud deployments 912. For example, a particular software service accessing a data store may be an example of an action that is associated with the additional cloud deployments 912, especially where the software service and the data store are components of a particular additional cloud deployment 914a. Likewise, a message, request, or other form of data communications that are exchanged between the additional cloud deployments 912 and actors that are external to the additional cloud deployments 912 may be an example of an action that is associated with the additional cloud deployments 912. For example, a server that is external to any of the additional cloud deployments 912 may send requests to access some software service within a particular additional cloud deployment 914a.

[00722] In other embodiments, the one or more actions associated with the additional cloud deployments 912 may include one or more user interactions with the additional cloud deployments 912. Such user interactions can include a description of which resources are accessed and/or utilized by particular users, particular business units (e.g., the finance department of a business, the engineering department of a business), particular personas (e.g., a system administrator, a software developer, a human resources manager), and so on. The one or more actions associated with the additional cloud deployments 912 may also include, for example, one or more interactions involving external applications, external computing devices, or similar external actor and the additional cloud deployments 912. Such user interactions can include, for example, a description of which resources within the additional cloud deployments 912 are accessed and/or utilized by particular external application, what IP address is associated with an external entity that is communicating with the additional cloud deployments 912, a description of the specific requests that an external actor is issuing to the resources within the additional cloud deployments 912, and so on.

[00723] In the example method depicted in Fig. 9, receiving 904 information 916 describing one or more actions associated with the additional cloud deployments 912 may be carried out by receiving (directly or indirectly) such information 916 from the additional cloud deployments 912 themselves. In fact, the additional cloud deployments 912 may be queried for such information. In other embodiments, the information 916 describing one or more actions associated with the additional cloud deployments 912 may be retained by the systems described above as part of monitoring the additional cloud deployments 912. In such an example, receiving 904 information 916 describing one or more actions associated with the additional cloud deployments 912 may be carried out by querying a data repository (e.g., a data warehouse) that contains such information that was gathered while monitoring the additional cloud deployments 912. Readers will appreciate that information 916 may be received 904 describing other types of actions associated with the additional cloud deployments 912.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00648

[00724] The example method depicted in Fig. 9 also includes receiving 906 information 918 describing configurations associated with the additional cloud deployments 912. The information 918 describing configurations associated with the additional cloud deployments 912 may be embodied, for example, as information describing how components within a cloud deployment are organized (including which other components they may communication with), information describing what permissions are granted to various users, information describing the manner in which internal (i.e., occurring entirely within the cloud deployment) data communications and/or external (i.e., occurring at least partially external to the cloud deployment) data communications are carried out, and so on. Such information 918 may be received 906 in a similar manner as described above with respect to step 904.

[00725] The example method depicted in Fig. 9 also includes identifying 908, based on the configurations and the one or more actions, one or more configurations to adopt for the first cloud deployment 910. Readers will appreciate that by identifying 908 one or more configurations to adopt for the first cloud deployment 910 in such a way, the configuration of the first cloud deployment 910 may be influenced by the monitoring of the additional cloud deployments 912. In such an example, once the configurations that the first cloud deployment 910 should adopt have been identified 908, the first cloud deployment 910 (or associated entities) may be reconfigured to implement such configurations.

[00726] Identifying 908 one or more configurations to adopt for the first cloud deployment 910 may be carried out, for example, by identifying configurations in the additional cloud deployments 912 that were effective in dealing with various threats, securing vulnerabilities, or otherwise contributed to a healthy cloud deployment. Some configurations associated with the additional cloud deployments 912 may have been put in place in response to some action. For example, a configuration to always backup data stored in a first storage service (e.g., AWS S3) to a second, distinct storage service (e.g., AWS Glacier) may have been put in place in response to some attack that was directed to a particular cloud deployment's 914a S3 buckets. In such an embodiment, if the first cloud deployment 910 also leverages S3 as its object store, it may be desirable for the first cloud deployment 910 to adopt a configuration setting that would result in its S3 buckets being backed up to Glacier so that the first cloud deployment 910 can be ready to survive a similar attack that was experienced by the particular cloud deployment 914a.

[00727] For further explanation, Fig. 10 sets forth a flowchart illustrating an example method of learning from similar cloud deployments in accordance with some embodiments of the present disclosure. The example method depicted in Fig. 10 is similar to the example depicted in Fig. 9, as the example depicted in Fig. 10 also includes identifying 902 one or more additional cloud deployments 912 to utilize for cross-customer learning, receiving 904 information 916 describing

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00649

one or more actions associated with the additional cloud deployments 912, receiving 906 information 918 describing configurations associated with the additional cloud deployments 912, and identifying 908 one or more configurations to adopt for the first cloud deployment 910.

[00728] In the example method depicted in Fig. 10, receiving 904 information 916 describing one or more actions associated with the additional cloud deployments 912 can include receiving 1002 information describing a security threat to one or more of the additional cloud deployments 912. The security threat may be embodied, for example, as a ransomware attack that was directed to one or more of the additional cloud deployments 912, as a denial of service attack that was directed to one or more of the additional cloud deployments 912, as an SQL injection attack that was directed to one or more of the additional cloud deployments 912, or as some other security threat. The information describing a security threat to one or more of the additional cloud deployments 912 can include, for example, information describing where an attack originated from, information describing the components within the cloud deployment that were targeted by an attack, information describing data access patterns that were associated with an attack, or some other information that would be useful in detecting subsequent security threats.

