UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/535,574	09/22/2020	10783228	SEI-10740-02	5886

24956 7590 09/02/2020

MATTINGLY & MALUR, PC
1800 DIAGONAL ROAD
SUITE 210
ALEXANDRIA, VA 22314

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

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

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

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

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Masayuki HIRABAYASHI, Osaka, JAPAN;
Maxell, Ltd., Kyoto, JAPAN;
Yasunobu HASHIMOTO, Osaka, JAPAN;
Kazuhiko YOSHIZAWA, Osaka, JAPAN;

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

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

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

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

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

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

24956 7590 06/10/2020
MATTINGLY & MALUR, PC
1800 DIAGONAL ROAD
SUITE 210
ALEXANDRIA, VA 22314

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

Certificate of Mailing or Transmission

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

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/535,574	08/08/2019	Masayuki HIRABAYASHI	SEI-10740-02	5886

TITLE OF INVENTION: INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	09/10/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
TRUONG, THANHNGA B	2498	726-005000

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

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

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

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

1 Mattingly & Malur, PC
2
3

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

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

(A) NAME OF ASSIGNEE: Maxell, Ltd.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Kyoto, Japan

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

4a. Fees submitted: ☒ Issue Fee ❑ Publication Fee (if required) ❑ Advance Order - # of Copies _____

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

☒ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 501417

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

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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

Authorized Signature /John R. Mattingly/ Date August 14, 2020

Typed or printed name John R. Mattingly Registration No. 30293

IPR2025-01313; Samsung
Ex. 1002 - Page 2

Electronic Patent Application Fee Transmittal

Application Number:	16535574
Filing Date:	08-Aug-2019
Title of Invention:	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD
First Named Inventor/Applicant Name:	Masayuki HIRABAYASHI
Filer:	John Roberts Mattingly/Krista Hargrove
Attorney Docket Number:	SEI-10740-02

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	1501	1	1000	1000

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1000**

Electronic Acknowledgement Receipt	
EFS ID:	40283238
Application Number:	16535574
International Application Number:	
Confirmation Number:	5886
Title of Invention:	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD
First Named Inventor/Applicant Name:	Masayuki HIRABAYASHI
Customer Number:	24956
Filer:	John Roberts Mattingly/Krista Hargrove
Filer Authorized By:	John Roberts Mattingly
Attorney Docket Number:	SEI-10740-02
Receipt Date:	14-AUG-2020
Filing Date:	08-AUG-2019
Time Stamp:	09:00:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1000
RAM confirmation Number	E20208D000264291
Deposit Account	501417
Authorized User	Krista Hargrove
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	10740-02-issuefeetransmittal.pdf	89579 00358b139eb28ecf5e2aed51f0aae11f2d6104c5	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30738 4279f591af5b90caf1fc0369b3c62fd75d5f7333	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	120317		

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

24956 7590 06/10/2020

MATTINGLY & MALUR, PC
1800 DIAGONAL ROAD
SUITE 210
ALEXANDRIA, VA 22314

EXAMINER
TRUONG, THANHNGA B

ART UNIT	PAPER NUMBER
2498	

DATE MAILED: 06/10/2020

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/535,574	08/08/2019	Masayuki HIRABAYASHI	SEI-10740-02	5886

TITLE OF INVENTION: INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	09/10/2020

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

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

HOW TO REPLY TO THIS NOTICE:

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

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

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

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

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

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

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

IPR2025-01313; Samsung
Ex. 1002 - Page 7

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

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

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

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

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

24956 7590 06/10/2020
MATTINGLY & MALUR, PC
1800 DIAGONAL ROAD
SUITE 210
ALEXANDRIA, VA 22314

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

Certificate of Mailing or Transmission

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

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/535,574	08/08/2019	Masayuki HIRABAYASHI	SEI-10740-02	5886

TITLE OF INVENTION: INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	09/10/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
TRUONG, THANHNGA B	2498	726-005000

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

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

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

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

1_____
2_____
3_____

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

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

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

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

4a. Fees submitted: ❑Issue Fee ❑Publication Fee (if required) ❑Advance Order - # of Copies _____

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

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

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

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

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

IPR2025-01313; Samsung
Ex. 1002 - Page 8

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/535,574	08/08/2019	Masayuki HIRABAYASHI	SEI-10740-02	5886

24956 7590 06/10/2020

MATTINGLY & MALUR, PC
1800 DIAGONAL ROAD
SUITE 210
ALEXANDRIA, VA 22314

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	**PAPER NUMBER**
2498	

DATE MAILED: 06/10/2020

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

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

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

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

PTOL-85 (Rev. 02/11)

IPR2025-01313; Samsung
Ex. 1002 - Page 9

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

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

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 16/535,574	Applicant(s) HIRABAYASHI et al.	
	Examiner THANHNGA B TRUONG	Art Unit 2498	AIA (FITF) Status Yes

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

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

1. ☑ This communication is responsive to 5/21/20.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

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

3. ☑ The allowed claim(s) is/are 1-11 and 19-29 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information , please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

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

   Certified copies:

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

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

   * Certified copies not received: _____ .

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

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

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

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

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☑ Interview Summary (PTO-413), Paper No./Mail Date. 6/5/20.
5. ☑ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/THANHNGA B TRUONG/
Primary Examiner, Art Unit 2498

DETAILED ACTION

1. Applicant's amendment filed on May 21, 2020 has been entered. Claims 1-29 are pending.

Notice of Pre-AIA or AIA Status

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

Examiner's Amendment

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given by Mr. John R. Mattingly on June 5, 2020.

CLAIMS:

Please cancel claims 12-18.

Allowable Subject Matter

4. Claims 1-11 and 19-29 are allowed for the reasons argued by Applicants on pages 14-15 of Remarks, filed May 21, 2020 and Interview Summary conducted on June 5, 2020. None of the prior art of record, either taken by itself or in any combination, would have anticipated or made obvious the claimed invention of the present application at or before the date it was effectively filed.

In addition, the prior arts of record Aoki; Takahiro et al (US 9373047 B2), CANTRELL; Tame; Gavin Randall (US 20100131414 A1); Haddad; Waleed Sami (US 9314193 B2); Stucker; Brian (US 8218459 B1); and LeBeau; Michael J et al (US 8667562 B2), do not disclose these specific limitations of *acquiring dynamic biometric information from a body of a user by a dynamic biometric information acquisition sensor of a first device; transmitting the acquired dynamic biometric information through a first communication interface of the first device to a second device; acquiring static biometric information by a static biometric information acquisition sensor of the second device; performing user authentication to obtain an authentication result based on the acquired*

static biometric information; performing communication with a second communication interface relating to the authentication result with the first communication interface and receiving the dynamic biometric information transmitted from the first communication interface; performing communication relating to the authentication result between the first communication interface and the second communication interface and executing an unlock operation to unlock the first device in response to the communication relating to the authentication result, acquiring the dynamic biometric information from the dynamic biometric information acquisition sensor of the first device after unlocking, and maintaining the unlocked state during a condition that the dynamic biometric information can be acquired; receiving the dynamic biometric information by the second device via communication between the first communication interface and the second communication interface; and displaying on a display screen information based on a state of the user that is determined using the received dynamic biometric information (emphasis added), as set forth in claim 19 and similar to claim 1.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to THANHNGA B TRUONG whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Yin-Chen Shaw can be reached on 571-272-8593. The central fax number for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/THANHNGA B TRUONG/

Primary Examiner, Art Unit 2498

June 7, 2020

Examiner-Initiated Interview Summary	Application No. 16/535,574	Applicant(s) HIRABAYASHI et al.	
	Examiner THANHNGA B TRUONG	Art Unit 2498	AIA (FITF) Status Yes

All participants (applicant, applicant's representative, PTO personnel):

(1) THANHNGA B. TRUONG. (3) _____.

(2) Mr. John R. Mattingly. (4) _____.

Date of Interview: 05 June 2020.

Type: ☑ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☑ No.
If Yes, brief description: _____.

Issues Discussed ☐ 101 ☐ 112 ☐ 102 ☐ 103 ☑ Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: 12-18.

Identification of prior art discussed: N/A.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant's Representative and Examiner has discussed on the withdrawn claims 12-18. Examiner has proposed to cancel the withdrawn claims 12-18 in order to move the application in condition for allowance. Applicant has agreed and authorized Examiner to do the Examiner's Amendment..

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

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

☐ Attachment

	/THANHNGA B TRUONG/ Primary Examiner, Art Unit 2498

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/535,574	HIRABAYASHI et al.
	Examiner	Art Unit
	THANHNGA B TRUONG	2498

CPC - Searched*		
Symbol	Date	Examiner
G05B19/00; H04L9/32; G06K9/00; H04L12/16; H04L9/32; G06F21/32; G06F21/12; G06F21/31; G06F21/35; G06F21/60; G06F21/62; H04W12/06	02/17/2020; 6/7/20	TBT

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

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

Search Notes		
Search Notes	Date	Examiner
Inventor Name Searched; Assignee Searched	02/16/2020; 02/17/2020; 6/7/20	TBT
TEXT Searched; EAST Searched; NPL Searched - Google/Patents and Scholar	02/17/2020; 6/7/20	TBT

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
G05B/H04L/G06K/G06F/H04W	G05B19/00; H04L9/32; G06K9/00; H04L12/16; H04L9/32; G06F21/32; G06F21/12; G06F21/31; G06F21/35; G06F21/60; G06F21/62; H04W12/06	06/07/2020	TBT

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/535,574	HIRABAYASHI et al.
	Examiner	**Art Unit**
	THANHNGA B TRUONG	2498

CPC							
Symbol						**Type**	**Version**
G06F	/	21	/	32		F	2013-01-01
G06F	/	21	/	12		I	2013-01-01
G06F	/	21	/	35		I	2013-01-01
G06F	/	21	/	6218		I	2013-01-01
H04W	/	12	/	06		I	2013-01-01
G06F	/	21	/	31		I	2013-01-01
G06F	/	21	/	604		I	2013-01-01
G06F	/	2221	/	2105		A	2013-01-01

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

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	22	
/THANHNGA B TRUONG/ Primary Examiner, Art Unit 2498	07 June 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	6

U.S. Patent and Trademark Office — Part of Paper No.: 20200607

IPR2025-01313; Samsung
Ex. 1002 - Page 17

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/535,574	HIRABAYASHI et al.
	Examiner	**Art Unit**
	THANHNGA B TRUONG	2498

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06F	/	21	/	32

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

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

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	22	
/THANHNGA B TRUONG/ Primary Examiner, Art Unit 2498	07 June 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	6

U.S. Patent and Trademark Office — Part of Paper No.: 20200607

IPR2025-01313; Samsung
Ex. 1002 - Page 18

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/535,574	HIRABAYASHI et al.
	Examiner	**Art Unit**
	THANHNGA B TRUONG	2498

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

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	10	10	12	19	21	28								
2	2	11	11	13	20	22	29								
3	3		12	14	21										
4	4		13	15	22										
5	5		14	16	23										
6	6		15	17	24										
7	7		16	18	25										
8	8		17	19	26										
9	9		18	20	27										

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	22	
/THANHNGA B TRUONG/ Primary Examiner, Art Unit 2498	07 June 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	6

U.S. Patent and Trademark Office — Part of Paper No.: 20200607

IPR2025-01313; Samsung
Ex. 1002 - Page 19

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/535,574	HIRABAYASHI et al.
	Examiner	Art Unit
	THANHNGA B TRUONG	2498

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

CLAIMS

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

CLAIM		DATE								
Final	Original	10/09/2019	02/15/2020	06/07/2020						
1	1	÷	✓	=						
2	2	÷	✓	=						
3	3	÷	✓	=						
4	4	÷	✓	=						
5	5	÷	✓	=						
6	6	÷	✓	=						
7	7	÷	✓	=						
8	8	÷	✓	=						
9	9	÷	✓	=						
10	10	÷	✓	=						
11	11	÷	✓	=						
	12	÷	N	-						
	13	÷	N	-						
	14	÷	N	-						
	15	÷	N	-						
	16	÷	N	-						
	17	÷	N	-						
	18	÷	N	-						
12	19	÷	✓	=						
13	20	÷	✓	=						
14	21	÷	✓	=						
15	22	÷	✓	=						
16	23	÷	✓	=						
17	24	÷	✓	=						
18	25	÷	✓	=						
19	26	÷	✓	=						
20	27	÷	✓	=						
21	28	÷	✓	=						
22	29	÷	✓	=						

Google transmitting the acquired dynamic biometric information through a first c

Sign in

All News Shopping Images More Settings Tools

About 104,000 results (0.55 seconds)

www.google.com/patents/CN102937938A?cl=en

Fingerprint processing device as well as control method and ...

The invention discloses a fingerprint processing device as well as a control method ... of: acquiring user fingerprint information through a first transmission channel; ... the upper machine through the second transmission channel, wherein the first ... keyboard communication-type USB interfaces, and thus the communication ...
App. - Filed Nov 29, 2012 - Published Feb 20, 2013 - 杨春林 - 北京天诚盛业科技有限公司
Overview · Related · Discuss

www.google.com/patents/US9342674

Man-machine interface for controlling access to electronic ...

After requesting the user authentication, the first device detects biometric information associated with the user with the one or more biometric sensors.
Grant - Filed Mar 5, 2015 - Issued May 17, 2016 - David S. Abdallah - Apple Inc.
Overview · Related · Discuss

www.google.com/patents/US20150379322

Method and apparatus for communication using fingerprint input

The program includes first instructions for detecting a fingerprint information input, second instructions for changing a communication mode according to the ...
App. - Filed Jun 30, 2015 - Published Dec 31, 2015 - Suha Yoon - Samsung Electronics Co., Ltd.
Overview · Related · Discuss

www.google.com/patents/US8260350

Embedded biometrics in telecommunication devices for feature ...



One or more biometric characteristics are detected when a request to place an outgoing ... call is a verbal request, one or more biometric voice samples are obtained. ... and transmitted from the first telecommunication device to the outgoing call ... a graphical user interface, an icon, and a ringtone are generated at a second ...
Grant - Filed Oct 24, 2008 - Issued Sep 4, 2012 - Peeyush Jaiswal - International Business Machines Corporation
Overview · Related · Discuss

www.google.com/patents/US8942433

System for scheduling, recordation and biometric validation ...

A system for scheduling and recording interpersonal interactions using biometric validation to verify user identity and assure user conformance with preselected ...
Grant - Filed Dec 3, 2007 - Issued Jan 27, 2015 - Luke Small - Luke Small
Overview · Related · Discuss

www.google.com/patents/US8151334

Communication card for mobile network devices and ...



A removable communication card for mobile network devices, respectively a ... card includes a network interface module for bidirectional transmission of data with a ... The PIN is either checked and verified using locally stored identification data for ... first biometric feature of the one user with the stored biometric information ...
Grant - Filed Oct 7, 2005 - Issued Apr 3, 2012 - Eric Lauper - Swisscom Ag
Overview · Related · Discuss

www.google.com/patents/WO2017219925A1?cl=en

Information sending method and apparatus, and computer ...

The method comprises: obtaining to-be-recognized voice characteristic corresponding to to-be-recognized voice information of a first user (201); determining ...
App. - Filed Jun 16, 2017 - Published Dec 28, 2017 - 马骁龙 - 深圳市中兴微电子技术有限公司
Overview · Related · Discuss

www.google.com/patents/US9426660

EHF secure communication device

A communication device employs a contactless secure communication interface to transmit and receive data with a computing device using close proximity ...
Grant - Filed Dec 19, 2013 - Issued Aug 23, 2016 - Gary Davis McCormack - Keyssa, Inc.
Overview · Related · Discuss

www.google.com/patents/US20140157384

Biometric Authentication



For example, a first party using first party system 104 may be engaged in an ... using biometric data capture devices that may be coupled to first party system 104. ... The voice print may also be transmitted and converted into an audio signal and ... biometric information to the requesting second party via network interface 266.
App. - Filed May 3, 2013 - Published Jun 5, 2014 - Benjamin J. Stern - At&T Intellectual Property I, L.P.
Overview · Related · Discuss

www.google.com/patents/US20150190094

Sensor device and electronic device having the same

The mobile electronic device includes at least one processor, a display module electrically connected with the at least one processor, a communication module ...
App. - Filed Jan 6, 2015 - Published Jul 9, 2015 - Seung-Hoon Lee - Samsung Electronics Co., Ltd.
Overview · Related · Discuss

Google performing communication relating to the authentication result between t

All News Shopping Videos More Settings Tools

About 32,600 results (0.70 seconds)

www.google.com/patents/US20160316367

Method and system for secure peer-to-peer mobile communications



Executing these cryptographic based functions entirely in the token have ... The present invention relates to tokens for unlocking secure systems or data. ... the first mobile communications device, unlocking first authentication data of ... authentication data through the interface in the second mobile device, ...

App. - Filed Apr 22, 2016 - Published Oct 27, 2016 - Kenneth Hugh Rose - Kenneth Hugh Rose

Overview · Related · Discuss

www.google.com/patents/US8667562

Input to locked computing device



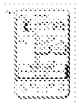
The method further includes executing in response to the user inputs to unlock the device an unlocking operation to convert the device from a locked state to an ...

Grant - Filed Sep 30, 2011 - Issued Mar 4, 2014 - Michael J LeBeau - Google Inc.

Overview · Related · Discuss

www.google.com/patents/US20130219346

Input to Locked Computing Device



The at least one command executes so that results of executing the at least one command are first displayed on the device to a user ... be embodied in, among other things, a method that includes receiving at a computing device that is ... executing in response to the user inputs to unlock the device an unlocking operation by ...

App. - Filed Mar 19, 2013 - Published Aug 22, 2013 - Michael J. Lebeau - Michael J. Lebeau

Overview · Related · Discuss

www.google.com/patents/WO2006098690A1?cl=en

A method for unlocking a lock by a lock device enabled for ...



A method is presented for unlocking a lock by a lock device (140) enabled for ... the lock device; b) determining a wireless communication address of the key device; ... eva luation result from said evaluating step c) , wherein a match between the ... stamp in the authentication data updating information received, said first time ...

App. - Filed Mar 17, 2006 - Published Sep 21, 2006 - Olle Bliding - Phoniro Ab

Overview · Related · Discuss

www.google.com/patents/US20130333020

Method and Apparatus for Unlocking an Electronic Device that ...



The method further includes the electronic device determining that the first pattern input matches an unlocking pattern associated with a first ...

App. - Filed Jun 8, 2012 - Published Dec 12, 2013 - Rupalee A. Deshpande - Motorola Mobility, Inc.

Overview · Related · Discuss

www.google.com/patents/US20120328096

Two-way authentication between two communication endpoints ...



Techniques for two-way authentication between two communication endpoints (e.g., . Here, only the first device gets authenticated and not the second device

App. - Filed Sep 7, 2012 - Published Dec 27, 2012 - Rahul C. Shah - Shah Rahul C

Overview · Related · Discuss

www.google.com/patents/EP2811724A1?cl=en

Mobile wireless communications device providing near field ...

IPR2025-01313; Samsung
Ex. 1002 - Page 23



A mobile wireless communications device may include a near field ... when the tag data is successfully verified, perform at least one device unlock operation.
App. - Filed Jun 7, 2013 - Published Dec 10, 2014 - Juan Martin Garcia - BlackBerry Limited
Overview · Related · Discuss

www.google.com/patents/US20160191515

User authentication method and electronic device performing ...

Provided are a user authentication method and an electronic device performing the method. The method is performed under the control of a processor and ...
App. - Filed Dec 14, 2015 - Published Jun 30, 2016 - Yong-Pyo Kim - Yong-Pyo Kim
Overview · Related · Discuss

www.google.com/patents/US9456349

Electronic device and network temporary unlocking method ...

The electronic device includes a communication interface configured to ... The present disclosure relates to an electronic device and, more particularly to, ... operation of performing a temporary unlock in an electronic device according to this ... For example, both a first electronic device and a second electronic device are ...
Grant - Filed May 20, 2015 - Issued Sep 27, 2016 - Min-Ju Kim - Samsung Electronics Co., Ltd
Overview · Related · Discuss

www.google.com/patents/US9710984

Method for the authentication of at least one first unit on ...

Furthermore, a computer program product executes the method and a ... a wireless communication line, in place between the first unit and the second unit, ... This type of authentication optimizes operating convenience for the consumer client at ... frequently linked to a control center via an analog or digital interface, e.g. via ...
Grant - Filed Sep 2, 2015 - Issued Jul 18, 2017 - Tilman Benkert - Endress+Hauser Conducta Gmbh+Co. Kg
Overview · Related · Discuss

IPR2025-01313; Samsung
Ex. 1002 - Page 24

Pocket encrypting and **authenticating communications device**

AA Caputo, VP Amoruso - US Patent 5,778,071, 1998 - Google Patents

... Google has not **performed** a legal analysis and makes no representation as to the accuracy ... H04L63/0428—Network architectures or network **communication** protocols for network security for providing a confidential data exchange **among** entities **communicating** through data ...

☆ 99 Cited by 213 Related articles All 2 versions »

Mobile telephone gateway apparatus, **communication** system, and gateway **operating** system

Y Sela - US Patent 9,521,705, 2016 - Google Patents

... B2 US9521705 B2 US 9521705B2 Authority US United States Prior art keywords mobile phone **communication** network signaling means Prior art date 2003-11-02 Legal status (The legal status is an assumption and is not a legal conclusion. Google has not **performed** a legal ...

☆ 99 Cited by 137 Related articles All 4 versions »

Mobile portable wireless **communication** system

CW Spaur, MF Brailberg, PJ Kennedy... - US Patent ..., 1998 - Google Patents

... protocol/Internet protocol) stack acts on a received request or command by **performing** a number ... stack, in conjunction with the operating system, enables multiple tasks to be **performed** in a ... controller in the vehicle is also associated with an **interface** for **communication** with one ...

☆ 99 Cited by 1095 Related articles All 2 versions »

Active Message applications programming **interface** and **communication** subsystem organization

AM Mainwaring, DE Culler - 1996 - pdfs.semanticscholar.org

... create multiple endpoints, gather them into endpoint bundles and succinctly **perform** operations on ... will occur (access mode is AM_SEQ); the system then **performs** no automatic ... Implementations can optimize **performance** for sequential access, or they can optimize **performance** ...

☆ 99 Cited by 95 Related articles All 13 versions »

Inter-domain **communication** system using remote **procedure** calls for message **communications between** applications in different domains

BC Appleton, S Meschkat, T Tran, A Sah... - US Patent ..., 2012 - Google Patents

... In one implementation, a computer-implemented method for **performing** inter-domain **communication** in a web ... In **doing** so, it may (1) compute the hostname of the mapplet iframe from the ... 4A generally shows operations that may be **performed** by one or more servers interacting ...

☆ 99 Cited by 158 Related articles All 4 versions »

Mobile **communications device** providing heuristic security **authentication** features and **related** methods

MA Goldsmith, A Papo, RJ Lombardi... - US Patent ..., 2015 - Google Patents

... **Communication** functions, including data and voice **communications**, are **performed** through the **communications** ... a transaction terminal to cooperate with the processor to **perform** the mobile ... LOA falls below the security threshold, generating the challenge, **performing** the given ...

☆ 99 Cited by 42 Related articles All 4 versions »

Connector **interface** system facilitating **communication between** a media player and accessories

EC Schubert, WC Leung, GT Lydon, S Krueger... - US Patent ..., 2007 - Google Patents

... Google has not **performed** a legal analysis and makes no representation as to the accuracy of ... In so **doing** the media player can efficiently and effectively interact with the accessory in the ... The microphone lingo is used by the remote connector on the multi-**communication** device ...

☆ 99 Cited by 137 Related articles All 2 versions »

Messaging with a locked **communication device**

DK Bhupati - US Patent 8,218,734, 2012 - Google Patents

... in (or otherwise associated the device with the user) and then **performed** a lock ... an access-controlled operation (no at 416), the **communication** device may **perform** the operation ... readable storage medium encoding a set of device-executable instructions for **performing** a ...

☆ 99 Cited by 36 Related articles All 4 versions »

Unlocking a **device** by **performing** gestures on an **unlock** image

I Chaudhri, B Ording, FA Anzures, M Van Os... - US Patent ..., 2010 - Google Patents

... 11F illustrate the GUI display of a device at various points in the **performance** of an ... programs and/or sets of instructions stored in the memory 102 to **perform** various functions ... The RF circuitry 112 may include well-known circuitry for **performing** these functions, including but not ...

☆ 99 Cited by 1217 Related articles All 4 versions »

Hands-free wireless **communication** in a vehicle

PJ Kennedy, RC Poplawsky, CW Spaur... - US Patent ..., 2002 - Google Patents

Hands-free wireless **communication** in a vehicle. Download PDF ... Authority US United States Prior art keywords **interface** module pocket telephone vehicle **communications** Prior art ... Google has not **performed** a legal analysis and makes no representation as to the accuracy of the ...

☆ 99 Cited by 414 Related articles All 2 versions »

Keystroke dynamics as a **biometric** for **authentication**

F Monrose, AD Rubin - Future Generation computer systems, 2000 - Elsevier

... **Verification** is **performed** by comparing the test signature T (**acquired** at login time) with M and ... **based** on free-text may be more desirable, free-text recognition did not **perform** as well as ... The **performance** of our classifiers on a dataset of 63 **users** ranges from 83.22% to 92.14 ...

☆ 99 Cited by 909 Related articles All 27 versions

Method for **biometric-based authentication** in wireless communication for **access** control

RM Bolle, SL Nunes, S Pankanti, NK Ratha .. - US Patent ..., 2004 - Google Patents

... of signatures corresponding to the same **user**, and upon **authentication**, **performs** a specific ... if a match exists, and upon successful matching, an action is **performed** (like opening a ... a portable device, the **authentication** status is temporarily maintained to **perform** various privileged ...

☆ 99 Cited by 457 Related articles All 2 versions »

User authentication using keystroke dynamics for cellular phones

P Campisi, E Maiorana, ML Bosco, A Neri - IET Signal Processing, 2009 - IET

... speaking, **biometric** systems are essentially pattern-recognition applications, **performing** **authentication** using **biometric** ... by using a statistical classifier, which allows **obtaining** significant **performance** with respect to ... PR, PP, RP, RR}, can be employed to **perform** the **authentication** ...

☆ 99 Cited by 105 Related articles All 6 versions

Authentication gets personal with **biometrics**

J Ortega-Garcia, J Bigun, D Reynolds .. - IEEE signal ..., 2004 - ieeexplore.ieee.org

... This leads to significantly improved **perform-** ance for face **authentication** applications ... puts his/her hand on a highly reflective surface, such as a platen, **performing** an orthographic ... Even greater verifica- tion **performance** improvement can be expected through the **use** of multiple ...

☆ 99 Cited by 216 Related articles All 15 versions

Enabling continuous or instantaneous identity recognition of a large group of people **based** on physiological **biometric** signals **obtained** from members of a small ...

