

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

---

**BEFORE THE PATENT TRIAL AND APPEAL BOARD**

---

NETSKOPE, INC.,

Petitioner,

v.

FORTINET, INC.,

Patent Owner.

---

PTAB Case No. IPR2026-00474

U.S. Patent No. 11,449,623

---

**PETITION FOR *INTER PARTES* REVIEW  
OF U.S. PATENT NO. 11,449,623**

## TABLE OF CONTENTS

|                                                           |   |
|-----------------------------------------------------------|---|
| EXHIBIT LIST .....                                        | v |
| I. INTRODUCTION .....                                     | 1 |
| II. MANDATORY NOTICES .....                               | 1 |
| A. Real party in interest.....                            | 1 |
| B. Related matters .....                                  | 1 |
| C. Counsel and service information.....                   | 1 |
| D. Fees.....                                              | 2 |
| III. IPR REQUIREMENTS .....                               | 2 |
| A. Standing.....                                          | 2 |
| B. Challenged claims and relief requested.....            | 2 |
| 1. Prior Art .....                                        | 3 |
| 2. Grounds for challenge and challenged claims .....      | 3 |
| IV. NO DISCRETIONARY DENIAL FACTORS ARE PRESENT.....      | 4 |
| V. TECHNOLOGY DESCRIPTION.....                            | 4 |
| A. '623 Patent Overview .....                             | 4 |
| 1. Prosecution history.....                               | 5 |
| B. Technology Landscape as of the '623 Priority Date..... | 6 |
| 1. Cryptographic Background.....                          | 6 |
| 2. Cryptographic Controls for File Access .....           | 7 |
| 3. Risk-Based Scoring Systems .....                       | 8 |

|       |                                                                                                   |    |
|-------|---------------------------------------------------------------------------------------------------|----|
| VI.   | LEVEL OF ORDINARY SKILL .....                                                                     | 9  |
| VII.  | CLAIM CONSTRUCTION .....                                                                          | 9  |
| VIII. | SPECIFIC GROUNDS.....                                                                             | 9  |
| A.    | Ground 1: Combining Cheng and Bleckmann Renders Claims<br>1-15 Obvious.....                       | 9  |
| 1.    | Cheng .....                                                                                       | 9  |
| 2.    | Bleckmann .....                                                                                   | 11 |
| 3.    | Motivations to Combine .....                                                                      | 12 |
| 4.    | Claim 1 .....                                                                                     | 16 |
| 5.    | Claim 2 .....                                                                                     | 34 |
| 6.    | Claim 3 .....                                                                                     | 35 |
| 7.    | Claim 4.....                                                                                      | 36 |
| 8.    | Claim 5 .....                                                                                     | 37 |
| 9.    | Claim 6.....                                                                                      | 39 |
| 10.   | Claim 7 .....                                                                                     | 40 |
| 11.   | Claim 8.....                                                                                      | 42 |
| 12.   | Claims 9-15 .....                                                                                 | 42 |
| B.    | Ground 2: Combining Cheng and Bleckmann with Kirti<br>Renders Claims 2, 4, and 10-13 Obvious..... | 45 |
| 1.    | Kirti .....                                                                                       | 45 |
| 2.    | Motivation to Combine .....                                                                       | 45 |
| 3.    | Claim 2.....                                                                                      | 48 |
| 4.    | Claim 4.....                                                                                      | 48 |

|     |                                                                                                      |    |
|-----|------------------------------------------------------------------------------------------------------|----|
| 5.  | Claims 10-13 .....                                                                                   | 49 |
| C.  | Ground 3: Combining Cheng and Bleckmann with Van Dijk<br>Renders Claims 3, 9-13, and 15 Obvious..... | 49 |
| 1.  | Van Dijk.....                                                                                        | 49 |
| 2.  | Motivation to Combine .....                                                                          | 50 |
| 3.  | Claim 3 .....                                                                                        | 52 |
| 4.  | Claims 9-13, 15 .....                                                                                | 52 |
| D.  | Ground 4: Combining Ford and Van Dijk Renders Claims 1-15<br>Obvious. ....                           | 53 |
| 1.  | Ford .....                                                                                           | 53 |
| 2.  | Motivation to Combine .....                                                                          | 54 |
| 3.  | Claim 1 .....                                                                                        | 55 |
| 4.  | Claim 2 .....                                                                                        | 65 |
| 5.  | Claim 3 .....                                                                                        | 66 |
| 6.  | Claim 4 .....                                                                                        | 70 |
| 7.  | Claim 5 .....                                                                                        | 70 |
| 8.  | Claim 6 .....                                                                                        | 71 |
| 9.  | Claim 7 .....                                                                                        | 71 |
| 10. | Claim 8 .....                                                                                        | 72 |
| 11. | Claims 9-15 .....                                                                                    | 73 |
| E.  | Ground 5: Combining Ford and Van Dijk with Kirti Renders<br>Claims 2, 10-13 Obvious.....             | 74 |
| 1.  | Motivation to Combine .....                                                                          | 74 |

|     |                                                                                                   |    |
|-----|---------------------------------------------------------------------------------------------------|----|
| 2.  | Claims 2, 10-13 .....                                                                             | 76 |
| F.  | Ground 6: Combining Ford and Van Dijk with Bleckmann<br>Renders Claims 1-15 Obvious.....          | 76 |
| 1.  | Motivation to Combine .....                                                                       | 76 |
| 2.  | Claim 1 .....                                                                                     | 78 |
| G.  | Ground 7: Combining Ford, Van Dijk, Bleckmann, and Kirti<br>Renders Claims 2, 10-13 Obvious ..... | 78 |
| IX. | CONCLUSION.....                                                                                   | 78 |

## **EXHIBIT LIST**

| <b>Exhibit No.</b> | <b>Description</b>                                                                                                                                                                                                                                                                                                               |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1001               | U.S. Patent No. 11,449,623                                                                                                                                                                                                                                                                                                       |
| 1002               | Prosecution History of U.S. Patent No. 11,449,623 (the “’623 Prosecution History”)                                                                                                                                                                                                                                               |
| 1003               | Declaration of Dr. Paul Martin                                                                                                                                                                                                                                                                                                   |
| 1004               | Reserved                                                                                                                                                                                                                                                                                                                         |
| 1005               | U.S. Patent Application Publication 2013/0232543 A1 (“Cheng”)                                                                                                                                                                                                                                                                    |
| 1006               | U.S. Patent Application Publication 2009/0144813 A1 (“Bleckmann”)                                                                                                                                                                                                                                                                |
| 1007               | U.S. Patent 8,978,159 (“Van Dijk”)                                                                                                                                                                                                                                                                                               |
| 1008               | U.S. Patent 10,063,654 (“Kirti”)                                                                                                                                                                                                                                                                                                 |
| 1009               | International Patent Application 2015/164521 A1 (“Ford”)                                                                                                                                                                                                                                                                         |
| 1010               | US Pat. Pub. No. 2019/0319945 (“Levy”)                                                                                                                                                                                                                                                                                           |
| 1011               | US Pat. Pub. No. 2004/0221172 (“Stamos”)                                                                                                                                                                                                                                                                                         |
| 1012               | Reserved                                                                                                                                                                                                                                                                                                                         |
| 1013               | Archived capture of webpage from Cisco.com titled ‘What Is Encryption?’ (Internet Archive Wayback Machine: <a href="https://www.cisco.com/site/us/en/learn/topics/security/what-is-encryption.html">https://www.cisco.com/site/us/en/learn/topics/security/what-is-encryption.html</a> ), captured Sep 14, 2026                  |
| 1014               | Archived capture of webpage from Okta.com titled ‘RSA Encryption: Definition, Architecture, Benefits & Use’ (Internet Archive Wayback Machine: <a href="https://www.okta.com/identity-101/rsa-encryption/">https://www.okta.com/identity-101/rsa-encryption/</a> ), captured Sep 14, 2026                                        |
| 1015               | Archived capture of webpage from csrc.nist.gov titled ‘Policy Based Access Control (PBAC)’ (Internet Archive Wayback Machine: <a href="https://csrc.nist.gov/glossary/term/policy_based_access_control">https://csrc.nist.gov/glossary/term/policy_based_access_control</a> ), captured Sep 14, 2026                             |
| 1016               | Archived capture of webpage from csrc.nist.gov titled ‘Risk Adaptive (Adaptable) Access Control’ (Internet Archive Wayback Machine: <a href="https://csrc.nist.gov/glossary/term/risk_adaptive_adaptable_access_control">https://csrc.nist.gov/glossary/term/risk_adaptive_adaptable_access_control</a> ), captured Sep 14, 2026 |
| 1017               | Archived capture of webpage from Microsoft.com titled ‘Risk-                                                                                                                                                                                                                                                                     |

| Exhibit No. | Description                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | based access policies’ (Internet Archive Wayback Machine: <a href="https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-policies">https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-policies</a> ), captured Sep 14, 2026                                                                                                               |
| 1018        | Archived capture of webpage from csrc.nist.gov titled ‘A Survey Of Access Control Modules’ (Internet Archive Wayback Machine: <a href="https://csrc.nist.gov/csrc/media/events/privilege-management-workshop/documents/pvm-model-survey-aug26-2009.pdf">https://csrc.nist.gov/csrc/media/events/privilege-management-workshop/documents/pvm-model-survey-aug26-2009.pdf</a> ), captured Sep 14, 2026 |
| 1019        | Archived capture of webpage from ibm.com titled ‘What is machine learning?’ (Internet Archive Wayback Machine: <a href="https://www.ibm.com/think/topics/machine-learning">https://www.ibm.com/think/topics/machine-learning</a> ), captured Sep 14, 2026                                                                                                                                            |

## **I. INTRODUCTION**

United States Patent No. 11,449,623 (“the ’623 patent”) is directed to a fundamental, decades-old computing concept: controlling access to a file. The ’623 patent purports to improve on that well-known concept by evaluating a user’s historical behavior before granting or denying access. But even that idea was well-known long before the March 2019 priority date. For example, Cheng (published in 2013) and Ford (in 2015) already disclosed the concept of controlling file access based on user behavior. Because the ’623 patent’s alleged invention was well-known before its priority date, Petitioner respectfully requests cancellation of its claims 1-15 under 35 U.S.C. § 103.

## **II. MANDATORY NOTICES**

### **A. Real party in interest**

Netskope, Inc. is the sole real party-in-interest.

### **B. Related matters**

Patentee originally asserted the ’623 against Petitioner in the United States District Court for the Northern District of California, Case No. 4-25-cv-02360-HSG. That claim has now been severed into Case No. 4:26-cv-08886-HSG.

### **C. Counsel and service information**

Lead Counsel: Thomas N. Millikan (Reg. No. 72,316).

Back-up counsel: Joseph P. Reid (Reg. No. 72,317), Nicholas G. Lipperd (Reg. No. 83,084), and Andrew Klein (*pro hac vice* forthcoming).

These attorneys can be reached by mail at Sheppard, Mullin, Richter & Hampton LLP, 12275 El Camino Real, Suite 100, San Diego, California, 92130, by phone at (858) 720-8900, and by fax at (858) 509-3691.

Petitioner consents to electronic service. All services and communications to the attorneys listed above may be sent to:

**LegalTm-NetskopeFortinetII-IPRs@sheppard.com.**

A Power of Attorney for Petitioner is being filed concurrently.

**D. Fees**

Petitioner paid the required fees. The Office is authorized to charge any fee deficiency, or credit overpayment, to Deposit Account No. 50-4561.

**III. IPR REQUIREMENTS**

**A. Standing**

Petitioner certifies the '623 patent is available for inter partes review ("IPR"), and Petitioner is not barred or estopped from challenging the claims on the grounds herein.

**B. Challenged claims and relief requested**

Petitioner respectfully requests cancellation of the challenged claims under §103.

## 1. Prior Art

Petitioner relies on the references listed in the Table of Exhibits, including:

- U.S. Patent Application Publication 2013/0232543 A1 (“Cheng”)
- International Patent Application 2015/164521 A1 (“Ford”)
- U.S. Patent 8,978,159 (“Van Dijk”)
- U.S. Patent 10,063,654 (“Kirti”)
- U.S. Patent Application Publication 2009/0144813 A1 (“Bleckmann”)

Petitioner also relies on the declaration of Dr. Paul Martin, the Chief Scientist at Harbor Experts and a part-time lecturer in the Department of Computer Science at Johns Hopkins University (“Martin Decl.”). Ex-1003.

## 2. Grounds for challenge and challenged claims

Petitioner requests *inter partes* review and cancelation of the challenged claims on the following grounds:

| Ground | Basis | Reference(s)                   | Challenged Claims |
|--------|-------|--------------------------------|-------------------|
| 1      | §103  | Cheng and Bleckmann            | 1-15              |
| 2      | §103  | Cheng, Bleckmann, and Kirti    | 2, 4, 10-13       |
| 3      | §103  | Cheng, Bleckmann, and Van Dijk | 3, 9-13, 15       |
| 4      | §103  | Ford and Van Dijk              | 1-15              |
| 5      | §103  | Ford, Van Dijk, and Kirti      | 2, 10-13          |
| 6      | §103  | Ford, Van Dijk, and Bleckmann  | 1-15              |

|   |      |                                      |          |
|---|------|--------------------------------------|----------|
| 7 | §103 | Ford, Van Dijk, Bleckmann, and Kirti | 2, 10-13 |
|---|------|--------------------------------------|----------|

#### **IV. NO DISCRETIONARY DENIAL FACTORS ARE PRESENT**

Petitioner submits that *inter partes* review is warranted here because, in addition to the claimed invention being known before the '623 patent, there are no discretionary factors that weigh against review. For example:

- 1) None of the prior art discussed herein was before the Examiner during prosecution.
- 2) There are no settled expectations because the '623 patent issued four years ago.
- 3) No schedule is set, including no set trial date, in the parallel district court proceeding.
- 4) Petitioner has not taken inconsistent positions on claim construction—indeed, claim construction proceedings have not begun in the parallel district court proceeding.
- 5) Netskope is a U.S.-based cloud security company.

#### **V. TECHNOLOGY DESCRIPTION**

##### **A. '623 Patent Overview**

The '623 patent concerns “[s]ystems and methods for a machine-learning driven fine-grained file access control approach.” Ex-1001, 2:66-67.

The patent describes a network architecture that obtains and stores information regarding historical user behavior by observing file access requests. This architecture includes a management server, permission server, and analytics

server on an enterprise network. Files within the network are encrypted to prevent access without validation of a user's access rights. When a user requests access, the system determines a risk score based on a plurality of factors, including the user's behavioral information and data observed from the request. *Id.* at 14:14-62.