[00729] In the example method depicted in Fig. 10, receiving 906 information 918 describing configurations associated with the additional cloud deployments 912 can include receiving 1004 information describing configuration settings used to combat the security threat. The configuration settings used to combat the security threat may be embodied, for example, as configuration settings that caused the additional cloud deployments 912 to blacklist certain IP addresses or network domains, as configuration settings that caused the additional cloud deployments 912 to close vulnerabilities that allowed an attack to succeed, or some other configuration that would be useful in detecting/preventing/mitigating a security threat.

[00730] In the example method depicted in Fig. 10, receiving 904 information 916 describing one or more actions associated with the additional cloud deployments 912 can also include receiving 1006 information describing a detected vulnerability associated with one or more of the additional cloud deployments 912. The detected vulnerability may be embodied, for example, as a vulnerability to some known security threat, as a vulnerability to some data loss event, as a data breach vulnerability, or as some other vulnerability. The information describing a detected vulnerability of one or more of the additional cloud deployments 912 can include, for example, information describing vulnerable components, information describing data communications protocols, endpoints, or other data communications components that expose vulnerabilities, or some other information that would be useful in detecting a vulnerability.

[00731] In the example method depicted in Fig. 10, receiving 906 information 918 describing configurations associated with the additional cloud deployments 912 can also include receiving

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00650

1008 information describing configuration settings used to address the vulnerability. The configuration settings used to address the vulnerability may be embodied, for example, as configuration settings that caused the additional cloud deployments 912 to blacklist certain IP addresses or network domains, as configuration settings that caused certain components within the additional cloud deployments 912 to not connect to external data communications networks, as configuration settings that caused certain components to be accessible only by using enhanced authentication protocols, or as some other configuration that would be useful in detecting, preventing, or otherwise mitigating a vulnerability.

[00732] For further explanation, Fig. 11 sets forth a flowchart illustrating an example method of learning from similar cloud deployments in accordance with some embodiments of the present disclosure. The example method depicted in Fig. 11 is similar to the examples depicted in Fig. 9 and Fig. 10, as the example depicted in Fig. 11 also includes identifying 902 one or more additional cloud deployments 912 to utilize for cross-customer learning, receiving 906 information 918 describing configurations associated with the additional cloud deployments 912, and identifying 908 one or more configurations to adopt for the first cloud deployment 910.

[00733] In the example method depicted in Fig. 11, receiving 906 information 918 describing configurations associated with the additional cloud deployments 912 can include receiving 1102 information describing permissions for one or more users of the additional cloud deployments 912. The one or more users of the additional cloud deployments 912 may be embodied, for example, as individual users (e.g., Bob Smith), as a collection of users (e.g., Finance Group, Marketing Group), and so on. The one or more users of the additional cloud deployments 912 may also be embodied as different personas within an organization, where each persona is associated with a certain role. For example, there may be 'software developer' personas, 'database administrator' personas, 'customer support' personas, and many others. Receiving 1102 information describing permissions for one or more users of the additional cloud deployments 912 may be carried out, for example, by receiving (directly or indirectly) information from one or more of the additional cloud deployments 912 that described what resources a particular user/persona/group can access, what level of privileges they have with respect to a particular resource, and any other information describing the user/persona/group's privileges. In fact, such information may be retained in a data warehouse during monitoring of the additional cloud deployments 912 and received 1102 by querying such a data warehouse.

[00734] The example method depicted in Fig. 11 also includes determining 1104, based on the information describing permissions for one or more users of the additional cloud deployments, that one or more users of the first cloud deployment 910 are over-permissioned. A particular user may be over-permissioned in the sense that the user has privileges or permissions beyond those

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00651

that should be associated with the user. Consider the example of two distinct personas within an organization: 1) a software engineer, and 2) an accounts payable administrator. In such an example, the software engineer might have sufficient privileges to access a code repository, a dev/test environment, a code documentation tool, and so on. The accounts payable administrator, however, might have sufficient privileges to access bill paying software, a financial ledger, and so. The software developer having access to bill paying software or the accounts payable administrator having access to a code repository may be examples of the users being over-permissioned, as the user has access to resources that they should not be able to access. Such situations can create vulnerabilities as an over-permissioned user (or a malicious actor using the over-permissioned user's credentials) may intentionally or unintentionally perform some harmful act that they would not be capable of performing if they weren't over-permissioned.

[00735] Determining 1104 that one or more users of the first cloud deployment 910 are over-permissioned may be carried out, for example, by examining the information describing permissions for one or more users of the additional cloud deployments 912 to determine whether similar users in the additional cloud deployments 912 have different/fewer privileges. As such, a user in a first cloud deployment 910 may be determined to be over-permissioned if other cloud deployments 912 are giving similar users fewer permissions than such a user has in the first cloud deployment 910.

[00736] In the example method depicted in Fig. 11, identifying 908 one or more configurations to adopt for the first cloud deployment 910 can include identifying 1106 a reduced privilege level to give to the one or more users. Identifying 1106 a reduced privilege level to give to the one or more users may be carried out, for example, by giving an over-permissioned user of the first cloud deployment 910 privileges that are similar to those held by similar users in the additional cloud deployments 912.

[00737] For further explanation, Fig. 12 sets forth a flowchart illustrating an example method of learning from similar cloud deployments in accordance with some embodiments of the present disclosure. The example method depicted in Fig. 12 is similar to the examples depicted in Figs. 9-11, as the example depicted in Fig. 12 also includes identifying 902 one or more additional cloud deployments 912 to utilize for cross-customer learning, receiving 906 information 918 describing configurations associated with the additional cloud deployments 912, and identifying 908 one or more configurations to adopt for the first cloud deployment 910.