F Agrafioti, FM Bui, D Hatzinakos - US Patent 9,646,261, 2017 - Google Patents

... Google has not **performed** a legal analysis and makes no representation as to the ... authorisation of security principals; G06F21/31—**User authentication**; G06F21/32—**User authentication** using **biometric** ... a password can make **biometric** systems more accessible and easy to **use** ...

☆ 99 Cited by 79 Related articles All 4 versions »

Comparing passwords, tokens, and **biometrics** for **user authentication**

L O'Gorman - Proceedings of the IEEE, 2003 - ieeexplore.ieee.org

... This is done for the purpose of **performing** trusted communications between parties for computing and ... For AES, the **user** chooses a private key to **perform** encryption and decryption ... authenticator **result** must be satisfied; in effect a Boolean AND operation is **performed** for each ...

☆ 99 Cited by 868 Related articles All 13 versions

Biometric-rich gestures: a novel approach to **authentication** on multi-touch devices

N Sae-Bae, K Ahmed, K Isbister, N Memon - proceedings of the SIGCHI ..., 2012 - dl.acm.org

... however, they could skip any gesture that they did not feel comfortable **performing** (all gestures ... Table 3: Correlation Coefficient of **performance** associated with self-report of **user** experience ... and easier the gesture, the more accurately **users** are likely to **perform** the gestures ...

☆ 99 Cited by 304 Related articles All 8 versions »

A k-nearest neighbor approach for **user authentication** through **biometric** keystroke dynamics

J Hu, D Gingrich, A Sentosa - 2008 IEEE International ..., 2008 - ieeexplore.ieee.org

... We measured the time taken to **perform** the full experiment then divided by the number of legitimate ... So people could type whatever they want such as **performing** correction ... By **doing** this, we generated a true behaviour in real life application since each **authentication** would be ...

☆ 99 Cited by 108 Related articles All 6 versions

IPR2025-01313; Samsung
Ex. 1002 - Page 27

Local ordinal contrast pattern histograms for spatiotemporal, lip-**based** speaker **authentication**

CH Chan, B Goswami, J Kittler... - ... on **Information** ..., 2011 - ieeexplore.ieee.org

... an overview of the perfor- mance of various lip-**biometric** systems that **perform** speaker **verification** ... The best **performance obtained** using lip features only on this database is by [14 ... The authors in [30] proposed Improved LBP which **performs** ordinal contrast measurement with ...

☆ 99 Cited by 51 Related articles All 7 versions

A **fingerprint based** bio-cryptographic security protocol designed for client/server **authentication** in mobile computing environment

K Xi, T Ahmad, F Han, J Hu - Security and Communication ..., 2011 - Wiley Online Library

... No **performance** evaluation was reported in literature ... After **performing** Equation (7), the distribution of points become more random, as demonstrated in Figure 2 ... **Perform** hash function and modulo operation on minutia coordinates ...

☆ 99 Cited by 100 Related articles All 5 versions »

STIC
Scientific and Technical Information Center

1. Patent Application Titled '**Information** Processing **Device**, Application Software Start-Up System, And Application Software Start-Up Method' Published Online (USPTO 20190362061)

In: **Information** Technology Newsweekly, Dec 17, 2019, 2279; NewsRX LLC
Language: English. Abstract: 2019 DEC 17 (VerticalNews) -- By a News Reporter-Staff News Editor at **Information** Technology Newsweekly -- According to news reporting originating from Washington, D.C., by VerticalNews journalists, a patent application [...] (*AN: edsgcl.608720217*), Database: Gale General OneFile

Subjects: Japan; Software quality; Software -- Methods; Software -- Intellectual property; Control equipment -- Methods; Control equipment -- Intellectual property

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 29

2. ELECTRONIC **DEVICE** AND METHOD FOR CONTROLLING A TRANSPORT **DEVICE** THEREOF

Patent Application: 15/361318. Filed: November 25, 2016. Published: June 1, 2017. , Database: USPTO Patent Applications

Abstract: According to various embodiments, a method for controlling a transport **device** of an electronic **device** that may communicate with the transport **device**, a **first** external **device**, and a **second** external **device** may include: acquiring state **information** of the transport **device** from the transport **device**, **transmitting** the **acquired** state **information** of the transport **device** to the **first** external **device**, receiving, from the **second** external **device**, a control instruction data for controlling the transport **device** based on the state **information** of the transport **device** when the state **information** of the transport **device** is provided **through** the **first** external **device** depending on the **transmitting** of the state **information**, and **transmitting** the received control instruction data to the transport **device** to control the transport **device**. Other embodiments may also be possible.

AN: edspap.20170155720

USPTO Full Text Options

3. SECURE DATA TRANSLATION USING A LOW-ENERGY WIRELESS **COMMUNICATION** LINK

Patent Application: 16/558052. Filed: August 31, 2019. Published: January 2, 2020. , Database: USPTO Patent Applications

Abstract: Disclosed are various embodiments for providing access control to the sensitive data, such as personal medical history. A **first** client **device** executes an application that ingests input data entered by a user via a user **interface** of the **first** client **device**, encrypts at least a **first** portion of the input data using a **first** cryptographic key, and transmits the encrypted input data over a low-power wireless private area network (WPAN), such as a Bluetooth Low-Energy (BLE) WPAN, for example. A **second** client **device** executing a **second** application receives the encrypted input data transmitted over the low-power WPAN by the **first** client **device** and use the **first** cryptographic key to decrypt the encrypted input data.

AN: edspap.20200008051

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 30

4. ## Method and apparatus for connecting between electronic **devices** using authentication based on **biometric information**

By: SAMSUNG ELECTRONICS CO., LTD. US Patent: 10425,409. Filed: February 17, 2017. Issued: September 24, 2019. , Database: USPTO Patent Grants

Abstract: A method and an apparatus for providing a connection between electronic **devices** using authentication based on **biometric information** are provided. The electronic **device** includes: a **first communication** circuit to support NFC; a **second communication** circuit to support non-NFC; a **biometric** sensor; a memory to store **first** authentication **information** corresponding to an external **device**; and a processor. The processor is configured to: acquire connection **information** related to a connection with the external **device** from the external **device** using the **first communication** circuit in response to NFC tagging between the electronic **device** and the external **device**; establish a **communication** connection with the external **device** using the **second communication** circuit based on at least the connection **information**; receive a request for authentication **information** from the external **device** in response to the **communication** connection being established; acquire **biometric information** corresponding to a user of the electronic **device** using the **biometric** sensor in response to the request; authenticate the user based on at least the **biometric information**; when the authenticating succeeds, generate **second** authentication **information** based on at least the **first** authentication **information**; and transmit the **second** authentication **information** to the external **device**.

AN: edspgr.10425409

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 31

5. METHOD AND APPARATUS FOR CONNECTING BETWEEN ELECTRONIC **DEVICES** USING AUTHENTICATION BASED ON **BIOMETRIC INFORMATION**

Patent Application: 15/436123. Filed: February 17, 2017. Published: August 24, 2017. , Database: USPTO Patent Applications

Abstract: A method and an apparatus for providing a connection between electronic **devices** using authentication based on **biometric information** are provided. The electronic **device** includes: a **first communication** circuit to support NFC; a **second communication** circuit to support non-NFC; a **biometric** sensor; a memory to store **first** authentication **information** corresponding to an external **device**; and a processor. The processor is configured to: acquire connection **information** related to a connection with the external **device** from the external **device** using the **first communication** circuit in response to NFC tagging between the electronic **device** and the external **device**; establish a **communication** connection with the external **device** using the **second communication** circuit based on at least the connection **information**; receive a request for authentication **information** from the external **device** in response to the **communication** connection being established; acquire **biometric information** corresponding to a user of the electronic **device** using the **biometric** sensor in response to the request; authenticate the user based on at least the **biometric information**; when the authenticating succeeds, generate **second** authentication **information** based on at least the **first** authentication **information**; and transmit the **second** authentication **information** to the external **device**.

AN: edspap.20170244703

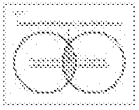
USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 32

6. ## Unregulated Health Research Using Mobile **Devices**: Ethical Considerations and Policy Recommendations.

By: Rothstein, Mark A.; Wilbanks, John T.; Beskow, Laura M.; Breisford, Kathleen M.; Brothers, Kyle B.; Doerr, Megan; Evans, Barbara J.; Hammack-Aviran, Catherine M.; McGowan, Michelle L.; Tovino, Stacey A. *Journal of Law, Medicine & Ethics*. 2020 Supplement, Vol. 48, p196-226. 31p. 1 Diagram, 1 Chart. Abstract: Mobile **devices** with health apps, direct-to-consumer genetic testing, crowd-sourced **information**, and other data sources have enabled research by new classes of researchers. Independent researchers, citizen scientists, patient-directed researchers, self-experimenters, and others are not covered by federal research regulations because they are not recipients of federal financial assistance or conducting research in anticipation of a submission to the FDA for approval of a new drug or medical **device**. This article addresses the difficult policy challenge of promoting the welfare and interests of research participants, as well as the public, in the absence of regulatory requirements and without discouraging independent, innovative scientific inquiry. The article recommends a series of measures, including education, consultation, transparency, self-governance, and regulation to strike the appropriate balance. [ABSTRACT FROM AUTHOR] DOI: 10.1177/1073110520917047. (*AN: 143194286*), Database: Academic Search Complete

Subjects: PUBLIC health research & ethics; GOVERNMENT regulation; BIG data; CITIZEN science; SMARTPHONES; MOBILE apps; MEDICAL research laws; EXPERIMENTAL design; HEALTH; MEDICAL ethics; POLICY sciences; PRIVACY; RESEARCH ethics; **INFORMATION** resources; RULES; HEALTH Insurance Portability & Accountability Act of 1996 (U.S.); DATA security; RESEARCH subjects (Persons); STANDARDS; UNITED States; Computer systems design and related services (except video game design and development); Other Computer Related Services; Research and development in the physical, engineering and life sciences




HTML Full Text **PDF Full Text** (405KB)

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 33

7. ## Mind Your Mind: EEG-Based Brain-Computer **Interfaces** and Their Security in Cyber Space.

By: LANDAU, OFIR; PUZIS, RAMI; NISSIM, NIR. *ACM Computing Surveys.* Feb2020, Vol. 53 Issue 1, p1-38. 38p. Abstract: A brain-computer **interface** (BCI) system is a system that leverages brainwave **information acquired** by a designated brain monitoring **device** to interact with a computerized system. Over the past 40 years, many BCI applications have been developed in a variety of domains, from entertainment to medical field and even to computer securitymechanisms. Until now, the development of BCI systems has focused on improving their accuracy, functionality, and ease of use, and not enough effort and attention has been invested in securing these systems and the sensitive data they acquire. In this article, we present the principles of brain activity data acquisition, with a special focus on EEG, and we present a taxonomy of BCI applications and domains. We also provide a comprehensive survey that covers eight possible attacks aimed at BCI systems. For each BCI application, we created an ecosystem and data and attack flow-diagram, which comprehensively describes the roles and interactions of the players associated with the BCI application and presents the most vulnerable vectors and components within its ecosystem; we identified gaps between existing security solutions and the presented attacks and vulnerabilities. Finally, we provide several concrete suggestions for improving the security of BCI systems in cyber-space. [ABSTRACT FROM AUTHOR] DOI: 10.1145/3372043. (*AN: 141670891*), Database: Business Source Complete

Subjects: Security systems; Systems development; Wired Telecommunications Carriers; Internet Publishing and Broadcasting and Web Search Portals; Security Systems Services (except Locksmiths); Brain-computer **interfaces**; Internet security; Acquisition of data; Brain; Electroencephalography

Show all 16 Images



PDF Full Text (6.2MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 34

8. Method for controlling **communication** and electronic **device** thereof

By: Samsung Electronics Co., Ltd. US Patent: 9,730,262. Filed: January 05, 2016. Issued: August 08, 2017. , Database: USPTO Patent Grants

Abstract: A method of operating a **first** electronic **device** for improving call quality is provided. The method includes the operations of **transmitting** call data received **through** a **first** call between the **first** electronic **device** and a third electronic **device** to a **second** electronic **device**, using short-range wireless **communication** connected with the **second** electronic **device**, if a **communication** abnormality of the short-range wireless **communication** takes place, connecting a **second** call between the **first** electronic **device** and the **second** electronic **device**, generating a third call by merging the **first** call and the **second** call, and releasing a call connection of the **first** electronic **device** from the third call.

AN: edspgr.09730262

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 35

9. ## 5G in the Internet of Things era: an overview on security and privacy challenges

By Sicari, Sabrina; Rizzardi, Alessandra; Coen-Porisini, Alberto. In *Computer Networks*. January 2020 Language: English. DOI: 10.1016/j.comnet.2020.107345 Abstract: Now reaching 2020, the world is witnessing the initial diffusion of 5G networks, which promise to revolutionize the mobile wireless **communications**, providing faster services, very low delays, and a very pervasive connectivity via mobile **devices**. It is worth to remark that the main paradigm which will take advantage from 5G is really the Internet of Things (IoT). However, the spreading of 5G technology also generates important concerns in terms of security and privacy, due to the continuous and wireless connection to the network, which hinders the reliability of the involved **devices**. This paper deeply analyzed the current state of the art about the existing security and privacy solutions tailored to 5G. More in detail, the following requirements are discussed: data integrity, confidentiality, authentication, access control, non-repudiation, trust, privacy, identity management, key management, policy enforcement, and intrusion detection. Furthermore, the paper aims to shed the light on future research directions towards the realization of secure and privacy aware 5G systems. To this end, the role of emerging paradigms, such as IoT, fog computing, and blockchain is investigated. (*AN: S1389128620300827*), Database: ScienceDirect

Subjects: 5G; Internet of Things; Fog Computing; Blockchain; Security; Privacy

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 36

10. ## Authentication Techniques and Methodologies used in Wireless Body Area Networks

By Hussain, Munir; Mehmood, Amjad; Khan, Shafiullah; Khan, M. Altaf; Iqbal, Zeeshan. In *Journal of Systems Architecture*. December 2019 101 Language: English. DOI: 10.1016/j.sysarc.2019.101655 Abstract: Wireless body area network (WBAN), got the IEEE standard in February 2012, is the most significant and highly focused research area among researchers, academicians, and practitioners; applied to the patient's body for monitoring various physiological parameters and then the sensitive measured data is passed to the concerned medical doctor or server for taking the necessary actions. In order to pass the sensitive data securely, authentication is the first step towards it. The authentication schemes help network to reduce unwanted users and prevent from deceptions effectively since the authentication process identifies the user's identity that he or she claims to be. In connection to the safe **communication**, authentication is one of the key aspects. So, it is important to design novel authentication schemes; those offer secure authentication and prevent various security attacks in WBANs. A lot of methods and techniques have been proposed for authentication in WBANs. In this survey paper for improving the authentication process in WBANs, an overview of WBAN and their characteristics, various authentication types and classification of authentication schemes has been done. It further provides a complete comparison of different authentication schemes and highlights their pros, cons, limitations, challenges, performance evaluation and their robustness against different security attacks which open doors of new opportunities. This finally ends with the most significant open issues, future research directions and draw interesting conclusions. (*AN: S138376211930462X*), Database: ScienceDirect

Subjects: Authentication; **Biometric**; Security; Wireless body area network; Smart card

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 37

11. ## Estimation of crowd flow and load on pedestrian bridges using machine learning with sensor fusion

By Mustapha, S.; Kassir, A.; Hassoun, K.; Dawy, Z.; Abi-Rached, H.. In *Automation in Construction*. April 2020 112 Language: English. DOI: 10.1016/j.autcon.2020.103092 Abstract: Unfortunate tragedies have been the result of crowd behavior in high-density pedestrian flows as a reaction to an incident aggravating the conditions and resulting in trampling and crushing situations. Therefore, it is important to monitor such crowd motion for danger warning and prevention. In this work, we utilize a recently introduced framework for simultaneous crowd and structural monitoring based on a novel combination of sensing technologies that includes the employment of structurally mounted Fiber Bragg Grating (FBG) Fiber Optic Sensors (FOSs) in conjunction with individually held wearable sensing **devices** incorporating Inertial Measurement Units (IMUs). We propose effective approaches for the estimation of crowd flow and load on pedestrian bridges using advanced machine learning techniques with sensor data extracted from both structural sensors and wearable **devices**. A key novelty of the approaches presented is the utilization of sensor fusion at both the input and feature level within the machine learning methods used. The machine learning approaches include Convolutional Neural Networks (CNN) and Support Vector Machines (SVM); they are **first** applied on each of the sensing sources, FOSs and IMUs, individually and then extended for multi-modal data fusion at both the input and feature levels. Data fusion enriches the learning models and enhances the system efficiency and robustness against noise and input data time-shifting errors. The proposed approaches are validated using experimental measurements from a crowd replication scenario run on a small-scaled test bridge. The trained machine learning models demonstrate effectiveness in crowd attribute classification for motion speed and load designation, along with a regression model for load estimation. Results show that the proposed monitoring solution is highly effective with peak testing accuracy for single class motion speed classification at 98%, multi-class motion speed and load characterization classification at 91%, and percentage error for load estimation regression reaching a minimum of 9%. (*AN: S0926580519310295*), Database: ScienceDirect

Subjects: Crowd management; Crowd monitoring; Structural health monitoring; Sensor fusion; Machine learning

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 38

12. ## Internet of Things: A survey of enabling technologies in healthcare and its applications

By Dhanvijay, Mrinai M.; Patil, Shailaja C.. In *Computer Networks*. 22 April 2019 153:113-131 Language: English. DOI: 10.1016/j.comnet.2019.03.006 Abstract: Internet of Things (IoT) on the Wireless Body Area Network (WBAN) for healthcare applications is an operative scenario for IoT **devices** that has gained attention from vast research fields in recent years. The IoT connects all subjects and the healthcare system seamlessly. This paper describes the WBAN based IoT healthcare system and reviews the state-of-the-art of the network architecture topology and applications in the IoT based healthcare solutions. Moreover, this paper analyzes the security and the privacy features consisting of privacy, authentication, energy, power, resource management, Quality of Services and the real-time wireless health monitoring that are quite problematic in many IoT healthcare architectures. Because, system architecture is not well-defined, data restriction and its integrity preservation is still a challenge. At present 90% of the **information** available is **acquired** in the recent two years. This survey mainly aims at analyzing healthcare purpose which is based on digital healthcare system. Further, it reports many IoT and the e-healthcare policies and systems that decide how to ease all bearable development. Thus, the overall system provides large possibilities for future research based on IoT healthcare system. Finally, research gaps are reviewed and the possible future aspects have been discussed. (*AN: S1389128619302695*), Database: ScienceDirect

Subjects: IoT; WBAN; Healthcare system; Body sensor

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 39

13. ## A survey on methods and challenges in EEG based authentication

By Jalaly Bidgoly, Amir; Jalaly Bidgoly, Hamed; Arezoumand, Zeynab. In *Computers & Security*. June 2020 93 Language: English. DOI: 10.1016/j.cose.2020.101788 Abstract: EEG is the recording of electrical activities of the brain, usually along the scalp surface, which are the results of synaptic activations of the brain's neurons. In recent years, it has been shown that EEG is an appropriate signal for the **biometric** authentication and has important features such as resistance to spoofing attacks and impossibility to use under pressure and coercion states. In this paper, the state-of-the-art methods in EEG based authentication are reviewed. This review includes a number of aspects such as the various tasks that the user required to perform during the authentication, **devices** and available datasets, the preprocessing procedures and the classification methods used in the EEG **biometric** authentication. Both shallow and deep classification methods are reviewed in this paper. The study shows that the deep learning approaches which are used in the past few years, although still require further research, have shown great results. Moreover, the paper summarizes the works to address the open challenges of this area. The EEG authentication challenges have been discussed from a variety of points of view, including privacy, user-friendliness, attacks, and authentication requirements such as universality, permanency, uniqueness, and collectability. This paper can be used as a preliminary plan and a roadmap for researchers interested in EEG **biometric**. (*AN: S0167404820300730*), Database: ScienceDirect

Subjects: EEG; **Biometric** factor; Authentication; User identification; Pattern recognition; Survey

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 40

14. ## Probability-based path discovery protocol for electromagnetic nano-networks

By Galal, Akram; Hesselbach, Xavier. In *Computer Networks*. 19 June 2020 174 Language: English. DOI: 10.1016/j.comnet.2020.107246 Abstract: One of the major challenges for nano-network is the forfeit of **communication** protocols to exploit the potential **communication** between nano-machines forming fully operational nano-network. Because nano-machines face some restrictions such as limited processing power and confined computing capabilities, up-to-date nano-machines cannot perceive partial or full routing tables, which are the main decision-makers for data routing in legacy **communication** networks. The reason is that creating and updating routing tables continuously require adequate processing power with sufficient memory and computing capabilities, which is not the case of nano-nodes. So, new innovative routing schemes have to be proposed for nano-networks to deal with such extremely low resources. This paper focuses on decoupling the routing intelligence from nano-network towards a computational architecture using Software Defined Networking (SDN) and Network Function Virtualization (NFV) technologies by externalizing routing decisions and complex computations from nano-nodes to be fully compiled externally. Moreover, the paper proposes a probability-based path discovery protocol denoted by (PBPD) for electromagnetic nano-nodes suitable for **dynamic** nano-network applications. The performance of the proposed protocol is evaluated and compared with other routing protocols discussed in the literature. The proposed scheme provides low energy consumption inside nano-nodes and low computational complexity thanks to SDN/NFV system. *(AN: S1389128619308801)*, Database: ScienceDirect

Subjects: Nano-network; Packet routing; Internet of nano-things; Software defined networking; Network function virtualization; Virtual routing

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 41

15. ## A context-aware system to secure enterprise content: Incorporating reliability specifiers

By Oluwatimi, Oyindamola; Damiani, Maria Luisa; Bertino, Elisa. In *Computers & Security*. August 2018 77:162-178 Language: English. DOI: 10.1016/j.cose.2018.04.001 Abstract: The sensors of a context-aware system extract contextual **information** from the environment and relay that **information** to higher-level processes of the system so to influence the system's control decisions. However, an adversary can maliciously influence such controls indirectly by manipulating the environment in which the sensors are monitoring, thereby granting privileges the adversary would otherwise not normally have. To address such context monitoring issues, we extend CASSEC by incorporating sentience-like constructs, which enable the emulation of "confidence", into our proximity-based access control model to grant the system the ability to make more inferable decisions based on the degree of reliability of extracted contextual **information**. In CASSEC 2.0, we evaluate our confidence constructs by implementing two new authentication mechanisms. Co-proximity authentication employs our time-based challenge-response protocol, which leverages Bluetooth Low Energy beacons as its underlying occupancy detection technology. **Biometric** authentication relies on the accelerometer and fingerprint sensors to measure behavioral and physiological user features to prevent unauthorized users from using an authorized user's **device**. We provide a feasibility study demonstrating how confidence constructs can improve the decision engine of context-aware access control systems. (*AN: S0167404818303018*), Database: ScienceDirect

Subjects: Access control; Context awareness; BYOD; Security; Mobility; **Biometric**; Authentication; Reliability; Proximity

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 42

16. METHOD FOR CONTROLLING **COMMUNICATION** AND ELECTRONIC **DEVICE** THEREOF

Patent Application: 14/988071. Filed: January 05, 2016. Published: July 7, 2016. , Database: USPTO Patent Applications

Abstract: A method of operating a **first** electronic **device** for improving call quality is provided. The method includes the operations of **transmitting** call data received **through** a **first** call between the **first** electronic **device** and a third electronic **device** to a **second** electronic **device**, using short-range wireless **communication** connected with the **second** electronic **device**, if a **communication** abnormality of the short-range wireless **communication** takes place, connecting a **second** call between the **first** electronic **device** and the **second** electronic **device**, generating a third call by merging the **first** call and the **second** call, and releasing a call connection of the **first** electronic **device** from the third call.

AN: edspap.20160198515

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 43

17. Seeing the whole picture: visualising socio-spatial power **through** augmented reality.

By: Kateli, Michael; Dechesne, Francien; Koops, Bert-Jaap; Meessen, Paulus. *Law, Innovation & Technology.* Dec2019, Vol. 11 Issue 2, p279-310. 32p. Abstract: Augmented Reality (AR) will have important effects on the ways in which spaces and places take meaning for both users and non-users of AR. As the market penetration of AR increases, new claims will be made on certain spaces, superimposing AR contexts on the meanings and functions traditionally associated with these spaces, not only by AR users but also by AR designers and service providers, raising important and complex questions about regulatory approaches to mitigating **information** and power asymmetries. A regulatory strategy that promotes civil society and individual privacy requires that we thoroughly consider the implications of AR on the construction of public and private space. We employ a mix of real and fictional AR scenarios to interrogate the potential effects of AR use and design on the construction of spatial meaning, the orientation of social relations, and distributions of social power, and we make initial recommendations for regulation to address AR's possible negative effects. [ABSTRACT FROM AUTHOR] DOI: 10.1080/17579961.2019.1665800. (*AN: 139413399*), Database: Academic Search Complete

Subjects: AUGMENTED reality; PUBLIC spaces; MARKET penetration; **INFORMATION** asymmetry; SOCIAL power; CIVIL society

HTML Full Text **PDF Full Text** (2.4MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 44

18. ## Secure IoT **communications** for smart healthcare monitoring system

By El Zouka, Hesham A.; Hosni, Mustafa M.. In *Internet of Things*. January 2018 Language: English. DOI: 10.1016/j.iot.2019.01.003 Abstract: Healthcare monitoring systems in hospitals and other health centers have witnessed throughout the last decade a tremendous growth and wireless healthcare monitoring **devices** with various technologies have become of great interest in many nations around the world. The proposed paper aims at integrating artificial intelligence technology, such as the neural networks and fuzzy system in a secure healthcare monitoring system in order to enable the system to work as a smart healthcare model that decides the priority by itself depending on the collected health parameters from the senor nodes. The proposed model consists of a trust environment that is responsible for collecting authenticated physiological data from patient's body which is then sent **through** GSM module to Azure IoT Hub where raw data is converted into linguistic representation, with the help of logic-based algorithm, which is trained in fuzzy-based inference system (FBIS) to get the status of the patient. The proposed system, then, provides reliable, accurate, secure and real-time patient monitoring. The following sections describe how the FBIS can be integrated with a secure healthcare monitoring system to get the states of the patient and send it to the medical advisory for the preliminary precautions. (*AN: S254266051830088X*), Database: ScienceDirect

Subjects: Internet of Things (IoT); health monitoring; sensors; security; trust; fuzzy

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 45

19. ## Handbook of Green **Information** and **Communication** Systems

By: Woungang, Isaac; Anpalagan, Alagan; Obaidat, Mohammad S. Amsterdam : Academic Press. 2013. eBook. Description: This book gives a comprehensive guide on the fundamental concepts, applications, algorithms, protocols, new trends and challenges, and research results in the area of Green **Information** and **Communications** Systems. It is an invaluable resource giving knowledge on the core and specialized issues in the field, making it highly suitable for both the new and experienced researcher in this area. Key Features: Core research topics of green **information** and **communication** systems are covered from a network ... (*AN 485200*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Signals & Signal Processing; SCIENCE / Environmental Science; Sustainable engineering--Handbooks, manuals, etc; Telecommunication--Environmental aspects--Handbooks, manuals, etc; Telecommunication--Energy conservation--Handbooks, manuals, etc

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 46

20. ## An Implantable Wireless Neural **Interface** System for Simultaneous Recording and Stimulation of Peripheral Nerve with a Single Cuff Electrode.