Based on the resulting risk score, access is permitted or denied by returning or withholding the decryption key. The patent discloses a three-tier, two-threshold access scheme: if the risk score is less than a first threshold, the permission server provides full access by returning the decryption key; if the risk score falls between the first and second thresholds, the permission server limits access by returning the decryption key with limitations, the only such disclosed being directing file access through a lower-risk channel (via VPN); and if the risk score exceeds the second threshold, the permission server withholds the decryption key to block access entirely. *Id.* at 6:16-24.

### **1. Prosecution history**

The '623 patent's application faced two Office Actions, wherein all pending claims were rejected as obvious under 35 U.S.C. § 103. Ex-1002 at 114. In each rejection, the examiner found that Levy (U.S. 2019/0319945) taught collecting historical user behavior across an enterprise network, receiving a file access request, and determining a risk score, while Stamos (U.S. 2004/0221172) supplied

the mechanism of returning or withholding a decryption key. *Id.* at 116-18; 170-176.

After the final rejection, the applicant further amended the application to add an “intermediate access” condition between the two previously-claimed threshold-based outcomes and the examiner allowed the claims. *Id.* at 215, 220.

## **B. Technology Landscape as of the '623 Priority Date**

### **1. Cryptographic Background**

Fundamental to modern information security, cryptography protects information from unauthorized access, disclosure, or alteration. It relies on encryption, which renders readable information unreadable using a “key,” and decryption, which reverses the process. A POSITA as of the March 2019 priority date would refer to readable information as “plaintext” and encrypted information as “ciphertext.” The “key” is the value that determines how a cryptographic algorithm transforms plaintext into ciphertext; the same or a related key is used to reverse that transformation during decryption.

Together, encryption, decryption, and key-generation algorithms comprise a cryptosystem, of which there are two types: symmetric and asymmetric. Symmetric (shared key) cryptosystems use the same key for encryption and decryption, requiring the key to be securely distributed and kept secret between the

parties. Public key (asymmetric) cryptosystems instead use a mathematically-linked key pair—a public key and a private key—such that data encrypted with the public key can only be decrypted with the corresponding private key, which its holder must keep secret. Ex-1003, ¶¶ 41-47.

## **2. Cryptographic Controls for File Access**

Many organizations use cryptographic file protection systems to distribute digital content while restricting its use to defined, sanctioned policies. Encryption alone cannot reliably enforce time-limited access: once a user receives a decryption key, that access may persist indefinitely absent additional controls. Achieving finite-duration access therefore typically requires policy-based mechanisms that revoke or restrict access after a defined cutoff, such as at the end of an employee's employment.<sup>1</sup> A POSITA as of the priority date would be familiar with Policy-Based Access Control (PBAC),<sup>2</sup> which governs access through predefined policies specifying conditions under which a user may access a resource (e.g., identity, role, or clearance), and which must be maintained as users and circumstances change—for example, revoking access when an employee departs.<sup>3</sup> Ex-1003, ¶¶ 48-51.

---

<sup>1</sup> Ex-1001, 1:46-58.

<sup>2</sup> Ex-1015.

<sup>3</sup> Ex-1001, 1:63-2:1.

### 3. Risk-Based Scoring Systems

A POSITA, as of March 2019, would be familiar with Risk-Based Access Control,<sup>4</sup> which evaluates access requests according to the level of risk associated with a user, resource, and access context, rather than relying solely on predefined permissions. User behavioral-based risk scoring systems evaluate access requests based on deviations from established patterns of user activity—such as file-access history, location, timing, network trust status, and peer-group behavior—rather than treating authorization as a static, role-based decision.<sup>5</sup> A risk score is assigned by comparing activity against this baseline, and predefined thresholds then determine whether to allow access.

Machine learning (ML) is a type of artificial intelligence that enables computers to identify patterns in training data and make inferences about new data<sup>6</sup> rather than following fixed instructions. ML systems can be trained on historical user behavior data—such as the factors discussed above—to model normal behavior, then analyze a new access request to generate a numerical score reflecting its deviation from that baseline. A low score reflects consistency with

---

<sup>4</sup> Ex-1017.

<sup>5</sup> Ex-1001, 6:7-16.

<sup>6</sup> Ex-1019.

historical behavior, while a high score—for example, an access request at 3:00 a.m. from outside the enterprise network—reflects a deviation warranting closer scrutiny. Ex-1003, ¶¶ 52-59.

## **VI. LEVEL OF ORDINARY SKILL**

A POSITA in March 2019 would have had a bachelor’s degree in computer science, computer engineering, or electrical engineering, or a related field, and/or at least two years of practical experience in analyzing or implementing network security, data access control, or key management. *Id.*, ¶ 34.

## **VII. CLAIM CONSTRUCTION**

The challenged claims should be construed “in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” 37 C.F.R. § 42.100(b); *see Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005). For this proceeding, Petitioner does not believe any construction is needed.

## **VIII. SPECIFIC GROUNDS**

### **A. Ground 1: Combining Cheng and Bleckmann Renders Claims 1-15 Obvious.**

#### **1. Cheng**

Cheng is directed to controlling access to data, more particularly to providing a server to control access to client data. Ex-1005, [0004].

Cheng discloses a data protection system that processes decryption key requests from mobile devices via policy decision to determine user eligibility to access an encrypted data item. The policy decision module determines eligibility based on an accumulated authentication score representing the level of confidence in the user that is compared to a minimum score required for access. The module's risk engine assesses likelihood that data may be misused based on the sensitivity score of the data item, access history, and deviation from access patterns. *Id.*, [0063], [0064], [0067].

Cheng discloses server-based data protection architecture where encrypted data items are stored on a server and transferred to a mobile device. Users initiate access by requesting a decryption key; the server evaluates the request against a confidence score derived from authentication history, access history, and current device context, then permits or denies access by returning or withholding the appropriate decryption key. *Id.*, [0062]-[0065], Fig. 6. If access is not initially permitted, reduced access to the file may be granted or the request may be denied outright. *Id.*, [0064]-[0068]. Cheng discloses multiple ways to reduce access, including creating multiple files with various redactions, released either with their own decryption key or a single decryption key, passwords, and invertible and non-invertible obfuscation techniques. *Id.*, [0044]-[0046].

Cheng additionally evaluates the likelihood of data leakage based on deviation from historical access, allowing graduated access where a decryption key corresponding to an appropriate level of redaction is released, and a continuous authentication mechanism where background-collected authentication information is used to update the accumulated authentication score. *Id.*, [0024], [0028], [0029], [0067], [0069], [0079]. Ex-1003, ¶¶ 66-70.

Though Cheng describes certain aspects of its invention as “preferred embodiments,” a POSITA would immediately recognize the disclosed elements together as obvious, regardless of the particular embodiments in which they are disclosed. *See* Ex-1005, [0097]; Ex-1003, ¶ 70. *See also General Electric Co. v. Raytheon Tech. Corp.*, 983 F.3d 1334, 1351–52 (Fed. Cir. 2020).

## **2. Bleckmann**

Bleckmann discloses a system for controlling access to network resources by generating a trust score for a requesting computer system and comparing that score against a policy to determine the appropriate level of access. Ex-1006, Abstract. The system discloses an integrity validator (140) between an external network (110) and an internal network (135) to validate computer systems outside the organization requesting access to internal resources. *Id.*, [0019]. The validator (220) compares signatures against a database of known-valid signatures and

returns an indication of trustworthiness. *Id.*, [0038]. The trust score generator (225) then produces a trust score-based signature validation. *Id.*, [0039].

Bleckmann's policy (230) may include two threshold scores governing three access outcomes: if the trust score is at least as high as the first threshold score (235), full access is granted; if the trust score is below the second threshold (240), access is denied; and if the trust score is between the two threshold scores, partial access is granted. *Id.*, [0043]. Bleckmann's integrity validator operates regardless of how the resource is sent or requested: whether it is encrypted or unencrypted and whether the request arrives over a standard or VPN-secured channel. The policy describes different access rules for different resources, and where the integrity validator serves multiple organizations, it can store and enforce separate policies for each. Bleckmann discloses two-threshold, three-tier access framework, trusted versus untrusted network architecture, and scored, policy-driven access determination. Ex-1003, ¶¶ 71-74.

### **3. Motivations to Combine**

A POSITA would have been motivated to combine Cheng and Bleckmann with a reasonable expectation of success.

Cheng and Bleckmann are analogous art because both generally relate to resource access mechanisms based on a confidence or trust score. Both are directed

to server-based systems that compute a score reflecting a requester's trustworthiness or risk, and that score is compared against one or more thresholds to determine the degree of access a requester is permitted to protected resources. *See, e.g.*, Ex-1001, 1:11-26, 1:30-2:45, 7:55-8:25, Figs. 3A-3B. Both Cheng and Bleckmann teach systems that compute a score reflecting the trustworthiness or eligibility of a requester and use that score to gate access to protected data or network resources. *See, e.g.*, Ex-1005, [0028], [0079], [0089], [0095]; Ex-1006, [0039], [0043], Figs. 2, 8.

Both Cheng and Bleckmann seek to solve the same problem, namely, the need for dynamic, score-driven access control to protected resources that provides finer-grained access decisions than rigid, binary approaches. Both consider the risk of the user accessing a file and how the file is transferred to the user. *See, e.g.*, Ex-1005, [0006]-[0008], [0024], [0027]; Ex-1006, [0003]-[0007], [0032], [0039]-[0044].

A POSITA would have been motivated to apply Bleckmann's multi-threshold access control framework to Cheng's score-based data protection system to provide tiered, granular access to protected data based on a computed score rather than a binary grant-or-deny decision. Users present varying degrees of risk depending on context and authentication history, and a system capable of granting

limited access in intermediate-risk scenarios provides both greater security and greater usability than one forced to make an all-or-nothing determination.

Cheng acknowledges this tension, explaining the tradeoff between security and usability and the limitations of existing approaches that “do not sufficiently address both security and usability of a mobile device.” Ex-1005, [0007]. Bleckmann addresses this by disclosing two threshold scores, allowing full, partial, or no access. Ex-1006, [0043].

Cheng’s policy decision module 222, as modified with Bleckmann’s two-threshold framework, would compare the user’s accumulated authentication score to a first threshold score and a second threshold score, returning a decryption key for full access when the score exceeds the first threshold, returning a decryption key and providing limited access, including access only by VPN, when the score falls between the two thresholds, and withholding the decryption key when the score falls below the second threshold.

Moreover, a POSITA would have been motivated to incorporate Bleckmann’s multi-tiered threshold framework into Cheng’s data protection system because it enables context-sensitive access control to protected data items—a recognized design goal explicitly pursued by Cheng.

When file access is enabled from outside an enterprise network, there is a threat of unauthorized access. This includes Man-In-The-Middle (MITM) attacks where bad actors operate proxies between the service provider and network, intercepting connections to capture login credentials and view sensitive files being transmitted. A POSITA armed with this knowledge would be motivated to prevent MITM attacks and would understand providing access within certain restrictions, including using a VPN, would increase file transfer protection where there is increased security concern, including when the user resides outside the enterprise network.

Granting limited access when a risk score is intermediate, rather than a binary grant/deny, better serves users in moderate-risk contexts and increases file protection. Where releasing a decryption key provides file access, a POSITA would have been motivated to add intermediate restrictions. Cheng contemplates this outcome through redaction-based systems, sending “only one decryption key that only allows access to a version that is appropriate for the current device context (e.g., only allowing access to a highly redacted version of the data item in a device context that is considered insecure like an airport).” Ex-1005, [0029].

A POSITA implementing this graduated-access concept in Cheng would have looked to Bleckmann for a concrete mechanism for restricting access short of

full denial, including the VPN-gated restricted-access option Bleckmann discloses for computer systems that are not directly connected to the internal network.

Because Cheng teaches a policy decision module that compares an accumulated authentication score to a minimum score to determine whether to release a decryption key (*Id.*, [0028], [0079], [0089], [0095]), implementing Bleckmann's two-threshold framework in Cheng's data protection system would have been a straightforward modification.

Similar to Cheng, Bleckmann teaches applying the two explicit threshold scores to produce three distinct tiers of resource access: full access, partial access, and denial. Ex-1006, [0043]. A POSITA would have understood that Cheng's policy decision module could be implemented with two threshold scores consistent with Bleckmann's threshold score 235 and threshold score 240. Thus, a POSITA would have found it straightforward and advantageous to apply Bleckmann's two-threshold access control to Cheng's data protection system, and would have known such a combination, yielding the "first threshold" and "second threshold" limitations of the '623 patent claims, would provide the expected functionality. Ex-1003, ¶¶ 75-90.

#### **4. Claim 1**

**1[a]: "A method comprising: obtaining and storing,  
by one or more servers associated with an enterprise**

**network, information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users;”**

Cheng discloses or renders obvious a method (e.g., “methods for protecting sensitive data items”) comprising: obtaining and storing, by one or more servers associated with an enterprise network, information regarding historical user behavior of a plurality of users of the enterprise network (e.g., obtaining and storing, by “server 206,” including “data protection system 212,” “access history” information in “access history 312”) by observing file access requests initiated by the plurality of users (e.g., “request to access the protected data item”). Ex-1005, Abstract, [0006], [0010], [0052]-[0053], [0065].

Cheng discusses its invention in the context of enterprise networks, describing the shift from office-centric work to mobile models where enterprise data is accessed remotely. *Id.*, [0006].

Cheng discloses server-based protection before transferring the file where server 206 and data protection system 212 exercise control. *Id.*, [0037], [0053].

A POSITA would recognize or find it obvious that data protection system 212 can be a component of server 206: Cheng manipulates data on the server before transferring to the user. *See, e.g., id.*, [0025]. To the extent Cheng does not explicitly disclose data protection system 212 as a component of server 206, it

would have been obvious to a POSITA. Cheng modifies data transferred from server 206 according to data protection system 212: “functions and components of the data protection system 212 may be integrated into one or more systems.” *Id.*, [0052], [0053]. Cheng further states “The present principles provide **server-based** protection **before** the transfer of a data item from a server to a mobile device.” *Id.*, [0037] (emphasis added). A POSITA would recognize data protection system 212 would reside on server 206. Ex-1003, ¶¶ 91-94.

Cheng’s method includes obtaining and storing user “access history” by such employees in “**access history 312**” and “**authentication and context history 314**.” Ex-1005, Fig. 3, [0006], [0009]-[0011], [0053], [0065]-[0068].

Cheng suggests or renders obvious one or more servers are associated with an enterprise network. *Id.*, [0024]. Cheng describes its disclosures in the context of remote access to enterprise systems, including the use of VPNs. *See id.*, [0006]. Cheng does not limit server 206 to any particular architecture, and provides examples of servers typically associated with enterprise networks. *See id.*, [0049]. It would have been obvious to a POSITA that Cheng’s server system was associated with an enterprise network.

Cheng’s data protection system maintains two data stores regarding user activity: **access history store 312**, which determines which encrypted data items

were previously accessed and authentication and context history store 314, which determines the most recent device context. *Id.*, [0065].