[00738] The example method depicted in Fig. 12 also includes receiving 1202 information 1204 describing one or more deployment processes associated with the additional cloud deployments 912. The information 1204 describing one or more deployment processes associated with the additional cloud deployments 912 can include, for example, information describing how a

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00652

particular component within an additional cloud deployment was created (e.g., who requested that the component be created, when was the request to create the component issued). In addition, in some embodiments such information 1204 can include information describing the software development processes that were used to develop software that will be deployed in a particular cloud deployment (e.g., was a code repository used, who has access to the repository, who committed the last change to some code before deployment). In such a way, the information 1204 describing one or more deployment processes associated with the additional cloud deployments 912 can describe the processes that are being implemented in other cloud deployments. Such information 1204 may be used, for example, to determine whether the development and deployment processes associated with the first cloud deployment 910 are abnormal, to use as the basis for making recommended changes to the development and deployment processes associated with the first cloud deployment 910, to initiate remediation workflows to back out changes to the first cloud deployment 910 that deviated from normal activity or violated some policy, and so on.

[00739] The example method depicted in Fig. 12 also includes identifying 1206 abnormally configured components in the first cloud deployment 910. Abnormally configured components in the first cloud deployment 910 may be embodied as components that are configured in a way that deviates from typical configurations observed by monitoring the additional cloud deployments 912. Monitoring the additional cloud deployments 912 may reveal, for example, that a connection to a server that is contained in another cloud deployment 914a should always go through an authentication server that is contained in another cloud deployment 914a. In such an example, if an examination of the first cloud deployment 910 reveals that an authentication server has been bypassed by a connection to a server, this may be an indication of a breach or misconfiguration regardless of customer's network topology. In such an example, the component (i.e., the server) may be identified 1206 as being abnormally configured based on its deviation from typical configurations observed in the additional cloud deployments 912.

[00740] Although the examples described above relate to embodiments where one or more configurations to adopt for the first cloud deployment 910 are identified 908 using the information described above, in other embodiments such information may be used for other purposes. For example, information gained by observing additional cloud deployments 912 may be leveraged to identify best-of-breed deployments, similar deployments, and so on.

[00741] In some embodiments, the distributions that identify 'normal' behavior for a particular cluster set may be used for a variety of purposes. For example, anomaly detection may be performed by identifying members of the cluster set that are operating outside of a particular typical distribution. Likewise, best practices may be identified using distributions and members of the cluster set that are not adhering to best practices may be identified if they are operating

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00653

outside of a particular typical distribution. Vulnerabilities may also be identified using distributions, for example, by identifying members of the cluster set that have over-privileged users or components that may be able access things that they should not be able to access. Readers will appreciate that that deviation from an established baseline of normal behavior, normal activity, normal configuration, or other form of normal operation may be indicative of many other things, all of which may be detected through the usage of the distributions described above paired with the monitoring of particular clusters.

[00742] In some embodiments, the distributions that identify 'normal' behavior for a particular cluster set may be used to not only detect threats, vulnerabilities, compromise, and things of that nature, but the distributions that identify 'normal' behavior for a particular cluster set may be used to optimize the operation or configuration of a particular cluster. For example, cloud deployments that utilize fewer resources may be examined and characteristics that are common across such the cloud deployments may be identified as being high efficiency characteristics. Likewise, cloud deployments that are the subject of fewer alerts may be examined and characteristics that are common across such the cloud deployments may be identified as being high efficiency characteristics.

[00743] In some embodiments, historical information may also be retained and utilized to show the trajectory of a particular one or more clusters. For example, historical information may be used to compare the current state of a particular cluster (as measured by one or more quantifiable characteristics associated with the cluster) with a previous state of the cluster such that trends and/or trajectories may be identified. Consider an example in which a particular characteristic associated with a cluster identifies how many users are accessing the cluster. Historical information associated with the cluster may be compared to current (or most recent) information associated with the cluster to determine, for example, that more or less users are accessing the cluster, that the number of users that are accessing the cluster is increasing or decreasing at a certain rate, and so on. In some situations, some changes may be acceptable (e.g., if the cluster represents an interface to an online store, and increase in the number of users accessing the online store may be perfectly acceptable given an expansion in the organization's customer base) whereas in other situations changes may be troubling (e.g., if the cluster represents a source code repository and more users are accessing the repository in spite of a contraction in the number of developers that are employed by an organization) and my require alerts, further investigation, or some other remediation workflow.

[00744] In some embodiments, historical information may also be retained and utilized to show the trajectory of a particular cluster relative to other members of a cluster set. For example, historical information may be used to compare the failure rate of particular cluster (as measured

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00654

by one or more quantifiable characteristics associated with the cluster) over time with the failure rate over time of other clusters in the cluster set. Such a comparison may reveal, for example, that a particular cluster was previously failing at a rate that was in line with the failure rate of other members of the cluster set, but that the particular cluster has more recently been failing more/less than other members of the cluster set. As such, through the use of such techniques a determination may be made as to whether a particular cluster is becoming more/less healthy than other members of the cluster set, more/less secure than other members of the cluster set, more/less efficient than other members of the cluster set, more/less reliable than other members of the cluster set, more/less compliant with relevant regulations than other members of the cluster set, slower/faster than other members of the cluster set, and so on. Such an analysis may be part of identifying best-of-breed deployments, best practices, providing remediation actions, providing recommendations, or utilized for a variety of other purposes.

[00745] Although the examples described above relate to embodiments where components within a cloud deployment are analyzed, monitored, or otherwise observed, in other embodiments the techniques described herein may be applied to other entities. For example, the techniques described above may be applied to analyze, monitor, or otherwise observe different personas with an organization, different users with an organization, different user groups with an organization, and so on. Using such techniques, 'normal' behaviors for a particular persona (e.g., a database administrator, a network administrator) can be identified, 'normal' behaviors for a particular user group (e.g., users that are part of an organization's finance department, users that are part of an organization's engineering department) can be identified, and so on.