By: Shon, Ahnsei; Chu, Jun-Uk; Jung, Jiuk; Kim, Hyungmin; Youn, Inchan. *Sensors (14248220)*. Jan2018, Vol. 18 Issue 1, p1. 26p. Abstract: Recently, implantable **devices** have become widely used in neural prostheses because they eliminate endemic drawbacks of conventional percutaneous neural **interface** systems. However, there are still several issues to be considered: low-efficiency wireless power transmission; wireless data **communication** over restricted operating distance with high power consumption; and limited functionality, working either as a neural signal recorder or as a stimulator. To overcome these issues, we suggest a novel implantable wireless neural **interface** system for simultaneous neural signal recording and stimulation using a single cuff electrode. By using widely available commercial off-the-shelf (COTS) components, an easily reconfigurable implantable wireless neural **interface** system was implemented into one compact module. The implantable **device** includes a wireless power consortium (WPC)-compliant power transmission circuit, a medical implant **communication** service (MICS)-band-based radio link and a cuff-electrode path controller for simultaneous neural signal recording and stimulation. During in vivo experiments with rabbit models, the implantable **device** successfully recorded and stimulated the tibial and peroneal nerves while communicating with the external **device**. The proposed system can be modified for various implantable medical **devices**, especially such as closed-loop control based implantable neural prostheses requiring neural signal recording and stimulation at the same time. [ABSTRACT FROM AUTHOR] DOI: 10.3390/s18010001. (*AN: 127823826*), Database: Academic Search Complete

Subjects: WIRELESS **communications**; WIRELESS power transmission; ENERGY consumption; ELECTRODES; PERIPHERAL nervous system; NEURAL stimulation; Radio and Television Broadcasting and Wireless **Communications** Equipment Manufacturing; Wireless Telecommunications Carriers (except Satellite)

HTML Full Text **PDF Full Text** (1.6MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 47

21. ## Artificial Immune Systems approaches to secure the internet of things: A systematic review of the literature and recommendations for future research

By Aldhaheri, Sahar; Alghazzawi, Daniyal; Cheng, Li; Barnawi, Ahmed; Alzahrani, Bandar A.. In *Journal of Network and Computer Applications*. 1 May 2020 157 Language: English. DOI: 10.1016/j.jnca.2020.102537

Abstract: As the Internet of Things (IoT) recently attains tremendous popularity, this promising technology leads to a variety of security challenges. The traditional solutions do not fit the new challenges brought by the IoT ecosystem. Although the development's area of Artificial Immune Systems (AIS) provides an opportunity to improve security issues and create a fertile and exciting environment for further research and experiments, there is not any systematic and comprehensive study about analyzing its importance for IoT environment. Therefore, this work aims to identify, evaluate, and perform a comprehensive study of empirical research on the studies of AIS approaches to secure the IoT environment. The relevant and high-quality studies are addressing using three research questions about the main research motivations, existing solutions, and future gaps and directions. The AIS approaches have been divided into three main categories based on IoT layers, and detailed classifications have also been included based on different parameters. To achieve this aim, the authors use a systematic literature review (SLR) as a powerful method to collect and critically analyze the research papers. Also, the authors discuss the selected studies and their main techniques, as well as their benefits and drawbacks in general. This research process strives to build a knowledge base for AIS solutions under the umbrella of IoT security and suggest directions for future research. (*AN: S1084804520300114*), Database: ScienceDirect

Subjects: Artificial intelligence; Artificial immune system; Artificial immune networks; Clonal selection; Cyber security; Danger theory; Dendritic cell; Internet of things; IoT; Negative selection; Network security

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 48

22. ## An Autonomous Alarm System for Personal Safety Assurance of Intimate Partner Violence Survivors Based on Passive Continuous Monitoring **through** Biosensors.

By: Rodríguez-Rodríguez, Ignacio; Rodríguez, José-Víctor; Elizondo-Moreno, Aránzazu; Heras-González, Purificación. *Symmetry (20738994).* Mar2020, Vol. 12 Issue 3, p460. 1p. Abstract: Featured Application: An alarm system based on passive monitoring **through** biosensors is hereby presented with the aim of managing and preventing risky situations suffered by intimate partner violence (IPV) survivors. The proposal would be able to autonomously detect an aggressive situation and then activate an alarm without any user intervention, thereby assuring symmetry among individuals in regard to personal safety. Intimate Partner Violence (IPV) dramatically compromises the free and complete development of many women around the world, therefore leading to social asymmetry regarding the right to personal safety. In many cases, a woman who has reported her partner to police for gender-based violence needs to ensure her protection (either before the trial of the aggressor or after their freedom). Thus, it would be ideal if autonomous alarm systems could be developed in order to call the police if necessary. Up to now, many proposals have been presented in this regard, including solutions based on **Information** and **Communication** Technologies (ICT) but, unfortunately, these approaches usually rely on the active participation of the victims (survivors), who have to turn the system on by themselves if needed. Therefore, in order to overcome such limitations, in this work, a passive continuous monitoring system is proposed which uses biosensors attached to the survivor as well as machine learning techniques to infer if an abnormal situation related to gender-based violence is taking place, activating in this case an alarm. The monitoring structure of the system supervises a great deal of bio-signals according to the current status of technology of wearables and biomedical **devices**. The presented biosensors-based surveillance solution can also be manually disconnected for 30/60/90 min (on demand) in order to avoid false positives when a woman is, for example, practicing sports or carrying out other inoffensive activities that could incorrectly activate the alarm. [ABSTRACT FROM AUTHOR] DOI: 10.3390/sym12030460. (*AN: 142566414*), Database: Academic Search Complete

Subjects: INTIMATE partner violence; ALARMS; ELECTRONIC alarm systems (Security systems); SYSTEM safety; BIOSENSORS; **INFORMATION & communication** technologies; WEARABLE technology; POLICE brutality; Security Systems Services (except Locksmiths)

HTML Full Text **PDF Full Text** (3.7MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 49

23. ## Towards a Holistic ICT Platform for Protecting Intimate Partner Violence Survivors Based on the IoT Paradigm.

By: Rodríguez-Rodríguez, Ignacio; Rodríguez, José-Víctor; Elizondo-Moreno, Aránzazu; Heras-González, Purificación; Gentili, Michele. *Symmetry (20738994)*. Jan2020, Vol. 12 Issue 1, p37-37. 1p. Abstract: Featured Application: A complete review of **information** and **communication** technology (ICT) strategies to manage intimate partner violence (IPV) and protect IPV survivors is provided. A holistic ICT solution which would overcome the limitations of previous works is presented, promoting symmetry in society. Intimate partner violence (IPV) remains a scourge that compromises the rights of many women around the world, shaping an asymmetry in civil rights. Fighting gender-based violence, especially when it is committed by an intimate partner, is an important responsibility that needs to be addressed from all angles. It is also remarkable that our society is clearly conditioned by **information** and **communication** technology (ICT), which involves many aspects of our daily life. Unfortunately, violence that is performed in the real world is also replicated in this 'virtual' existence, by offenders in ICT contexts. On the other hand, the same technologies also provide a plethora of opportunities to fight IPV, which are enhanced by the innovative paradigm of the so-called Internet of Things (IoT). In this work, we **first** present a thorough compilation of ICT proposals already published—based on either hardware or software—aimed at protecting IPV survivors, and which can be applied in real life situations but also within social networks. The challenges that still lie ahead are highlighted and, a complete ICT-based platform for IPV management, within an IoT framework, that overcomes the limitations of previous works is proposed, and then promoting a symmetry between individuals in society. [ABSTRACT FROM AUTHOR] DOI: 10.3390/sym12010037. (*AN: 141410952*), Database: Academic Search Complete

Subjects: INFORMATION & communication technologies; INTIMATE partner violence; INTERNET of things; WOMEN'S rights; CIVIL rights; SOCIAL networks; Other Individual and Family Services

HTML Full Text **PDF Full Text** (1.2MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 50

24. ## Genomic and Personalized Medicine : V1-2

By: Willard, Huntington F.; Ginsburg, Geoffrey S. Edition: **2nd** ed. London : Academic Press. 2013. eBook. Description: Genomic and Personalized Medicine, **Second** Edition — winner of a 2013 Highly Commended BMA Medical Book Award for Medicine — is a major discussion of the structure, history, and applications of the field, as it emerges from the campus and lab into clinical action. As with the **first** edition, leading experts review the development of the new science, the current opportunities for genome-based analysis in healthcare, and the potential of genomic medicine in future healthcare. The inclusion of the latest ... (*AN 485475*), Database: eBook Collection (EBSCOhost)

Subjects: SCIENCE / Life Sciences / Genetics & Genomics; MEDICAL / Pharmacology; Proteomics; Genomics; Medical genetics

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

25. ## Applied Cryptography : Protocols, Algorithms and Source Code in C

By: Schneier, Bruce. Edition: **Second** edition, 20th anniversary edition. Indianapolis, IN : Wiley. 2015. eBook. Description: From the world's most renowned security technologist, Bruce Schneier, this 20th Anniversary Edition is the most definitive reference on cryptography ever published and is the seminal work on cryptography. Cryptographic techniques have applications far beyond the obvious uses of encoding and decoding **information**. For developers who need to know about capabilities, such as digital signatures, that depend on cryptographic techniques, there's no better overview than Applied Cryptography, the definitive ... (*AN 1535854*), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Security / Cryptography & Encryption; Cryptography; C (Computer program language)

EPUB Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 51

26. A SURVEY OF **BIOMETRICS** FOR WEARABLE **DEVICES**.

By: Cornelius, Cory; Gutierrez, Christopher N. *Intel Technology Journal*. 2014, Vol. 18 Issue 4, p46-63. 18p. Abstract: **Biometrics** are characteristics about ourselves that we use to recognize each other. Whether it is the structure of our face or the way we walk, we can measure these physiological or behavioral signals and use statistical methods to distinguish amongst users. Rather than "something you know"-as in traditional password-based authentication systems-these **biometric**-based methods enable systems to authenticate you based on "something you are." In this survey we describe the current state-of-the-art of **biometric** techniques and evaluate their use in authentication systems with a particular focus on client **devices** and emerging wearable **devices**. We examine the academic literature and commercial offerings of **biometrics** and summarize each **biometrics**' utility over a variety of criteria and provide guidance for their use in client and wearable **devices**. [ABSTRACT FROM AUTHOR] (*AN: 97377853*), Database: Computer Source

Subjects: BIOMETRIC identification software; COMPUTER security management; COMPUTER systems management; COMPUTER security software; DATA management

PDF Full Text (2.2MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 52

27. ## Self-Organizing Peer-To-Peer Middleware for Healthcare Monitoring in Real-Time.

By: Hyun Ho Kim; Hyeong Gon Jo; Soon Ju Kang. *Sensors (14248220).* Nov2017, Vol. 17 Issue 11, p2650. 19p. Abstract: As the number of elderly persons with chronic illnesses increases, a new public infrastructure for their care is becoming increasingly necessary. In particular, technologies that can monitoring bio-signals in real-time have been receiving significant attention. Currently, most healthcare monitoring services are implemented by wireless carrier **through** centralized servers. These services are vulnerable to data concentration because all data are sent to a remote server. To solve these problems, we propose self-organizing P2P middleware for healthcare monitoring that enables a real-time multi bio-signal streaming without any central server by connecting the caregiver and care recipient. To verify the performance of the proposed middleware, we evaluated the monitoring service matching time based on a monitoring request. We also confirmed that it is possible to provide an effective monitoring service by evaluating the connectivity between Peer-to-Peer and average jitter. [ABSTRACT FROM AUTHOR] DOI: 10.3390/s17112650. (*AN: 126442110*), Database: Academic Search Complete

Subjects: SELF-organizing maps; PEER-to-peer architecture (Computer networks); INFRASTRUCTURE (Economics); MIDDLEWARE; CLIENT/SERVER computing

PDF Full Text (5.7MB) **USPTO Full Text Options**

28. ## Wireless Technologies : Concepts, Methodologies, Tools and Applications

By: **Information** Resources Management Association. Hershey, PA : IGI Global. 2012. eBook. (*AN 396408*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Mobile & Wireless **Communications**; TECHNOLOGY & ENGINEERING / Radio; Wireless **communication** systems; Telecommunication

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 53

29. ## A Survey on Detection, Tracking and Identification in Radio Frequency-Based **Device**-Free Localization.

By: Denis, Stijn; Berkvens, Rafael; Weyn, Maarten. *Sensors (14248220)*. Dec2019, Vol. 19 Issue 23, p5329. 1p. Abstract: The requirement of active localization techniques to attach a hardware **device** to the targets that need to be located can be difficult or even impossible for certain applications. For this reason, there has been an increasing interest in tagless or **device**-free localization (DFL) approaches. In particular, the research domain of RF-based **device**-free localization has been steadily evolving since its inception slightly over a decade ago. Many novel techniques have been developed regarding the three core aspects of DFL: detection, tracking, and identification. The increasing use of channel state **information** (CSI) has contributed considerably to these developments. In particular, the progress it enabled regarding the exceptionally difficult 'identification problem' has been highly impressive. In this survey, we provide a comprehensive overview of this evolutionary process, describe essential DFL concepts and highlight several key techniques whose creation marked important milestones within this field of research. We do so in a structured manner in which each technique is categorized according to the DFL core aspect it emphasizes most. Additionally, we discuss current blocking issues within the state-of-the-art and suggest multiple high-level research directions which will aid in the search towards eventual solutions. [ABSTRACT FROM AUTHOR] DOI: 10.3390/s19235329. (*AN: 140236138*), Database: Academic Search Complete

Subjects: LOCALIZATION (Mathematics); KERNEL (Mathematics); WIRELESS sensor networks; IDENTIFICATION; RADIOS; ARTIFICIAL satellite tracking; Space Research and Technology; Other telecommunications; All Other Telecommunications; Consumer Electronics Repair and Maintenance; Electronic components, navigational and **communications** equipment and supplies merchant wholesalers; Audio and Video Equipment Manufacturing; Home entertainment equipment merchant wholesalers

HTML Full Text **PDF Full Text** (900KB)

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 54

30. CONTENT DELIVERY VIA HYBRID MOBILE NETWORK/BROADCAST NETWORK INFRASTRUCTURE

Patent Application: 15/591665. Filed: May 10, 2017. Published: November 15, 2018. , Database: USPTO Patent Applications

Abstract: A system includes a hybrid mobile network/television antenna and a routing **device** connected to the antenna. The hybrid mobile network/television antenna receives content via a broadcast television network and receives content via a mobile network. The routing **device** includes a **first communication interface** that connects to the hybrid mobile network/television antenna, and a **second communication interface** that connects to a user **device** and receives a request for content from the user **device**. The routing **device** selects a network from the broadcast television network or the mobile network. The **first communication interface** receives the requested content via the selected network, and the routing **device** forwards the requested content to the user **device** via the **second communication interface**.

AN: edspap.20180332313

USPTO Full Text Options

EBSCO Connect | Privacy Policy | A/B Testing | Terms of Use | Copyright | Cookie Policy | Contact Us

powered by EBSCO*host*

© 2020 EBSCO Industries, Inc. All rights reserved.

IPR2025-01313; Samsung
Ex. 1002 - Page 55

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1,474	("HIRABAYASHI, MASAYUKI" or "HASHIMOTO, YASUNOBU" or "YOSHIZAWA, KAZUHIKO").inv.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:14
L2	1	l1 and ((acquir$3 with (dynamic with biometric with information)) with (((body with user) with (dynamic with biometric with information)) with ((acquisition with sensor) with (first with device))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:14
L3	2	l1 and ((transmit$4 or forward$3 or send$3) with (((acquired with (dynamic with biometric with information)) with (first with communication with interface)) with ((first with device) with (second with device))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:14
L4	1	l1 and ((acquir$3 with (static with biometric with information)) with ((static with biometric with information) with ((acquisition with sensor) with (second with device))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:15
L5	1	l1 and (((perform$3 with user with authentication) with (obtain$3 with authentication with result)) with (based with (acquired with static with biometric with information)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:15
L6	1	l1 and (((perform$3 with communication) with (second with communication with interface)) with ((relat$3 with authentication with result) with (first with communication with interface)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:15
L7	2	l1 and ((receiv$3 with (dynamic with biometric with information)) with (transmit$4 with (first with communication with interface)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:15

L8	1	l1 and (((perform$3 with communication) with (relat$3 with authentication with result)) with (between with ((first with communication with interface) and (second with communication with interface))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:15
L9	1	l1 and (((execut$3 with unlock with operation) with (unlock with first with device)) with ((response with communication) with (relat$3 with authentication with result)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:16
L10	1	l1 and ((acquir$3 with (dynamic with biometric with information)) with (((dynamic with biometric with information) with (acquisition with sensor)) with ((first with device) with ("after" with unlock$3))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:16
L11	1	l1 and ((maintain$3 with unlock$3 with state) with (("during" with condition) with (dynamic with biometric with information with acquir$3)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:16
L12	1	l1 and (((receiv$3 with (dynamic with biometric with information)) with (second with device)) with ((communication with "between") with ((first with communication with interface) and (second with communication with interface))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:16
L13	1	l1 and (((display$3 with (display with screen with information)) with (based with state with user)) with ((determin$3 with using) with (receiv$3 with (dynamic with biometric with information))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:17
L14	41,309	("HITACHI MAXELL" or "MAXELL")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:17
L15	1	l14 and ((acquir$3 with (dynamic with biometric with information)) with (((body with user) with (dynamic with biometric with information)) with ((acquisition with sensor) with (first with device))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:17

L16	2	l14 and ((transmit$4 or forward$3 or send$3) with (((acquired with (dynamic with biometric with information)) with (first with communication with interface)) with ((first with device) with (second with device))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:17
L17	1	l14 and ((acquir$3 with (static with biometric with information)) with ((static with biometric with information) with ((acquisition with sensor) with (second with device))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:17
L18	1	l14 and (((perform$3 with user with authentication) with (obtain$3 with authentication with result)) with (based with (acquired with static with biometric with information)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:18
L19	1	l14 and (((perform$3 with communication) with (second with communication with interface)) with ((relat$3 with authentication with result) with (first with communication with interface)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:18
L20	2	l14 and ((receiv$3 with (dynamic with biometric with information)) with (transmit$4 with (first with communication with interface)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:18
L21	1	l14 and (((perform$3 with communication) with (relat$3 with authentication with result)) with (between with ((first with communication with interface) and (second with communication with interface))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:18
L22	1	l14 and (((execut$3 with unlock with operation) with (unlock with first with device)) with ((response with communication) with (relat$3 with authentication with result)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:18
L23	1	l14 and ((acquir$3 with (dynamic with biometric with information)) with (((dynamic with biometric with information) with (acquisition with sensor)) with ((first with device) with ("after" with unlock$3))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:18

L24	1	l14 and ((maintain$3 with unlock$3 with state) with (("during" with condition) with (dynamic with biometric with information with acquir$3)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:18
L25	1	l14 and (((receiv$3 with (dynamic with biometric with information)) with (second with device)) with ((communication with "between") with ((first with communication with interface) and (second with communication with interface))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:18
L26	1	l14 and (((display$3 with (display with screen with information)) with (based with state with user)) with ((determin$3 with using) with (receiv$3 with (dynamic with biometric with information))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:19
L27	231,486	(G05B19/00; H04L9/32; G06K9/00; H04L12/16; H04L9/32; G06F21/32; G06F21/12; G06F21/31; G06F21/35; G06F21/60; G06F21/62; H04W12/06).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:19
L28	1	l27 and ((acquir$3 with (dynamic with biometric with information)) with (((body with user) with (dynamic with biometric with information)) with ((acquisition with sensor) with (first with device))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:19
L29	2	l27 and ((transmit$4 or forward$3 or send$3) with (((acquired with (dynamic with biometric with information)) with (first with communication with interface)) with ((first with device) with (second with device))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:19
L30	1	l27 and ((acquir$3 with (static with biometric with information)) with ((static with biometric with information) with ((acquisition with sensor) with (second with device))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:19
L31	1	l27 and (((perform$3 with user with authentication) with (obtain$3 with authentication with result)) with (based with (acquired with static with biometric with information)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:20

L32	3	l27 and (((perform$3 with communication) with (second with communication with interface)) with ((relat$3 with authentication with result) with (first with communication with interface)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:20
L33	2	l27 and ((receiv$3 with (dynamic with biometric with information)) with (transmit$4 with (first with communication with interface)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:20
L34	1	l27 and (((perform$3 with communication) with (relat$3 with authentication with result)) with (between with ((first with communication with interface) and (second with communication with interface))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:20
L35	1	l27 and (((execut$3 with unlock with operation) with (unlock with first with device)) with ((response with communication) with (relat$3 with authentication with result)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:20
L36	1	l27 and ((acquir$3 with (dynamic with biometric with information)) with (((dynamic with biometric with information) with (acquisition with sensor)) with ((first with device) with ("after" with unlock$3))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:20
L37	1	l27 and ((maintain$3 with unlock$3 with state) with (("during" with condition) with (dynamic with biometric with information with acquir$3)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:21
L38	1	l27 and (((receiv$3 with (dynamic with biometric with information)) with (second with device)) with ((communication with "between") with ((first with communication with interface) and (second with communication with interface))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:21
L39	1	l27 and (((display$3 with (display with screen with information)) with (based with state with user)) with ((determin$3 with using) with (receiv$3 with (dynamic with biometric with information))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/06/07 15:21

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L40	31,097	(G05B19/00; H04L9/32; G06K9/00; H04L12/16; H04L9/32; G06F21/32; G06F21/12; G06F21/31; G06F21/35; G06F21/60; G06F21/62; H04W12/06).cpc.	USPAT	OR	OFF	2020/06/07 15:21
L41	0	l40 and ((acquir$3 with (dynamic with biometric with information)) with (((body with user) with (dynamic with biometric with information)) with ((acquisition with sensor) with (first with device)))).clm.	USPAT	OR	OFF	2020/06/07 15:21
L42	1	l40 and ((transmit$4 or forward$3 or send$3) with (((acquired with (dynamic with biometric with information)) with (first with communication with interface)) with ((first with device) with (second with device)))).clm.	USPAT	OR	OFF	2020/06/07 15:22
L43	0	l40 and ((acquir$3 with (static with biometric with information)) with ((static with biometric with information) with ((acquisition with sensor) with (second with device)))).clm.	USPAT	OR	OFF	2020/06/07 15:22
L44	0	l40 and (((perform$3 with user with authentication) with (obtain$3 with authentication with result)) with (based with (acquired with static with biometric with information))).clm.	USPAT	OR	OFF	2020/06/07 15:23
L45	0	l40 and (((perform$3 with communication) with (second with communication with interface)) with ((relat$3 with authentication with result) with (first with communication with interface))).clm.	USPAT	OR	OFF	2020/06/07 15:23
L46	1	l40 and ((receiv$3 with (dynamic with biometric with information)) with (transmit$4 with (first with communication with interface))).clm.	USPAT	OR	OFF	2020/06/07 15:23
L47	0	l40 and (((perform$3 with communication) with (relat$3 with authentication with result)) with (between with ((first with communication with interface) and (second with communication with interface)))).clm.	USPAT	OR	OFF	2020/06/07 15:23
L48	0	l40 and (((execut$3 with unlock with operation) with (unlock with first with device)) with ((response with communication) with (relat$3 with authentication with result))).dm.	USPAT	OR	OFF	2020/06/07 15:24
L49	0	l40 and ((acquir$3 with (dynamic with biometric with information)) with (((dynamic with biometric with information) with	USPAT	OR	OFF	2020/06/07 15:24

		(acquisition with sensor)) with ((first with device) with ("after" with unlock$3)))).clm.				
L50	0	l40 and ((maintain$3 with unlock$3 with state) with (("during" with condition) with (dynamic with biometric with information with acquir$3))).clm.	USPAT	OR	OFF	2020/06/07 15:24
L51	0	l40 and (((receiv$3 with (dynamic with biometric with information)) with (second with device)) with ((communication with "between") with ((first with communication with interface) and (second with communication with interface)))).clm.	USPAT	OR	OFF	2020/06/07 15:24
L52	0	l40 and (((display$3 with (display with screen with information)) with (based with state with user)) with ((determin$3 with using) with (receiv$3 with (dynamic with biometric with information)))).clm.	USPAT	OR	OFF	2020/06/07 15:24

6/7/2020 3:25:23 PM
C:\Users\ttruong4\Documents\EAST\Workspaces\Case-16535574-080819.wsp

Google displaying on a display screen information based on a state of the user t

Sign in

All Images News Videos More Settings Tools

About 118,000 results (0.57 seconds)

www.google.com/patents/US8836473

Dynamic keypad and fingerprinting sequence authentication



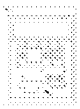
The receiver may receive information from the first fingerprint scanner, the information relating to user biometric information input into the first fingerprint scanner.

Grant - Filed Apr 5, 2012 - Issued Sep 16, 2014 - Rustam N. Wadia - Bank Of America Corporation

Overview · Related · Discuss

www.google.com/patents/US20130264384

Automatic teller machine ("atm") including a user-accessible ...



The method further includes using a second receiver to receive information from a fingerprint scanner relating to first biometric information input into the ...

App. - Filed Apr 5, 2012 - Published Oct 10, 2013 - Rustam N. Wadia - Bank Of America

Overview · Related · Discuss

www.google.com/patents/US20150324564

Dynamic activation of user profiles based on biometric ...

The apparatus may compare the detected biometric information with stored biometric information associated with a stored user profile of a ...

App. - Filed May 7, 2014 - Published Nov 12, 2015 - Debesh Kumar Sahu - Qualcomm Incorporated

Overview · Related · Discuss

www.google.com/patents/US9329771

Embedded authentication systems in an electronic device

An electronic device with a display and a fingerprint sensor may authenticate a user ... is in a locked state, the device displays a graphical element on the display, the ... based at least in part on fingerprint information of the finger detected by the ... receive and convert physical contact inputs (e.g., from a multi-touch screen), ...

Grant - Filed Jun 20, 2014 - Issued May 3, 2016 - Anthony Fadell - Apple Inc

Overview · Related · Discuss

www.google.com/patents/US9721107

Using biometric verification to grant access to redacted ...

When the content redaction engine receives verification data indicating that the user is biometrically verified, the device displays content without any portion ...

Grant - Filed Jun 8, 2013 - Issued Aug 1, 2017 - Byron Bay Han - Apple Inc.

Overview · Related · Discuss

www.google.com/patents/US20130057573

Smart Display with Dynamic Face-Based User Preference Settings



The display can include a processor configured to adjust a user preference or display an indicator to the user based on the detected user parameter.