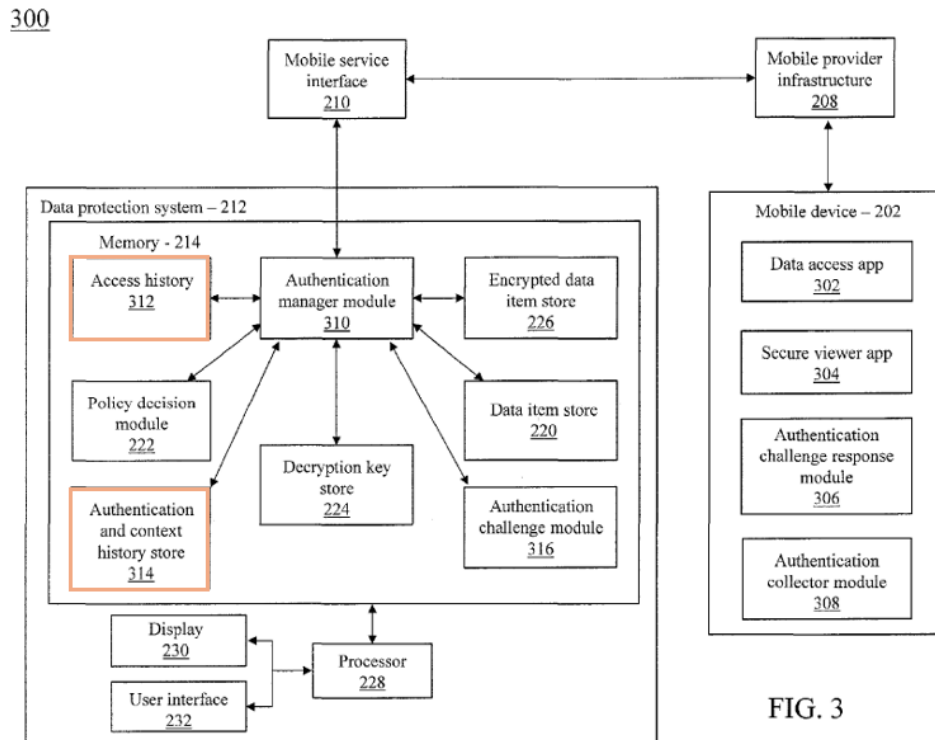


FIG. 3

*Id.*, Fig. 3 (orange outlining added).

Historical behavioral information is obtained and stored: “responsive to a request to access the protected data item.” *Id.*, [0010]-[0011]. The data protection system determines a confidence level based on the context of client devices, authentication history of devices, and access history of users. *Id.*

Confidence level is based on the historical data access to determine “if the data accessed or current context of the mobile device 202 is unusual.” *Id.*, [0065].

Authentication and context history store 314 captures behavioral history based on factors including the device's current location, the device's location history, and the history of device compromises, as well as user-specific factors including "the history of the user's access to data of known sensitivity" and "the aggregated sensitivity score of all data items accessed by the user." *Id.*, [0066].

Cheng discloses an access history 312 and authentication and context history 314 across the plurality of users, describing "an increasingly mobile model in which employees access enterprise data remotely through various channels from a wide range of devices," framing the invention as addressing data protection needs across an organization's workforce. *Id.*, [0006]. Nothing in Cheng's architecture is limited to a single user. *Id.*, [0049]-[0053]. Ex-1003, ¶¶ 95-101, 103, 106.

**1[b]: "receiving, by the one or more servers, a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network in encrypted form;"**

Cheng discloses or renders obvious receiving, by the one or more servers, a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network (e.g., a "request to access the protected data item") in encrypted form (e.g., "stored in the encrypted data item store 226"). Ex-1005, [0010]-[0011], [0059].

Cheng discloses server 206 initiates the file transfer in response to a device request. *Id.*, [0050]. The file is “protected before being transferred from a server ... using the data protection system.” *Id.*, [0025]. *See also id.*, [0024], [0052]. The data protection system “applies appropriate protections” on data items, e.g., files, including encrypting them in an “encrypted data item store.” *Id.*, [0056], [0059].

File transfers are initiated by user request. *Id.*, [0050], [0077]. The policy decision module determines if a file requires protection then applies “appropriate protections” including encryption, storing encrypted files on encrypted data item store 226. *Id.*, [0056], [0059], [0061]. Files are stored on server 206, then the data protection systems 212 modifies these data items as necessary for use, applying “appropriate protections” including encryption. *Id.*, [0049], [0052]. Thus, the requested files may reside on an enterprise network server before transfer to the mobile device. Cheng also discloses or suggests that files stored on server 206 are stored in encrypted form before additional protection is applied by data protection system 212 by analyzing a sensitivity score that includes current encryption level before applying further protection. *Id.*, [0039], [0041], [0054].

Cheng’s data protection system 212 includes encrypted data item store 226 and decryption key store 224 maintained within the data protection system. [Access](#)

history 312 and authentication and context history store 314 reside within the data protection system.

300

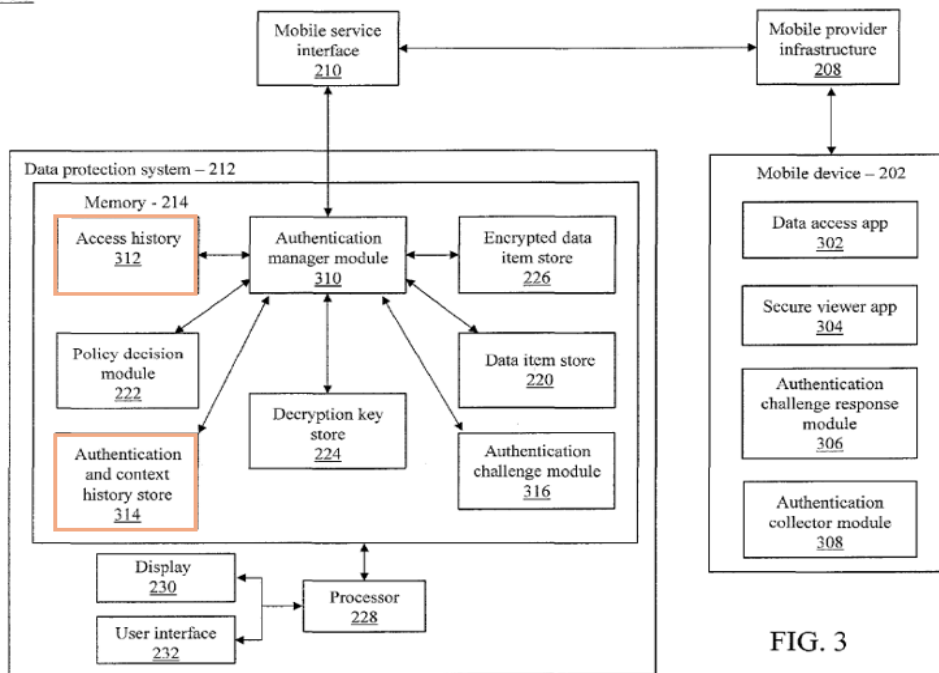


FIG. 3

*Id.*, Fig. 3 (orange outlining added).

Cheng’s policy decision module evaluates the request and determines access eligibility. *Id.*, [0014], [0064]. Upon the file request, a confidence level is determined “based on one or more of a context of the client device, an authentication history of the client device, and an access history of the user of the client device.” *Id.*, [0014]. An authentication manager module provides access based on “level of confidence” needed to access the file. *Id.*

Cheng describes protection methods of the files requested, including the use of encryption and decryption keys. *See id.*, [0056]. The “secure mobile migration manager module 216” utilizes encryption keys as well as other forms of file protection to securely transfer the file. *Id.*, [0057], [0060]. Ex-1003, ¶¶ 107-112, 115-119.

**1[c]: “responsive to receipt of the file access request, determining, by the one or more servers, a risk score for the first user based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request; and”**

Cheng discloses or renders obvious responsive to receipt of the file access request, determining, by the one or more servers, a risk score for the first user (e.g., “responsive to a request to access the protected data item, determining a level of confidence”) based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request (e.g., based on “one or more” factors including “an access history of the user”; the “sensitivity score of the protected data item” being requested and the “method of authentication”; and a “context” of the request, “the time of last successful authentication,” and “confidence in that method of authentication”). Ex-1005, [0010]-[0011], [0014]-[0015], [0027], [0065].

Cheng discloses that authentication manager module 310 “determine[s] a level of confidence,” responsive to a request, to determine access eligibility. Ex-1005, [0010]-[0011], [0014]-[0015]. This “level of confidence” may be an “accumulated authentication score” based on device context, device authentication history, and user access history. *Id.*, [0010], [0064], [0079]. Context includes current and historical locations and prior device compromises, as well as user-specific factors like prior access sensitive data, and history of lost or stolen devices. *Id.*, [0066]. Ex-1003, ¶¶ 120-126.

**1[d]: “based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key”**

Cheng discloses or renders obvious based on the risk score (e.g., “[b]ased on the level of confidence” including an “authentication score”), permitting or denying, by the one or more servers, access to the file (e.g., “determine whether access to the encrypted data item is allowed.”) by returning a decryption key for the file or withholding the decryption key (e.g., “authentication manager module 310 retrieves the decryption key...and sends it to the mobile device”; “send a message ... indic[a]ting that access is denied” if “access is not allowed”). Ex-1005, [0064], [0068].

Authentication manager module 310 processes decryption key requests using policy decision module 222 to determine user eligibility to access the encrypted file. *Id.*, [0063]. Depending on confidence level, the system permits or denies access to the file: “Based on the level of confidence, the policy decision module 222 may determine whether access to the encrypted data item is allowed.” *Id.*, [0068]. If the authentication score exceeds a “minimally required authentication score,” then the system “send[s] a decryption key” to the user for the “protected data item.” *Id.*, [0029], [0095]. If the authentication score does not satisfy this threshold, then the system “sends a message...indicating that access is denied.” *Id.*, [0095]. Ex-1003, ¶¶ 127-130.

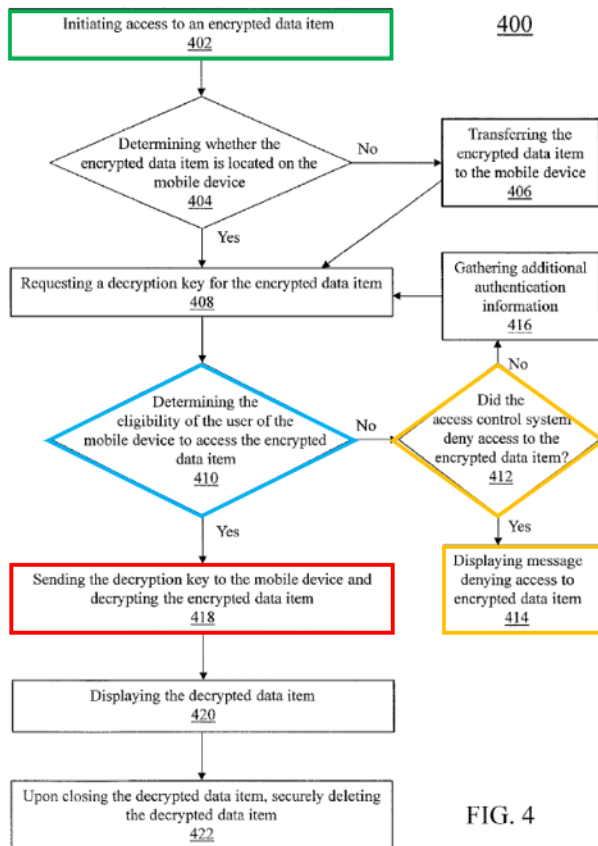


FIG. 4

*Id.*, Fig. 4 (colored outlining added).

**1[e]: “wherein said permitting or denying comprises when the risk score is less than a first threshold, returning the decryption key and providing full access to the file;”**

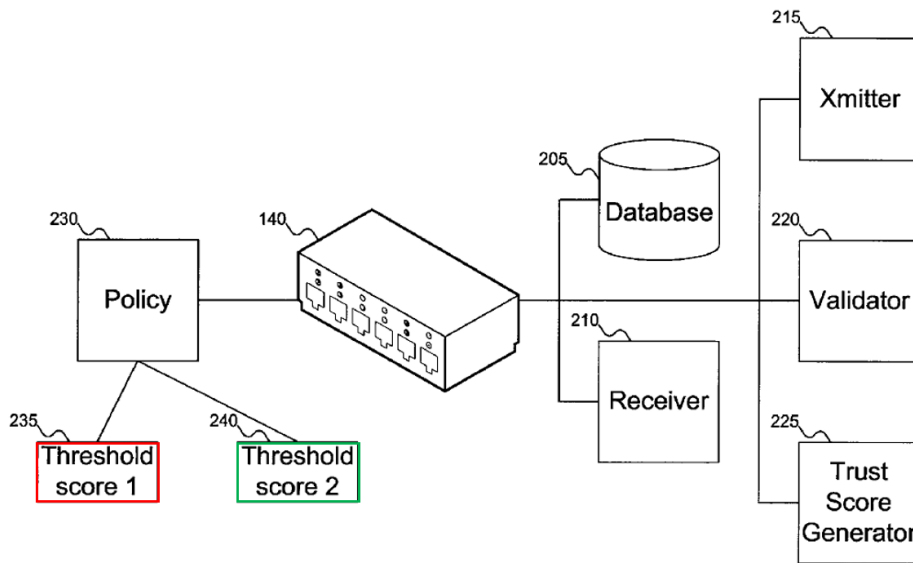
Cheng discloses or renders obvious wherein said permitting or denying comprises: when the risk score is less than a first threshold (e.g., the “level of confidence” greater than “a minimally required authentication score”), returning the decryption key and providing full access to the file (e.g., “send a decryption key” to access the protected data item). Ex-1005, [0028]-[0029].

The accumulated authentication score was compared to a minimum authentication score. Ex-1005, [0028]. This accumulated authentication score dictated whether full access is granted to decrypt a file; so long as it met the minimum threshold, the decryption key was released allowing access. *Id.*, [0028]-[0029].

Cheng discloses comparing its confidence level to a minimum threshold for full access: “The accumulated authentication score may be compared with the minimum authentication score to determine whether a user is eligible.” *Id.*, [0079]. “If the user was found to be eligible, a decryption key may be sent to the mobile device.” *Id.*, [0080]-[0081], [0087], [0095]. Ex-1003, ¶¶ 131-133.

To the extent Cheng did not disclose or suggest this element, it would have been obvious in light of Bleckmann.

Bleckmann discloses **Threshold score 1**, i.e., a first threshold. “In one embodiment, policy 230 includes **threshold score 235**. To be granted access to the resource, the computer system should have a trust score at least as high as threshold score 235.” Ex-1006, [0042]. A file is one resource considered by Bleckmann. *Id.*, [0019].