[00746] In some embodiments, by identifying 'normal' behaviors (i.e., those behaviors that are consistent with standard distributions for particular characteristics associated with an entity) with different personas, different users, different user groups, or other entities, abnormal behavior may also be identified. Consider an example in which a group of users is identified as a cluster by virtue of those users accessing the same set of applications (e.g., all of the users access a set of applications that are finance-related applications). Further assume that similar clusters are identified for other customers, such that a cluster set may be formed. In such an example, a distribution may be identified for the set of applications that members of the cluster typically access. For example, each member of the cluster set may typically access an accounting application, a spreadsheet application, a payroll application, and so on. If one member of the cluster set consists of one or more users that also access an organization's source code repository, such behavior may be determined to be outside of the typical distribution for members of the cluster set. In response to making some determination, alerts may be generated, access to the

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00655

source code repository may be blocked for the users in the cluster, a remediation workflow may be initiated, or some other action may be taken.

[00747] In some embodiments, the techniques described above may be particularly useful for identifying over-privileged users, user groups, personas, or other entity. Identifying over-privileged users, user groups, personas may be carried out, at least in part, by identifying what set of privileges is 'normal' for a particular entity to have based on evaluating what privileges are given to similar or identical members of a cluster set. That is, an evaluation may be made as to what privileges are given to users, user groups, personas, or other entity by one or more other customers. If the set of privileges given to a particular customer's users, user groups, personas, or other entity are not consistent with (e.g., the set of privileges are much greater than) the privileges given to similar or identical users, user groups, personas, or other entity of another customer (i.e., the other members of the cluster set), a determination may be made that the particular customer's users, user groups, personas, or other entities are over-privileged. In some embodiments, an evaluation as to whether a user, user group, persona, or other entity is over-privileged may also include identifying privileges that the user has and comparing that with the privileges that the user actually utilizes. If some privileges are never used, this may be taken as an indication that the user is over-privileged.

[00748] In some embodiments, the cross customer techniques described above may be used to provide additional context to issues identified in a particular customer's cloud deployment, to provide recommendations to a particular customer, or even to drive remediation actions. Consider an example in which a particular threat was detected in a first customer's cloud deployment, where the threat turned out to be a ransomware attack, which may in some embodiments include an encryption component and/or a data theft or leakage component. In such an example, if an identical (or sufficiently similar, following a general recognized pattern or 'fingerprint') threat is detected in a second customer's cloud deployment, additional context may be provided by including information in an alert that is delivered to the second customer that indicates that the threat matches the profile of a ransomware attack that was detected in the first customer's cloud deployment. In fact, information describing the remedial actions (e.g., disabling encryption, increasing the frequency of backups, locking down a backup system, blocking transmission of data externally, etc.) that were taken by the first customer may even be included in the alert to the second customer or otherwise recommended to the second customer. Furthermore, if many customers had experienced the same attack and the data platform could determine with sufficient certainty that the second customer's cloud deployment was experiencing the same attack, workflows may be automatically initiated to carry out various remedial actions.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00656

[00749] In some embodiments, the way other customers investigated or responded to a particular alert may also be used when presenting alerts to a particular customer. Consider an example in which a particular threat was detected in ten different customer's cloud deployments. In such an example, assume that 9 of the 10 customers ignored the alert. In such an example, the conditions that are indicative of the particular threat are detected in a particular customer's cloud deployment, when raising the alert to the particular customer, information may be included in the alert indicating that most other customers ignored the alert. In such an embodiment, it is the behavior of users of the data platform – not components in a cloud deployment – that is being monitored and evaluated for the benefit of other customers. In other embodiments, information indicating that customers do or do not ignore a particular alert may be used when scoring or ranking the alert. For example, alerts that are ignored by most customers may be ranked as less critical than alerts that are acted upon by most customers. In addition, the particular security stance of a particular customer may be utilized when determining the extent to which their usage of the data platform should be utilized when guiding other customers. If a first customer has relatively poor security practices, for example, the first customer's usage of the data platform may be ignored (or given less weight) for the purposes of guiding other customers. If a second customer has relatively good security practices, however, the second customer's usage of the data platform may be taken into consideration (or given more weight) for the purposes of guiding other customers. Likewise, if users that ignored the alert experienced a security breach while users that did not ignore the alert did not experience a security breach, such an outcome could be taken into consideration when ranking the alert, determining what information to include in the alert, and so on.

[00750] In addition to using other customers interactions with the data platform to score, rank, suppress, or provide context for the alerts provided to other customers, the remediation actions taken by other customers may also be used for guiding a particular customer. Consider an example in which a particular threat was detected in ten different customer's cloud deployments. In such an example, assume that 9 of the 10 customers investigated the threat by accessing a particular customer support page. In this example, if the conditions that are indicative of the threat are detected in a particular customer's cloud deployment, information may be included in an alert indicating that most other customers that received the alert investigated the alert by accessing the particular customer support page. Likewise, if other customers successfully resolved the issue, information may be included in an alert indicating the solution that was implemented by other customers.