App. - Filed Nov 11, 2011 - Published Mar 7, 2013 - Hari Chakravarthula - DigitalOptics Corporation Europe Limited

Overview · Related · Discuss

www.google.com/patents/US20140359757

User authentication biometrics in mobile devices

The control system may be capable of receiving, from the finger tap sensing system, information regarding one or more finger taps and of determining a finger ...

App. - Filed Feb 11, 2014 - Published Dec 4, 2014 - Muhammed Ibrahim Sezan - Qualcomm Incorporated

Overview · Related · Discuss

www.google.com/patents/US9235733

Mobile biometrics information collection and identification

A biometric mobile device is capable of interacting with existing cellular, ... of a biometric mobile device may comprises a touch display screen for showing a ...
Grant - Filed Feb 23, 2012 - Issued Jan 12, 2016 - J. Douglas Birdwell - J. Douglas Birdwell

Overview · Related · Discuss

www.google.com/patents/US9342674

Man-machine interface for controlling access to electronic ...

In response to detecting the biometric information associated with the user, in accordance with a determination that the detected biometric information ...
Grant - Filed Mar 5, 2015 - Issued May 17, 2016 - David S. Abdallah - Apple Inc.

Overview · Related · Discuss

www.google.com/patents/US9288207

Secure communications smartphone system

When a communication is received by a recipient computing device, the recipient will typically be presented with information displayed in the user interface of ...
Grant - Filed Sep 4, 2014 - Issued Mar 15, 2016 - John Cronin - Grandios Technologies, Llc

Overview · Related · Discuss

IPR2025-01313; Samsung
Ex. 1002 - Page 64

Google acquiring static biometric information by a static biometric information ac

Sign in

All News Images Shopping More Settings Tools

About 29,300 results (0.54 seconds)

www.google.com/patents/US20120268241

Biometric chain of provenance



The transaction device may link the acquired biometric information to a universal biometric record of the individual. A biometric integrity engine may compare ...
App. - Filed Apr 18, 2012 - Published Oct 25, 2012 - Keith J. Hanna - Eyelock Inc.
Overview · Related · Discuss

www.google.com/patents/US20050089203

Multi-biometric finger sensor using different biometrics ...



A multi-biometric finger sensor may sense different biometric characteristics that have different matching selectivities and that have at least a known spatial ...
App. - Filed Sep 3, 2004 - Published Apr 28, 2005 - Dale Setlak - Authentec, Inc.
Overview · Related · Discuss

www.google.com/patents/US9721142

Multi-resolution fingerprint sensor

The multi-resolution fingerprint sensors each include a portion of the imaging area or ... software stack, which expects a uniform resolution for the entire image acquired. ... and the second image to determine biometric information of the input object. ... access memories (DRAM), and static random access memories (SRAM).
Grant - Filed Jun 26, 2015 - Issued Aug 1, 2017 - Anthony P. Russo - Synaptics Incorporated
Overview · Related · Discuss

www.google.com/patents/US7358515

Multi-biometric finger sensor including electric field ...



In some embodiments, the electric field finger sensing pixels and the at least one other finger biometric sensor may operate based upon static placement of the ...
Grant - Filed Sep 3, 2004 - Issued Apr 15, 2008 - Dale R. Setlak - Authentec, Inc.
Overview · Related · Discuss

www.google.com/patents/US20100208953

Illuminated Fingerprint Sensor and Method



A fingerprint sensing device includes a fingerprint sensor and a light source proximate the fingerprint sensor. The light source is capable of ...
App. - Filed Feb 12, 2010 - Published Aug 19, 2010 - Lawrence C. Gardner - Validity Sensors, Inc.
Overview · Related · Discuss

www.google.com/patents/US9314193

Biometric apparatus and method for touch-sensitive devices

The processor is further configured to generate biometric signature ... modern touch screen technology to acquire the patterns of one, two, ... information, a time-dependent pattern is used, not just a simple static finger geometry pattern. ... and a touch sensor of the electronic device is acquired, from which a ...
Grant - Filed Oct 13, 2012 - Issued Apr 19, 2016 - Waleed Sami Haddad - Biogy, Inc.
Overview · Related · Discuss

www.google.com/patents/US7197168

Method and system for biometric image assembly from multiple ...

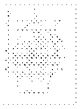


Capability to adjust sensor settings during acquisition process to obtain ... that any fingerprint processing system can use information if when called upon to do so.
Grant - Filed Jul 12, 2002 - Issued Mar 27, 2007 - Anthony P. Russo - Atrua Technologies, Inc.

Overview · Related · Discuss

www.google.com/patents/US6289114

Fingerprint-reading system

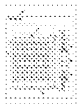


A fingerprint-reading system includes a fingerprint sensor having an active ... In most cases, the sensors give an analog type of information element and the ...
Grant - Filed Jun 5, 1997 - Issued Sep 11, 2001 - Jean-François Mainguet - Thomson-Csf

Overview · Related · Discuss

www.google.com/patents/US6720712

Piezoelectric identification device and applications thereof



More particularly, it relates to a piezoelectric device for obtaining biometric data or information, such as a fingerprint, and using the obtained information to ...
Grant - Filed Mar 23, 2001 - Issued Apr 13, 2004 - Walter G. Scott - Cross Match Technologies, Inc.

Overview · Related · Discuss

www.google.com/patents/US9177191

Fingerprint sensing assemblies and methods of making

A fingerprint sensing module includes a sensor substrate having a sensing side and a circuit side, an image sensor including conductive traces on the circuit ...
Grant - Filed Oct 20, 2014 - Issued Nov 3, 2015 - Fred G Benkley, III - Synaptics Incorporated

Overview · Related · Discuss

IPR2025-01313; Samsung
Ex. 1002 - Page 66

… a user to an application in a **first communications** network by means of a mobile station **communicating** with the application through a **second communications** …
E Turtiainen - US Patent 6,430,407, 2002 - Google Patents
... Google has not **performed** a legal analysis and makes no representation as to the ... In addition, users are not able to **perform** the calculations required in the **authentication** ... only one ISP through which both networks **communicate** towards the Internet, **communication** could be ...
☆ 99 Cited by 110 Related articles All 2 versions »

Communication card for mobile network devices and **authentication** method for users of mobile network devices
E Lauper - US Patent 8,151,334, 2012 - Google Patents
... Google has not **performed** a legal analysis and makes no representation as to the accuracy of ... radio systems, such as eg with GSM (Global System for Mobile **Communications**) and/or ... US13/411,757 US8752155B2 (en), 2004-10-11, 2012-03-05, **Communication** card for mobile ...
☆ 99 Cited by 76 Related articles All 4 versions »

Authentication of data **communications**
M Baentsch, P Buhler, T Eirich, T Kramp… - US Patent …, 2015 - Google Patents
... for wireless **communication** with mobile phone 7, together with security logic 12 for **performing** the **authentication** ... I(X) with camera 17 of mobile phone 7, and by **doing** so the ... the **resulting** **authentication** response is received by server 3, the server can **perform** several calculations ...
☆ 99 Cited by 49 Related articles All 4 versions »

Communication interface device for managing wireless data **transmission** between a vehicle and the internet
HB Kolls - US Patent 7,003,289, 2006 - Google Patents
Communication interface device for managing wireless data transmission between a vehicle and the internet. Download PDF ... Google has not **performed** a legal analysis and makes no representation as to the accuracy of the status listed.) Active, expires 2023-01-25 Application ...
☆ 99 Cited by 204 Related articles All 2 versions »

External **communication interface** for a digital camera
T Hashimoto, H Fukuoka, T Ohkuma - US Patent 5,815,205, 1998 - Google Patents
... Google has not **performed** a legal analysis and makes no representation as to ... another apparatus; H04N2201/0034—Details of the connection, eg connector, **interface**; ... Detecting or checking connection. H—ELECTRICITY; H04—ELECTRIC **COMMUNICATION** TECHNIQUE; H04N ...
☆ 99 Cited by 92 Related articles All 2 versions »

Method of using fingerprints to **authenticate** wireless **communications**
Y Li, DRK Rao, S Subbiah - US Patent 6,219,793, 2001 - Google Patents
... B—**PERFORMING** OPERATIONS; TRANSPORTING; B60—VEHICLES IN GENERAL; B60R—VEHICLES, VEHICLE FITTINGS, OR ... above for the central **authentication** node, the source may **perform** the following ... call is blocked at step 315 (and step 318 is optionally **performed**) ...
☆ 99 Cited by 289 Related articles All 2 versions »

Secure data **communication** over a memory-mapped serial **communications interface** utilizing a distributed firewall
PS Levy, S Cornelius - US Patent 8,212,633, 2001 - Google Patents
... Google has not **performed** a legal analysis and makes no representation as to the ... over a serial **communications interface**, as well as to secure data **communication** incorporating data ... with other electronic devices for the purpose of constructing systems that **perform** useful tasks ...
☆ 99 Cited by 204 Related articles All 2 versions »

Method and **interface** for facilitating **communication** between a cellular telephone or similar wireless device and other devices or systems via an **interface**
D Ma, J Lu - US Patent App. 10/910,002, 2005 - Google Patents
... Google has not **performed** a legal analysis and makes no representation as to ... with another apparatus; H04N2201/0034—Details of the connection, eg connector, **interface**; ... 0039—Connection via a network. H—ELECTRICITY; H04—ELECTRIC **COMMUNICATION** TECHNIQUE; ...
☆ 99 Cited by 132 Related articles All 2 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 67

Pocket encrypting and **authenticating communications** device

AA Caputo, VP Amoruso - US Patent 5,778,071, 1998 - Google Patents

... Google has not **performed** a legal analysis and makes no representation as to the accuracy ... H04L63/0428—Network architectures or network **communication** protocols for network security for providing a confidential data exchange among entities **communicating** through data ...

☆ 99 Cited by 213 Related articles All 2 versions »

Pocket encrypting and **authenticating communications** device

AA Caputo, VP Amoruso - US Patent 5,878,142, 1999 - Google Patents

... Google has not **performed** a legal analysis and makes no representation as to the ... to cryptographic mechanisms or cryptographic arrangements for secret or secure **communication** H04L9/00; ... The capability to **perform** this cryptography is herein referred simply to as encryption ...

☆ 99 Cited by 159 Related articles All 2 versions »

Google maintaining the unlocked state during a condition that the dynamic biom Sign in

All News Videos Images More Settings Tools

About 12,400 results (0.50 seconds)

www.google.com/patents/US7020308

Personal authentication system using biometrics information



The system includes a biometrics information inputting section having a function to acquire the to-be-verified biometrics information; a biometrics information ...
Grant - Filed Aug 15, 2000 - Issued Mar 28, 2006 - Takashi Shinzaki - Fujitsu Limited
Overview · Related · Discuss

www.google.com/patents/US9329771

Embedded authentication systems in an electronic device

While displaying the graphical element, the device detects an input that includes movement of a finger in the first direction over the fingerprint sensor and ...
Grant - Filed Jun 20, 2014 - Issued May 3, 2016 - Anthony Fadell - Apple Inc
Overview · Related · Discuss

www.google.com/patents/US20130287272

Methods and Apparatus of Integrating Fingerprint Imagers ...



The touch panel behind the layer of fingerprint imagers can sense ... Info: Patent citations (15) ... the computing system is unlocked and it is in accessible state (350). ... that comprises the touch-fingerprint apparatus can keep verifying the ... of dynamic user interaction artifact over fingerprint imager for user ...
App. - Filed Apr 29, 2012 - Published Oct 31, 2013 - Yang Lu - Yang Lu
Overview · Related · Discuss

www.google.com/patents/EP3101868A1?cl=en

Device, method, and graphical user interface for ...

When a fingerprint sensor is used without a separate touch-sensitive surface, the fingerprint sensor can serve as a substitute for many of the functions of the ...
App. - Filed Sep 9, 2014 - Published Dec 7, 2016 - Byron Han - Apple Inc.
Overview · Related · Discuss

www.google.com/patents/CN104200145A?cl=en

Embedded authentication systems in an electronic device

In some embodiments, the authentication system may be operative to detect a visual ... access restricted files, applications (e.g., applications purchased by the user), ... Thereby that can preserve by the biometrics attribute that relatively detects ... function of equipment is in the lock state: display graphics element on display, ...
App. - Filed Sep 9, 2008 - Published Dec 10, 2014 - A·法德尔 - 苹果公司
Overview · Related · Discuss

www.google.com/patents/US20060120573

Integrated system for detecting and matching fingerprints



As a consequence, one can obtain the acquisition of a fingerprint image even under critical conditions and still keep a correct contrast between ridges and ...
App. - Filed Feb 4, 2004 - Published Jun 8, 2006 - Marco Iori - Salbert Co. Ltd.
Overview · Related · Discuss

www.google.com/patents/US9715616

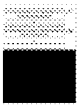
Fingerprint sensing and enrollment

One or more portions of at least one image of biometric data in the set of images can be selected to be included in the unified image of biometric data.
Grant - Filed Oct 21, 2016 - Issued Jul 25, 2017 - Byron B. Han - Apple Inc.
Overview · Related · Discuss

IPR2025-01313; Samsung
Ex. 1002 - Page 69

www.google.com/patents/US20150042575

Information processing method and electronic device



The method includes: determining whether an unlock operation is received in when the electronic device is in a lock-screen state, to obtain a first determination ...
App. - Filed Mar 30, 2014 - Published Feb 12, 2015 - Qiang Dong - Lenovo (Beijing) Co., Ltd.
Overview · Related · Discuss

www.google.com/patents/US20090158423

Locking mobile device cradle



Moreover, many traditional locking systems can be ignorant of environmental conditions in relation to a locking state. For example, where a laptop is unlocked ...
App. - Filed Dec 14, 2007 - Published Jun 18, 2009 - Mark Orlassino - Symbol Technologies, Inc.
Overview · Related · Discuss

www.google.com/patents/US7974448

Personal authentication system using biometrics information



The system includes a biometrics information inputting section having a function to acquire the to-be-verified biometrics information, a biometrics information ...
Grant - Filed Jan 23, 2006 - Issued Jul 5, 2011 - Takashi Shinzaki - Fujitsu Limted
Overview · Related · Discuss

IPR2025-01313; Samsung
Ex. 1002 - Page 70

50 years of **biometric** research: Accomplishments, challenges, and opportunities
AK Jain, K Nandakumar, A Ross - Pattern Recognition Letters, 2016 - Elsevier
... This progress has enabled current **state**-of-the-art **biometric** systems to accurately recognize ... small database (current size of the National DNA Index **in** the United **States** is about 12 ... Due to the diverse nature of **biometric** applications (eg, mobile phone **unlocking** to international ...
☆ 99 Cited by 331 Related articles All 9 versions

Biometrics: a tool **for information** security
AK Jain, A Ross, S Pankanti - IEEE transactions on information ..., 2006 - ieeexplore.ieee.org
... compromise security; complex passwords are difficult to remember and, thus, are expensive to **maintain**.1 Some ... have a large number of cuts and bruises on their fingerprints that **keep** changing ... over time due to age, medical **conditions** (such as common cold), emotional **state**, etc ...
☆ 99 Cited by 1257 Related articles All 18 versions

Eraser: A **dynamic** data race detector **for** multithreaded programs
S Savage, M Burrows, G Nelson, P Sobalvarro... - ACM Transactions on ..., 1997 - dl.acm.org
... To ensure that each lockset index represents a unique set of locks we **maintain** a hash ... To **keep** the race detector from reporting such races, we used the EraserIgnoreOn/Off( ) annotations ... The first set of races was detected **in** the code **maintaining** the fingerprints **in** cache entries ...
☆ 99 Cited by 1775 Related articles All 104 versions

Biometric antispoofing methods: A survey **in** face recognition
J Galbally, S Marcel, J Fierrez - IEEE Access, 2014 - ieeexplore.ieee.org
... **in** the area of anti-spoofing requires a significant condensation effort to **keep** track of all ... benchmarks **for** face anti- spoofing approaches, summarizing the detection rates achieved by **state**-of-the ... previous two categories, are focused on the study of **biometric** systems **at** score-level ...
☆ 99 Cited by 252 Related articles All 7 versions

System and method **for** providing secure access to an electronic device using both a screen gesture and facial **biometrics**
C Azar, G Brosioff - US Patent 8,627,096, 2014 - Google Patents
... Hence, this process provides a simplified means of **maintaining** security of a personal computer or other ... Re-authentication of the user's face allows the highest degree of security **while keeping** the system **unlocked** ... If it is the existing authenticated user, the device is **unlocked** 335 ...
☆ 99 Cited by 92 Related articles All 4 versions »

Mobile iris challenge evaluation (MICHE)-I, **biometric** iris dataset and protocols
M De Marsico, M Nappi, D Riccio, H Wechsler - Pattern Recognition Letters, 2015 - Elsevier
... MICHE) competition (Part I). The aim of the competition is to assess the **state** of the ... this type; as an example, subjects wearing eyeglasses were allowed to remove or **keep** them according ... A mobile device gets **unlocked** and ready **for** use when its owner/legitimate user initiates a ...
☆ 99 Cited by 137 Related articles All 5 versions

A survey on **biometric** cryptosystems and cancelable **biometrics**
C Rathgeb, A Uhl - EURASIP Journal on information Security, 2011 - Springer
... A comprehensive discussion including the current **state**-of-the-art approaches to both technologies, security ... set B overlaps largely with A, k is reconstructed, ie, the vault V A is **unlocked** ... **During** authentication, Reed-Solomon codes are applied to reconstruct the polynom p out of ...
☆ 99 Cited by 542 Related articles All 14 versions »

Surveying the development of **biometric** user authentication on mobile phones
W Meng, DS Wong, S Furnell... - ... Surveys & Tutorials, 2014 - ieeexplore.ieee.org
... STAR's Institute **for** Infocomm Research to look **for** a specific voice signature, **in** which the phone **can unlock** without gestures ... Text-independent: no text constraints **during** enrollment and ... **can** be considered such as spatial coordinate of x **at** time t, spatial coordinate of y **at** time t ...
☆ 99 Cited by 177 Related articles All 7 versions

Combined **fingerprint acquisition** and control device
AW Senior - US Patent 6,400,836, 2002 - Google Patents
... stored **in** these computers, such users have a strong interest **in maintaining** the security ... The system, or the attached computer, **could maintain** a flag which contains data indicating the ... the finger **for** authentication, ensuring a high level of security is **maintained** without interrupting ...
☆ 99 Cited by 233 Related articles All 4 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 71

Information processing device, application software start-up system, and application software start-up method

M Hirabayashi, Y Hashimoto... - US Patent App. 16 ..., 2019 - Google Patents

... US 201916535574 A US201916535574 A US 201916535574A US 2019362061 A1 US2019362061 A1 US 2019362061A1 Authority US United **States** Prior art keywords **biometric information information** user processing device **dynamic biometric** Prior art date ...

☆ 99 All 2 versions »

Combined **fingerprint acquisition** and control **device**

AW Senior - US Patent 6,400,836, 2002 - Google Patents

... The status flag, along with the finger coordinates extracted at steps 450 and 460, are **transmitted** to the relevant computer software at step 490 ... 22. The system of claim 1 further comprising a data **transmission** circuit for **transmitting** said at least one contact parameter to the ...

☆ 99 Cited by 233 Related articles All 4 versions »

Method and system in a client-server for automatically converting messages **from** a **first** format to a **second** format compatible with a message retrieving **device**

ST Segur - US Patent 6,212,550, 2001 - Google Patents

... (d) receiving a **transmit** selected message command **from** one of the one or more subscriber units for selecting a message to be **transmitted** to the ... of claim 14, wherein step (a) further includes the steps of: (a1) receiving a message query; (a2) **transmitting** a greeting ...

☆ 99 Cited by 553 Related articles All 2 versions »

Communication interface device for managing wireless data **transmission** between a vehicle and the internet

HB Kolis - US Patent 7,003,289, 2006 - Google Patents

Communication interface device for managing wireless data **transmission** between a vehicle and the internet. Download PDF **Info** ... patent/US6615186B1/en 2000-06-14 Priority to US09/593,881 priority patent/US7003289B1/en 2000-06-14 Application filed **by** USA Technologies ...

☆ 99 Cited by 204 Related articles All 2 versions »

... for managing, controlling and enabling data **transmission from** a **first device** to at least one other **second device**, wherein the **first** and **second devices** are on different ...

A Youssefian, R Tabbara - US Patent App. 14/099,950, 2014 - Google Patents

... Social applications; Multiplayer Games; Group Chat Rooms; Event **Broadcasting**; Real-time Collaboration; Real ... the customer **by** asking for photo ID **using** the secure data **transmission** protocols as ... The **communication** medium can include any suitable means of **transmitting** and ...

☆ 99 Cited by 23 Related articles All 2 versions »

Using a **first device** to engage in a digital rights management transaction on behalf of a **second device**

A Narin, MA DeMello - US Patent 7,185,363, 2007 - Google Patents

... 6 is a block diagram of an exemplary system in which content may be **acquired**; ... **by** remote processing **devices** that are linked **through** a **communications** network or other data **transmission** medium ... use of the content in the presence of the **first** private key; and. **transmitting** the data ...

☆ 99 Cited by 57 Related articles All 2 versions »

Method and apparatus for **acquiring**, maintaining, and **using information** to be communicated in bar code form with a mobile **communications device**

VT Gobburu, K Narayanan, N Challa... - US Patent ..., 2004 - Google Patents

Method and apparatus for **acquiring**, maintaining, and **using information** to be communicated in bar code form with a ... **Info** ... US 6736322 B2 US6736322 B2 US 6736322B2 Authority US United States Prior art keywords **information communications device** mobile **communications** ...

☆ 99 Cited by 585 Related articles All 4 versions »

Physiological data **acquisition** for integration in a user's avatar via a mobile **communication device**

J Nihtila - US Patent App. 10/988,797, 2005 - Google Patents

... a user involves **acquiring** physiological data associated with the user and **transmitting** the physiological ... fitness data, including various processed data and avatar depictions, and **transmit** the fitness ... In response to **transmission** of the monitoring signals, the resistance between a ...

☆ 99 Cited by 142 Related articles All 2 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 73

Dynamic bandwidth monitor and adjuster for remote **communications** with a medical **device**

CG Nelson, RA Stauffer, CR Stomberg - US Patent 6,564,104, 2003 - Google Patents

... For example, the IMD may contain a **transmission device** capable of **transmitting through** human tissue such ... 1, IMD 112 is equipped with or linked to a **transmission** and receiving **device** such ... patient physiologic data detected **by** a deployed IMD 112 will be **transmitted** via IMDNI ...

☆ 99 Cited by 420 Related articles All 4 versions »

Wireless inter-**device** data processing configured **through** inter-**device transmitted** data

R Dua - US Patent 8,244,179, 2012 - Google Patents

US8244179B2 - Wireless inter-**device** data processing configured **through** inter-**device transmitted** data - Google Patents. Wireless inter-**device** data processing configured **through** inter-**device transmitted** data. Download PDF **Info** ...

☆ 99 Cited by 620 Related articles All 4 versions »

Multiple protocol smart card **communication device**

WC Bonneau, T Vilhelmsen, C Ribeiro... - US Patent ..., 2003 - Google Patents

... of personal identification **information**, like personal identification number [PIN] or **biometric** data; ... the valid smart card **communication** protocol in a **dynamically** reconfigurable manner ... different **communication** protocols utilize different modulation techniques to **transmit** and receive ...

☆ 99 Cited by 315 Related articles All 2 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 74

STIC
Scientific and Technical Information Center

1. Patent Application Titled 'Information Processing **Device**, Application Software Start-Up System, And Application Software Start-Up Method' Published Online (USPTO 20190362061)

In: Information Technology Newsweekly, Dec 17, 2019, 2279; NewsRX LLC
Language: English. Abstract: 2019 DEC 17 (VerticalNews) -- By a News Reporter-Staff News Editor at Information Technology Newsweekly -- According to news reporting originating from Washington, D.C., by VerticalNews journalists, a patent application [...] (*AN: edsgcl.608720217*), Database: Gale General OneFile

Subjects: Japan; Software quality; Software -- Methods; Software -- Intellectual property; Control equipment -- Methods; Control equipment -- Intellectual property

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 75

2. ## RAM Dumps, Hash Algorithms, Smearing, Encryption, and Order of Volatility.