*Id.*, Fig. 2 (colored outlining added).

In the Cheng-Bleckmann combination, a POSITA would find it obvious to implement Bleckmann’s **Threshold score 1** with Cheng. Cheng discloses a “minimum authentication score.” Ex-1005, [0072]. Bleckmann’s **Threshold score 1** provides an explicit value to input as the minimum authentication score, such that Cheng compares the confidence level against this explicit score. *See id.* A POSITA would have been motivated to incorporate Bleckmann with Cheng as discussed above. *See supra* §VIII.A.3. Ex-1003, ¶¶ 134-139.

**1[f]: “when the risk score is greater than a second threshold, withholding the decryption key; and”**

Cheng discloses or renders obvious when the risk score is greater than a second threshold, withholding the decryption key.

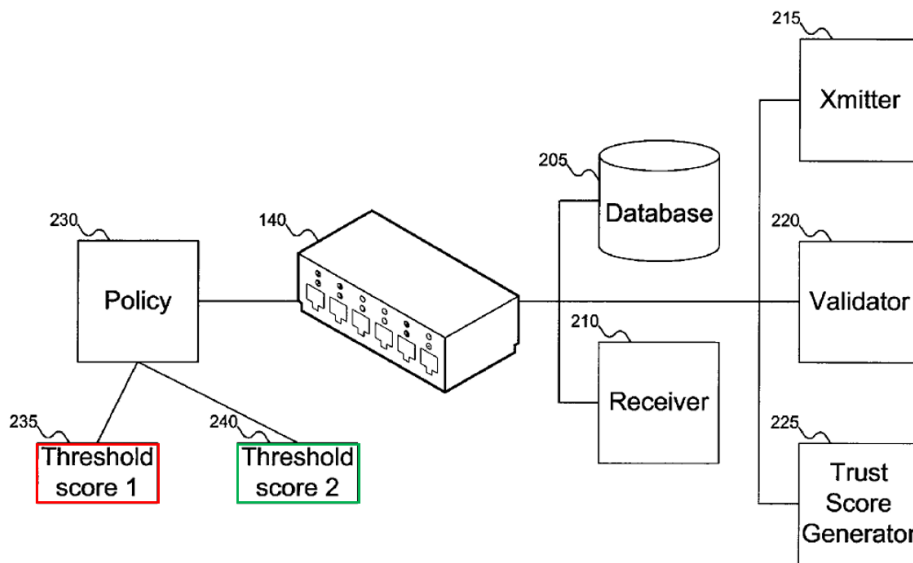
Cheng discloses that when the confidence level is below a certain authentication threshold (i.e., risk is sufficiently high), the decryption key is withheld. Ex-1005, [0080]. “If the user was not found to be eligible, in block 412,” denying access to the encrypted data item. *Id.*; *see also id.*, [0073]. Ex-1003, ¶¶ 140-142.

To the extent Cheng does not disclose a second threshold different from the first threshold, a POSITA would have understood or at least found it obvious to implement the disclosures of Cheng with a second threshold. Cheng discloses limited access beyond simple access/denied options. *See id.*, [0029], *infra* 1[g]. A POSITA would have understood or found it obvious to implement additional thresholds to determine different levels of access. Cheng further discusses embodiments where a range of authentication scores may be used; a POSITA would have understood or found it obvious to implement multiple thresholds to address different ranges/scores. Ex-1005, [0028], [0064]. Ex-1003, ¶ 143.

To the extent Cheng alone does not disclose or render obvious this limitation, it would have been obvious over Bleckmann.

Bleckmann discloses Threshold score 2, i.e., a second threshold. “For example, in FIG. 2, policy 230 is shown as including two threshold scores 235 and 240.” Ex-1006, [0043] Bleckmann further discloses that “if the trust score for the

computer system is smaller than **threshold score 240**, the computer system can be denied access to the resource.” *Id.*



*Id.*, Fig. 2.

A POSITA would find it obvious to implement Bleckmann’s Threshold score 2 with Cheng. Cheng discloses comparing its authentication score against baseline values and denying access. Ex-1005, [0072], [0080]. Bleckmann’s **Threshold score 2** provides an explicit score, such that Cheng compares the current confidence level against this score to determine if denial criteria are met. Ex-1003, ¶¶ 144-148.

**1[g]: “when the risk score is between the first threshold and the second threshold, returning the decryption key and providing limited access to the file.”**

Cheng discloses or renders obvious when the risk score is between the first threshold and the second threshold, returning the decryption key and providing limited access to the file. (*e.g.*, “level of confidence” between the unredacted item’s “sensitivity score” and the “lower” sensitivity score of a “redacted version,” providing access to a “redacted version”).

Cheng discloses providing limited access by creating redacted versions. The policy decision module 222 determines, based on the confidence level, which version the user may access. Ex-1005, [0074], [0026]. Cheng describes various levels of access to files, including levels of redaction: “*e.g.*, a heavily redacted version permissible to be viewed everywhere and a lightly redacted version that may only be viewed in locations with some level of access control.” *Id.*, [0046]. Cheng provides a decryption key for each version of limited access. *Id.*, [0029]. Policy decision module 222 determines, based on confidence level, whether redacted file versions may be accessed. *Id.*, [0074], [0081]. Ex-1003, ¶¶ 149-151.

To the extent this limitation is not met because Cheng describes decryption keys unique to each version, Cheng discloses utilizing a single decryption key: “the same encryption key may be used for all data items.” Ex-1005, [0057]. Using a single decryption key further would have been obvious to a POSITA; encryption keys may be reused under Cheng’s various implementations and settings. It would

be obvious for a POSITA to implement Cheng with the same key used to decrypt multiple versions or data items to simplify key management. Ex-1003, ¶ 152.

To the extent a second threshold is not disclosed or suggested, it would have been obvious to a POSITA. Cheng discloses providing limited access to files, including redacted versions, i.e., an intermediate access tier. Ex-1005, [0046], [0074]. Because more than a binary grant/deny option is disclosed, it would have been obvious that more than a single threshold existed. Ex-1003, ¶ 153.

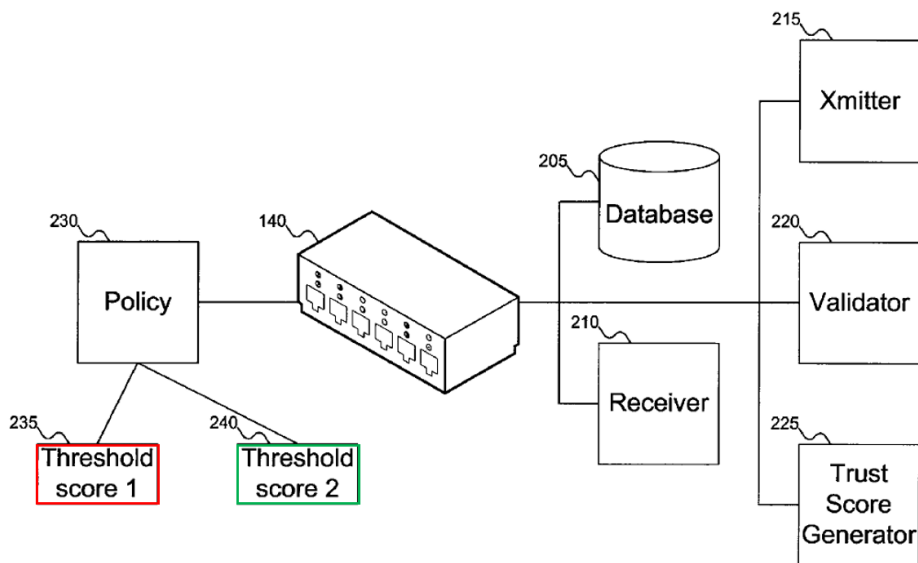
Additionally, to the extent providing a redacted version of a file is not providing “limited access,” Cheng considers other protection techniques for intermediate access, each with a unique decryption key. *Id.*, [0044]. Other well-known methods of access control known before the ’623 patent include redirecting a user’s connection through a virtual private network or requiring access through a specific terminal. Ex-1003, ¶ 154.

To the extent Cheng does not disclose or suggest this limitation, it would have been obvious in light of Bleckmann.

Bleckmann describes that “policy 230 can include multiple threshold scores.” Ex-1006, [0043]. If Bleckmann’s trust score was at least as high as **threshold score 235**, full access was granted, if the trust score was less than **threshold score 235** but at least as high as **threshold score 240**, partial access was

granted, and if the trust score was smaller than threshold score 240, access was denied. *Id.*

Further, Bleckmann discloses the same functionality as the '623 patent for limiting file access when the risk score is between the two thresholds. The '623 patent describes limiting access by releasing the decryption key and directing access to the file a VPN. Ex-1001, 6:20-24. Describing a computer system not directly connected to an internal network, and therefore less secure, Bleckmann discloses “resource 145 might be requested over a virtual private network (VPN) used to secure access to resources.” Ex-1006, [0032].



*Id.*, Fig. 2 (colored outlining added).

A POSITA would find it obvious to implement Bleckmann's Threshold score 1 and Threshold score 2 with Cheng. Cheng discloses intermediate levels of

file access. *See* Ex-1005, [0074], [0081]. Bleckmann's threshold scores provide explicit values for Cheng's authentication manager module 310 to compare against the current confidence level to determine the resulting access tier. Ex-1003, ¶¶ 155-161.

## 5. Claim 2

**“The method of claim 1, wherein said determining, by the one or more servers, the risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine learning,”**

Cheng discloses or renders obvious the method of claim 1, wherein said determining, by one or more servers, the risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine-learning.

Cheng discloses utilizing user history to determine if a data access request or current user context is unusual; Cheng does not limit how this is determined, including by machine learning. Ex-1005, [0065]. A POSITA would have understood and at least found it obvious that this includes evaluating a file access request by utilizing artificial intelligence, i.e. machine learning, to analyze/determine a risk score. Ex-1003, ¶¶ 162-164.

**6. Claim 3**

**3[pre]: “The method of claim 1, wherein the information regarding historical user behavior includes for each user of the plurality of users:”**

To the extent the preamble is found to be limiting, Cheng discloses or renders obvious the method of claim 1, wherein the information regarding historical user behavior includes for each user of the plurality of users.

Cheng discloses information regarding historical user behavior (e.g., “**access history 312**”). *See* Ex-1005, [0065], Fig. 3; *see also* [1]. Ex-1003, ¶¶ 165-167.

**3[a]: “historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time;”**

Cheng discloses or renders obvious historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time (e.g., “history of data access” “based on volume”), types of the files accessed (e.g., “history of the user’s access to data of known sensitivity”), and applications used by the user over the predetermined period of time (“applications installed on the [user’s] device”). Ex-1005, [0065], [0066].

Cheng further discloses “The level of confidence may be determined based on the history of data access (e.g., based on volume, topic, average sensitivity scores, etc.).” *Id.*, [0092]; *see also id.*, [0065], [0094], Fig. 3. Cheng analyzes

“history of previous compromises of the mobile device” and “history of the user’s access to data of known sensitivity,” as well as “history loss or theft of devices and history of the accessing individual.” *Id.* [0066]. Ex-1003, ¶¶ 168-170.

**3[b]: “historical data regarding observed locations of the user; and”**

Cheng discloses or renders obvious historical data regarding observed locations of the user (e.g., “history of previous locations of the mobile device”). Ex-1005, [0066], [0093]. Ex-1003, ¶¶ 171-173.

**3[c]: “historical data regarding observed times at which the user accesses files.”**

Cheng discloses or renders obvious historical data regarding observed times at which the user accesses files (e.g., “time of last successful authentication”). Ex-1005, [0065].

Cheng further discloses “time of [the] last successful authentication of the user through the mobile device 202.” *Id.*, [0065]. Cheng discloses that historical data includes deviation from stored access patterns *Id.*, [0067]. To analyze history, Cheng discloses a data protection system to collect information relating to the data item including access history. *Id.*, [0091]. Ex-1003, ¶¶ 174-176.

**7. Claim 4**

**“The method of claim 1, wherein the observed data includes a current location of the first user as**

**determined based on a source Internet Protocol (IP)  
address contained in the first access request.”**

Cheng discloses or renders obvious the method of claim 1, wherein the observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address contained in the file access request (e.g., “the user’s geographic location”). Ex-1005, [0041].

Cheng discloses user context includes geographic location and level of access based on a location. Ex-1005, [0041], [0046], [0066]. A POSITA would have understood and at least found it obvious that determining a geographic location would be based on the user’s IP address. Ex-1003, ¶¶ 177-179.

**8. Claim 5**

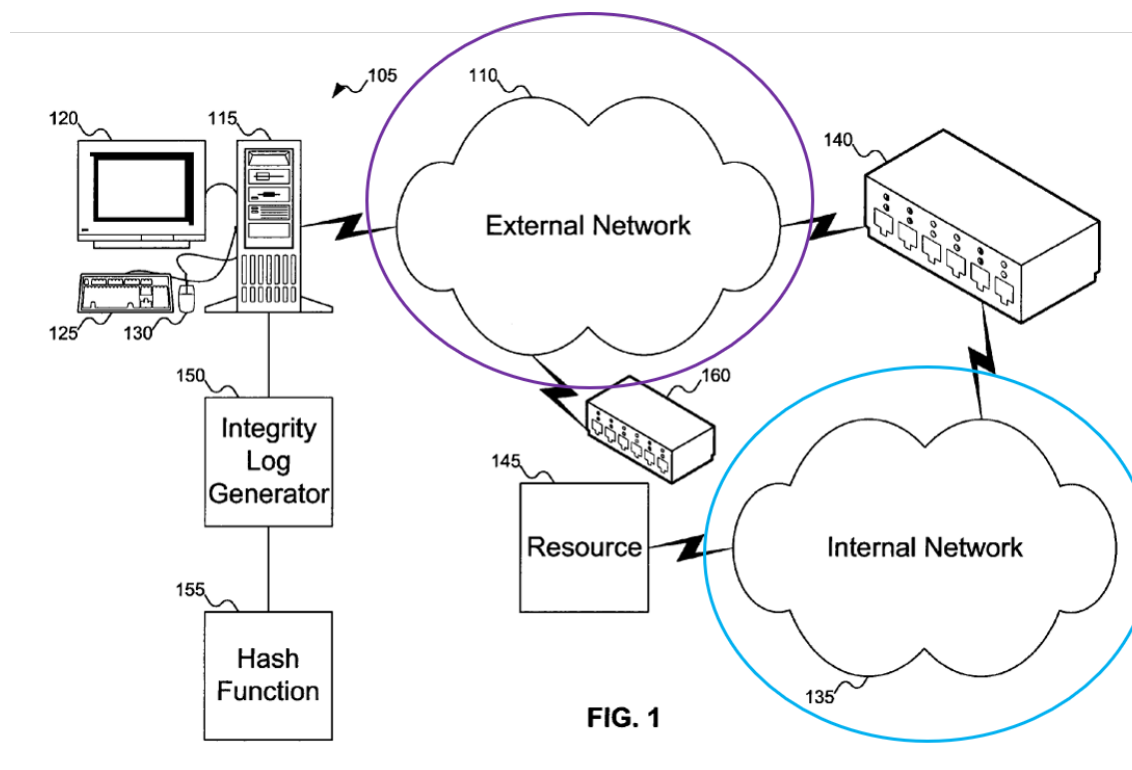
**“The method of claim 1, wherein the observed data  
includes a status indicative of whether the connection  
through which the first user initiated the file access  
request is trusted or untrusted.”**

Cheng discloses or renders obvious the method of claim 1, wherein the observed data includes a status indicative of whether the connection through which the first user initiated the file access request is trusted or untrusted (e.g., “the security status of the networks”). Ex-1005, [0066].