[00751] In some embodiments, the way customers investigated or responded to a particular alert may be used with other information to determine whether the customer's responses were actually

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00657

correct. Consider an example in which an alert is sent to 10 customers identifying a vulnerability that would allow crypto miners to use the customer's resources for solving complex computational problems for the purposes of acquiring cryptocurrency. In such an example, assume that 9 of 10 customers ignored the alert. Further assume that in this example, the 9 customers that ignored the alert subsequently had their cloud resources utilized by hackers for crypto mining, whereas the 1 customer that did not ignore the alert did not suffer such an attack. In such an example, the data platform described above should not cease issuing alerts when detecting this vulnerability by virtue of 9 of 10 customers ignoring the alert. Instead, by taking the ultimate outcome for each customer into consideration, rather than suppressing the alert, the data platforms should respond by taking actions that would make it more likely that customers would not ignore these alerts. For example, the severity level of the alert may be raised, a user of the data platform may be required to confirm receipt of the alert, contextual information could be included in the alert indicating that recipients that do not respond to the alert end up having their systems hijacked by crypto miners, or some other action may be taken.

[00752] In some embodiments, a customer's interactions may be analyzed to improve how alerts are delivered to a customer. For example, if an evaluation of customer interactions with the data platform indicates that most customer ignore alerts issued between 11:00 PM – 7:00 AM whereas most customers take action in response to alerts issued between 7:01 AM – 10:59 PM, then alerts that are issued between 11:00 PM – 7:00 AM may be reissued between 7:01 AM – 10:59 PM. Likewise, if a particular class of alerts (e.g., those related to vulnerability threats) are largely acted upon whereas another class of alerts (e.g., those related to a lack of compliance with regulatory requirements) are largely ignored, the manner in which alerts are generated may be altered. For example, alerts that are related to a lack of compliance with regulatory requirements may be issued to additional users, such as some user that is designated as having a compliance persona within a customer's organization. In other embodiments, other aspects of the customer's interactions with the data platform may be used to improve the manner in which the data platform interacts with customers (e.g., what type of devices received alerts, were alerts delivered in a primary or secondary window, do the parties that the alerts were sent to have other obligations at the time of alert as determined from an inspection of their calendar, and so on). While the example described above related to embodiments where the interactions of multiple customers with the data platform is analyzed, in other embodiments a single customer's interaction with the date platform may serve as the basis for altering the way that the data platform interacts with the customer.

[00753] In some embodiments, the same or additional cross customer learning techniques may be applied to earlier stages of a software development pipeline and even before an actual cloud

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00658

deployment is in place for a particular customer. Stated differently, the same or additional cross customer learning techniques may be applied to things other than a deployed system. For example, cross customer learning may be applied to development processes, testing processes, deployment processes, and so on.

[00754] Readers will appreciate that developing, testing, and deploying software in cloud environment comes with a few requirements that were not always present in software development. In particular, software is always expected to be running but the software is also expected to continue to be updated with fixes, new features, or other improvements. As such, it is not desirable to cease running a software application, install a new version, and begin running the new version. As a result of these changes to the software development paradigm, the software development processes, software testing and validation processes, and deployment processes tend to be fairly independent of each other. In some embodiments, each of these processes may be analyzed, monitored, or otherwise observed by the data platforms described herein. Because each of these processes are analyzed, monitored, or otherwise observed by the data platforms described herein, an opportunity exists to leverage cross customer learning to these processes.

[00755] In some embodiments, the development processes for a particular customer may be analyzed, monitored, or otherwise observed by the data platforms described herein. For example, interactions with a code repository may be monitored, permissions granted to each user of the code repository may be monitored, the number of people that are checking in and checking out code may be monitored, the extent to which code revisions are documented may be monitored, and so on. In such an example, the development processes for a particular customer may be learned and compared to normal behavior for other customers. Through such comparisons, inefficiencies may be identified, vulnerabilities may be identified, and other shortcomings may be identified. In response to the identification of inefficiencies, vulnerabilities, or other shortcoming, alerts may be issued, remediation workflows may be initiated, or some other action may be taken.

[00756] In some embodiments, the testing processes for a particular customer may be analyzed, monitored, or otherwise observed by the data platforms described herein. For example, the number of tests that are run may monitored, the type of tests that are run may be monitored, the number of people that are running tests and evaluating test results may be monitored, the processes through which the results of testing are communicated with developers may be monitored, and so on. In such an example, the testing processes for a particular customer may be learned and compared to normal behavior for other customers. Through such comparisons, inefficiencies may be identified, vulnerabilities may be identified, and other shortcomings may be identified. In response to the identification of inefficiencies, vulnerabilities, or other

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00659

shortcoming, alerts may be issued, remediation workflows may be initiated, or some other action may be taken.

[00757] In some embodiments, the results of testing may be carried forward and utilized when an application is deployed. Consider an example in which testing reveals that the code performs some action that appears to create a possible vulnerability, but further testing and validation reveals that a vulnerability is not created. When this piece of code is subsequently deployed, it presumably will perform the same action (i.e., the action that was flagged during testing) that appears to create a possible vulnerability. Rather than raising an alert, initiating some investigative action, initiating a remedial action, or responding in a similar way, by carrying forward the knowledge gained during testing (i.e., that a vulnerability was not, in fact, created) the possible vulnerability may be ignored based on the conclusions reached during testing.

[00758] In some embodiments, the deployment processes for a particular customer may be analyzed, monitored, or otherwise observed by the data platforms described herein. In such an example, the deployment processes for a particular customer may be learned and compared to normal behavior for other customers. Through such comparisons, inefficiencies may be identified, vulnerabilities may be identified, and other shortcomings may be identified. In response to the identification of inefficiencies, vulnerabilities, or other shortcoming, alerts may be issued, remediation workflows may be initiated, or some other action may be taken.