By: Hannon, Michael J. *Computer & Internet Lawyer*. Jun2020, Vol. 37 Issue 6, p8-18. 11p. Abstract: The article discusses that digital evidence created and stored on computers, smartphones, and other digital **devices** has become increasingly important in criminal investigations and trials. It mentions that volatile memory forensics can be classified into two major types: live analysis and acquiring and analyzing RAM dumps; and also mentions that memory on a live computer is constantly changing during acquisition of a random access memory (RAM) dump. (*AN: 143053261*), Database: Computer Source

Subjects: ELECTRONIC evidence; SMARTPHONES; CRIMINAL investigation; RANDOM access memory; FLASH memories

PDF Full Text (461KB) **USPTO Full Text Options**

3. ## **Devices** and Methods for Adjusting the Provision of Notifications

Patent Application: 16/142599. Filed: September 26, 2018. Published: November 7, 2019. , Database: USPTO Patent Applications
Abstract: While an electronic **device** with a display is in a reduced notification mode, the **device** receives one or more **communications**. After receiving the one or more **communications**, the **device** detects an alert condition for the reduced notification mode. In **response** to detecting the alert condition for the reduced notification mode, the **device** displays a **first** user **interface** that includes a **first** affordance which, when activated, causes deactivation of the reduced notification mode of the electronic **device**. In **response** to detecting a **first** input that activates the **first** affordance, the **device** deactivates the reduced notification mode, and displays a **second** user **interface**. The **second** user **interface** does not display content from any one of the one or more **communications**. While the **second** user **interface** is displayed, in **response** to detecting a **second** input, the **device** displays notifications that include content for at least some of the one or more **communications**.
AN: edspap.20190342447

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 76

4. ## Applied Cryptography : Protocols, Algorithms and Source Code in C

By: Schneier, Bruce. Edition: **Second** edition, 20th anniversary edition. Indianapolis, IN : Wiley. 2015. eBook. Description: From the world's most renowned security technologist, Bruce Schneier, this 20th Anniversary Edition is the most definitive reference on cryptography ever published and is the seminal work on cryptography. Cryptographic techniques have applications far beyond the obvious uses of encoding and decoding information. For developers who need to know about capabilities, such as digital signatures, that depend on cryptographic techniques, there's no better overview than Applied Cryptography, the definitive ... (*AN 1535854*), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Security / Cryptography & Encryption; Cryptography; C (Computer program language)

EPUB Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

5. ## Inventive **Communication** and Computational Technologies : Proceedings of ICICCT 2019

By: G. Ranganathan; Joy Chen; Álvaro Rocha. Series: Lecture Notes in Networks and Systems, Vol. 89. Edition: **1st** ed. 2020. Singapore : Springer. 2020. eBook. Description: This book gathers selected papers presented at the Inventive **Communication** and Computational Technologies conference (ICICCT 2019), held on 29–30 April 2019 at Gnanamani College of Technology, Tamil Nadu, India. The respective contributions highlight recent research efforts and advances in a new paradigm called ISMAC (IoT in Social, Mobile, Analytics and Cloud contexts). Topics covered include the Internet of Things, Social Networks, Mobile **Communications**, Big Data Analytics, Bio-inspired Computing ... (*AN 2364338*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; BUSINESS & ECONOMICS / Industries / Computers & Information Technology; COMPUTERS / Artificial Intelligence / General; TECHNOLOGY & ENGINEERING / Mobile & Wireless **Communications**; COMPUTERS / Programming / Mobile **Devices**

Full Text Finder **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 77

6. Proceedings of the **First** International Conference on Intelligent Computing and **Communication**

By: Mandal, Jyotsna Kumar; Satapathy, Suresh Chandra; Sanyal, Manas Kumar; Bhateja, Vikrant. Series: Advances in Intelligent Systems and Computing, v. 458. Singapore : Springer. 2017. eBook. Description: The book covers a wide range of topics in Computer Science and Information Technology including swarm intelligence, artificial intelligence, evolutionary algorithms, and bio-inspired algorithms. It is a collection of papers presented at the **First** International Conference on Intelligent Computing and **Communication** (ICIC2) 2016. The prime areas of the conference are Intelligent Computing, Intelligent **Communication**, Bio-informatics, Geo-informatics, Algorithm, Graphics and Image Processing, Graph Labeling, ... (*AN 1281875*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Engineering (General); COMPUTERS / Artificial Intelligence / General; COMPUTERS / Security / General; TECHNOLOGY & ENGINEERING / Telecommunications; Artificial intelligence--Congresses

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 78

7. Recent Trends in Information and **Communication** Technology : Proceedings of the **2nd** International Conference of Reliable Information and **Communication** Technology (IRICT 2017)

By: Saeed, Faisal; Gazem, Nadhmi; Patnaik, Srikanta; Saed Balaid, Ali Saleh; Mohammed, Fathey. Series: Lecture Notes on Data Engineering and **Communications** Technologies, v. 5. Cham : Springer. 2018. eBook. Description: This book presents 94 papers from the **2nd** International Conference of Reliable Information and **Communication** Technology 2017 (IRICT 2017), held in Johor, Malaysia, on April 23–24, 2017. Focusing on the latest ICT innovations for data engineering, the book presents several hot research topics, including advances in big data analysis techniques and applications; mobile networks; applications and usability; reliable **communication** systems; advances in computer vision, artificial intelligence and soft ... (*AN 1526117*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Engineering (General); TECHNOLOGY & ENGINEERING / Telecommunications; Artificial intelligence--Congresses; Information technology--Congresses

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 79

8. Intelligent **Communication**, Control and **Devices** : Proceedings of ICICCD 2017

By: Singh, Rajesh; Choudhury, Sushabhan; Gehlot, Anita. Series: Advances in Intelligent Systems and Computing, volume 624. Singapore : Springer. 2018. eBook. Description: The book focuses on the integration of intelligent **communication** systems, control systems, and **devices** related to all aspects of engineering and sciences. It contains high-quality research papers presented at the **2nd** international conference, ICICCD 2017, organized by the Department of Electronics, Instrumentation and Control Engineering of University of Petroleum and Energy Studies, Dehradun on 15 and 16 April, 2017. The volume broadly covers recent advances of intelligent **communication**, intelligent ... (*AN 1789148*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Engineering (General); TECHNOLOGY & ENGINEERING / Automation; TECHNOLOGY & ENGINEERING / Electronics / General; TECHNOLOGY & ENGINEERING / Telecommunications; Telecommunication systems--Control--Congresses; Artificial intelligence--Industrial applications--Congresses; Automatic control--Congresses

Full Text Finder USPTO Full Text Options

9. Wireless **Communications** Security : Solutions for the Internet of Things

By: Penttinen, Jyrki T. J. Chichester, West Sussex, United Kingdom : Wiley. 2016. eBook. Description: This book describes the current and most probable future wireless security solutions. The focus is on the technical discussion of existing systems and new trends like Internet of Things (IoT). It also discusses existing and potential security threats, presents methods for protecting systems, operators and end-users, describes security systems attack types and the new dangers in the ever-evolving Internet. The book functions as a practical guide describing the evolvement of the wireless environment, ... (*AN 1399111*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; Wireless **communication** systems--Security measures; Internet--Security measures; Computer networks--Security measures

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 80

10. ## Information and **Communication** Technology : Proceedings of ICICT 2016

By: Mishra, Durgesh Kumar; Azar, Ahmad Taher; Joshi, Amit. Series: Advances in Intelligent Systems and Computing, volume 625. Singapore : Springer, 2018. eBook. Description: This book volume contains 31 papers presented at ICICT 2016: **Second** International Congress on Information and **Communication** Technology. The conference was held during 12-13 December 2016, Bangkok, Thailand and organized communally by G R Foundation, and Computer Society of India Division IV – **Communication** and Division V – Education and Research. This volume contains papers mainly focused on ICT for computation, algorithms and data analytics, and IT security. (*AN 1614958*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; COMPUTERS / Data Science / Data Analytics; COMPUTERS / Security / General; Computer networks--Congresses; Information technology--Congresses

Full Text Finder **USPTO Full Text Options**

11. ## Mechanical Engineering and Green Manufacturing II

By: Qu, Xilong; Zhong, Shaobo. Series: Applied Mechanics and Materials, v. 155-156. Durnten-Zurich, Switzerland : Trans Tech Publications Ltd, 2012. eBook. Description: Selected, peer reviewed papers from the **2nd** International Conference on Mechanical Engineering and Green Manufacturing (MEGM 2012), March 16-18, 2012, Chongqing, China (*AN 517183*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Materials Science / General; Machine design--Congresses; Sustainable engineering--Congresses; Mechanical engineering--Congresses; Green technology--Congresses

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 81

12. ## Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web.

By: Ghappour, Ahmed. *Stanford Law Review*, Apr2017, Vol. 69 Issue 4, p1075-1136. 62p. Abstract: The use of hacking tools by law enforcement to pursue criminal suspects who have anonymized their **communications** on the dark web presents a looming flashpoint **between** criminal procedure and international law. Criminal actors who use the dark web (for instance, to commit crimes or to evade authorities) obscure digital footprints left behind with third parties, rendering existing surveillance methods obsolete. In **response**, law enforcement has implemented hacking techniques that deploy surveillance software over the Internet to directly access and control criminals' **devices**. The practical reality of the underlying technologies makes it inevitable that foreign-located computers will be subject to remote "searches" and "seizures." The **result** may well be the greatest extraterritorial expansion of enforcement jurisdiction in U.S. law enforcement history. This Article examines how the government's use of hacking tools on the dark web profoundly disrupts the legal architecture on which cross-border criminal investigations rest. These overseas cyberoperations raise increasingly difficult questions regarding who may authorize these activities, where they may be deployed, and against whom they may lawfully be executed. The rules of criminal procedure fail to regulate law enforcement hacking because they allow these critical decisions to be made by rank-and-file officials despite potentially disruptive foreign relations implications. This Article outlines a regulatory framework that reallocates decisionmaking to the institutional actors who are best suited to determine U.S. foreign policy and avoids sacrificing law enforcement's ability to identify and locate criminal suspects who have taken cover on the dark web. [ABSTRACT FROM AUTHOR] (*AN: 123165938*), Database: Academic Search Complete

Subjects: LAW enforcement; CRIMINAL procedure; INTERNATIONAL law; COMPUTER hacking; INVISIBLE Web; CRIMINAL investigation; INTERNATIONAL relations -- Law & legislation; International Affairs; Foreign affairs; UNITED States

PDF Full Text (2MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 82

13. **Communication** and Computing Systems : Proceedings of the International Conference on **Communication** and Computing Systems (ICCCS 2016), Gurgaon, India, 9-11 September, 2016

By: Prasad, B.M.K; Singh, Krishna Kant; Ruhil, Neelam; Singh, Karan; O'Kennedy, Richard. Boca Raton : CRC Press. 2017. eBook. Description: This book is a collection of accepted papers that were presented at the International Conference on **Communication** and Computing Systems (ICCCS-2016), Dronacharya College of Engineering, Gurgaon, September 9 –11, 2016. The purpose of the conference was to provide a platform for interaction **between** scientists from industry, academia and other areas of society to discuss the current advancements in the field of **communication** and computing systems. The papers submitted to the proceedings were peer-reviewed ... (*AN 1470173*), Database: eBook Index

Subjects: COMPUTERS / Computer Engineering; MATHEMATICS / General; Telecommunication--Congresses; Computer systems--Congresses

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 83

14. ## Interactive Mobile **Communication** Technologies and Learning : Proceedings of the 11th IMCL Conference

By: Auer, Michael E.; Tsiatsos, Thrasyvoulos. Series: Advances in Intelligent Systems and Computing, volume 725. Cham, Switzerland : Springer. 2018. eBook. Description: Interactive mobile technologies have now become the core of many—if not all—fields of society. Not only do the younger generation of students expect a mobile working and learning environment, but also the new ideas, technologies and solutions introduced on a nearly daily basis also boost this trend.Discussing and assessing key trends in the mobile field were the primary aims of the 11th International Conference on Interactive Mobile **Communication**, Technologies and Learning (IMCL2017), which was held ... (*AN 1709632*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Engineering (General); COMPUTERS / Artificial Intelligence / General; TECHNOLOGY & ENGINEERING / Telecommunications; Educational technology--Congresses; Mobile **communication** systems in education--Congresses; Distance education--Computer-assisted instruction--Congresses

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung Ex. 1002 - Page 84

15. ## Advanced Computational and **Communication** Paradigms : Proceedings of International Conference on ICACCP 2017, Volume 2

By: Bhattacharyya, Siddhartha; Chaki, Nabendu; Konar, Debanjan; Chakraborty, Udit Kr; Singh, Chingtham Tejbanta. Series: Advanced Computational and **Communication** Paradigms, Volume 2. Singapore : Springer, 2018. eBook. Description: The book titled Advanced Computational and **Communication** Paradigms: Proceedings of International Conference on ICACCP 2017, Volume 2 presents refereed high-quality papers of the **First** International Conference on Advanced Computational and **Communication** Paradigms (ICACCP 2017) organized by the Department of Computer Science and Engineering, Sikkim Manipal Institute of Technology, held from 8– 10 September 2017. ICACCP 2017 covers an advanced computational paradigms and **communications** technique which ... (*AN 1795284*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Electronics / General; COMPUTERS / Networking / Hardware; TECHNOLOGY & ENGINEERING / Telecommunications; Telecommunication systems--Congresses; Soft computing--Congresses; Computer networks--Congresses

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 85

16. ## Modeling, Methodologies and Tools for Molecular and Nano-scale **Communications** : Modeling, Methodologies and Tools

By: Suzuki, J.; Nakano, Tadashi; Moore, Michael John. Series: Modeling and Optimization in Science and Technologies, v. 9. Cham, Switzerland : Springer, 2017. eBook. Description: This book reports on cutting-edge modeling techniques, methodologies and tools used to understand, design and engineer nanoscale **communication** systems, such as molecular **communication** systems. Moreover, it includes introductory materials for those who are new to the field. The book's interdisciplinary approach, which merges perspectives in computer science, the biological sciences and nanotechnology, will appeal to graduate students and researchers in these three areas.The book is organized into ... (*AN 1486446*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Nanotechnology & MEMS; COMPUTERS / Networking / Hardware; MEDICAL / Allied Health Services / Medical Technology; TECHNOLOGY & ENGINEERING / Materials Science / Electronic Materials; **Communication**--Technological innovations; Nanonetworks

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 86

17. ## Emerging Wireless **Communication** and Network Technologies : Principle, Paradigm and Performance

By: Arya, Karm Veer; Bhadoria, Robin Singh; Chaudhari, Narendra S. Singapore : Springer. 2018. eBook. Description: The book covers a wide range of wireless **communication** and network technologies, and will help readers understand the role of wireless technologies in applications touching on various spheres of human life, e.g. healthcare, agriculture, building smart cities, forecasting and the manufacturing industry.The book begins by discussing advances in wireless **communication**, including emerging trends and research directions for network technologies. It also highlights the importance of and need to actively ... (*AN 1827903*), Database: eBook Index

Subjects: COMPUTERS / Networking / Hardware; TECHNOLOGY & ENGINEERING / Electronics / General; TECHNOLOGY & ENGINEERING / Telecommunications; COMPUTERS / Programming / Mobile **Devices**; Computer networks; Wireless **communication** systems

Full Text Finder USPTO Full Text Options

18. ## Renewable and Sustainable Energy

By: Li, Yongguang; Ren, Jianxing; Pan, Weiguo. Series: Advanced Materials Research, 347-353. Durnten-Zurich : Trans Tech Publications Ltd. 2012. eBook. Description: Selected, peer reviewed papers from the 2011 International Conference on Energy, Environment and Sustainable Development (ICEESD 2011), October 21-23, 2011, Shanghai, China (*AN 517080*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Materials Science / General; Renewable energy sources--Congresses

PDF Full Text USPTO Full Text Options Full Download

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 87

19. ## Human Computer Interaction Handbook : Fundamentals, Evolving Technologies, and Emerging Applications, Third Edition

By: Jacko, Julie A. Series: Human Factors and Ergonomics. Edition: 3rd ed. Boca Raton : CRC Press. 2012. eBook. Description: Winner of a 2013 CHOICE Outstanding Academic Title Award The third edition of a groundbreaking reference, The Human–Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications raises the bar for handbooks in this field. It is the largest, most complete compilation of HCI theories, principles, advances, case studies, and more that exist within a single volume. The book captures the current and emerging sub-disciplines within HCI related to research, development, and ... (*AN 452086*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Industrial Health & Safety; Human-computer interaction--Handbooks, manuals, etc; Computer simulation--Handbooks, manuals, etc; Virtual reality--Handbooks, manuals, etc

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

20. ## Computer Engineering : Concepts, Methodologies, Tools and Applications

By: Information Resources Management Association. Hershey, Pa : IGI Global. 2012. eBook. Description: Features perspectives on the fundamental aspects, tools and technologies, methods and design, applications, managerial impact, social/behavioral perspectives, critical issues, and emerging trends in the field of computer engineering. (*AN 431988*), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Computer Engineering; COMPUTERS / Machine Theory; COMPUTERS / Hardware / General; Computer engineering

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 88

21. ## Design Thinking Research : Making Distinctions: Collaboration Versus Cooperation

By: Plattner, Hasso; Meinel, Christoph; Leifer, Larry. Series: Understanding Innovation. Cham, Switzerland : Springer. 2018. eBook. Description: This book summarizes the **results** of Design Thinking Research Program at Stanford University in Palo Alto, California, USA and the Hasso Plattner Institute in Potsdam, Germany. Offering readers a closer look at design thinking, its innovation processes and methods, it covers topics ranging from how to design ideas, methods and technologies, to creativity experiments and creative collaboration in the real world, and the interplay **between** designers and engineers. But the topics go beyond this in their ... (*AN 1622553*), Database: eBook Index

Subjects: BUSINESS & ECONOMICS / Information Management; BUSINESS & ECONOMICS / Industries / Media & **Communications**; BUSINESS & ECONOMICS / Production & **Operations** Management; COMPUTERS / Software Development & Engineering / General; Creative ability in business; Creative ability in technology; Cooperation; Industrial management--Technological innovations

 **Full Text Finder** **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 89

22. Innovations in Electronics and **Communication** Engineering : Proceedings of the 6th ICIECE 2017

By: Saini, H. S.; Singh, Ravi Kishore; Patel, Vishal M.; Santhi, K.; Ranganayakulu, S. V. Series: Lecture Notes in Networks and Systems, volume 33. Singapore : Springer. 2019. eBook. Description: The book is a collection of best selected research papers presented at 6th International Conference on Innovations in Electronics and **Communication** Engineering at Guru Nanak Institutions Hyderabad, India. The book presents works from researchers, technocrats and experts about latest technologies in electronic and **communication** engineering. The book covers various streams of **communication** engineering like signal processing, VLSI design, embedded systems, wireless **communications**, and electronics and .. (*AN 1881267*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; TECHNOLOGY & ENGINEERING / Electronics / General; TECHNOLOGY & ENGINEERING / Machinery; Image processing--Digital techniques--Congresses; Electrical engineering--Congresses; Signal processing--Digital techniques--Congresses

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 90

23. ## Third International Congress on Information and **Communication** Technology : ICICT 2018, London

By: Sherratt, Simon; Dey, Nilanjan; Joshi, Amit. Series: Advances in Intelligent Systems and Computing, v. 797. Singapore : Springer. 2019. eBook. Description: The book includes selected high-quality research papers presented at the Third International Congress on Information and **Communication** Technology held at Brunel University, London on February 27--28, 2018. It discusses emerging topics pertaining to information and **communication** technology (ICT) for managerial applications, e-governance, e-agriculture, e-education and computing technologies, the Internet of Things (IOT), and e-mining. Written by experts and researchers working on ICT, the book is suitable ... (*AN 1905768*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; COMPUTERS / Data Science / Data Analytics; COMPUTERS / Security / General; Computer networks--Congresses; Information technology--Congresses; Internet of things--Congresses

Full Text Finder USPTO Full Text Options

24. ## Impact of Advances in Computing and **Communications** Technologies on Chemical Science and Technology : Report of a Workshop

By: National Research Council (U.S.). Series: Compass Series. Washington, D.C. : National Academies Press. 1999. eBook. Description: Papers from a workshop held Nov. 1-2, 1998, in Washington, D.C. (*AN 11729*), Database: eBook Collection (EBSCOhost)

Subjects: SCIENCE / Chemistry / Clinical; Chemistry--Data processing--Congresses; Chemistry, Technical--Data processing--Congresses; **Communication** in chemistry--Technological innovations--Congresses

PDF Full Text USPTO Full Text Options Full Download

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 91

25. Wireless **Communications**, Networking and Applications : Proceedings of WCNA 2014

By: Zeng, Qing-An. Series: Lecture Notes in Electrical Engineering, volume 348. New Delhi : Springer. 2016. eBook. Description: This book is based on a series of conferences on Wireless **Communications**, Networking and Applications that have been held on December 27-28, 2014 in Shenzhen, China. The meetings themselves were a **response** to technological developments in the areas of wireless **communications**, networking and applications and facilitate researchers, engineers and students to share the latest research **results** and the advanced research methods of the field. The broad variety of disciplines involved in this research and ... (*AN 1087962*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; COMPUTERS / Information Technology; COMPUTERS / Networking / Hardware; Computer networks--Congresses; Wireless **communication** systems--Congresses

Full Text Finder USPTO Full Text Options

26. IoT and Edge Computing for Architects : Implementing Edge and IoT Systems From Sensors to Clouds with **Communication** Systems, Analytics, and Security, **2nd** Edition

By: Perry Lea. Birmingham : Packt Publishing. 2020. eBook. Description: Learn to design, implement, and secure your IoT infrastructure. Revised and expanded for edge computing.Key FeaturesBuild a complete IoT system that's the best fit for your organizationLearn about different concepts, tech, and trade-offs in the IoT architectural stackUnderstand the theory and implementation of each element that comprises IoT designBook DescriptionIndustries are embracing IoT technologies to improve operational expenses, product life, and people's well-being. An architectural guide ... (*AN 2391882*), Database: eBook Index

Subjects: COMPUTERS / Hardware / General; COMPUTERS / Distributed Systems / General; COMPUTERS / Networking / Hardware

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 92

27. Information and **Communication** Technologies in Tourism 2019 : Proceedings of the International Conference in Nicosia, Cyprus, January 30 –February 1, 2019

By: Pesonen, Juho; Neidhardt, Julia. Cham, Switzerland : Springer. 2019. eBook. Description: This book provides an extensive, up-to-date overview of the ways in which information and **communication** technologies (ICTs) can be used to develop tourism and hospitality. The coverage encompasses a wide variety of topics within the field, including virtual reality, sharing economy and peer-to-peer accommodation, social media use, hotel technology, big data, robotics, and recommendation systems, to name but a few. The content is based on the 2019 ENTER eTourism conference, organized in Nicosia, Cyprus ... (*AN 1983793*), Database: eBook Index

Subjects: BUSINESS & ECONOMICS / Industries / Hospitality, Travel & Tourism; BUSINESS & ECONOMICS / Industries / Service; BUSINESS & ECONOMICS / Information Management; BUSINESS & ECONOMICS / E-Commerce / Online Trading; COMPUTERS / Online Services; COMPUTERS / Electronic Commerce; Hospitality industry--Computer network resources--Congresses; Information technology--Congresses; Tourism--Data processing--Congresses; Tourism--Computer network resources--Congresses; Hospitality industry--Data processing--Congresses

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 93

28. ## Information and **Communication** Technology for Sustainable Development : Proceedings of ICT4SD 2016, Volume 1

By: Mishra, Durgesh Kumar; Nayak, Malaya Kumar; Joshi, Amit. Series: Information and **Communication** Technology for Sustainable Development, Volume 1. Singapore : Springer, 2018. eBook. Description: The book proposes new technologies and discusses future solutions for design infrastructure for ICT. The book contains high quality submissions presented at **Second** International Conference on Information and **Communication** Technology for Sustainable Development (ICT4SD - 2016) held at Goa, India during 1 - 2 July, 2016. The conference stimulates the cutting-edge research discussions among many academic pioneering researchers, scientists, industrial engineers, and students from all around the world. ... (*AN 1630855*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Engineering (General); COMPUTERS / Design, Graphics & Media / CAD-CAM; COMPUTERS / Data Science / Data Analytics; TECHNOLOGY & ENGINEERING / Telecommunications; Sustainable development--Congresses; Information technology--Congresses

Full Text Finder USPTO Full Text Options

29. ## Selfie Biometrics : Advances and Challenges

By: Ajita Rattani; Reza Derakhshani; Arun Ross. Series: Advances in Computer Vision and Pattern Recognition. Edition: **1st** ed. 2019. Cham : Springer, 2019. eBook. Description: This book highlights the field of selfie biometrics, providing a clear overview and presenting recent advances and challenges. It also discusses numerous selfie **authentication** techniques on mobile **devices**. Biometric **authentication** using mobile **devices** is becoming a convenient and important means of verifying identity for secured access and services such as telebanking and electronic transactions. In this context, face and ocular biometrics in the visible spectrum has gained increased attention from ... (*AN 2255532*), Database: eBook Index

Subjects: COMPUTERS / Artificial Intelligence / Computer Vision & Pattern Recognition; COMPUTERS / User **Interfaces**

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 94

30. A Comprehensive Guide to 5G Security

By: Liyanage, Madhusanka; Ahmad, Ijaz; Abro, Ahmed Bux; Gurtov, Andrei; Ylianttila, Mika. Hoboken, NJ : Wiley. 2018. eBook. Description: The **first** comprehensive guide to the design and implementation of security in 5G wireless networks and **devices** Security models for 3G and 4G networks based on Universal SIM cards worked very well. But they are not fully applicable to the unique security requirements of 5G networks. 5G will face additional challenges due to increased user privacy concerns, new trust and service models and requirements to support IoT and mission-critical applications. While multiple books already exist on 5G, this ... (*AN 1682279*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; Mobile **communication** systems--Security measures; Wireless **communication** systems--Security measures

 **Full Text Finder** **USPTO Full Text Options**

EBSCO Connect | Privacy Policy | A/B Testing | Terms of Use | Copyright | Cookie Policy | Contact Us

powered by EBSCO*host*

© 2020 EBSCO Industries, Inc. All rights reserved.

IPR2025-01313; Samsung
Ex. 1002 - Page 95

A novel force sensitive tablet for handwriting **information acquisition**

Z Wu, P Fang, M Meng, F Shen - Chinese Conference on **Biometric** ..., 2004 - Springer
... and chemical **biometrics** such as DNA and body odor have been **acquired** and analyzed ... As a comparison, **another** experiment was done to **acquire** handwriting **information** from the same ... Experimental results show that the tablet is indeed capable of **obtaining** forces, trajectory ...
☆ 99 Cited by 21 Related articles All 8 versions »

An anti-spoofing technique using **multiple** textural features in **fingerprint** scanners

E Marasco, C Sansone - 2010 IEEE workshop on **biometric** ..., 2010 - ieeexplore.ieee.org
... The effectiveness of the algorithm depends on efficient extraction of the evolving pattern from images **acquired** in **two** ... Performances depend on the technology of the **sensor** used to **acquire** the **fingerprint** images ... Aliveness detection of **fingerprint** using **multiple static** features ...
☆ 99 Cited by 41 Related articles All 2 versions

Fingerprint sensing device and recognition system having predetermined electrode activation

AG Knapp - US Patent 5,325,442, 1994 - Google Patents
... G—PHYSICS; G11—**INFORMATION** STORAGE; G11C—**STATIC** STORES; G11C11/00—Digital stores ... characters or for recognising patterns, eg fingerprints; G06K9/00006—**Acquiring** or recognising ... electrodes, according to the ridge/trough pattern of the **fingerprint**, and hence ...
☆ 99 Cited by 401 Related articles All 3 versions »

Methods and apparatus for **acquiring** a swiped **fingerprint** image

DJ Geoffroy, JJ Buxton - US Patent 8,077,935, 2011 - Google Patents
... printed or written characters or for recognising patterns, eg fingerprints; G06K9/00006—**Acquiring** or recognising ... scan of the drive plates, a linear one-dimensional slice of the **fingerprint** is **acquired** ... In order to **acquire** a useful **fingerprint** image, the user must position the finger ...
☆ 99 Cited by 95 Related articles All 4 versions »

Combining perspiration-and morphology-based **static** features for **fingerprint** liveness detection

E Marasco, C Sansone - Pattern Recognition Letters, 2012 - Elsevier
... to capture the non-regular shape typical of the ridges in an image **acquired** from a ... The formula for this **static** measure SM is given from the following:(8) SM = ∑ k = 11 ... The considered **sensors** are optical and the employed **fingerprint sensing** mechanism **acquires** the image by ...
☆ 99 Cited by 78 Related articles All 6 versions

Fusion of **static** and dynamic body **biometrics** for gait recognition

L Wang, H Ning, T Tan, W Hu - IEEE Transactions on circuits ..., 2004 - ieeexplore.ieee.org
... C. Overview of the Approach For **obtaining** optimal performance, an automatic person identification system should ... mean shapes from **multiple** sequences of the same subject, we may **acquire** an exemplar by ... [4] A. Bobick and A. Johnson, "Gait recognition using **static** activity-spe ...
☆ 99 Cited by 478 Related articles All 22 versions

Combined **fingerprint acquisition** and control **device**

AW Senior - US Patent 6,400,836, 2002 - Google Patents
... 5. The system of claim 3 wherein said system repeatedly **acquires fingerprint** images and ... said system comprising: a **fingerprint** image **acquisition** scanner for **acquiring** a **fingerprint** image ... an image processor for extracting from said **acquired fingerprint** image a **two** dimensional ...
☆ 99 Cited by 233 Related articles All 4 versions »

Fingerprint silicon replicas: **static** and dynamic features for vitality detection using an optical capture **device**

P Coli, GL Marcialis, F Roli - International Journal of Image and ..., 2008 - World Scientific
... The system **acquires** consecutive frames during the rotation of the fingertip ... In order to investigate **static** and dynamic features, we collected a **multiple**- frames/**multiple**-impressions ... Images were **acquired** from 82 different fingerprints from 50 people aged between 20 and 70 and ...
☆ 99 Cited by 47 Related articles All 6 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 96

Enclosure and **biometric** data collection for **fingerprint sensor device**

L O'gorman, WH Miller - US Patent 6,970,584, 2005 - Google Patents

... US7139414B1 (en) *, 1999-06-24, 2006-11-21, Nec Corporation, Method for removing **static** electricity in ... en), 2004-05-07, 2009-06-02, Yt **Acquisition** Corporation, System and method for upgrading **biometric** data ... Methods and apparatus for **acquiring** a swiped **fingerprint** image ...