Cheng determines “security status” of device’s networks, e.g., the level of trust in the network, including enterprise network connection. *Id.*, [0066]. Cheng contemplates an enterprise environment where a user requests access from the

network or from public networks. *See id.*, [0006]; *see also id.*, [0074]. Cheng's confidence level accounts for current context such as "security status" of the device's network. *Id.*, [0093]. A POSITA would understand that analyzing a user's current context, including network connection, discloses this claim limitation. Ex-1003, ¶¶ 180-181.

To the extent Cheng does not disclose or suggest this limitation, it would have been obvious in light of Bleckmann. Bleckmann teaches an "internal network 135" internal to the organization, differentiating this from an "External network 110." Ex-1006, [0019]. It distinguishes between organization controlled internal networks and external networks. *See id.*, [0028].



*Id.*, Fig. 1.

A POSITA would have been motivated to combine Cheng and Bleckmann for the same reasons described above. *See supra* §VIII.A.3. Ex-1003, ¶¶ 182-184.

**9. Claim 6**

**“The method of claim 5, wherein the connection is trusted when the first user is on the enterprise network or accessing the enterprise network remotely via a secure connection.”**

Cheng discloses or renders obvious the method of claim 5, wherein the connection is trusted when the first user is on the enterprise network or accessing the enterprise network remotely via a secure connection.

Cheng’s confidence level accounts for “security status” of device networks, only sending the decryption key when “trust is sufficient.” Ex-1005, [0066], [0093], [0095]. A POSITA would have understood or at least found it obvious that Cheng considers trustability of the network connection. Cheng contemplates its invention within the context of enterprise networks then describes that network security status affects the confidence level. *Id.*, [0006], [0093]. A POSITA would recognize an enterprise network would provide greater security, and thus would be trusted, whereas a public network would provide less, and would not be trusted. Ex-1003, ¶¶ 185-186.

To the extent Cheng does not disclose or suggest this limitation, it would have been obvious in light of Bleckmann.

As discussed in claim 5, Bleckmann discloses that there is an “implicit assumption that computer systems connected to [internal network 135](#) are known to be safe and validated.” Ex-1006, [0028], Fig. 1. A POSITA would understand an enterprise network to be an “internal network” as described by Bleckmann and that Bleckmann treats the internal network as trusted.

A POSITA would have been motivated to combine Cheng and Bleckmann for the same reasons as claim 5. Ex-1003, ¶¶ 187-190.

#### **10. Claim 7**

**“The method of claim 5, wherein the connection is untrusted when the first user is not on the enterprise network or accessing the enterprise network remotely via an insecure connection.”**

Cheng discloses or renders obvious the method of claim 5, wherein the connection is untrusted when the first user is not on the enterprise network or accessing the enterprise network remotely via an insecure connection.

Cheng prevents decryption key release when the confidence level is insufficient and accounting for network security status. *See* [1], [5]. A POSITA would have understood and at least found it obvious that the “untrusted” network of claim 7 is the logical inverse of claim 6’s trusted network. Cheng describes that,

for device lock methods, “15 minutes may be too long” for a user at a public bar, explaining that “a public location” is one with “a high risk of unauthorized access.” Ex-1005, [0007], [0074]. A POSITA would recognize that, compared to the security of an enterprise network, other connections including public connections would be untrusted. A POSITA would understand Cheng discloses the untrusted network of claim 7. Ex-1003, ¶¶ 191-192.

To the extent Cheng does not disclose or suggest this limitation, it would have been obvious in light of Bleckmann.

Bleckmann discloses an “implicit assumption that computer systems connected to **internal network 135** are known to be safe and validated.” Ex-1006, [0028]. It distinguishes this from **external network 110**, bypassing validation of **internal network 135**: “likelihood of infection by a virus or similar agent is reduced relative to computer systems outside the control of the organization.” *Id.* A POSITA would understand Bleckmann treats computer systems outside the control of the organization as untrusted. Ex-1003, ¶¶ 193-194.

A POSITA would have been motivated to combine Cheng and Bleckmann for the same reasons as claim 5. Ex-1003, ¶¶ 195-196.

**11. Claim 8**

**“The method of claim 1, wherein the encrypted form involves the file being encapsulated in a cryptographic wrapper.”**

Cheng discloses or renders obvious the method of claim 1, wherein the encrypted form involves the file being encapsulated in a cryptographic wrapper (e.g., “encrypted data item store 226”). Ex-1005, [0061].

“Encrypted data item store 226” securely transfers the encrypted data item to the mobile device, providing the file encapsulated in a cryptographic wrapper. Ex-1005, [0061]. Cheng encrypts data before storage and transfer, applying a dedicated key generated for the file. *Id.*, [0044]-[0045].

This encrypted file stored in the encrypted data item store is a file wrapped in a layer of cryptographic protection, held by encrypted data item store 226, requiring the corresponding decryption key, stored by decryption key store 224. *Id.*, [0059].

A POSITA would have understood and at least found it obvious that Cheng’s encrypted data items constitute files encapsulated in a cryptographic wrapper within the meaning of claim 8. Ex-1003, ¶¶ 197, 199-203.

**12. Claims 9-15**

Nearly all limitations of claims 9-15 are substantively identical to limitations of [1]-[8], though there are differences in 9[pre] and 14[a]. *See* Ex-1003, ¶ 205.

Accordingly, claims 9-15 are disclosed and/or rendered obvious for the reasons explained, and as further cross-referenced, below. Ex-1003, ¶¶ 209-222.

|                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>9[pre] A non-transitory computer-readable storage medium embodying a set of instructions, which when executed by one or more processors of one or more servers associated with an enterprise network, causes the one or more processors to perform a method comprising:</p> <p>14[a] A system, the system comprising: one or more processors; and a non-transitory computer-</p> | <p>Cheng discloses a non-transitory computer-readable storage medium embodying a set of instructions that, when executed by one or more processors of one or more servers associated with an enterprise network, causes those processors to perform a method.</p> <p>Cheng discloses system embodiments with aspects “may take the form of a computer program product embodied in one or more computer readable medium(s) having computer readable program code embodied thereon.” Ex-1005, [0030]. <i>See also id.</i>, [0031]-[0033].</p> <p>Cheng further discloses use of “the processor of the computer or other programmable data processing apparatus.” <i>Id.</i>, [0034]. Those functions are the access control method steps performed by the data protection server when processing a user’s file access request. <i>See id.</i>, Figs. 4, 6. Ex-1003, ¶¶ 206-208.</p> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                                                                                                                                                                                                      |                                                    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| readable storage medium coupled to the one or more processors and embodying a set of instructions, which when executed by the one or more processors of one or more servers associated with an enterprise network, causes the one or more processors to perform a method comprising: |                                                    |
| 9[a],<br>14[b]                                                                                                                                                                                                                                                                       | <i>See</i> 1[a]. Ex-1003, ¶ 209.                   |
| 9[b]-9[d],<br>15[a]-15[c]                                                                                                                                                                                                                                                            | <i>See</i> 3[a]-3[c]. Ex-1003, ¶¶ 210-212.         |
| 9[e]-9[j],<br>14[c]-14[h]                                                                                                                                                                                                                                                            | <i>See</i> 1[b]-1[g]. Ex-1003, ¶¶ 213-218.         |
| [10]-[13]                                                                                                                                                                                                                                                                            | <i>See</i> [2], [4]-[5], [8]. Ex-1003, ¶¶ 219-222. |

**B. Ground 2: Combining Cheng and Bleckmann with Kirti Renders Claims 2, 4, and 10-13 Obvious**

**1. Kirti**

Kirti discloses a cloud security system that analyzes user activity using machine learning to perform threat detection and recommendations. Ex-1008, 3:54-58. User activity data includes login and logout statistics, access IP addresses, access devices, and resources accessed. *Id.*, 10:30-39. These are logged with event details including a username, the acted upon resource, event time, and network IP address. *Id.*, 18:19-22. Activity data is organized using profiles that cover different time periods through fixed moving windows. *Id.*, 18:33-67. A risk score is calculated for the user based on the baseline profile, and risk scores are used to prioritize threat remediation actions within cloud applications, which helps organizations to remediate the most severe issues first. *Id.*, 1:57-65; 4:15-22. Ex-1003, ¶¶ 223-225.

**2. Motivation to Combine**

A POSITA would have been motivated to combine Cheng and Bleckmann with Kirti. These references are analogous art, which includes server-based access control systems to evaluate trustworthiness of a requesting user and make dynamic access decisions regarding data protection. They are reasonably pertinent to the same alleged problems, including the need to determine whether a requesting

user's access patterns deviate from normal behavior and computing a risk score that controls file access. Ex-1005, [0072]-[0074]; Ex-1008, 1:44-59; Ex-1006, [0008].

Cheng and Kirti collect user activity data over time, build profiles reflecting normal behavior, and evaluate current access activity against those profiles to identify potential threats to protected resources. *See, e.g.*, Ex-1005, [0024], [0028], [0064], [0089]; Ex-1008, 12:58-64; 14:5-13. Similarly, Bleckmann discloses determining conditions that permitted access to a remote resource. Ex-1006, [0042].

A POSITA would have been motivated to apply Kirti's machine learning techniques to Cheng and Bleckmann's score-based data protection system to provide a more accurate and adaptive user behavior model for determining access eligibility. Ex-1003, ¶¶ 226-231.

Cheng acknowledges the data protection system should evaluate "the level of confidence in the user's identity," in which Bleckmann provides explicit threshold scores, and adjust access decisions based on contextual factors, but does not expressly teach using machine learning to model user behavior. Kirti fills this gap, disclosing using activity data collected over time with machine learning

algorithms to generate user behavior profiles and training algorithms to generate a threat scores. Ex-1008, 12:58-13:40, Fig. 5C.

Kirti further discloses collecting and maintaining a baseline profile of valid IP addresses and associated geolocations for a user and recognizing threats from a geolocation not on that list. *Id.*, 13:35-42. Kirti's collected data includes user location determined by IP address. *Id.*; Ex-1003, ¶¶ 232-233.

Cheng's policy decision module 222, modified with Kirti's machine learning techniques, would employ a user behavior model developed by machine learning trained on historical access data including IP address geolocation patterns to generate the confidence level used to determine decryption key receipt eligibility.

Cheng's policy decision module evaluates user eligibility, incorporating access history and context of the client device/user. Ex-1005, [0028], [0064], [0089], [0095]. Implementing Kirti's machine learning techniques in Cheng's data protection system to enhance the user behavior model would have been a straightforward modification. Kirti teaches applying machine learning trained on historical activity data to detect deviation from normal user behavior and resolving source IP addresses from access events to geographic coordinates to identify anomalous access locations.

A POSITA would have found it straightforward and advantageous to apply Kirti's machine learning and IP geolocation teachings to Cheng and Bleckmann's data protection system, and would have known such a combination, yielding the limitations of Claims 2 and 4 of the '623 patent, would predictably work and provide the expected functionality. Ex-1003, ¶¶ 234-237.

### **3. Claim 2**

Kirti discloses or renders obvious “evaluating the file access request with reference to a model of user behavior developed by machine-learning” (e.g., “machine learning algorithms” to “analyze user activity”). Ex-1008, 3:53-61; 5:44-54.

Kirti discloses a risk score based on the baseline user profile. *Id.*, 2:14-17. User activity information is analyzed using machine learning algorithms. *Id.*, 3:53-56. Kirti further discloses the use of machine learning to “build user behavior profiles” (12:60-64), “establish baselines of user behavior” (4:60-66), and generate “risk scores” (24:39-50). Ex-1003, ¶¶ 238-240.

### **4. Claim 4**

Kirti discloses or renders obvious “observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address

contained in the file access request,” (e.g., “IP addresses and associated valid geolocations”). Ex-1008, 2:3-4.

Kirti’s disclosed baseline user profile includes “a list of IP addresses and associated valid geolocations” that determined threat level for a file access request. *Id.*, 2:3-7, 10:34-40. Kirti further discloses analyzing IP addresses to determine “normal” geolocations of access requests. *Id.*, 17:13-19. Ex-1003, ¶¶ 241-244.

## **5. Claims 10-13**

As discussed above, claims 10-13 add no limitations separate from claims 1-8. *See supra* §VIII.A.12. Claim 10 (and its dependent claims) includes the same limitations as claim 2. Claim 11 adds only the same limitation as claim 4. The Cheng-Bleckmann-Kirti combination discloses all limitations of claims 10-13 for the same reason as described above. Ex-1003, ¶¶ 245-246.

## **C. Ground 3: Combining Cheng and Bleckmann with Van Dijk Renders Claims 3, 9-13, and 15 Obvious**

### **1. Van Dijk**

Van Dijk discloses an adaptive authentication system that generates a risk score for access requests compared to user baseline profiles based on historical request behavior including login time and location, built from request records across a series of time windows. Ex-1007, 1:17-24.

Van Dijk stores a set of database entries that include user identifier, time period, and behavioral data drawn from observed requests, including a request timestamp. The system generates the baseline profile and computes a User Risk score by comparing the current request against the historical data-based behavioral patterns, using the formula “Overall Risk = User Risk x Transaction Risk.” *Id.*, 6:38-7:4; 5:17-35.

Based on the resulting overall risk score, Van Dijk’s access manager determines whether to grant or deny access; a key manager releases appropriate data protection keys for access. *Id.*, 8:36-48. The system ties risk-scored behavioral evaluation to key release. Van Dijk’s time-windowed historical database captures previous user request times, organized into a time window that serves as the basis for the risk score determination. Ex-1003, ¶¶ 247-251.

## **2. Motivation to Combine**

A POSITA would have been motivated to combine Cheng and Bleckmann with Van Dijk with a reasonable expectation of success. These references are analogous art: they are in the same field of risk-scored, server-mediated access control for encrypted data. Each reference addresses the problem of deciding the level of access to sensitive resources a request is permitted. Ex-1005, [0072]-[0074]; Ex-1007, 2:45-52; Ex-1006, [0008]. Ex-1003, ¶¶ 252-254.