[00759] In some embodiments, some forms of static analysis may be used (in conjunction with other features of the data platform) to detect anomalies, vulnerabilities, threats, misconfigurations, violations of regulatory requirements, and many other things. Consider an example in which a cloud deployment is deployed using IaC. In such an example, one or more configuration files may be examined, and the state of the cloud deployment may be monitored to identify situations in which the state of the cloud deployment drifts from the configuration of the cloud deployment that was described in the configuration file. As such, the intended configuration of the cloud deployment (at least as expressed in one or more configuration files) may be used as a baseline to measure the current cloud deployment, such that alerts may be issued or other remediation workflows may be initiated when a customer's cloud deployment deviates from its codified state.

[00760] In some embodiments, other forms of code other than an IaC configuration may be examined to detect anomalies, vulnerabilities, threats, misconfigurations, violations of regulatory requirements, and many other things. For example, the source code that has been deployed in a customer's environment may be examined to determine all the things that the code could do. This information may be compared to a polygraph for the customer's cloud deployment, which identifies all things that a customer's cloud deployment does do, as learned by monitoring and

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00660

observing the customer's cloud deployment. Consider an example in which a polygraph for a customer's cloud deployment indicates that a first microservice in their cloud deployment only communicates with other internal microservices. In such an example, however, assume that the source code for the first microservice includes a messaging library that it uses to communicate with the other internal microservices. Further assume in this example, however, that examining the source code for the first microservice reveals that the messaging library also includes functions that enable a user of the library to send messages to recipients on an external network using standard internet protocols (e.g., TCP/IP, HTTPS, and so on). In such an example, although the polygraph for the customer's cloud deployment reveals that the first microservice only communicates with other internal microservices, the presence of functions that could be used for communications with external services, machines, and other entities may be undesirable. As such and in accordance with some embodiments of the present disclosure, the data platform may be configured to alert a customer or initiate some other workflow upon detecting that source code includes features that, if executed, would rise to the level of anomalous or otherwise unusual activity. For example, the data platform may prompt the customer to delete or disable the library functions described above that enable undesirable data communications.

[00761] In another example, assume that some source code has all the necessary capabilities (e.g., hashing functions, mathematical calculations, etc.) to mine cryptocurrency, as the mining process may only require performing standard computations. During a crypto miner attack, however, the source code may be subverted such that the code runs in a loop to perform the standard computations required for mining cryptocurrency. An evaluation as to what functions the source code can perform may therefore not reveal anything concerning but monitoring the actual operation of the source code may reveal that the source code is operating in an undesirable way. Likewise, static analysis may reveal things like a non-incrementing counter or other mechanism that would result in an infinite loop or similar operation. As such and in accordance with some embodiments of the present disclosure, the data platform may be configured to alert a customer or initiate some other workflow upon detecting that source code includes features that, if or when executed, rise to the level of anomalous or otherwise unusual activity.

[00762] In another example, assume that some source code has all the necessary capabilities to carry out the steps required for a ransomware attack, as the ransomware attack may only require performing standard operations like reading data, encrypting data, sending data, communicating externally, and so on. During a ransomware attack, however, the source code may be subverted such that the code does far more encryption than would be expected in a typical code module. An evaluation as to what functions the source code can perform may therefore not reveal anything concerning but monitoring the actual operation of the source code may reveal that the source

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00661

code is operating in an undesirable way. Likewise, static analysis may reveal that all paths through the source result in data being encrypted, or that all paths through the source code results in some atypical pattern (e.g., equal amounts of reading data, encrypting data, and writing data, or unusual external data flows), which may rise to the level of being unusual or concerning behavior. As such and in accordance with some embodiments of the present disclosure, the data platform may be configured to alert a customer or initiate some other workflow upon detecting that source code includes features that, if or when executed, rise to the level of anomalous or otherwise unusual activity.

[00763] In some embodiments, the data platforms described above may be used to identify discriminates between two entities that may otherwise appear to be similar or identical. In the examples described herein, 'discriminates' may be embodied as characteristics of entities that, when not similar or identical, prevent the entities from being similar or identical. For example, many customers may have many Java processes. If the data platform were to identify the set of things that each Java process does for each customer and identify that set of things as the 'normal' or acceptable set of things that any Java process was allowed to do, this set would be far too large. As such, the data platform may be configured to look at things like command line arguments and know that one or more Java processes with one set of jar files and command line arguments is actually a separate program from one or more Java processes with another set of jar files and command line arguments. In other words, the data platform may identify discriminates (in the example, a first discriminate being distinct command line arguments and a second discriminate may be that the jar files for each process are distinct) between two sets of Java processes to determine that the Java processes are not actually similar or identical entities. As such, any attempt to engage in cross customer learning based on a first set of Java processes in a first customer's environment and a second set of Java processes in a second customer's environment may result in undesirable outcomes. Through the use of discriminates, however, a decision can be reached that these two sets of Java processes are not related and attempts to learn through an examination of these distinct entities would be undesirable.

[00764] In some embodiments, the usage of discriminates described above may be extended to other entities. For example, if a first user in a first customer's environment is a database administrator and a second user in a second customer's environment is also a database administrator, these users may initially be determined to be similar enough such that cross customer learning can take place. In such an example, however, if an examination of their activities, privileges, or something else reveals that they are not actually occupying the same roles, cross customer learning with respect to these two users may be disabled. In such embodiments, the data platform described above, and models leveraged by such a data platform

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00662

may be used to identify discriminates that may be used to decouple multiple users, applications, microservices, devices, or other entities that would otherwise be candidates for cross customer learning.