☆ 99 Cited by 131 Related articles All 4 versions »

Fingerprint recognition system

KS Champagne, JJ Turek ... - US Patent App. 11 ..., 2008 - Google Patents

... or written characters or for recognising patterns, eg fingerprints; G06K9/00006—**Acquiring** or recognising ... A swipe-based **sensor** can **acquire** higher resolution images of the finger using only ... Different mechanisms are employed for **obtaining** a **fingerprint** image as the finger is ...

☆ 99 Cited by 94 Related articles All 2 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 97

Google acquiring dynamic biometric information from a body of a user by a dyna

Sign in

All News Images Shopping More Settings Tools

About 34,100 results (0.49 seconds)

www.google.com/patents/US20070253602

Biometric data acquisition device, biometric data ...



A biometric data acquisition device for acquiring data of a living body by ... Preferably, in the biometric data acquisition device according to the first ... The quality of acquired vein pattern information can be improved while the dynamic range is ... authentication control unit 22 reads out user ID in the memory 19 and sends it ...
App. - Filed Apr 25, 2007 - Published Nov 1, 2007 - Kazuhiko Amano - Seiko Epson Corporation
Overview · Related · Discuss

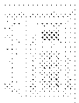
www.google.com/patents/US20160217310

System and method for partial fingerprint enrollment and ...

The mobile device includes a fingerprint registration unit configured to receive ... user are acquired and system registers the user by storing biometric information ...
App. - Filed Jan 27, 2016 - Published Jul 28, 2016 - Jidnya Samir SHAH - Samsung Electronics Co., Ltd.
Overview · Related · Discuss

www.google.com/patents/US8063889

Biometric data collection system



Other data about the user may be acquired during use of the touch screen. This data and information may be obtained about the user without the user being ...
Grant - Filed Apr 25, 2007 - Issued Nov 22, 2011 - Bruce W. Anderson - Honeywell International Inc.
Overview · Related · Discuss

www.google.com/patents/US9373047

Biometric authentication device, biometric authentication ...

A biometric authentication device includes a photographing unit configured to photograph a biological body and acquire biological body information; ...
Grant - Filed Mar 9, 2012 - Issued Jun 21, 2016 - Takahiro Aoki - Fujitsu Limited
Overview · Related · Discuss

www.google.com/patents/US7020308

Personal authentication system using biometrics information



A personal authentication system using biometrics information, which or to acquire and use time series data such as voice, keystroke or dynamic signature.
Grant - Filed Aug 15, 2000 - Issued Mar 28, 2006 - Takashi Shinzaki - Fujitsu Limited
Overview · Related · Discuss

www.google.com/patents/US9314193

Biometric apparatus and method for touch-sensitive devices

Contact data resulting from sensing contact between a user's body part and a touch sensor of the electronic device is acquired, from which a ...
Grant - Filed Oct 13, 2012 - Issued Apr 19, 2016 - Waleed Sami Haddad - Biogy, Inc.
Overview · Related · Discuss

www.google.com/patents/US8797140

Biometric authentication method and biometric authentication ...



... first biometric information of the user, providing first authentication, obtaining ... block diagram illustrating a configuration of a biometric authentication device ... vein constitutes information of an internal part of a living body, which is unaffected ... a group of registrants whose biometric information previously acquired for the ...
Grant - Filed Mar 3, 2008 - Issued Aug 5, 2014 - Takashi Shinzaki - Fujitsu Limited

Overview · Related · Discuss

www.google.com/patents/CN101099676A?cl=en

Biological information acquisition device, method for ...

A biological information acquisition device that acquires information from a ... and reflected light from the biological body irradiated with light by the light source; and ... with reference to patent documentation 1) of fingerprint, iris or the vein pattern ... Yet, since illumination light be defined by the dynamic range of light, so, exist ...
App. - Filed May 15, 2007 - Published Jan 9, 2008 - 天野和彦 - 精工愛普生株式会社;国立大学法人北海道大学
Overview · Related · Discuss

www.google.com/patents/US9400911

Fingerprint sensor and integratable electronic display

A fingerprint sensor which includes a conductive layer which is incorporatable within an electronic display is disclosed. The fingerprint sensor also includes a ...
Grant - Filed May 3, 2011 - Issued Jul 26, 2016 - Richard Alexander Erhart - Synaptics Incorporated
Overview · Related · Discuss

www.google.com/patents/US20160349104

Biometric monitoring device having a body weight sensor, and ...

A system comprising a biometric monitoring device including a housing including a platform to receive at least one foot of the user, a body weight sensor to ...
App. - Filed Jul 26, 2016 - Published Dec 1, 2016 - Shelten Gee Jao Yuen - Fitbit, Inc.
Overview · Related · Discuss

IPR2025-01313; Samsung
Ex. 1002 - Page 99

Method and wireless **device** for establishing a **communication interface** for a **communication** session

NJ Jenniges, PJ Smith, JT Jobling, S Gupta… - US Patent …, 2005 - Google Patents
... or content conversion, eg adaptation by the network of the transmitted or **received information** for the ... 2 may start **with** the wireless **device** 120 (eg, **via** the controller 230) **receiving** presence **information** ... 9 , for example, the user may **receive** an e-mail message from Buddy **#2**. As ...
☆ 99 Cited by 167 Related articles All 4 versions »

Digital electronic still camera which **receives** an input/output control program **through** a detachable **communication interface** card

H Fukuoka - US Patent 6,104,430, 2000 - Google Patents
Digital electronic still camera which **receives** an input/output control program **through** a detachable ... The camera 30 includes a card connector 17 for **receiving two** PCMCIA type cards such as a ... is that the digital electronic camera can remotely transmit and **receive** images from a ...
☆ 99 Cited by 260 Related articles All 2 versions »

Rechargeable mobile hand-held **fingerprint** scanner **with** a data and power **communication interface**

GW McClurg, D Brunell, WG Scott - US Patent 6,886,104, 2005 - Google Patents
... Mobile use is increasingly desired in **biometric** applications, such as law enforcement ... 150 can be any type of computer, processor(s), or logic which can **receive** and process ... rate of charging) of a rechargeable battery 224 when **fingerprint** scanner 102 is **receiving** power **through** ...
☆ 99 Cited by 240 Related articles All 2 versions »

Personal **communication** system to send and **receive** voice data positioning **information**

ML Obradovich, J Dinkel, M Kent - US Patent 6,148,261, 2000 - Google Patents
Personal **communication** system to send and **receive** voice data ... US 87995597 A US87995597 A US 87995597A US 6148261 A US6148261 A US 6148261A Authority US United States Prior art keywords map processor map **information information** communicator Prior art ...
☆ 99 Cited by 643 Related articles All 2 versions »

… **communications between** networks by translating **communications received** in ip protocol to non-ip protocol to remove address and routing services **information**

EJ Gelb - US Patent 5,550,984, 1996 - Google Patents
... UDP provides an connectionless delivery service to send and **receive** packets from specific processes **between** sending and **receiving** nodes of ... When a response is **received**, motherboard 20 translates the response from TCP/IP format back into IPX format and transmits it ...
☆ 99 Cited by 524 Related articles All 2 versions »

Method and system in a client-server for automatically converting messages from a **first** format to a **second** format compatible **with** a message retrieving **device**

ST Segur - US Patent 6,212,550, 2001 - Google Patents
... **with** one or more subscriber units, a **communication interface** adapted to **receive** one or ... units and for automatically converting one or more of the **received** messages from a ... **communications** client-server, comprising; a plurality of **communication interfaces** for **receiving** a plurality ...
☆ 99 Cited by 553 Related articles All 2 versions »

Dynamic modification of a messaging language

OK Thorn - US Patent 8,010,338, 2011 - Google Patents
... **Communication device** 110 may then **receive** a request to initiate an outgoing message in response to the ... associated **with** a **received** message or **with** a sender of the **received** message ... 1. A method performed in a **communication device**, the method comprising: **receiving**, by an ...
☆ 99 Cited by 185 Related articles All 4 versions »

Method for securing **communication** by selecting an encoding process **using** a **first** computer based upon ability of a **second** computer and deleting the process …

SJ Borza - US Patent 6,446,210, 2002 - Google Patents
... Upon **receiving** the **information**, an Internet server provides it to an encryption means for decryption ... {. //**Receive** data ... The processor 54 characterises the **biometric information** samples in accordance **with** the process **received** from the server 51 and the characterisations are ...
☆ 99 Cited by 164 Related articles All 2 versions »

Portable ECG **device with** wireless **communication interface** to remotely monitor patients and method of use

DE Brodnick, I Rowlandson - US Patent 6,970,737, 2005 - Google Patents

... which sends the GPS initialization signal to the ECG **device**, and once **received**, the ECG ... a lead wire assembly, each lead wire having a transducer capable of **receiving** an ECG ... a wireless **communication interface** integrated **with** the ECG monitor to **receive** patient ECG data ...

☆ 99 Cited by 78 Related articles All 2 versions »

Mobile **device interface with** dual windows

CL Chiang, CP Chiang, CW Tai, CY Chen - US Patent 8,600,446, 2013 - Google Patents

... has a Global Positioning System (GPS) receiver embedded in it to provide location **information** ... However, a GPS-enabled **device** generally **receives** location signals 108 from several satellites ... 116 is **another** mobile **device**, the call is routed **through** a **second** wireless network ...

☆ 99 Cited by 416 Related articles All 4 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 101

STIC
Scientific and Technical Information Center

1. **INFORMATION** PROCESSING **DEVICE**, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD

Patent Application: 16/535574. Filed: August 08, 2019. Published: November 28, 2019. , Database: USPTO Patent Applications

Abstract: The purpose of the present invention is to provide a portable terminal and an application software start-up system whereby the application software that is started up is limited depending on the state of a **user**, thereby providing an improved ease of use. For this purpose, an application software start-up method for an **information** processing **device** comprises: performing identity authentication based on static biological **information**; determining the state of the **user** by comparing **dynamic** biological **information** acquired from the **body** of the **user** with previously measured **dynamic** biological **information**; and limiting the application software that is started up in accordance with the determined state of the **user** and on the basis of a permission level that is set in advance for each application software item.

AN: edspap.20190362061

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 102

2. ## Possibilities of **dynamic biometrics** for authentication and the circumstances for using **dynamic biometric** signature.

By: Hortai, Frantisek. *Journal of Systems Integration (1804-2724)* , 2018, Vol. 9 Issue 1, p3-18, 16p Abstract: New **information** technologies alongside their benefits also bring new dangers with themselves. It is difficult to decide which authentication tool to use and implement in the **information** systems and electronic documents. The final decision has to compromise among the facts that it faces several conflicting requirements: highly secure tool, to be a **user**-friendly and **user** simplicity method, ensure protection against errors and failures of **users**, speed of authentication and provide these features for a reasonable price. Even when the compromised solution is found it has to fulfill the given technology standards. For the listed reasons the paper argues one of the most natural **biometric** authentication method the **dynamic biometric** signature and lists its related standards. The paper also includes measurement evaluation which solves the independence between the person's signature and **device** on which it was created. [ABSTRACT FROM AUTHOR] DOI: 10.20470/jsi.v9i1.326; (*AN 128354732*), Database: Applied Science & Technology Source

Subjects: Information technology; **Biometric** identification; Electronic authentication

PDF Full Text (3.2MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 103

3. ## Evaluation of stability of swipe gesture authentication across usage scenarios of mobile device.

By: Ellavarason, Elakkiya; Guest, Richard; Deravi, Farzin. *EURASIP Journal on Information Security* , 3/17/2020, Vol. 2020 Issue 1, p1-14, 14p Abstract: Background: User interaction with a mobile device predominantly consists of touch motions, otherwise known as swipe gestures, which are used as a behavioural biometric modality to verify the identity of a user. Literature reveals promising verification accuracy rates for swipe gesture authentication. Most of the existing studies have considered constrained environment in their experimental set-up. However, real-life usage of a mobile device consists of several unconstrained scenarios as well. Thus, our work aims to evaluate the stability of swipe gesture authentication across various usage scenarios of a mobile device. Methods: The evaluations were performed using state-of-the-art touch-based classification algorithms—support vector machine (SVM), k-nearest neighbour (kNN) and naive Bayes—to evaluate the robustness of swipe gestures across device usage scenarios. To simulate real-life behaviour, multiple usage scenarios covering stationary and dynamic modes are considered for the analysis. Additionally, we focused on analysing the stability of verification accuracy for time-separated swipes by performing intra-session (acquired on the same day) and inter-session (swipes acquired a week later) comparisons. Finally, we assessed the consistency of individual features for horizontal and vertical swipes using a statistical method. Results: Performance evaluation results indicate impact of body movement and environment (indoor and outdoor) on the user verification accuracy. The results reveal that for a static user scenario, the average equal error rate is 1%, and it rises significantly for the scenarios involving any body movement—caused either by user or the environment. The performance evaluation for time-separated swipes showed better verification accuracy rate for swipes acquired on the same day compared to swipes separated by a week. Finally, assessment on feature consistency reveal a set of consistent features such as maximum slope, standard deviation and mean velocity of second half of stroke for both horizontal and vertical swipes. Conclusions: The performance evaluation of swipe-based authentication shows variation in verification accuracy across different device usage scenarios. The obtained results challenge the adoption of swipe-based authentication on mobile devices. We have suggested ways to further achieve stability through specific template selection strategies. Additionally, our evaluation has established that at least 6 swipes are needed in enrolment to achieve acceptable accuracy. Also, our results conclude that features such as maximum slope and standard deviation are the most consistent features across scenarios. [ABSTRACT

IPR2025-01313; Samsung
Ex. 1002 - Page 104

FROM AUTHOR]; DOI: 10.1186/s13635-020-00103-0; (*AN 142293805*), Database: Applied Science & Technology Source

Subjects: Support vector machines; **Biometric** identification; Classification algorithms; Standard deviations; Biometry; Gesture; **Body** movement

HTML Full Text **PDF Full Text** (2MB) **USPTO Full Text Options**

4. ## **Information** processing **device**, application software start-up system, and application software start-up method

By: Maxell, Ltd. US Patent: 10423,769. Filed: June 12, 2014. Issued: September 24, 2019. , Database: USPTO Patent Grants

Abstract: The purpose of the present invention is to provide a portable terminal and an application software start-up system whereby the application software that is started up is limited depending on the state of a **user**, thereby providing an improved ease of use. For this purpose, an application software start-up method for an **information** processing **device** comprises: performing identity authentication based on static biological **information**; determining the state of the **user** by comparing **dynamic** biological **information** acquired from the **body** of the **user** with previously measured **dynamic** biological **information**; and limiting the application software that is started up in accordance with the determined state of the **user** and on the basis of a permission level that is set in advance for each application software item.

AN: edspgr.10423769

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 105

5. METHOD FOR REGISTERING AND AUTHENTICATING **BIOMETRIC** DATA AND ELECTRONIC **DEVICE** THEREOF

Patent Application: 16/469002. Filed: November 20, 2017. Published: October 17, 2019. , Database: USPTO Patent Applications

Abstract: The present invention is for registering and authenticating **biometric** data in an electronic **device**, the electronic **device** including: a display including a touch **sensor**; a fingerprint **sensor** for **acquiring** fingerprint data through at least a partial region of the display region of the display; and a processor. Here, the processor can be set to: acquire **first** touch **information** from a **first user** input using the touch **sensor**, in response to the **first user** input for registering a fingerprint of a **user**; acquire **first** fingerprint data using the fingerprint **sensor**; register the **first** fingerprint data as fingerprint **information** based on the **first** touch **information**, the registering operation including an operation for classifying the **first** fingerprint data based on the **first** touch **information**; acquire second touch **information** from a second **user** input using the touch **sensor**, in response to the second **user** input for authenticating the fingerprint of the **user**; acquire second fingerprint data using the fingerprint **sensor**; select a candidate group for comparison from among the fingerprint **information** based on the second touch **information**; and compare fingerprint data included in the candidate group with the second fingerprint data.

AN: edspap.20190318073

USPTO Full Text Options

6. AUTOMATIC **SENSOR** POSITIONING FOR **BIOMETRIC** SENSING

Patent Application: 16/721455. Filed: December 19, 2019. Published: April 23, 2020. , Database: USPTO Patent Applications

Abstract: A method for positioning a **sensor** configured to receive **biometric** signals includes receiving a **biometric** signal using a **biometric sensor** at a **first** position, the **biometric** signal comprising a set of raw **biometric** signal data. In some implementations, signal analysis is used to determine whether at least one signal criteria is met and to determine whether the **biometric sensor** is moved from the **first** position to a second position.

AN: edspap.20200124863

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 106

7. ## **Biometric**-based authentication scheme for Implantable Medical **Devices** during emergency situations

By Belkhouja, Taha; Du, Xiaojiang; Mohamed, Amr; Al-Ali, Abdulla K.; Guizani, Mohsen. In *Future Generation Computer Systems*. September 2019 98:109-119 Language: English. DOI: 10.1016/j.future.2019.02.002 Abstract: **Biometric** recognition and analysis are among the most trusted features to be used by Implantable Medical **Devices** (IMDs). We aim to secure these **devices** by using these features in emergency scenarios. As patients can witness unpredictable lethal accidents, any implantable medical **device** should allow access to urgent medical interventions from legitimate parties. Any delay in providing immediate medical support can endanger the patient's life. Hence, we propose in this work an authentication scheme that allows access to the implanted **devices** in emergency situations for only legitimate **users**. We have designed in the **first** place a scheme for authentication using Electrocardiogram instantaneous readings. Then, we joined the latter to a fixed **biometric** reading, which is fingerprint reading, to enable access to emergency medical teams. We have designed a scheme in a way to prevent attackers from accessing/hijacking the **device** even during emergency situations. This scheme has been assisted with elliptic curve cryptography to protect the wireless exchange of requested keys. The scheme relies on the instantaneous reading of the patient's heartbeat and his/her fingerprint reading to create a secure key. This key will validate the authentication request of the new medical team. We have analyzed this scheme deeply to verify that they offer the necessary security for the patient's life. We have tested if the wireless exchange of the key will expose the **device**'s privacy. We have also tested the accuracy of the authentication process to ensure a safe and a valid performance of the authentication process. The scheme has been designed with consideration to any hardware/software limitation that characterize any implantable medical **device**. (*AN: S0167739X18325792*), Database: ScienceDirect

Subjects: Implantable Medical **Devices**; Emergency access; **Biometric** readings; Wireless authentication

Full Text Finder **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 107

8. ## A survey on methods and challenges in EEG based authentication

By Jalaly Bidgoly, Amir; Jalaly Bidgoly, Hamed; Arezoumand, Zeynab. In *Computers & Security*. June 2020 93 Language: English. DOI: 10.1016/j.cose.2020.101788 Abstract: EEG is the recording of electrical activities of the brain, usually along the scalp surface, which are the results of synaptic activations of the brain's neurons. In recent years, it has been shown that EEG is an appropriate signal for the **biometric** authentication and has important features such as resistance to spoofing attacks and impossibility to use under pressure and coercion states. In this paper, the state-of-the-art methods in EEG based authentication are reviewed. This review includes a number of aspects such as the various tasks that the **user** required to perform during the authentication, **devices** and available datasets, the preprocessing procedures and the classification methods used in the EEG **biometric** authentication. Both shallow and deep classification methods are reviewed in this paper. The study shows that the deep learning approaches which are used in the past few years, although still require further research, have shown great results. Moreover, the paper summarizes the works to address the open challenges of this area. The EEG authentication challenges have been discussed from a variety of points of view, including privacy, **user**-friendliness, attacks, and authentication requirements such as universality, permanency, uniqueness, and collectability. This paper can be used as a preliminary plan and a roadmap for researchers interested in EEG **biometric**. (*AN: S0167404820300730*), Database: ScienceDirect

Subjects: EEG; **Biometric** factor; Authentication; **User** identification; Pattern recognition; Survey

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 108

9. ## A context-aware system to secure enterprise content: Incorporating reliability specifiers

By Oluwatimi, Oyindamola; Damiani, Maria Luisa; Bertino, Elisa. In *Computers & Security*. August 2018 77:162-178 Language: English. DOI: 10.1016/j.cose.2018.04.001 Abstract: The **sensors** of a context-aware system extract contextual **information** from the environment and relay that **information** to higher-level processes of the system so to influence the system's control decisions. However, an adversary can maliciously influence such controls indirectly by manipulating the environment in which the **sensors** are monitoring, thereby granting privileges the adversary would otherwise not normally have. To address such context monitoring issues, we extend CASSEC by incorporating sentience-like constructs, which enable the emulation of "confidence", into our proximity-based access control model to grant the system the ability to make more inferable decisions based on the degree of reliability of extracted contextual **information**. In CASSEC 2.0, we evaluate our confidence constructs by implementing two new authentication mechanisms. Co-proximity authentication employs our time-based challenge-response protocol, which leverages Bluetooth Low Energy beacons as its underlying occupancy detection technology. **Biometric** authentication relies on the accelerometer and fingerprint **sensors** to measure behavioral and physiological **user** features to prevent unauthorized **users** from using an authorized **user**'s **device**. We provide a feasibility study demonstrating how confidence constructs can improve the decision engine of context-aware access control systems. (*AN: S0167404818303018*), Database: ScienceDirect

Subjects: Access control; Context awareness; BYOD; Security; Mobility; **Biometric**; Authentication; Reliability; Proximity

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 109

10. ## Weaponizing **information** systems for political disruption: The Actor, Lever, Effects, and Response Taxonomy (ALERT)

By Desouza, Kevin C.; Ahmad, Atif; Naseer, Humza; Sharma, Munish. In *Computers & Security*. January 2020 88 Language: English. DOI: 10.1016/j.cose.2019.101606 Abstract: **Information** systems continue to be used by actors who want to undermine public institutions and disrupt political systems. In recent times, actors have engaged in acts of **information** warfare ranging from attempts to compromising voting systems, to spreading false propaganda and even direct attacks on public infrastructure via **information** systems. Initial analysis points to the fact that most of these attempts have been successful in achieving their intended objectives. Given this reality, we expect them to intensify and be more creative in the future. In this paper we draw on a critical analysis of the role of **information** systems in creating political disruption to propose that **information** systems can be 'weaponized' by compromising their goals and values even while they remain protected. Building on this proposition we develop a risk-based Actor, Lever, Effects and Response Taxonomy (ALERT) to assist security practitioners and policymakers to analyze and respond to attacks enabled by **information** systems aimed at political disruption. We illustrate the utility of ALERT using representative examples of weaponized attacks from credible news sources. Finally, we leverage the insights gained from ALERT to propose a theoretical framework where we assert that over time as actors gain maturity and experience using levers to disrupt political systems, so too does the public sector gain experience in response thus building their response capacity. This **dynamic** relationship increasingly pushes both actors and defenders to come up with more innovative, agile and sophisticated methods to weaponize and respond to **information** systems enabled attacks. (*AN: S0167404819301579*), Database: ScienceDirect

Subjects: Information systems; **Information** warfare; Cyber; Cybersecurity; Cyber conflict; Critical infrastructure; Threat modeling; Taxonomy

 **Full Text Finder** **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 110

11. Internet of Things: A survey of enabling technologies in healthcare and its applications

By Dhanvijay, Mrinal M.; Patil, Shailaja C.. In *Computer Networks*. 22 April 2019 153:113-131 Language: English. DOI: 10.1016/j.comnet.2019.03.006 Abstract: Internet of Things (IoT) on the Wireless **Body** Area Network (WBAN) for healthcare applications is an operative scenario for IoT **devices** that has gained attention from vast research fields in recent years. The IoT connects all subjects and the healthcare system seamlessly. This paper describes the WBAN based IoT healthcare system and reviews the state-of-the-art of the network architecture topology and applications in the IoT based healthcare solutions. Moreover, this paper analyzes the security and the privacy features consisting of privacy, authentication, energy, power, resource management, Quality of Services and the real-time wireless health monitoring that are quite problematic in many IoT healthcare architectures. Because, system architecture is not well-defined, data restriction and its integrity preservation is still a challenge. At present 90% of the **information** available is acquired in the recent two years. This survey mainly aims at analyzing healthcare purpose which is based on digital healthcare system. Further, it reports many IoT and the e-healthcare policies and systems that decide how to ease all bearable development. Thus, the overall system provides large possibilities for future research based on IoT healthcare system. Finally, research gaps are reviewed and the possible future aspects have been discussed. (*AN: S1389128619302695*), Database: ScienceDirect

Subjects: IoT; WBAN; Healthcare system; **Body sensor**

 **Full Text Finder** **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 111

12. A review of data **acquisition** and difficulties in **sensor** module of **biometric** systems.

By: Singla, Sunil Kumar; Kumar, Santosh. *Songklanakarin Journal of Science & Technology.* Sep/Oct2013, Vol. 35 Issue 5, p589-597. 9p.

Abstract: **Biometrics** refers to the recognition of individuals based on their physiological and/or behavioral characteristics. The **biometric** traits which may be considered for the authentication of a person are face, hand geometry, finger print, vein, iris, etc. A competent selection of a **sensor**, its mechanism and adaptability is required, as the absence of these will leave the **biometric sensor** deceptive to **information** sensing. Selecting a **sensor** for a **biometric** application from the large number of available **sensors** with different technologies always brought the issue of performance and accuracy. Therefore, various error rates and sensibility contention differentiate the available **biometric sensors**. This paper presents the difficulties faced in the **sensor** module of the **biometric** system and the incomparable alternatives on the basis of availability of **information** at **sensor** module of the various systems. [ABSTRACT FROM AUTHOR] (*AN: 101635588*), Database: Academic Search Complete

Subjects: DATA **acquisition** systems; **BIOMETRIC** identification; **INFORMATION** theory; COMPUTER access control; SENSITIVITY analysis

PDF Full Text (1.3MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 112

13. A SURVEY OF **BIOMETRICS** FOR WEARABLE **DEVICES**.

By: Cornelius, Cory; Gutierrez, Christopher N. *Intel Technology Journal*. 2014, Vol. 18 Issue 4, p46-63. 18p. Abstract: **Biometrics** are characteristics about ourselves that we use to recognize each other. Whether it is the structure of our face or the way we walk, we can measure these physiological or behavioral signals and use statistical methods to distinguish amongst **users**. Rather than "something you know"-as in traditional password-based authentication systems-these **biometric**-based methods enable systems to authenticate you based on "something you are." In this survey we describe the current state-of-the-art of **biometric** techniques and evaluate their use in authentication systems with a particular focus on client **devices** and emerging wearable **devices**. We examine the academic literature and commercial offerings of **biometrics** and summarize each **biometrics**' utility over a variety of criteria and provide guidance for their use in client and wearable **devices**. [ABSTRACT FROM AUTHOR] (*AN: 97377853*), Database: Computer Source

Subjects: BIOMETRIC identification software; COMPUTER security management; COMPUTER systems management; COMPUTER security software; DATA management

PDF Full Text (2.2MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 113

14. ## Beat-ID: Towards a computationally low-cost single heartbeat **biometric** identity check system based on electrocardiogram wave morphology.