A POSITA would have been motivated to apply Van Dijk's time-window-indexed behavioral baseline to Cheng's **access history module 312**, coupled with Bleckmann, to improve threat detection. Cheng's confidence level is determined based on data access history; **access history 312** may be used to determine if the data accessed or the current context of the device is unusual. Ex-1005, [0065]. To the extent that Cheng and Bleckmann do not specify that access history includes observing the times of user access, a POSITA would have recognized Van Dijk as an advantageous addition. Van Dijk discloses that adaptive authentication techniques compare access attempts against historical baseline records. Ex-1007, 1:20-25; 4:33-40. Ex-1003, ¶¶ 255-257.

A POSITA would have understood that applying Van Dijk's time-period-indexed structure to Cheng and Bleckmann would make deviation detection more precise by comparing a current access attempt against behavior during the same time window in prior periods, rather than an undifferentiated all-time average. This combination would yield the expected and predictable result of a more granular threat detection system. In the meantime, a POSITA would have been motivated to keep Cheng's policy decision module 222 modified with Bleckmann's two-threshold framework as discussed in *supra* §VIII.A.3. Ex-1003, ¶ 258.

### **3. Claim 3**

To the extent it is argued that further disclosure of “historical data regarding observed times at which the user accesses files” is required, Van Dijk discloses this limitation (e.g. a “timestamp from request 11”) as recited in Claim 3[c]. Ex-1007, 5:19-20.

Van Dijk discloses utilizing historical data, including observed time of file access, e.g. timestamps from request 11, in determining file access. *Id.*, 1:17-25. Authenticator requestor 18 sends request 11 to a user device upon request. *Id.*, 5:17-18. “Processor 22 stores data such as username, fact values and timestamp from request 11.” *Id.*, 5:19-20. *See also id.*, 4:29-47. Ex-1003, ¶¶ 259-261.

### **4. Claims 9-13, 15**

As discussed above, claims 9-15 do not add additional limitations separate from claims 1-8. *See supra* §VIII.A.12. Claim 9 and its dependent claims include the same limitations from claim 3. Claim 15 adds the same limitations to its independent claim as does claim 3. The Cheng-Van Dijk combination discloses all limitations of claims 9-13, 15 for the same reason as described above. Ex-1003, ¶¶ 262-263.

**D. Ground 4: Combining Ford and Van Dijk Renders Claims 1-15 Obvious.**

**1. Ford**

Ford is directed to “methods and systems contributing to managing digital rights management (DRM) protected content sharing” in an “enterprise network.” Ex-1009, [0005].

Ford discloses transmission and reception of sensitive documents over a network. *Id.*, [0055]. Ford’s exchange host server “may be distributed over a plurality of server computers.” *Id.*, [0061].

Ford discloses secure content sharing with encryption-based protection. *Id.*, [00344], [00354]. Files are stored in encrypted form, users initiate access requests, the server evaluates requests against a dynamic risk rating (“DRR”) derived from contextual and behavioral factors, and the server permits or denies access by returning or withholding a decryption key. *Id.*, [00344]-[00345]. Ford discloses a matrix of DRR states for varied access. *Id.* This includes a graduated access control including partial file access based on the user’s risk level. *Id.*, [00350]. When a user is granted access, a decryption key is released. *Id.*, [00354]-[00357]. Ford, alone or in combination with Van Dijk, expressly discloses, or at minimum renders obvious to a POSITA, each limitation of Claims 1-15 of the ’623 patent. Ex-1003, ¶¶ 264-267.

Ford discloses a single secure-exchange platform; despite describing various “embodiments,” this language describes discrete components and functions. A POSITA would at once envisage the disclosed elements together as obvious, regardless of the particular embodiments in which they are disclosed. *See* Ex-1009, [00573]; Ex-1003, ¶ 267. *See also General Electric*, 983 F.3d at 1351–52.

## **2. Motivation to Combine**

A POSITA would have been motivated to combine Ford and Van Dijk with a reasonable expectation of success. Both are server-based access control systems evaluating behavioral risk signals, addressing whether a requester’s current behavior is consistent with normal activity. Ford teaches risk-based detection from user or device history, including pattern of use; Van Dijk teaches comparing login attempt information, including time, with a historical record of typical user behavior.

A POSITA would have been motivated to apply Van Dijk’s time-window-indexed behavioral baseline architecture to Ford’s risk detection framework to provide more precision to model normal access behavior. Ford’s DRR may be based on user or device history, including access timestamps. To the extent Ford does not specify further historical data inputs, a POSITA would turn to Van Dijk. Van Dijk discloses a historical baseline comprising a database where each entry

includes user identifier, time period, and user data organized into non-overlapping time intervals, such that a current access attempt is compared against the user's behavior during the same time window in prior periods. Ex-1007, 4:33-40; 5:10-35.

Because Ford teaches collecting timestamps associated with user access, incorporating Van Dijk's time-period-indexed structure into Ford's access history records would have been a straightforward modification yielding the expected and predictable result of a more granular system. Ex-1003, ¶¶ 268-271.

### 3. Claim 1

**1[a]: “A method comprising: obtaining and storing, by one or more servers associated with an enterprise network, information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users;”**

Ford discloses or renders obvious a method (e.g., “methods...contributing to managing digital rights management (DRM) protected content sharing”) comprising: obtaining and storing, by one or more servers associated with an enterprise network (e.g., obtaining and storing, in “data stores” by an “exchange host server”), information regarding historical user behavior of a plurality of users of the enterprise network (e.g., information for “risk-based questioning and detection based on a user or device history”) by observing file access requests

initiated by the plurality of users (e.g., by “tracking access, downloading and uploading of such documents” by users).

Ford discloses a “method” in a DRM system using an “exchange host server” for managing “DRM” content sharing that comprises “a plurality of server computers”. Ex-1009, [0053], [0061]. The server’s data stores contain information for “authentication” and “risk-based questioning” for user access. *Id.*, [0061], [0071], [00221]. Historical behavior information is collected for protected files in the system, including “tracking access, downloading and uploading of such documents” and “audit and access history.” *Id.*, [0055], [0087]. Ex-1003, ¶¶ 272-273.

Further, Ford’s “Contextual Sharing Facility” “manages the sharing of data

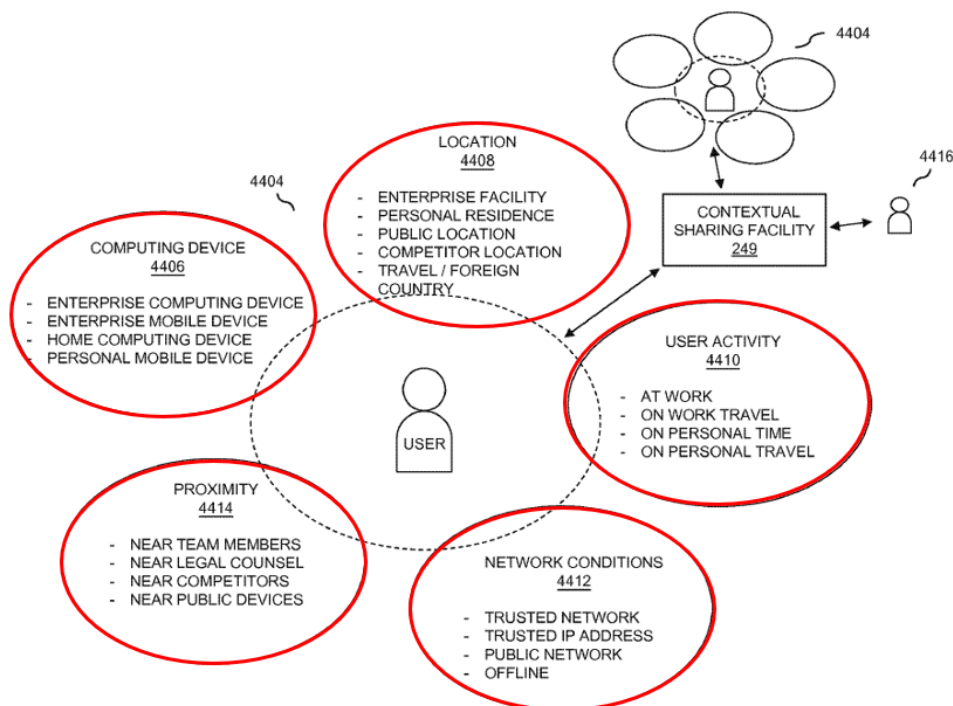
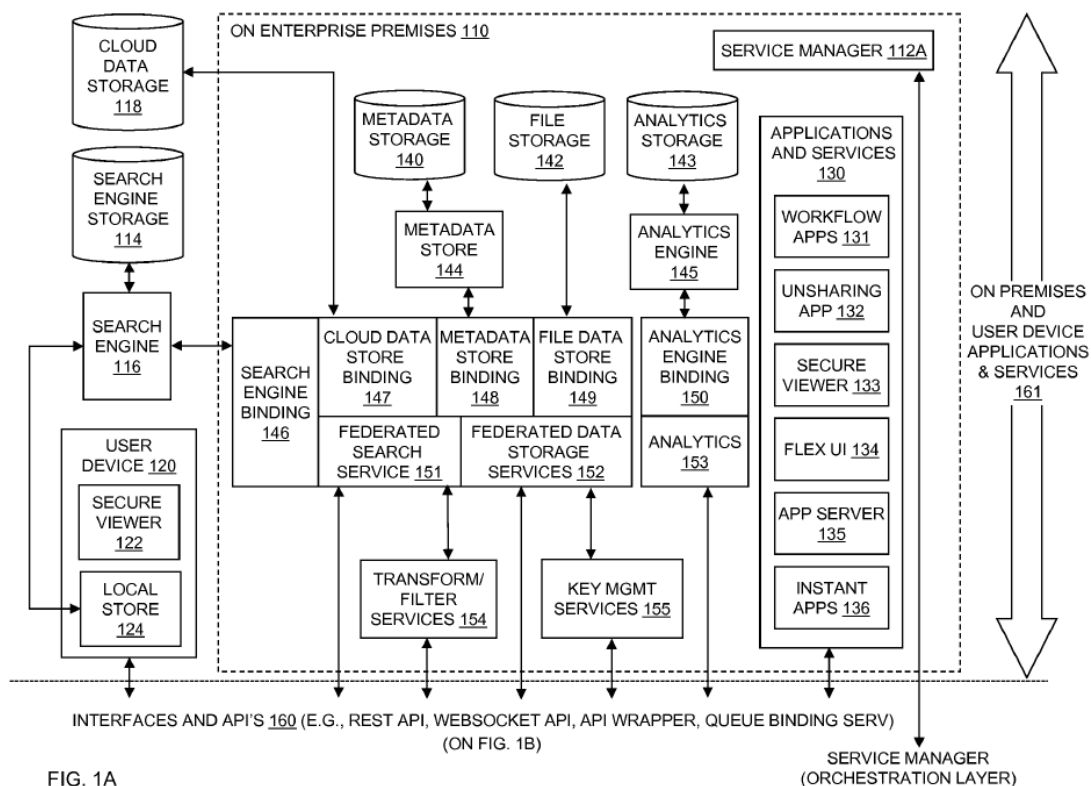


Fig. 44

based on the **contextual environment 4404** of a user.” *Id.*, [00287]. The contextual sharing facility is utilized in restricting secure file sharing. *Id.*, [00287]-[00289].

*Id.*, Fig. 44 (colored outlining added).

Ford’s collaborative computer data exchange methods contributing to managing digital rights management (DRM). *Id.*, [0005]. Over exchange servers, including enterprise servers, documents and files are stored and exchanged. *Id.*, [0055], [0087], [00352].



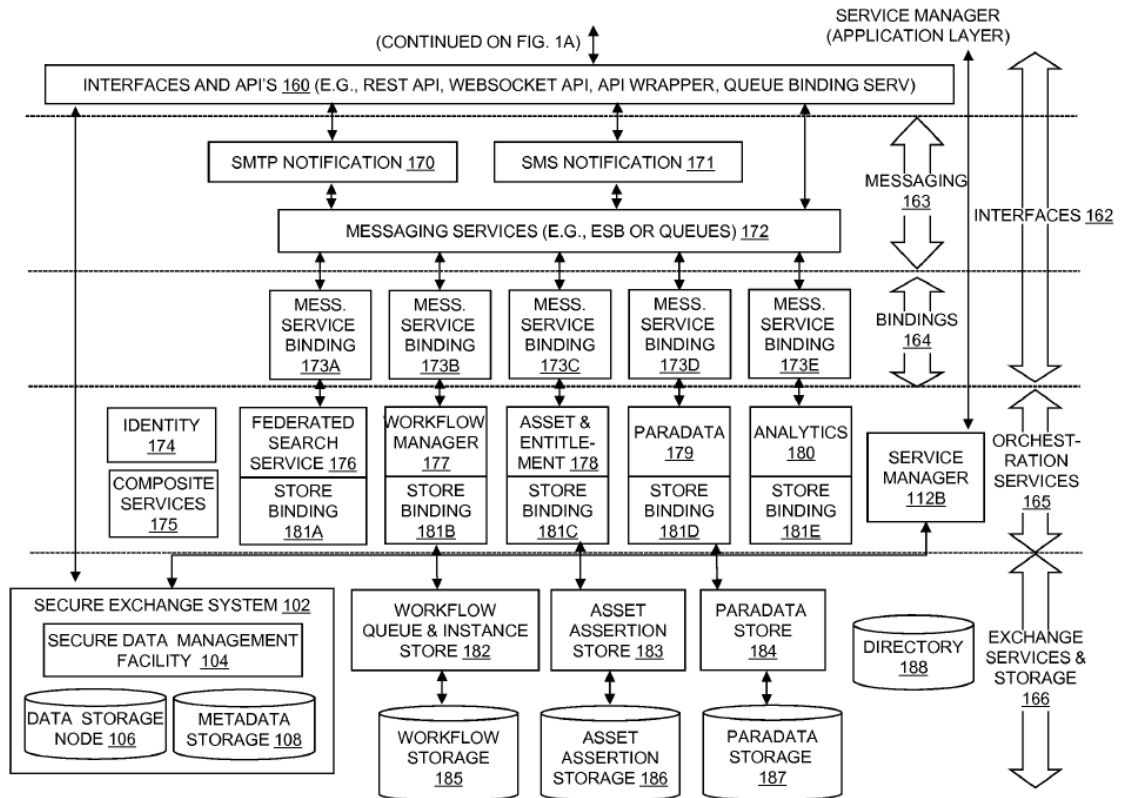


FIG. 1B

*Id.*, Figs. 1A, 1B.