[00765] In some embodiments, the data platforms may be configured to analyze, monitor, or otherwise observe environments other than cloud deployments. In fact, the data platforms described here could apply the principles and techniques described herein to any environment such as, for example, an on-premises environment, a hybrid cloud environment, or some special purpose environment. As one example of a special purpose environment, consider an example in which the data platforms described herein are used to analyze, monitor, or otherwise observe a container orchestration environment such as a Kubernetes cluster (which may be deployed on-premises, in a public cloud, or in some other way). In such an example, the data platform may be configured to ingest Kubernetes audit logs via one or more agents or in some other way. Through the ingestion and subsequent analysis of such audit logs, the data platform may model normal behaviors of a Kubernetes cluster, normal behavior of a cluster administrator, and so on. As described above, any deviations from such normal behaviors may result in an alert being generated or some other remediation workflow being initiated. For example, if the ingestion and subsequent analysis of audit logs revealed that workloads are deployed and deleted according to some pattern, a customer deploying or deleting a workload in a manner that is inconsistent with the identified pattern may result in an alert being generated or some other remediation workflow being initiated. In fact, by evaluating audit logs from multiple customer's Kubernetes clusters, cross customer learning can be carried out to help define normal behavior for a Kubernetes cluster, a Kubernetes administrator, or some other entity associated with a Kubernetes cluster. For example, evaluating audit logs from the Kubernetes deployment of multiple customers may reveal that one entity (presumed to be a Kubernetes administrator, or related group of such administrators) is generally responsible for creating and deleting nodes from the cluster whereas another entity (perhaps a developer) is responsible for deploying new versions of the code that is executing in a container that is supported by the cluster. In such an example, if a single entity (or related group of entities) is observed creating nodes and modifying the code that is executing on a node by deploying a new container, an alert may be generated or some other remediation workflow may be initiated as a consequence of observing this atypical pattern.

[00766] One or more embodiments may be described herein with the aid of method steps illustrating the performance of specified functions and relationships thereof. The boundaries and sequence of these functional building blocks and method steps have been arbitrarily defined herein for convenience of description. Alternate boundaries and sequences can be defined so long as the specified functions and relationships are appropriately performed. Any such alternate

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00663

boundaries or sequences are thus within the scope and spirit of the claims. Further, the boundaries of these functional building blocks have been arbitrarily defined for convenience of description. Alternate boundaries could be defined as long as the certain significant functions are appropriately performed. Similarly, flow diagram blocks may also have been arbitrarily defined herein to illustrate certain significant functionality.

[00767] To the extent used, the flow diagram block boundaries and sequence could have been defined otherwise and still perform the certain significant functionality. Such alternate definitions of both functional building blocks and flow diagram blocks and sequences are thus within the scope and spirit of the claims. One of average skill in the art will also recognize that the functional building blocks, and other illustrative blocks, modules and components herein, can be implemented as illustrated or by discrete components, application specific integrated circuits, processors executing appropriate software and the like or any combination thereof.

[00768] While particular combinations of various functions and features of the one or more embodiments are expressly described herein, other combinations of these features and functions are likewise possible. The present disclosure is not limited by the particular examples disclosed herein and expressly incorporates these other combinations.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00664

CLAIMS

What is claimed is:

1. A method of learning from other cloud deployments to combat security threats, the method comprising:

identifying, for at least a portion of a first cloud deployment, one or more additional cloud deployments to utilize for cross-customer learning;

receiving information describing a security threat to one or more of the additional cloud deployments;

receiving information describing configuration settings used to combat the security threat; and

identifying, based on the information describing configuration settings used to combat the security threat, one or more configurations to adopt for the first cloud deployment.

2. The method of claim 1, wherein the configuration settings comprise configuration settings that caused the one or more of the additional cloud deployments to blacklist one or more internet protocol (IP) addresses.

3. The method of claim 1, wherein the configuration settings comprise configuration settings that caused the one or more of the additional cloud deployments to blacklist one or more network domains.

4. The method of claim 1, wherein the configuration settings comprise configuration settings that caused the one or more of the additional cloud deployments to close a vulnerability that allowed an attack to succeed.

5. The method of claim 1 further comprising:

receiving information describing one or more actions associated with the additional cloud deployments; and

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00665

wherein identifying the one or more configurations to adopt for the first cloud deployment is further based on the one or more actions.

6. The method of claim 5 wherein:

receiving information describing one or more actions associated with the additional cloud deployments further comprises receiving information describing a detected vulnerability associated with one or more of the additional cloud deployments; and

receiving information describing configurations associated with the additional cloud deployments further comprises receiving information describing configuration settings used to address the vulnerability.

7. The method of claim 1 further comprising identifying abnormally configured components in the first cloud deployment.

8. The method of claim 1 further comprising receiving information describing one or more deployment processes associated with the additional cloud deployments.

9. A system for learning from other cloud deployments to combat security threats, the system comprising at least one processor and memory storing computer program instructions that, when executed, cause the system to carry out the steps of:

identifying, for at least a portion of a first cloud deployment, one or more additional cloud deployments to utilize for cross-customer learning;

receiving information describing a security threat to one or more of the additional cloud deployments;

receiving information describing configuration settings used to combat the security threat; and

identifying, based on the information describing configuration settings used to combat the security threat, one or more configurations to adopt for the first cloud deployment.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00666

10. The system of claim 9, wherein the configuration settings comprise configuration settings that caused the one or more of the additional cloud deployments to blacklist one or more internet protocol (IP) addresses.

11. The system of claim 9, wherein the configuration settings comprise configuration settings that caused the one or more of the additional cloud deployments to blacklist one or more network domains.

12. The system of claim 9, wherein the configuration settings comprise configuration settings that caused the one or more of the additional cloud deployments to close a vulnerability that allowed an attack to succeed.

13. The system of claim 9, wherein the steps further comprise:

receiving information describing one or more actions associated with the additional cloud deployments; and

wherein identifying the one or more configurations to adopt for the first cloud deployment is further based on the one or more actions.