By: Paiva, Joana S.; Dias, Duarte; Cunha, João P. S. *PLoS ONE*. 7/18/2017, Vol. 12 Issue 7, p1-32. 32p. Abstract: In recent years, safer and more reliable **biometric** methods have been developed. Apart from the need for enhanced security, the media and entertainment sectors have also been applying **biometrics** in the emerging market of **user**-adaptable objects/systems to make these systems more **user**-friendly. However, the complexity of some state-of-the-art **biometric** systems (e.g., iris recognition) or their high false rejection rate (e.g., fingerprint recognition) is neither compatible with the simple hardware architecture required by reduced-size **devices** nor the new trend of implementing smart objects within the **dynamic** market of the Internet of Things (IoT). It was recently shown that an individual can be recognized by extracting features from their electrocardiogram (ECG). However, most current ECG-based **biometric** algorithms are computationally demanding and/or rely on relatively large (several seconds) ECG samples, which are incompatible with the aforementioned application fields. Here, we present a computationally low-cost method (patent pending), including simple mathematical operations, for identifying a person using only three ECG morphology-based characteristics from a single heartbeat. The algorithm was trained/tested using ECG signals of different duration from the Physionet database on more than 60 different training/test datasets. The proposed method achieved maximal averaged accuracy of 97.450% in distinguishing each subject from a ten-subject set and false acceptance and rejection rates (FAR and FRR) of 5.710±1.900% and 3.440±1.980%, respectively, placing Beat-ID in a very competitive position in terms of the FRR/FAR among state-of-the-art methods. Furthermore, the proposed method can identify a person using an average of 1.020 heartbeats. It therefore has FRR/FAR behavior similar to obtaining a fingerprint, yet it is simpler and requires less expensive hardware. This method targets low-computational/energy-cost scenarios, such as tiny wearable **devices** (e.g., a smart object that automatically adapts its configuration to the **user**). A hardware proof-of-concept implementation is presented as an annex to this paper. [ABSTRACT FROM AUTHOR] DOI: 10.1371/journal.pone.0180942. (*AN: 124177976*), Database: Academic Search Complete

Subjects: HEART beat measurement; **BIOMETRIC** identification; ELECTROCARDIOGRAPHY; WEARABLE technology; INTERNET of things

PDF Full Text (4.6MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 114

15. The role of **devices** in managing risk

By Rugg-Gunn, Fergus. In *Prevent 21: SUDEP Summit, Epilepsy & Behavior*. February 2020 103 Part B Part B Language: English. DOI: 10.1016/j.yebeh.2019.106456 Abstract: Over the last few years, there has been significant expansion of wearable technologies and **devices** into the health sector, including for conditions such as epilepsy. Although there is significant potential to benefit patients, there is a paucity of well-conducted scientific research in order to inform patients and healthcare providers of the most appropriate technology. In addition to either directly or indirectly identifying seizure activity, the ideal **device** should improve quality of life and reduce the risk of sudden unexpected death in epilepsy (SUDEP). **Devices** typically monitor a number of parameters including electroencephalographic (EEG), cardiac, and respiratory patterns and can detect movement, changes in skin conductance, and muscle activity. Multimodal **devices** are emerging with improved seizure detection rates and reduced false positive alarms. While convulsive seizures are reliably identified by most unimodal and multimodal **devices**, seizures associated with no, or minimal, movement are frequently undetected. The vast majority of current **devices** detect but do not actively intervene. At best, therefore, they indicate the presence of seizure activity in order to accurately ascertain true seizure frequency or facilitate intervention by others, which may, nevertheless, impact the rate of SUDEP. Future **devices** are likely to both detect and intervene within an autonomous closed-loop system tailored to the individual and by self-learning from the analysis of patient-specific parameters. The formulation of standards for regulatory **bodies** to validate seizure detection **devices** is also of paramount importance in order to confidently ascertain the performance of a **device**; and this will be facilitated by the creation of a large, open database containing multimodal annotated data in order to test **device** algorithms.This paper is for the Special Issue: Prevent 21: SUDEP Summit - Time to Listen. *(AN: S1525505019306791)*, Database: ScienceDirect

Subjects: SUDEP; Medical **devices**; Wearable technology; Epilepsy

Full Text Finder **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 115

16. An Internet of Things based physiological signal monitoring and receiving system for virtual enhanced health care network.

By: Rajan, J. Pandia; Rajan, S. Edward. *Technology & Health Care*. 2018, Vol. 26 Issue 2, p379-385. 7p. Abstract: <bold>Background: </bold>Wireless physiological signal monitoring system designing with secured data communication in the health care system is an important and **dynamic** process.<bold>Objective: </bold>We propose a signal monitoring system using NI myRIO connected with the wireless **body sensor** network through multi-channel signal **acquisition** method. Based on the server side validation of the signal, the data connected to the local server is updated in the cloud. The Internet of Things (IoT) architecture is used to get the mobility and fast access of patient data to healthcare service providers.<bold>Methods: </bold>This research work proposes a novel architecture for wireless physiological signal monitoring system using ubiquitous healthcare services by virtual Internet of Things.<bold>Results: </bold>We showed an improvement in method of access and real time **dynamic** monitoring of physiological signal of this remote monitoring system using virtual Internet of thing approach. This remote monitoring and access system is evaluated in conventional value. This proposed system is envisioned to modern smart health care system by high utility and **user** friendly in clinical applications.<bold>Conclusion: </bold>We claim that the proposed scheme significantly improves the accuracy of the remote monitoring system compared to the other wireless communication methods in clinical system. [ABSTRACT FROM AUTHOR] DOI: 10.3233/THC-171173. (*AN: 129253878*), Database: Academic Search Complete

Subjects: INTERNET of things; HEALTH care networks; UBIQUITOUS computing; WIRELESS communications; REMOTE sensing; Wireless Telecommunications Carriers (except Satellite); Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing

HTML Full Text **PDF Full Text** (1.5MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 116

17. ## Design and development of an EOG-based simplified Chinese eye-writing system

By Ding, XiaoJuan; Lv, Zhao. In *Biomedical Signal Processing and Control*. March 2020 57 Language: English. DOI: 10.1016/j.bspc.2019.101767
Abstract: Highlights •Design an EOG-based simplified Chinese eye-writing system.•Employ DTW algorithm to compute the similarity between input strokes and templates.•Use cross-entropy to match encoded character with recognized input stroke sequence.•Experimental results reveal feasibility of the proposed eye writing system. (*AN: S1746809419303489*), Database: ScienceDirect

Subjects: Electrooculography (EOG); Stroke; **Dynamic** time warping (DTW); Eye-writing

Full Text Finder USPTO Full Text Options

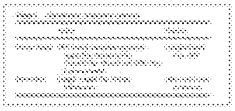
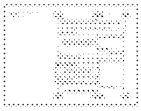
IPR2025-01313; Samsung
Ex. 1002 - Page 117

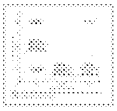
18. Technical feasibility of context-aware passive payment authorization for physical points of sale.

By: Wójtowicz, Adam; Chmielewski, Jacek. *Personal & Ubiquitous Computing* , Dec2017, Vol. 21 Issue 6, p1113-1125, 13p Abstract: In this work, the technical feasibility of passive secure payments for brick-and-mortar points of sale is analyzed. The core element of the proposed approach is a new application for context-based risk and trust assessment. It allows for **dynamic** selection of payment authorization methods that constitutes accurate trade-off between security and convenience. Particularly, the payments can be performed and authorized in the background using **biometric** means (face recognition), without **user's** explicit action. Generally, in the proposed approach, multiple **devices** are used for authorization: mobile, wearables, or stationary, client's or seller's, and multiple authorization methods are used: **biometric**, knowledge-based, and possession-based. The reported research includes requirement identification, novel architecture and protocol proposition, proof-of-concept prototype system deployment, and evaluation-based lessons learned. The research confirms that with the proposed approach, it is possible to take advantage of client-seller trust dynamism to simplify the payment process while maintaining the security level. [ABSTRACT FROM AUTHOR]; DOI: 10.1007/s00779-017-1035-z; (*AN 126405199*), Database: Applied Science & Technology Source

Subjects: Payment systems; Context-aware computing; Ubiquitous computing; **Biometric** identification; Financial Transactions Processing, Reserve, and Clearinghouse Activities; Contactless payment systems

Show all 6 images



PDF Full Text (800KB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 118

19. **Biometrics** Systems and Technologies: A survey.

By: Buciu, I.; Gacsadi, A.. *International Journal of Computers, Communications & Control* , Jun2016, Vol. 11 Issue 3, p315-330, 16p

Abstract: In a nutshell, a **biometric** security system requires a **user** to provide some **biometric** features which are then verified against some stored **biometric** templates. Nowadays, the traditional password based authentication method tends to be replaced by advanced **biometrics** technologies. **Biometric** based authentication is becoming increasingly appealing and common for most of the human-computer interaction **devices**. To give only one recent example, Microsoft augmented its brand new Windows 10 OS version with the capability of supporting face recognition when the **user** login in. This chapter does not intend to cover a comprehensive and detailed list of **biometric** techniques. The chapter rather aims at briefly discussing **biometric** related items, including principles, definitions, **biometric** modalities and technologies along with their advantages, disadvantages or limitations, and **biometric** standards, targeting unfamiliar readers. It also mentions the attributes of a **biometric** system as well as attacks on **biometrics**. Important reference sources are pointed out so that the interested reader may gain deeper in-depth knowledge by consulting them. [ABSTRACT FROM AUTHOR]; DOI: 10.15837/ijccc.2016.3.2556; (*AN 114266005*), Database: Applied Science & Technology Source

Subjects: Security systems; Biometry software; **Biometric** identification software; Human-computer interaction; Human face recognition (Computer science); Security Systems Services (except Locksmiths); Microsoft Windows (Operating system)

PDF Full Text (621KB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 119

20. ## Handbook of Green **Information** and Communication Systems

By: Woungang, Isaac; Anpalagan, Alagan; Obaidat, Mohammad S. Amsterdam : Academic Press. 2013. eBook. Description: This book gives a comprehensive guide on the fundamental concepts, applications, algorithms, protocols, new trends and challenges, and research results in the area of Green **Information** and Communications Systems. It is an invaluable resource giving knowledge on the core and specialized issues in the field, making it highly suitable for both the new and experienced researcher in this area. Key Features: Core research topics of green **information** and communication systems are covered from a network ... (*AN 485200*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Signals & Signal Processing; SCIENCE / Environmental Science; Sustainable engineering--Handbooks, manuals, etc; Telecommunication--Environmental aspects--Handbooks, manuals, etc; Telecommunication--Energy conservation--Handbooks, manuals, etc

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 120

21. Privacy-Constrained **Biometric** System for Non-Cooperative **Users**.

By: S. Jahromi, Mohammad N.; Buch-Cardona, Pau; Avots, Egils; Nasrollahi, Kamal; Escalera, Sergio; Moeslund, Thomas B.; Anbarjafari, Gholamreza. *Entropy*. Nov2019, Vol. 21 Issue 11, p1033-1033. 1p. Abstract: With the consolidation of the new data protection regulation paradigm for each individual within the European Union (EU), major **biometric** technologies are now confronted with many concerns related to **user** privacy in **biometric** deployments. When individual **biometrics** are disclosed, the sensitive **information** about his/her personal data such as financial or health are at high risk of being misused or compromised. This issue can be escalated considerably over scenarios of non-cooperative **users**, such as elderly people residing in care homes, with their inability to interact conveniently and securely with the **biometric** system. The primary goal of this study is to design a novel database to investigate the problem of automatic people recognition under privacy constraints. To do so, the collected data-set contains the subject's hand and foot traits and excludes the face **biometrics** of individuals in order to protect their privacy. We carried out extensive simulations using different baseline methods, including deep learning. Simulation results show that, with the spatial features extracted from the subject sequence in both individual hand or foot videos, state-of-the-art deep models provide promising recognition performance. [ABSTRACT FROM AUTHOR] DOI: 10.3390/e21111033. (*AN: 139863108*), Database: Academic Search Complete

Subjects: OLDER people; DATABASE design; PERSONALLY identifiable **information**; DATA protection; DEEP learning; MULTIMODAL **user** interfaces; EUROPEAN Union

HTML Full Text **PDF Full Text** (8.9MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 121

22. **INFORMATION** PROCESSING APPARATUS, **INFORMATION** PROCESSING METHOD, AND PROGRAM

Patent Application: 15/560214. Filed: December 28, 2015. Published: February 15, 2018. , Database: USPTO Patent Applications
Abstract: Provided is an **information** processing apparatus including a processing unit configured to perform a predetermined process on the basis of **first information** about a **user** that is acquired by a **first** apparatus from around a **body** of the **user**, and second **information** about a **user** that is acquired by a second apparatus different from the **first** apparatus.
AN: edspap.20180046788

USPTO Full Text Options

23. WEARABLE ELECTRONIC **DEVICE** AND OPERATING METHOD THEREFOR

Patent Application: 16/095999. Filed: June 02, 2017. Published: May 9, 2019. , Database: USPTO Patent Applications
Abstract: According to various examples of the present invention, a wearable electronic **device** comprises: an energy harvester for generating electric energy on the basis of a movement or a change in the shape of the wearable electronic **device**; a **first** processor for controlling the energy harvester; a **first sensor** and a second **sensor**; and a second processor for controlling the **first sensor** and the second **sensor**, wherein the **first** processor transmits, to the second processor, a control signal for transitioning the second processor into an activated state if the electric energy generated by the energy harvester satisfies a designated **first** condition, and the second processor can be set such that **first sensor** data is acquired through the **first sensor** and second **sensor** data is selectively acquired from the second **sensor** according to whether the **first sensor** data satisfies a designated second condition, when the second processor is transitioned from an inactivated state to the activated state by responding to the control signal.
AN: edspap.20190138068

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 122

24. An Open Platform for Seamless **Sensor** Support in Healthcare for the Internet of Things.

By: Miranda, Jorge; Cabral, Jorge; Wagner, Stefan Rahr; Pedersen, Christian Fischer; Ravelo, Blaise; Memon, Mukhtiar; Mathiesen, Morten. *Sensors (14248220)*. Dec2016, Vol. 16 Issue 12, p2089. 22p. Abstract: Population aging and increasing pressure on health systems are two issues that demand solutions. Involving and empowering citizens as active managers of their health represents a desirable shift from the current culture mainly focused on treatment of disease, to one also focused on continuous health management and well-being. Current developments in technological areas such as the Internet of Things (IoT), lead to new technological solutions that can aid this shift in the healthcare sector. This study presents the design, development, implementation and evaluation of a platform called Common Recognition and Identification Platform (CRIP), a part of the CareStore project, which aims at supporting caregivers and citizens to manage health routines in a seamless way. Specifically, the CRIP offers **sensor**-based support for seamless identification of **users** and health **devices**. A set of initial requirements was defined with a focus on usability limitations and current **sensor** technologies. The CRIP was designed and implemented using several technologies that enable seamless integration and interaction of **sensors** and people, namely Near Field Communication and fingerprint **biometrics** for identification and authentication, Bluetooth for communication with health **devices** and web services for wider integration with other platforms. Two CRIP prototypes were implemented and evaluated in laboratory during a period of eight months. The evaluations consisted of identifying **users** and **devices**, as well as seamlessly configure and acquire vital data from the last. Also, the entire Carestore platform was deployed in a nursing home where its usability was evaluated with caregivers. The evaluations helped assess that seamless identification of **users** and seamless configuration and communication with health **devices** is feasible and can help enable the IoT on healthcare applications. Therefore, the CRIP and similar platforms could be transformed into a valuable enabling technology for secure and reliable IoT deployments on the healthcare sector. [ABSTRACT FROM AUTHOR] DOI: 10.3390/s16122089. (*AN: 120375895*), Database: Academic Search Complete

Subjects: INTERNET of things; HEALTH care industry; POPULATION aging; MEDICAL technology; DEPLOYMENT (Military strategy); Surgical Appliance and Supplies Manufacturing; Medical, Dental, and Hospital Equipment and Supplies Merchant Wholesalers; Surgical and Medical Instrument Manufacturing; All Other Health and Personal Care Stores

PDF Full Text (6.4MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 123

25. Lightweight **Biometric** Sensing for Walker Classification Using Narrowband RF Links.

By: Tong Liu; Zhuo-qian Liang. ***Sensors*** *(14248220)*. Dec2017, Vol. 17 Issue 12, p2815. 16p. Abstract: This article proposes a lightweight **biometric** sensing system using ubiquitous narrowband radio frequency (RF) links for path-dependent walker classification. The fluctuated received signal strength (RSS) sequence generated by human motion is used for feature representation. To capture the most discriminative characteristics of individuals, a three-layer RF sensing network is organized for building multiple sampling links at the most common heights of upper limbs, thighs, and lower legs. The optimal parameters of sensing configuration, such as the height of link location and number of fused links, are investigated to improve sensory data distinctions among subjects, and the experimental results suggest that the synergistic sensing by using multiple links can contribute a better performance. This is the new consideration of using RF links in building a **biometric** sensing system. In addition, two types of classification methods involving vector quantization (VQ) and hidden Markov models (HMMs) are developed and compared for closed-set walker recognition and verification. Experimental studies in indoor line-of-sight (LOS) and non-line-of-sight (NLOS) scenarios are conducted to validate the proposed method. [ABSTRACT FROM AUTHOR] DOI: 10.3390/s17122815. (*AN: 126948809*), Database: Academic Search Complete

Subjects: BIOSENSORS; RADIO frequency; MARKOV processes; VECTOR quantization; **BIOMETRIC** identification

PDF Full Text (2.6MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 124

26. ## A comparative analysis of signal processing and classification methods for different applications based on EEG signals

By Khosla, Ashima; Khandnor, Padmavati; Chand, Trilok. In *Biocybernetics and Biomedical Engineering*. April-June 2020 40(2):649-690 Language: English. DOI: 10.1016/j.bbe.2020.02.002 Abstract: Electroencephalogram (EEG) measures the neuronal activities in the form of electric currents that are generated due to the synchronized activity by a group of specialized pyramidal cells inside the brain. The study presents a brief comparison of various functional neuroimaging techniques, revealing the excellent neuroimaging capabilities of EEG signals such as high temporal resolution, inexpensiveness, portability, and non-invasiveness as compared to the other techniques such as positron emission tomography, magnetoencephalogram, functional magnetic resonance imaging, and transcranial magnetic stimulation. Different types of frequency bands associated with the brain signals are also being summarized. The main purpose of this literature survey is to cover the maximum possible applications of EEG signals based on computer-aided technologies, ranging from the diagnosis of various neurological disorders such as epilepsy, major depressive disorder, alcohol use disorder, and dementia to the monitoring of other applications such as motor imagery, identity authentication, emotion recognition, sleep stage classification, eye state detection, and drowsiness monitoring. After reviewing them, the comparative analysis of the publicly available EEG datasets and other local data **acquisition** methods, preprocessing techniques, feature extraction methods, and the result analysis through the classification models and statistical tests has been presented. Then the research gaps and future directions in the present studies have been summarized with the aim to inspire the readers to explore more opportunities on the current topic. Finally, the survey has been completed with the brief description about the studies exploring the fusion of brain signals from multiple modalities. (*AN: S0208521620300231*), Database: ScienceDirect

Subjects: EEG applications; Signal processing; Classification models; EEG data collection; Brain rhythms; Functional neuroimaging techniques

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 125

27. ## Approach for the Development of a Framework for the Identification of Activities of Daily Living Using **Sensors** in Mobile **Devices**.

By: Pires, Ivan Miguel; Garcia, Nuno M.; Pombo, Nuno; Flórez-Revuelta, Francisco; Spinsante, Susanna. ***Sensors** (14248220)*. Feb2018, Vol. 18 Issue 2, p640. 22p. 2 Diagrams, 7 Charts. Abstract: **Sensors** available on mobile **devices** allow the automatic identification of Activities of Daily Living (ADL). This paper describes an approach for the creation of a framework for the identification of ADL, taking into account several concepts, including data **acquisition**, data processing, data fusion, and pattern recognition. These concepts can be mapped onto different modules of the framework. The proposed framework should perform the identification of ADL without Internet connection, performing these tasks locally on the mobile **device**, taking in account the hardware and software limitations of these **devices**. The main purpose of this paper is to present a new approach for the creation of a framework for the recognition of ADL, analyzing the allowed **sensors** available in the mobile **devices**, and the existing methods available in the literature. [ABSTRACT FROM AUTHOR] DOI: 10.3390/s18020640. (*AN: 128283724*), Database: Academic Search Complete

Subjects: AUTOMATIC identification; ACTIVITIES of daily living; DATA **acquisition** systems; MULTISENSOR data fusion; PATTERN recognition systems; CELL phones; Electronics Stores; Electronic components, navigational and communications equipment and supplies merchant wholesalers; Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing; Wireless Telecommunications Carriers (except Satellite)

HTML Full Text **PDF Full Text** (2.5MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 126

28. ## Modelling a smart environment for nonintrusive analysis of attention in the workplace.

By: Durães, Dalila; Carneiro, Davide; Bajo, Javier; Novais, Paulo. *Expert Systems.* Oct2018, Vol. 35 Issue 5, p1-1. 13p. Abstract: Abstract: Nowadays, the world is getting increasingly competitive and the quality and the amount of the work presented are one of the decisive factors when choosing an employee. It is no longer necessary to only perform but, to achieve a product with quality, on time, at the lowest possible cost and with the minimum resources. For this reason, the employee must have a high score of attention when performing a task, and the factors that influence attention negatively must be reduced. This is true in many different domains, from the workplace to the classroom. In this paper, we present a nonintrusive smart environment for monitoring people's attention when working in teams. The presented system provides real time **information** about each individual and **information** about the team. It can be very useful for team managers to identify potentially distracting events or individuals because when the attention of an individual is not at its best when performing the proposed task, her/his performance will be negatively affected, with consequences for the individual and for the organization. [ABSTRACT FROM AUTHOR] DOI: 10.1111/exsy.12275. (*AN: 132203599*), Database: Academic Search Complete

Subjects: EMPLOYEES; ATTENTION; DISTRIBUTED computing; ARTIFICIAL intelligence; DIGITAL technology

HTML Full Text **PDF Full Text** (536KB)

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 127

29. ## Activity Recognition Using Wearable Physiological Measurements: Selection of Features from a Comprehensive Literature Study.

By: Mohino-Herranz, Inma; Gil-Pita, Roberto; Rosa-Zurera, Manuel; Seoane, Fernando. ***Sensors*** *(14248220)*. 12/15/2019, Vol. 19 Issue 24, p1-27. 27p. 1 Color Photograph, 4 Diagrams, 4 Charts, 6 Graphs. Abstract: Activity and emotion recognition based on physiological signal processing in health care applications is a relevant research field, with promising future and relevant applications, such as health at work or preventive care. This paper carries out a deep analysis of features proposed to extract **information** from the electrocardiogram, thoracic electrical bioimpedance, and electrodermal activity signals. The activities analyzed are: neutral, emotional, mental and physical. A total number of 533 features are tested for activity recognition, performing a comprehensive study taking into consideration the prediction accuracy, feature calculation, window length, and type of classifier. Feature selection to know the most relevant features from the complete set is implemented using a genetic algorithm, with a different number of features. This study has allowed us to determine the best number of features to obtain a good error probability avoiding over-fitting, and the best subset of features among those proposed in the literature. The lowest error probability that is obtained is 22.2%, with 40 features, a least squares error classifier, and 40 s window length. [ABSTRACT FROM AUTHOR] DOI: 10.3390/s19245524. *(AN: 141367135)*, Database: Academic Search Complete

PDF Full Text (1.2MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 128

30. A 3-D hand gesture signature based **biometric** authentication system for smartphones.

By: Sun, Ziwen; Wang, Yao; Qu, Gang; Zhou, Zhiping. *Security & Communication Networks* , 7/25/2016, Vol. 9 Issue 11, p1359-1373, 15p

Abstract: The authentication mechanism being equipped in most of the smartphones, by detecting a 4-digit password or a simple pattern, are easy to be hacked and impersonated. In this paper, a 3-D hand gesture signature (HGS) based **biometric** authentication system is designed and implemented by taking advantage of the on-phone accelerometer to capture the 3-D acceleration **information** when **user** makes a gesture to gain access to the phone. The captured data will be processed through a sequence of signal processing such as data smooth, gesture spotting, sequence alignment, and interpolation, and then a match rule will be used to compare the processed data and the genuine **user's** registered pattern to determine whether granting the access to the phone to the **user**. And an automatic template updating strategy based on cluster analysis is proposed to improve the stability of the system. The 3-D HGS authentication system has been implemented on real smartphones, and the results tested for a total of 76 520 times by 19 **users** show very low false acceptance (0.27%) and false rejection rates (4.65%). Furthermore, comparison tests have been carried out among the 3-D HGS and two similar authentication systems by exporting the real gesture samples from the phones to a desktop PC, the simulation results reveal the 3-D HGS system has the best authentication accuracy. Copyright © 2016 John Wiley & Sons, Ltd. [ABSTRACT FROM AUTHOR]; DOI: 10.1002/sec.1422; (*AN 116123722*), Database: Applied Science & Technology Source

Subjects: Computer access control; Passwords (Computers); Computer hacking; **Biometric** identification; Accelerometers; Signal processing; Other Measuring and Controlling **Device** Manufacturing

PDF Full Text (992KB) **USPTO Full Text Options**

EBSCO Connect | Privacy Policy | A/B Testing | Terms of Use | Copyright | Cookie Policy | Contact Us

powered by EBSCO*host*

© 2020 EBSCO Industries, Inc. All rights reserved.

IPR2025-01313; Samsung
Ex. 1002 - Page 129

STIC
Scientific and Technical Information Center

1. Patent Application Titled '**Information** Processing Device, Application Software Start-Up System, And Application Software Start-Up Method' Published Online (USPTO 20190362061)

In: **Information** Technology Newsweekly, Dec 17, 2019, 2279; NewsRX LLC
Language: English. Abstract: 2019 DEC 17 (VerticalNews) -- By a News Reporter-Staff News Editor at **Information** Technology Newsweekly -- According to news reporting originating from Washington, D.C., by VerticalNews journalists, a patent application [...] (*AN: edsgcl.608720217*), Database: Gale General OneFile

Subjects: Japan; Software quality; Software -- Methods; Software -- Intellectual property; Control equipment -- Methods; Control equipment -- Intellectual property

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 130

2. ## Plantation Records as a Source of Historical Weather and Agricultural Data.