Ford discloses “risk-based questioning and detection” based on user or device history, including location, device, and pattern of use. *Id.*, [00221]. Ex-1003, ¶¶ 274-277.

To the extent Ford does not disclose or suggest this limitation, it would have been obvious in light of Van Dijk. Van Dijk teaches baseline profiles stored within a database, equivalent to the servers associated historical user behavior information.

Access manager 340 observes user-initiated file access requests and determines access based on the user's data; Van Dijk stored per-user historical records in database storage to analyze a request's threat level. Ex-1007, 5:17-25; 4:44-47.

Van Dijk discloses the access manager, key manager, adaptive authentication device, and database storage may be server-side components within an enterprise network. *Id.*, 6:45-48. Van Dijk's server-side adaptive authentication device and database storage components obtain and store user baseline profile data in its database. *Id.*, 6:38-63; Ex-1003, ¶¶ 278-282.

**1[b]: “receiving, by the one or more servers, a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network in encrypted form;”**

Ford discloses or renders obvious receiving, by the one or more servers, a file access request initiated by a first user of the plurality of users (e.g., “a download of the document is requested”), wherein the file access request relates to a file stored within the enterprise network in encrypted form (e.g., “encrypted...through a randomly generated encryption key”). Ex-1009, [00170].

Ford discloses a user requesting “download of the document” from a server. *Id.* These documents are stored on the server in encrypted form. *Id.* The secure

managed key facility manage encryption and decryption keys for transfer. *Id.*, [00354]-[00357]. Ex-1003, ¶¶ 283-287.

**1[c]: “responsive to receipt of the file access request, determining, by the one or more servers, a risk score for the first user based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request;”**

Ford discloses or renders obvious responsive to receipt of the file access request, determining, by the one or more servers, a risk score for the first user (e.g., responsive to an access request, the servers assigning a DRR to a user), based on a plurality of factors including information regarding historical user behavior (e.g., DRR “may change as conditions associated with the user change” and based on “user or device history”), the file access request (e.g., based on the “action the user wishes to take”) and observed data determined based on the file access request (e.g., “the context of their current location”). Ex-1009, [00345].

Ford discloses that in response to an access request, the server determines user eligibility and assigns a DRR to a user based on historical user and device information, requested actions, and current location. *Id.*, [0087], [00221], [00345], [00349].

This enterprise policy analyzes user profiles to determine access. *Id.*, [00345]. The level of control may be based on current risk profile determined by

DRR, which includes IP address, geography, and data requested, among other factors *Id.* Ford further discloses processing historical information including access date and time information, providing historical user information validating user identity. *Id.*, [00414], [00249].

Further, Ford discloses contextual sharing for file access control to determine access privileges. *Id.*, [00287]. Contextual sharing facility 249, which may reside on a server, continuously gathers environmental parameters of user devices to manage sharing permissions. *Id.*, [00291]. Ex-1003, ¶¶ 288-292.

Ford's contextual sharing facility analyzes the “contextual environment 4404 of a user,” including “computing device 4406,” “location 4408 of the computing device,” “user's current activity state 4410,” “network conditions 4412” and access time. Ex-1009, [00287]. A POSITA would recognize that Ford's contextual sharing facility disclosures were a part of Ford's user or device history and resulting DRR score, or at least would have been obvious to include. Ex-1003, ¶¶ 293-295.

**1[d]: “based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key”**

Ford discloses or renders obvious based on the risk score, permitting or denying, by the one or more servers, access to the file (e.g., based on the “risk

score,” servers determine user access permissions) by returning a decryption key for the file or withholding the decryption key (e.g., by “provid[ing] the receiver user with a decryption key if access is permitted”). Ex-1009, [00345].

Ford discloses servers that determine user access depending on the user’s DRR. *Id.* The servers “provide the receiver user with a decryption key” only if “access is permitted.” *Id.*, [00356]-[00357].

“If a user’s risk score is not higher than X” then access will not be allowed. *Id.*, [00345]. Different classifications of risk score are disclosed: “DRR may have a classification such as highly sensitive, low sensitivity, and the like.” *Id.*

When access is enabled, decryption keys are generated and sent with the file to users. *See id.*, [00346]. Ford’s secure management key facility determines user access permission before sending the key. *Id.* A POSITA would recognize or at least find obvious that this necessarily requires withholding the decryption key if conditions are not met. Ex-1003, ¶¶ 296-301.

**1[e]: “wherein said permitting or denying comprises when the risk score is less than a first threshold, returning the decryption key and providing full access to the file;”**

Ford discloses or renders obvious wherein said permitting or denying comprises: when the risk score is less than a first threshold (e.g., in “a matrix of DRR states,” when the “risk score” is “higher than X”), returning the decryption

key and providing full access to the file (e.g., grant “access” and “provide the receiver user with a decryption key if access is permitted”). Ex-1009, [00345], [00357].

Ford discloses granting a user file access based on the user’s DRR based on “a matrix of DRR states.” *Id.*, [00345]. If the “risk score” is “higher than X” then access is granted to “highly sensitive” information and the decryption key is released. *Id.*, [00345], [00356]-[00357].

Ford states that “higher than” is exemplary; implementing this teaching by having a risk score be higher than a threshold (i.e., trust is higher) vs. lower than a threshold (i.e., risk is higher) disclose the same functionality. At most, the difference between this limitation and Ford’s teachings is merely an obvious design choice to a POSITA: nothing more than the selection between two known and substantially similar alternatives. *Id.* [00345]; Ex-1003, ¶¶ 302-305.

**1[f]: “when the risk score is greater than a second threshold, withholding the decryption key; and”**

Ford discloses or renders obvious when the risk score is greater than a second threshold, (e.g., in the “matrix of DRR states,” “user’s risk score is not higher than X” and should not see even a “portion of the file”) withholding the decryption key (e.g., determine the “user should not be able to access the document.”). Ex-1009 [00345].

Ford discloses a “risk score” not satisfying a threshold of “X” and thus preventing access to a document. *Id.* The secure managed key facility withholds the decryption key if access is denied. *Id.*, [00357].

A POSITA would have understood and at least found it obvious that multiple thresholds are in the “matrix of DRR states” such that at least two thresholds are considered. *Id.*, [00350]; Ex-1003, ¶¶ 306-309.

**1[g]: “when the risk score is between the first threshold and the second threshold, returning the decryption key and providing limited access to the file.”**

Ford discloses or renders obvious when the risk score is between the first threshold and the second threshold (e.g., in the “matrix of DRR states,” a “second user” may access “only a portion of a file” based on “risk level”), returning a decryption key and providing limited access to the file (e.g., “restrict access by providing a second user only a portion of a file, rather than the whole file, based on the second user’s risk level”). Ex-1009, [00345], [00350].

Ford teaches using intermediate levels for documents in an “uncertain security state,” including based on user location and identity. *Id.*, [00430], [00345]-[00346]. Access may be determined “per [an] access policy,” resulting in the secure managed key facility providing the decryption key to the user. *Id.*, [00356]. Ex-1003, ¶¶ 310-312.

Ford's context sharing facility further discloses restricting sharing opportunities based on user conditions. Ex-1009, [00287]. The contextual sharing facility may restrict sharing information based upon the "parameters 4406, 4408, 4410, 4412, 4414" or other parameters described as the "**contextual environment 4404.**" *Id.*, [00288].

Ford discloses that users also may be granted access to "only a portion of the file." *Id.*, [00345], [00350], [00227]-[00229], [00241]-[00242]. A POSITA would have understood and at least found it obvious that Ford discloses at least two separate thresholds for (1) denying and (2) granting partial file access instead of granting full access. *See id.* Ex-1003, ¶¶ 313-315.

#### **4. Claim 2**

**"The method of claim 1, wherein said determining, by the one or more servers, the risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine learning,"**

Ford discloses or renders obvious the method of claim 1, wherein said determining, by the one or more servers, the risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine-learning (e.g., "devices having artificial intelligence"). Ex.1009, [00569].

Ford discloses that authentication may utilize “patterns of use” and discusses the applicability of its disclosures for “devices having artificial intelligence,” e.g., the use of machine learning. *Id.*, [00221], [00569]. A POSITA would have understood and at least found it obvious that this includes evaluating a file access request by machine learning, to determine a risk score. Ex-1003, ¶¶ 316-318.

### **5. Claim 3**

**3[pre]: “The method of claim 1, wherein the information regarding historical user behavior includes for each user of the plurality of users:”**

To the extent the preamble of claim 3 is found to be limiting, Ford discloses or renders obvious the method of claim 1, wherein the information regarding historical user behavior includes for each user of the plurality of users.

Ford further discloses information regarding historical user behavior. Ex-1009, [0055], [0087].

To the extent Ford does not disclose or suggest this limitation, it would have been obvious in light of Van Dijk. Van Dijk teaches baseline profiles stored within a database that includes historical user behavior. Van Dijk stored per-user historical records in database storage keyed by user identifier across the plurality of enterprise network users. Ex-1007, 4:44-47. Ex-1003, ¶¶ 319-323.

**3[a]: “historical data regarding general file access, including one or more of a number of files accessed by**

**the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time;”**

Ford discloses or renders obvious historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time (e.g., “user or device history, such as...pattern of use”).

Ford discloses using “historical” user information to determine access decisions, including “user or device history” and other “patterns of use.” Ex-1009, [00221]. It was well understood that a user’s “pattern of use” comprises the frequency, number, and type of files and applications used. Ex-1003, ¶¶ 324-326.

Ford’s “contextual environment 4404” analyzes “computing device 4406” “location 4408,” and “current activity state 4410,” among other factors. Ex-1009, [00287]. Ford’s contextual environment continuously gathers parameters to manage permissions. *Id.*, [00291]. A POSITA would understand that “continuously gather[ing]” contextual information, alongside analyzing a “pattern of use” disclosed historical data. Ex-1003, ¶¶ 327-328.

To the extent Ford does not disclose or suggest this limitation, it would have been obvious in light of Van Dijk. Van Dijk discloses historical data regarding file

access, including the number of files a user accessed over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time. Ex-1007, 6:38-7:4.

Van Dijk's access manager analyzes "previous browsing and other network access history" and compares "factors of the client device" with "prior results obtained from the same user," including number and type of prior access events and applications used to initiate access. *Id.*, *see also id.*, 1:13-25; 4:33-47. Ex-1003, ¶¶ 329-332.

**3[b]: "historical data regarding observed locations of the user; and"**

Ford discloses or renders obvious historical data regarding observed locations of the user (e.g., "determining the geographical location of a person using the device"): Ford's "location-based security facility 290" provides file access based on location of the device requesting the file or resource. Ex-1009, [00220]. The user's location informs the risk profile. *Id.*, [00286].

Ford further discloses "**contextual environment 4404**" that includes access locations: device "location 4408" and "proximity 4414" *Id.*, [00287]-[00292].

To the extent that Ford does not disclose or suggest this limitation, it would have been obvious in light of Van Dijk, which discloses adaptive authentication techniques comparing login attempt information including login location. Ex-1007,

1:13-25. Current access location is compared to typical user locations, teaching historical data regarding observed user locations. Ex-1003, ¶¶ 333-339.

**3[c]: “historical data regarding observed times at which the user accesses files.”**

Ford discloses or renders obvious historical data regarding observed times at which the user accesses files (e.g., providing access for a limited time). Ex-1009, [00187]. Ford discusses “a policy, based on time-based factors” for file access. *Id.* Additionally, Ford discloses user historical access through the document history. *Id.*, [00161]. Ford further discloses a “contextual environment 4404” that includes access times. *Id.*, [00287]-[00292]. Ex-1003, ¶¶ 340-343.

A POSITA would have understood and found obvious, given Ford’s disclosure of the use of historical information, to include times at which a user accesses files in the historical user behavior. Ex-1003, ¶ 344.

To the extent that Ford does not disclose or suggest this limitation, it would have been obvious in light of Van Dijk, which discloses utilizing historical data, including observed time of file access, e.g. timestamps from request 11 stored by Processor 22, in determining file access. Ex-1007, 1:17-25, 5:17-20, 4:29-47. Ex-1003, ¶¶ 345-347.

**6. Claim 4**

**“The method of claim 1, wherein the observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address contained in the first access request.”**

Ford discloses or renders obvious the observed data includes a current location of the first user (e.g., user’s “DRR” is based on “current location” of the user) as determined based on a source Internet Protocol (IP) address contained in the file access request (e.g., using a “trusted IP address”). Ex-1009, [00345].

User location information includes, e.g., “network conditions 4412 (e.g., connected to a trusted network, using a trusted IP address[.]).” *Id.*, [00287]. Ford further teaches access rules based on IP addresses. *Id.*, [00371]; Ex-1003, ¶¶ 348-350.

**7. Claim 5**

**“The method of claim 1, wherein the observed data includes a status indicative of whether the connection through which the first user initiated the file access request is trusted or untrusted.”**

Ford discloses or renders obvious the observed data includes a status indicative of whether the connection through which the first user initiated the file access request is trusted or untrusted (e.g., “security level provided by a network connection”). Ex-1009, [00367].

Ford teaches contextual file protection, including the network security level. *Id.* Authorization may be determined by network connectivity, including “a trusted network” *Id.*, [00157]. User access may be prevented, e.g., through cellular networks. *Id.* Users connecting through a “trusted network” may be granted authorization, but not through a cellular network. *Id. See also id.*, [00287]-[00289]. Ex-1003, ¶¶ 351-354.

#### 8. Claim 6

**“The method of claim 5, wherein the connection is trusted when the first user is on the enterprise network or accessing the enterprise network remotely via a secure connection.”**

Ford discloses or renders obvious the connection is trusted when the first user is on the enterprise network or accessing the enterprise network remotely via a secure connection (e.g., when on the “enterprise network” or “trusted network”). Ex-1009, [00157].

Ford contemplates network connection for access control, describing connectivity through “enterprise,” “trusted,” “WiFi network, and the like” as trusted network connections. *Id.*, [00157], [00367]. *See also id.*, [00287]-[00289]. Ex-1003, ¶¶ 355-358.

#### 9. Claim 7

**“The method of claim 5, wherein the connection is untrusted when the first user is not on the enterprise**

**network or accessing the enterprise network remotely  
via an insecure connection.”**

Ford discloses or renders obvious the connection is untrusted when the first user is not on the enterprise network or accessing the enterprise network remotely via an insecure connection (e.g., use “may not be authorized” “outside their home” or “outside a small geographic area around an office around an enterprise...and the like”). Ex-1009, [00157].

Access may be denied or limited when not connected through the “enterprise,” “trusted,” or “like” connections, including cellular connections. *Id.* See also *id.*, [00287]-[00289] (constraining access of remote users). Ex-1003, ¶¶ 359-363.