14. The system of claim 13 wherein:

receiving information describing one or more actions associated with the additional cloud deployments further comprises receiving information describing a detected vulnerability associated with one or more of the additional cloud deployments; and

receiving information describing configurations associated with the additional cloud deployments further comprises receiving information describing configuration settings used to address the vulnerability.

15. The system of claim 9 wherein the steps further comprise identifying abnormally configured components in the first cloud deployment.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00667

16. The system of claim 9 wherein the steps further comprise receiving information describing one or more deployment processes associated with the additional cloud deployments.

17. A computer program product for learning from other cloud deployments to combat security threats, the computer program product disposed on a non-transitory computer readable medium, the computer program product including computer program instructions that, when executed, carry out the steps of:

identifying, for at least a portion of a first cloud deployment, one or more additional cloud deployments to utilize for cross-customer learning;

receiving information describing a security threat to one or more of the additional cloud deployments;

receiving information describing configuration settings used to combat the security threat; and

identifying, based on the information describing configuration settings used to combat the security threat, one or more configurations to adopt for the first cloud deployment.

18. The computer program product of claim 17, wherein the configuration settings comprise configuration settings that caused the one or more of the additional cloud deployments to blacklist one or more internet protocol (IP) addresses.

19. The computer program product of claim 17, wherein the configuration settings comprise configuration settings that caused the one or more of the additional cloud deployments to blacklist one or more network domains.

20. The computer program product of claim 17, wherein the configuration settings comprise configuration settings that caused the one or more of the additional cloud deployments to close a vulnerability that allowed an attack to succeed.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00668

ABSTRACT

Learning from other cloud deployments to combat security threats, including: identifying, for at least a portion of a first cloud deployment, one or more additional cloud deployments to utilize for cross-customer learning; receiving information describing a security threat to one or more of the additional cloud deployments; receiving information describing configuration settings used to combat the security threat; and identifying, based on the information describing configuration settings used to combat the security threat, one or more configurations to adopt for the first cloud deployment.

Netskope Ex. 1002
Netskope v. Fortinet IPR2026-00515
Page 00669

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/361,748	**07/28/2023 08:00:34 PM ET**	**L0041B1CIP2C1**

Title of Invention

Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4323	FILED BY	Ashley Jenkins
PATENT CENTER #	62527520	FILING DATE	-
CUSTOMER #	182115	FIRST NAMED INVENTOR	ÚLFAR ERLINGSSON
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Jason Fletcher

Documents

TOTAL DOCUMENTS: 5

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
2023-07-28_L0041B1CIP2C1_ADS.pdf	9	Application Data Sheet	2225 KB
2023-07-28_L0041B1CIP2C1_POA.pdf	3	Power of Attorney	298 KB
2023-07-28_L0041B1CIP2C1_FiledContinuationApplication-APP.TEXT.docx	0	Application body structured text document	151 KB
2023-07-28_L0041B1CIP2C1_Continu	49	Drawings-only black and white line drawings	2049 KB

ationDrawings.pdf			
2023-07-28_L0041B1CIP2C1_Declaration.pdf	2	Oath or Declaration filed	113 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
2023-07-28_L0041B1CIP2C1_ADS.pdf	3A0C22FA5AA3387266E1DA310D203374A458AD16F7810FBE0AF1FF25AB557969E63EB1D52C3D9260265F0DEC2CA3F21C0CBAD995E3C7E8B0175DED899FB04055
2023-07-28_L0041B1CIP2C1_POA.pdf	532DFDF89DC097E84B7659A3F7371538C659667DFC59402CC1EF7C1B994C93CB673B4BE8DC6B7A45B4145D9F5720700214CF124B9F0FDCE818FD5910AA890368
2023-07-28_L0041B1CIP2C1_FiledContinuationApplication-APP.TEXT.docx	C48FDCA6318A91879F1B03FB3440DD6DDFFF50DEFA3AF2BE439E3C5433E6E6FECA033170E511D0189BD386E6F743AA44109E2D146D23A6FFACE8A45D7422A43C
2023-07-28_L0041B1CIP2C1_ContinuationDrawings.pdf	EE48D95D15A8584C8BFFCF50F6A1C177180215AEB9556914D525B6110A77DD6F8E5B5A0AA9327FD005051CB5080783C78E521A5CA7C267CAB16A5BB93514F25B
2023-07-28_L0041B1CIP2C1_Declaration.pdf	B770A8A3DA8E33FB1102425E65B005FBD363A3DA7F53A07B5582CA7CC3B53986734D30A8DCEE9856C77016E4718777636627F61593FC01F5D984FE52CD26D5BC

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/361,748	**07/28/2023 08:00:34 PM ET**	**L0041B1CIP2C1**

Title of Invention

Enhancing Security Of A Cloud Deployment Based On Learnings From Other Cloud Deployments

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4323	FILED BY	Ashley Jenkins
PATENT CENTER #	62527520	AUTHORIZED BY	Jason Fletcher
CUSTOMER #	182115	FILING DATE	-
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	ÚLFAR ERLINGSSON

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1003	**E20237RK01259379**	**Ashley Jenkins**

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
1111	UTILITY PATENT APPL. SEARCH FEE	700.00	1	700.00
1011	BASIC FILING FEE - UTILITY (PAPER FILING ALSO REQUIRES NON-ELECTRONIC FILING FEE UNDER 1.16(T))	320.00	1	320.00
1311	PATENT APPL. EXAMINATION FEE	800.00	1	800.00
1081	UTILITY APPL. SIZE FEE >THAN 100 PAGES (FEE X PAGES >=101 IN 50 PAGE INCREMENTS)	420.00	1	420.00
			TOTAL	**$2,240.00**

AMOUNT:

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.