**10. Claim 8**

**“The method of claim 1, wherein the encrypted form  
involves the file being encapsulated in a cryptographic  
wrapper.”**

Ford discloses or renders obvious the encrypted form involves the file being encapsulated in a cryptographic wrapper (e.g., content uses “end-to-end encryption” and is “encrypted and remain[s] encrypted/protected for the rest of its lifecycle”; data encrypted using a “customer key” and “system master key”). Ex-1009, [00375].

Ford discloses encrypting stored content includes implementing “end-to-end encryption” where data is encrypted through its lifecycle. *Id.* Customer managed keys provide control of encryption keys, and “both the system-provided keys and the customer keys are needed in order to access the data.” *Id.*, [00362]. Because this end-to-end encryption means a cryptographic key is required to decrypt and access the content, a POSITA would have understood Ford discloses or renders obvious this limitation. *See id.*; Ex-1003, ¶¶ 364-368.

#### **11. Claims 9-15**

All limitations of claims 9-15 are presented in claims 1-8, except as described below. *See supra* §VIII.A.12. Claims 9-15 are disclosed or rendered obvious by Ford in combination with Van Dijk. Ex-1003, ¶¶ 369; 373-386.

##### **9[pre]/14[a]:**

Ford discloses or renders obvious a non-transitory computer-readable storage medium limitation of claim 9[pre]. Ex-1009, [00560]. Ford further discloses or renders obvious the system limitation of claim 14[a]. *Id.*, [00558]. Ford further discloses implementing these teachings in an enterprise *Id.*; Ex-1003, ¶¶ 370-372.

**E. Ground 5: Combining Ford and Van Dijk with Kirti Renders Claims 2, 10-13 Obvious**

**1. Motivation to Combine**

A POSITA would have been motivated to combine Ford and Van Dijk with Kirti with a reasonable expectation of success. These are analogous art—server-based access control systems evaluating risk from user behavior. They address the need to dynamically assess a requesting user’s current behavior against behavioral patterns.

Ford teaches server-based multi-factor authentication including risk-based questioning and detection based on user or device history. Ex-1009, [00221]. Van Dijk similarly teaches “access control systems that mediate access to derivatives of sensitive data,” including an adaptive authentication server. Ex-1007, 1:52-53; 6:45-49. Kirti likewise teaches activity data collected from various parameters over time used with machine learning to generate user behavior profiles. Ex-1008, 13:2-42.

Kirti’s machine-learning techniques applied to Ford’s risk-based access control framework in combination with Van Dijk provide a more accurate, adaptive model of user behavior to analyze access requests. Ex-1003, ¶¶ 387-390.

Aggregating user activity information enables the system to establish behavioral baselines, where machine learning detects deviations from baseline. Ex-

1008, 12:28-57; 13:2-42. Kirti discloses that machine learning algorithms are applied to user activity data to generate a threat score. *Id.*, 12:58-13:27.

Because Ford and Van Dijk teach collecting and using behavioral and contextual history, including user or device history and patterns of use, implementing Kirti's machine learning techniques within Ford's risk scoring framework to develop the underlying user behavior model would have been a straightforward modification. Ex-1009, [00221]; Ex-1007, 4:33-43. Similar to Ford's DRR or Van Dijk's "Overall Risk" calculation, Kirti teaches applying machine learning algorithms trained on historical activity data to generate a numerical risk score reflecting deviation from normal user behavior. Ex-1003, ¶¶ 391-393.

A POSITA would have understood that Ford's DRR engine could be implemented with Kirti's machine-learning behavioral model, such that the risk score reflects the degree to which the access request conforms to behavioral patterns. A POSITA would have found it straightforward and advantageous to apply Kirti's machine learning teachings to the Ford-Van Dijk combination, and would have known such a combination would predictably work. Ex-1003, ¶¶ 394-395.

## **2. Claims 2, 10-13**

As discussed above, Kirti discloses machine learning as required by claims 2, 10-13. *See supra* §VIII.B.3.

### **F. Ground 6: Combining Ford and Van Dijk with Bleckmann Renders Claims 1-15 Obvious**

#### **1. Motivation to Combine**

A POSITA would have been motivated to combine Ford and Van Dijk with Bleckmann with a reasonable expectation of success. These are analogous art—server-based access control systems evaluating risk from user behavior—structured, threshold-based access policies producing outcomes based on trust or risk.

Ford’s secure exchange server implements risk-based detection based on a user or device history. Ex-1009, [00221]. Van Dijk similarly teaches “access control systems that mediate access to derivatives of sensitive data,” including an adaptive authentication server. Ex-1007, 1:52-53; 6:45-49. Bleckmann similarly teaches a trust score-based access control system in which a policy controls access to a resource based on the trust score generated for the requesting computer. Ex-1006, [0042]. Ex-1003, ¶¶ 397-399.

A POSITA would have been motivated to apply Bleckmann’s two-threshold policy framework to a Ford-Van Dijk combination allowing the risk-based access

control system to advantageously include a structured, tiered access architecture that produces differentiated outcomes depending on the level of confidence in the requesting user, rather than relying solely on a binary grant or deny determination. Ford's DRR drives risk-based access decisions. To the extent it does not teach a two-threshold, three-outcome policy keyed to risk levels, Bleckmann fills this gap. Bleckmann discloses a policy including two threshold scores controlling resource access: if the trust score exceeds the first threshold, full access is granted; if the trust score falls between the first and second threshold, partial is granted; and if the trust score falls below the second threshold, access is denied. Ex-1006, [0043].

Because both Ford and Van Dijk teach computing a dynamic risk rating or Overall Risk based on behavioral and contextual signals associated with the access request, implementing Bleckmann's two-threshold policy framework within Ford and Van Dijk would have been a straightforward modification. A POSITA would have understood that Ford's DRR could be evaluated against two defined threshold values, as Bleckmann teaches, where the access control determination produces three discrete outcomes: full access when the rating satisfies the higher threshold, partial access when it falls between the two thresholds, and denial when it falls below the lower threshold. A POSITA would have found it straightforward and advantageous to apply Bleckmann's two-threshold access control policy to Ford

and Van Dijk's risk-based access control system, and would have known such a combination would predictably work. Ex-1003, ¶¶ 400-403.

## **2. Claim 1**

Bleckmann discloses a first and second threshold, as well as providing limited access to the file, as required by claim 1 for the same reasons discussed above. *See supra* §VIII.A.4.

A POSITA would find it obvious to implement Bleckmann's Threshold scores with Ford and Van Dijk. Ford discloses three tiers of access: grant, deny, or limited access. Ex-1006, [0043]; Ex-1009, [00345], [00350]. Bleckmann's Threshold scores provide a POSITA with values to replace "X" such that Ford's DRR falls into one of the three outcomes. Ex-1003, ¶¶ 404-407.

## **G. Ground 7: Combining Ford, Van Dijk, Bleckmann, and Kirti Renders Claims 2, 10-13 Obvious**

These limitations are met for the same reasons as in Ground 5. *See supra* §VIII.E. A POSITA would have been motivated to combine Ford, Van Dijk, and Kirti for the same reasons as above; Bleckmann does not change the motivation to combine. Ex-1003, ¶¶ 408-409.

## **IX. CONCLUSION**

Accordingly, the Board should institute IPR and cancel the challenged claims.

Dated: September 15, 2026

12275 El Camino Real, Ste 100  
San Diego, California, 92130  
Phone: (858) 720-8900  
Fax: (858) 509-3691

Respectfully submitted,

SHEPPARD, MULLIN,  
RICHTER & HAMPTON LLP

/s/ Thomas Millikan

Thomas Millikan (Reg. No. 72,316)

Back-up Counsel

Joseph P. Reid (Reg. No. 72,317)

Andrew Klein (*PHV* forthcoming)

Nicholas Lipperd (Reg. No. 83,084)

Attorneys for Netskope, Inc.

**LISTING OF CHALLENGED CLAIMS**

**1[pre]:** A method comprising:

**1[a]:** obtaining and storing, by one or more servers associated with an enterprise network, information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users;

**1[b]:** receiving, by the one or more servers, a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network in encrypted form;

**1[c]:** responsive to receipt of the file access request, determining, by the one or more servers, a risk score for the first user based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request; and

**1[d]:** based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key wherein said permitting or denying comprises:

**1[e]:** when the risk score is less than a first threshold, returning the decryption key and providing full access to the file;

**1[f]:** when the risk score is greater than a second threshold, withholding the decryption key; and

**1[g]:** when the risk score is between the first threshold and the second threshold, returning the decryption key and providing limited access to the file.

**2:** The method of claim 1, wherein said determining, by the one or more servers, the risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine-learning.

**3[pre]:** The method of claim 1, wherein the information regarding historical user behavior includes for each user of the plurality of users:

**3[a]:** historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time;

**3[b]:** historical data regarding observed locations of the user; and

**3[c]:** historical data regarding observed times at which the user accesses files.

**4:** The method of claim 1, wherein the observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address contained in the file access request.

**5:** The method of claim 1, wherein the observed data includes a status indicative of whether the connection through which the first user initiated the file access request is trusted or untrusted.

**6:** The method of claim 5, wherein the connection is trusted when the first user is on the enterprise network or accessing the enterprise network remotely via a secure connection.

**7:** The method of claim 5, wherein the connection is untrusted when the first user is not on the enterprise network or accessing the enterprise network remotely via an insecure connection.

**8:** The method of claim 1, wherein the encrypted form involves the file being encapsulated in a cryptographic wrapper.

**9[pre]:** A non-transitory computer-readable storage medium embodying a set of instructions, which when executed by one or more

processors of one or more servers associated with an enterprise network, causes the one or more processors to perform a method comprising:

**9[a]:** obtaining and storing information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users, wherein the information regarding historical user behavior includes for each user of the plurality of users:

**9[b]:** historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time;

**9[c]:** historical data regarding observed locations of the user; and

**9[d]:** historical data regarding observed times at which the user accesses files;

**9[e]:** receiving a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network in encrypted form;

**9[f]:** responsive to receipt of the file access request, determining a risk score for the first user based on a plurality of factors, including information

regarding historical user behavior, the file access request and observed data determined based on the file access request; and

**9[g]:** based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key; wherein said permitting or denying comprises:

**9[h]:** when the risk score is less than a first threshold, returning the decryption key and providing full access to the file;

**9[i]:** when the risk score is greater than a second threshold, withholding the decryption key; and

**9[j]:** when the risk score is between the first threshold and the second threshold, returning the decryption key and providing limited access to the file.

**10:** The non-transitory computer-readable storage medium of claim 9, wherein determining the risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine-learning.

**11:** The non-transitory computer-readable storage medium claim 10, wherein the observed data includes a current location of the first user as

determined based on a source Internet Protocol (IP) address contained in the file access request.

**12:** The non-transitory computer-readable storage medium claim 10, wherein the observed data includes a status indicative of whether the connection through which the first user initiated the file access request is trusted or untrusted.

**13:** The non-transitory computer-readable storage medium claim 10, wherein the encrypted form involves the 15 file being encapsulated in a cryptographic wrapper.

**14[a]:** A system, the system comprising: one or more processors; and a non-transitory computer-readable storage medium coupled to the one or more processors and embodying a set of instructions, which when executed by the one or more processors of one or more servers associated with an enterprise network, causes the one or more processors to perform a method comprising:

**14[b]:** obtaining and storing information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users;

**14[c]:** receiving a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network in encrypted form;

**14[d]:** responsive to receipt of the file access request, determining a risk score for the first user based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request; and

**14[e]:** based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key, wherein said permitting or denying comprises:

**14[f]:** when the risk score is less than a first threshold, returning the decryption key and providing full access to the file;

**14[g]:** when the risk score is greater than a second threshold, withholding the decryption key; and

**14[h]:** when the risk score is between the first threshold and the second threshold, returning the decryption key and providing limited access to the file.

**15[a]:** The system of claim 14, wherein the information regarding historical user behavior includes for each user of the plurality of users: historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time;

**15[b]:** historical data regarding observed locations of the user; and

**15[c]:** historical data regarding observed times at which the user accesses files.

**CERTIFICATE OF WORD COUNT UNDER 37 CFR §42.24(D)**

Under 37 C.F.R. §42.24(d), the undersigned certifies that the word count for this Petition for *Inter Partes* Review totals 13,900 words, excluding the parts exempted by 37 C.F.R. §42.24(a). The word count was made using the built-in word count function in the Microsoft® Word 365 software used to prepare this document.

Dated: September 15, 2026

12275 El Camino Real, Ste 100  
San Diego, California, 92130  
Phone: (858) 720-8900  
Fax: (858) 509-3691

Respectfully submitted,

SHEPPARD, MULLIN,  
RICHTER & HAMPTON LLP

/s/ Thomas Millikan

Thomas Millikan (Reg. No. 72,316)

Back-up Counsel

Joseph P. Reid (Reg. No. 72, 317)

Andrew Klein (*PHV* forthcoming)

Nicholas Lipperd (Reg. No. 83,084)

Attorneys for Netskope, Inc.

**CERTIFICATE OF SERVICE**

The undersigned hereby certifies that true copies of this PETITION FOR *INTER PARTES* REVIEW and supporting materials (Exhibits 1001-1003, 1005-1011, 1013-1019 and Power of Attorney) have been served via USPS Express Mail and electronically on counsel for patent owner as follows:

GISH PLLC  
50 California Street, Suite 1500  
San Francisco, CA 94111  
UNITED STATES  
ryan@gishpllc.com

In addition, the undersigned certifies that a true copy of the petition and supporting materials have been served on Patent Owner via email to its legal counsel:

David A. Nelson – davidnelson@quinnemanuel.com  
Athena D. Dalton – athenadalton@quinnemanuel.com  
Harrison Rose – harrisonrose@quinnemanuel.com  
Luiz Miranda – luizmiranda@quinnemanuel.com  
Alexander Rudis – alexanderrudis@quinnemanuel.com  
Jeff Gerchick – jeffgerchick@quinnemanuel.com  
Andrew M. Holmes – drewholmes@quinnemanuel.com  
Ognjen Zivojnovic – ogizivojnovic@quinnemanuel.com  
Justin Sorenson – justinsorensen@quinnemanuel.com

Andrew D. Gish – andrew@gishpllc.com  
Christopher Gerson – chris.gerson@gishpllc.com  
Josef Schenker – josef.schenker@gishpllc.com

Dated: September 15, 2026

12275 El Camino Real, Ste 100  
San Diego, California, 92130  
Phone: (858) 720-8900  
Fax: (858) 509-3691

Respectfully submitted,

SHEPPARD, MULLIN,  
RICHTER & HAMPTON LLP

/s/ Thomas Millikan

Thomas Millikan (Reg. No. 72,316)

Back-up Counsel

Joseph P. Reid (Reg. No. 72, 317)

Andrew Klein (*PHV* forthcoming)

Nicholas Lipperd (Reg. No. 83,084)

Attorneys for Netskope, Inc.