By: Burris, Gregory; Elsner, James; Doel, Ronald E. *Southeastern Geographer*. Winter2018, Vol. 58 Issue 4, p348-364. 17p. Abstract: Plantation records from the southeastern United **States** have long been an important source for historical, social, and cultural narratives. However, they also represent an underutilized source for meteorological, environmental, and agricultural data from the antebellum period. This study has two goals. Firstly, we advocate for a more systematic application of these records for quantitative analysis. Secondly, we present some early results from such a study using the records of Shirley Plantation in Virginia. We show how these records **can** be mined for data on weather and agricultural activity and how their broader usefulness is extended with the inclusion of appropriate meta-data. Observations of weather **conditions** and crop responses to seasonal changes lend themselves to quantitative analysis that **can** improve our understanding of the local weather and climate of that period. We present a case study comparing last spring freeze date in this region from the late 1820s to 2010s and suggest that last spring freeze now occurs approximately 23 days earlier compared to approximately 200 years ago. We also include summaries of the response of specific crops and cultivars since this knowledge may help the farmers' of today adapt to changing weather **conditions**. While individual plantation records may have idiosyncratic limitations, plantation records, along with other types of detailed historical records, **can** still provide rich detail for specific locations or events. Plantation records are not limited to the southeastern US and include diverse geographic locations in less developed areas which were often the same areas were enslaved labor was exploited under the plantation system. Por mucho tiempo, los registros de las plantaciones del sureste de los Estados Unidos han sido una fuente importante de narrativas históricas sociales y culturales. Sin embargo, también representan una fuente infrautilizada de datos meteorológicos, ambientales y agrícolas del período antebellum estadounidense. Este estudio tiene dos propósitos. Primero, abogamos por una aplicación más sistemática de estos registros para el análisis cuantitativo. En segundo lugar, presentamos algunos de los primeros resultados de un estudio de este tipo utilizando los registros de la plantación Shirley en Virginia. Mostramos cómo se pueden extraer estos registros para obtener datos sobre el clima y la actividad agrícola y su utilidad más amplia que se extiende con la inclusión de los metadatos apropiados. Las observaciones de las condiciones climáticas y las respuestas de los cultivos a los cambios estacionales se prestan al análisis cuantitativo que puede [End Page 348] mejorar nuestra comprensión del clima local y el clima de ese periodo. Presentamos un estudio de caso que compara la fecha de congelación de la primavera pasada en esta región desde finales de la

IPR2025-01313; Samsung
Ex. 1002 - Page 131

década de 1820 hasta la de 2010 y sugerimos que la congelación de la primavera anterior se produce aproximadamente 23 días antes en comparación con hace aproximadamente 100 años. Mientras que los registros de plantación individuales pueden tener limitaciones idiosincrásicas, los registros de plantación, junto con otros tipos de registros históricos detallados, aún pueden proporcionar detalles útiles para lugares o eventos específicos. Los registros de plantaciones no se limitan al sureste de los EE.UU. e incluyen diversas ubicaciones geográficas en áreas menos desarrolladas que muchas veces eran las mismas áreas donde el trabajo esclavo se explotaba bajo el sistema de plantaciones. La contextualización de los datos históricos con el conocimiento actual se puede utilizar para examinar cómo la sociedad interactuó con la variabilidad climática interanual y los extremos climáticos. [ABSTRACT FROM AUTHOR] DOI: 10.1353/sgo.2018.0035. (*AN: 135556868*), Database: Academic Search Complete

Subjects: HISTORICAL source material; PLANTATIONS; WEATHER; AGRICULTURAL meteorology; CONDITIONED response; VIRGINIA; UNITED **States**

HTML Full Text **PDF Full Text** (1.5MB) **USPTO Full Text Options**

3. ## Electronic apparatus and method for controlling functions in the electronic apparatus using a biometric sensor

By: Samsung Electronics Co., Ltd. US Patent: 10192044. Filed: June 24, 2016. Issued: January 29, 2019. , Database: USPTO Patent Grants
Abstract: According to various embodiments of the present disclosure, an electronic device may include a **biometric** sensor configured to detect a contact signal from at least two **biometric** electrodes and a processor configured to determine whether the contact signal received from the **biometric** sensor has biological characteristics. When the processor determines that the contact signal is a **biometric** input having biological characteristics, the processor executes a **biometric information** function. When the processor determines that the contact signal does not include the biological characteristics, the processor executes a general function related to an application.
AN: edspgr.10192044

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 132

4. Computer and **Information** Security Handbook

By: Vacca, John R. Series: The Morgan Kaufmann Series in Computer Security. Amsterdam : Morgan Kaufmann. 2009. eBook. Description: Presents **information** on how to analyze risks to your networks and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to physical and network threats. Also imparts the skills and knowledge needed to identify and counter some fundamental security risks and requirements, including Internet security threats and measures (audit trails IP sniffing/spoofing etc.) and how to implement security policies and procedures. In addition, this book covers security and network ... (*AN 248988*), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Networking / General; COMPUTERS / Security / General; Computer networks--Security measures

PDF Full Text **EPUB Full Text** **USPTO Full Text Options**

Full Download

Table of Contents Most Relevant Pages From This eBook

5. Computer Engineering : Concepts, Methodologies, Tools and Applications

By: **Information** Resources Management Association. Hershey, Pa : IGI Global. 2012. eBook. Description: Features perspectives on the fundamental aspects, tools and technologies, methods and design, applications, managerial impact, social/behavioral perspectives, critical issues, and emerging trends in the field of computer engineering. (*AN 431988*), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Computer Engineering; COMPUTERS / Machine Theory; COMPUTERS / Hardware / General; Computer engineering

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 133

6. ## ACCESS AND PORTABILITY OF USER PROFILES STORED AS TEMPLATES

Patent Application: 16/247128. Filed: January 14, 2019. Published: December 26, 2019. , Database: USPTO Patent Applications
Abstract: A system to access one or more user profiles that govern one or more vehicle functions. The system cooperates with a processor and verification module which are adapted to verify, using one or more of **biometric information**, gesture recognition, facial recognition and device identification **information**, that a user has authority to access the one or more user profiles, where the one or more profiles are stored in one or more of a vehicle, a cloud and a communications device. An edit module is further provided and adapted to allow the user to make one or more edits to the one or more user profiles.
AN: edspap.20190392107

USPTO Full Text Options

7. ## Human Computer Interaction Handbook : Fundamentals, Evolving Technologies, and Emerging Applications, Third Edition

By: Jacko, Julie A. Series: Human Factors and Ergonomics. Edition: 3rd ed. Boca Raton : CRC Press. 2012. eBook. Description: Winner of a 2013 CHOICE Outstanding Academic Title Award The third edition of a groundbreaking reference, The Human--Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications raises the bar for handbooks in this field. It is the largest, most complete compilation of HCI theories, principles, advances, case studies, and more that exist within a single volume. The book captures the current and emerging sub-disciplines within HCI related to research, development, and ... (*AN 452086*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Industrial Health & Safety; Human-computer interaction--Handbooks, manuals, etc; Computer simulation--Handbooks, manuals, etc; Virtual reality--Handbooks, manuals, etc

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 134

8. ## ELECTRONIC APPARATUS AND METHOD FOR CONTROLLING FUNCTIONS IN THE ELECTRONIC APPARATUS USING A BIO-METRIC SENSOR

Patent Application: 15/192952. Filed: June 24, 2016. Published: December 29, 2016. , Database: USPTO Patent Applications

Abstract: According to various embodiments of the present disclosure, an electronic device may include a **biometric** sensor configured to detect a contact signal from at least two **biometric** electrodes and a processor configured to determine whether the contact signal received from the **biometric** sensor has biological characteristics. When the processor determines that the contact signal is a **biometric** input having biological characteristics, the processor executes a **biometric information** function. When the processor determines that the contact signal does not include the biological characteristics, the processor executes a general function related to an application.

AN: edspap.20160378965

USPTO Full Text Options

9. ## 2018 Tech Gift Guide.

By: Allen, Jeffrey; Hallene, Ashley. *GPSolo*. Nov/Dec2018, Vol. 35 Issue 6, p42-69. 28p. 76 Color Photographs. Abstract: The article discusses about technology-related gifts for spouses, friends, family, partners, employees, and others focusing on how these gifts could professionally and provide enjoyable additions to your personal life. Topics include Internet of Things (IOT), requirement of the American Bar Association (ABA), and online sales of gift products. (*AN: 133551411*), Database: Academic Search Complete

Subjects: DIGITAL technology; GIFTS; INTERNET of things; INTERNET sales; AMERICAN Bar Association; Gift, Novelty, and Souvenir Stores

HTML Full Text **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 135

10. ## Biosensors for Epilepsy Management: **State**-of-Art and Future Aspects.

By: Tiwari, Shivani; Sharma, Varsha; Mujawar, Mubarak; Mishra, Yogendra Kumar; Kaushik, Ajeet; Ghosal, Anujit. *Sensors (14248220).* Apr2019, Vol. 19 Issue 7, p1525-1525. 1p. Abstract: Epilepsy is a serious neurological disorder which affects every aspect of patients' life, including added socio-economic burden. Unfortunately, only a few suppressive medicines are available, and a complete cure for the disease has not been found yet. Excluding the effectiveness of available therapies, the timely detection and monitoring of epilepsy are of utmost priority for early remediation and prevention. Inability to detect underlying epileptic signatures at early stage causes serious damage to the central nervous system (CNS) and irreversible detrimental variations in the organ system. Therefore, development of a multi-task solving novel smart biosensing systems is urgently required. The present review highlights advancements in **state**-of-art biosensing technology investigated for epilepsy diseases diagnostics and progression monitoring or both together. **State** of art epilepsy biosensors are composed of nano-enabled smart sensing platform integrated with micro/electronics and display. These diagnostics systems provide bio-**information** needed to understand disease progression and therapy optimization timely. The associated challenges related to the development of an efficient epilepsy biosensor and vision considering future prospects are also discussed in this report. This review will serve as a guide platform to scholars for understanding and planning of future research aiming to develop a smart bio-sensing system to detect and monitor epilepsy for point-of-care (PoC) applications. [ABSTRACT FROM AUTHOR] DOI: 10.3390/s19071525. (*AN: 135898611*), Database: Academic Search Complete

Subjects: EPILEPTICS; TREATMENT of epilepsy; BIOSENSORS; NANOTECHNOLOGY; NEURODEGENERATION; Research and Development in Biotechnology

HTML Full Text **PDF Full Text** (3.7MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 136

11. ## Financial Audit: Federal Deposit Insurance Corporation Funds' 2019 and 2018 Financial Statements.

By: Dalkin, James R. *GAO Reports*. 2/13/2020, following p1-194. 204p.

Abstract: The article offers **information** on financial audit of the 2019 and 2018 financial statements of the two funds of Federal Deposit Insurance Corp. (FDIC) administers. Topics discussed include **information** on funds involving Deposit Insurance Fund (DIF) and the Federal Savings and Loan Insurance Corp. (FSLIC) Resolution Fund (FRF); examination of noncompliance for 2019 with provisions of applicable laws, contracts, and grant agreements; and FDIC's internal control over financial reporting. (*AN: 141763234*), Database: Business Source Complete

Subjects: Financial statements; Auditing; Finance; Federal Deposit Insurance Corp.; Federal Savings & Loan Insurance Corp.; Other direct insurance (except life, health and medical) carriers

PDF Full Text (31.2MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 137

12. ## Sensors, Nanoscience, Biomedical Engineering, and Instruments : Sensors Nanoscience Biomedical Engineering

By: Dorf, Richard C. Series: The Electrical Engineering Handbook, Sensors, nanoscience, biomedical engineering, and instruments. Edition: 3rd ed. Boca Raton : CRC Press. 2006. eBook. Description: In two editions spanning more than a decade, The Electrical Engineering Handbook stands as the definitive reference to the multidisciplinary field of electrical engineering. Our knowledge continues to grow, and so does the Handbook. For the third edition, it has expanded into a set of six books carefully focused on a specialized area or field of study. Each book represents a concise yet definitive collection of key concepts, models, and equations in its respective domain, thoughtfully gathered for ... (*AN 154289*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Nanotechnology & MEMS; MEDICAL / Biotechnology; TECHNOLOGY & ENGINEERING / Sensors; Biosensors; Medical electronics; Biomedical engineering

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

13. ## 2017 Tech Gift Guide.

By: Allen, Jeffrey; Hallene, Ashley. *GPSolo*. Nov/Dec2017, Vol. 34 Issue 6, p36-61. 26p. Abstract: The article offers **information** on several products including the Microsoft Surface Pro laptop, the Sony Cyber-shot RX100 camera, and the Canon EOS digital camera. (*AN: 126830012*), Database: Academic Search Complete

Subjects: LAPTOP computers; DIGITAL cameras; CANON Inc.; SONY Corp.; MICROSOFT Corp.; Photographic and Photocopying Equipment Manufacturing; Commercial and service industry machinery manufacturing; Computer and peripheral equipment manufacturing; Electronic Computer Manufacturing

HTML Full Text **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 138

14. ## A comprehensive review of denoising techniques for abdominal CT images.

By: Kaur, Ravinder; Juneja, Mamta; Mandal, A. K.. *Multimedia Tools & Applications* , Sep2018, Vol. 77 Issue 17, p22735-22770, 36p Abstract: Computed Tomography (CT) is one of the effective imaging modality in medical sciences that assist in diagnosing various pathologies inside the human body. Despite considerable advancement in acquisition speed, signal to noise ratio and image resolution of computed tomography imaging technology, CT images are still affected by noise and artifacts. A tradeoff between the amount of noise reduced and conservation of genuine image details has to be made in such a way that it enhances the clinically relevant image content. Therefore, noise reduction in medical images is an important and challenging task, as it helps to improve the performance of other image processing procedures such as segmentation or classification to perform better diagnosis by clinicians. Different techniques have been suggested in the literature on denoising of CT images, and each technique has its own presumptions, benefits, and drawbacks. To the best of our knowledge, no survey paper was found in the literature that compares the performance of various denoising techniques for CT images. This study aims to compare the capabilities of several notable and contemporary denoising techniques in the presence of different types of noise present in abdominal CT images. This comparative analysis helps to determine the most suitable denoising technique for practitioners and researchers that can be used in real life scenarios. Furthermore, the advantages and disadvantages of considered denoising methods have also been discussed along with some recommendations for further research in this area. [ABSTRACT FROM AUTHOR]; DOI: 10.1007/s11042-017-5500-5; (*AN 131207839*), Database: Applied Science & Technology Source

Subjects: Image denoising; Computed tomography; Signal-to-noise ratio; Noise control; Image processing; Image segmentation; Diagnosis; Irradiation Apparatus Manufacturing; Photofinishing Laboratories (except One-Hour); One-Hour Photofinishing

HTML Full Text **PDF Full Text** (13.2MB)

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 139

15. ## Complete Book of Remote Access : Connectivity and Security

By: Kasacavage, Victor. Series: The Auerbach Best Practices Series. Boca Raton, Fla : Auerbach Publications. 2003. eBook. Description: As technology advances, the demand and necessity for seamless connectivity and stable access to servers and networks is increasing exponentially. Unfortunately the few books out there on remote access focus on Cisco certification preparation, one aspect of network connectivity or security. This text covers both-the enabling technology and how to make remote access secure. The definitive resource for network administrators and IT professionals implementing and **maintaining** remote access systems, The ... (*AN 135484*), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Networking / General; COMPUTERS / Security / General; Computer networks--Remote access; Computer networks--Security measures

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

16. ## Alan Simpson's Windows® XP Bible

By: Simpson, Alan. Series: Bible. Edition: 2nd ed. Indianapolis, IN : Wiley. 2005. eBook. Description: If Windows XP **can** do it, you **can** do it too... Windows XP is the undisputed market leader among operating systems, and the enhancements and security improvements in Service Pack 2 made it even better. So if you already know how to turn on a PC and use a mouse, here's the place to learn how to use every fabulous feature of Windows XP. Let an expert show you the new security features and help you customize your Windows, manage files, go online safely, work with digital media, set up a network, and solve ... (*AN 127314*), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Operating Systems / Windows Desktop; Operating systems (Computers)

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 140

17. FEDERAL REGISTER.

Federal Register (National Archives & Records Service, Office of the Federal Register). 4/8/2019, Vol. 84 Issue 67, pI-iii. 213p. Abstract: The article focuses on regulatory documents having general applicability and legal effect, most of which are keyed to and codified in the Code of Federal Regulations in the U.S. Topics include the U.S. Department of Homeland Security (DHS) stated to have reduced Greece's Electronic System for Travel Authorization (ESTA) travel authorization validity period for travel by nationals of Greece under the Visa Waiver Program (VWP) from two years to one year. (*AN: 135785883*), Database: Business Source Complete

Subjects: United **States**. Dept. of Homeland Security; Travel regulations; Electronic systems; Visas; Waiver

PDF Full Text (17MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 141

18. ## Security issues in cloud environments: a survey.

By: Fernandes, Diogo; Soares, Liliana; Gomes, João; Freire, Mário; Inácio, Pedro. *International Journal of Information Security.* Apr2014, Vol. 13 Issue 2, p113-170. 58p. Abstract: In the last few years, the appealing features of cloud computing have been fueling the integration of cloud environments in the industry, which has been consequently motivating the research on related technologies by both the industry and the academia. The possibility of paying-as-you-go mixed with an on-demand elastic operation is changing the enterprise computing model, shifting on-premises infrastructures to off-premises data centers, accessed over the Internet and managed by cloud hosting providers. Regardless of its advantages, the transition to this computing paradigm raises security concerns, which are the subject of several studies. Besides of the issues derived from Web technologies and the Internet, clouds introduce new issues that should be cleared out first in order to further allow the number of cloud deployments to increase. This paper surveys the works on cloud security issues, making a comprehensive review of the literature on the subject. It addresses several key topics, namely vulnerabilities, threats, and attacks, proposing a taxonomy for their classification. It also contains a thorough review of the main concepts concerning the security **state** of cloud environments and discusses several open research topics. [ABSTRACT FROM AUTHOR] DOI: 10.1007/s10207-013-0208-7. (*AN: 95064452*), Database: Computer Source

Subjects: CLOUD computing security measures; COMPUTER networks in business enterprises; ELASTICITY (Economics); WEB services; CLOUD computing; MANAGEMENT

PDF Full Text (1.7MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 142

19. ## Forensic Science : An Encyclopedia of History, Methods, and Techniques

By: Tilstone, William J.; Savage, Kathleen A.; Clark, Leigh A. Santa Barbara, Calif : ABC-CLIO. 2006. eBook. Description: Written by experts for the general audience, this A-Z presentation covers all aspects of forensic science from its beginning to its central place in modern law enforcement. (*AN 161024*), Database: eBook Collection (EBSCOhost)

Subjects: LAW / Forensic Science; REFERENCE / Encyclopedias; SOCIAL SCIENCE / Criminology; Forensic sciences--Encyclopedias; Forensic sciences--History; Criminal investigation--Encyclopedias; Criminal investigation--History

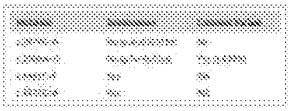
PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

20. ## Posters.

Bipolar Disorders. Mar2018 Supplement S1, Vol. 20, p63-141. 79p. 1 Chart. DOI: 10.1111/bdi.12619. (*AN: 128291334*), Database: Academic Search Complete

Subjects: AFFECTIVE disorders; BIPOLAR disorder in adolescence; BIPOLAR disorder in children; PSYCHIATRIC diagnosis; ANHEDONIA; DIAGNOSIS; PREVENTION; THERAPEUTICS



HTML Full Text **PDF Full Text** (2MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 143

21. FEDERAL REGISTER.

Federal Register (National Archives & Records Service, Office of the Federal Register). 2/21/2019, Vol. 84 Issue 35, pi-iv. 258p. Abstract. The article offers **information** on the public regulations and legal notices issued by different U.S. government agencies, as of February 21, 2019. Topics include **information** collection activities of the U.S. Alcohol, Tobacco, Firearms, and Explosives Bureau; **information** Collection Activities of the U.S. Centers for Disease Control and Prevention ; and Proposed Good Samaritan Settlement Agreement and Order on Consent for Removal Action by U.S. Environmental Protection Agency. (*AN: 134856735*), Database: Business Source Complete

Subjects: United **States**. Alcohol & Tobacco Tax & Trade Bureau; Centers for Disease Control & Prevention (U.S.); United **States**. Environmental Protection Agency; Administration of Public Health Programs; Administration of Air and Water Resource and Solid Waste Management Programs; Government agency rules & practices; Notice of proposed rulemaking (Administrative law)

PDF Full Text (19.9MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 144

22. LAW, VIRTUAL REALITY, AND AUGMENTED REALITY

By: Lemley, Mark A.; Volokh, Eugene. In: University of Pennsylvania Law Review. April 2018, Vol. 166 Issue 5, p1051, 88 p.; University of Pennsylvania, Law School Language: English. Abstract: INTRODUCTION 1053 I. THE RISE OF THE MACHINES 1058 A. The Technological Background 1058 B. The Practical Applications 1059 C. The Effect on our Interaction with the World 1063 1. [...] / Virtual Reality (VR) and Augmented Reality (AR) are going to be big--not just for gaming but for work, for social life, and for evaluating and buying real-world products. Like many big technological advances, they will in some ways challenge legal doctrine. In this Article, we will speculate about some of these upcoming challenges, asking: (1) How might the law treat 'street crimes' in VR and AR--behavior such as disturbing the peace, indecent exposure, deliberately harmful visuals (such as strobe lighting used to provoke seizures in people with epilepsy), and 'virtual groping'? Two key aspects of this, we will argue, are the Bangladesh problem (which will make criminal law very hard to practically enforce) and technologically enabled self-help (which will offer an attractive alternative protection to users, but also a further excuse for real-world police departments not to get involved). (2) How might the law handle tort lawsuits, by users against users, users against VR and AR environment operators, outsiders (such as copyright owners whose works are being copied by users) against users, and outsiders against the environment operators? (3) How might the law treat users' alteration of other users' avatars, or creation of their own avatars that borrow someone else's name and likeness? (4) How might privacy law deal with the likely pervasive storage of all the sensory **information** that VR and AR systems present to their users, and that they gather from the users in the course of presenting it? (5) How might these analyses reflect on broader debates even outside VR and AR, especially order without law and the speech--conduct distinction? (*AN: edsgcl.546878977*), Database: Gale OneFile: LegalTrac

Subjects: United **States**; Virtual reality technology; Government regulation; Augmented Reality -- Laws, regulations and rules; Criminal liability -- Analysis; Virtual reality -- Laws, regulations and rules; Tort liability -- Analysis; Intellectual property law -- Evaluation

PDF Full Text **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 145

23. AUSTRALIA BANKING.

Acquisdata Industry SnapShots: Australia Banking. 8/23/2018, Issue 13107, p1-91. 94p. Abstract: An industry report for the banking industry in Australia is presented from publisher Acquisdata Pty. Ltd. as of August 23, 2018, with topics including media releases, latest research, and overviews of leading companies. (*AN: 131430688*), Database: Business Source Complete

Subjects: Banking industry; AMP Bank Ltd.; Bank of Sydney Ltd.; Bank of Queensland Ltd.; Credit Suisse Australia Ltd.; Personal and commercial banking industry; Savings Institutions; Commercial Banking; Other Depository Credit Intermediation

PDF Full Text (10.6MB) **USPTO Full Text Options**

24. Urban Disaster Resilience and Security : Addressing Risks in Societies

By: Fekete, Alexander; Fiedrich, Frank. Series: The Urban Book Series. Cham, Switzerland : Springer, 2018. eBook. Description: This edited book investigates the interrelations of disaster impacts, resilience and security in an urban context. Urban as a term captures megacities, cities, and generally, human settlements, that are characterised by concentration of quantifiable and non-quantifiable subjects, objects and value attributions to them. The scope is to narrow down resilience from an all-encompassing concept to applied ways of scientifically attempting to ‚measure'this type of disaster related resilience. 28 chapters ... (*AN 1651592*), Database: eBook Index

Subjects: SCIENCE / Earth Sciences / Geography; BUSINESS & ECONOMICS / Development / Sustainable Development; NATURE / Natural Disasters; TECHNOLOGY & ENGINEERING / Civil / General; TECHNOLOGY & ENGINEERING / Environmental / General; Disaster relief; City planning; Disasters

Full Text Finder **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 146

25. ## Using Microsoft Windows XP

By: Cowart, Robert; Knittel, Brian. Edition: Platinum ed. Indianapolis, Ind : Pearson Education, Inc. 2004. eBook. Description: Title from ebook title screen (viewed on Apr. 28, 2005). (*AN 128872*), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Operating Systems / Mac OS; COMPUTERS / Operating Systems / Windows Desktop; COMPUTERS / Operating Systems / Windows Server; COMPUTERS / Operating Systems / DOS; COMPUTERS / System Administration / Windows Administration; Operating systems (Computers)

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

26. ## Kinematic Self-replicating Machines

By: Freitas, Robert A.; Merkle, Ralph C. Georgetown, Tex : CRC Press LLC. 2004. eBook. (*AN 125909*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Electronics / Digital; TECHNOLOGY & ENGINEERING / Electronics / Microelectronics; Molecular electronics; Nanotechnology; Artificial intelligence

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

27. ## Teladoc Health Inc Corporate Analyst Meeting - Final

Fair Disclosure Wire (Quarterly Earnings Reports). 03/05/2020. (*AN: 32U2974036929FDW*), Database: Regional Business News

HTML Full Text **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 147

28. ## Understanding Surveillance Technologies : Spy Devices, Their Origins & Applications

By: Petersen, Julie K. Boca Raton, FL : CRC Press. 2001. eBook.
Description: From electronic wire taps to baby monitors and long-distance video and listening devices, startling changes occur everyday in how we gather, interpret, and transmit **information**. An extraordinary range of powerful new technologies has come into existence to meet the requirements of this expanding field.Your search for a comprehensive resourc (*AN 154607*), Database: eBook Collection (EBSCOhost)

Subjects: BUSINESS & ECONOMICS / Commerce; COMPUTERS / Security / General; LAW / Forensic Science; SOCIAL SCIENCE / Criminology; Electronic surveillance

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

29. ## Gol Linhas Aereas Inteligentes SA Investors and Analysts Meeting - Final

Fair Disclosure Wire (Quarterly Earnings Reports). 01/09/2020. (*AN: 32U0858251481FDW*), Database: Regional Business News

HTML Full Text **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 148

30. Friday, August 25 / Vendredi 25 août.

Archives of Physiology & Biochemistry. Apr2000, Vol. 108 Issue 1/2, p57-162. 106p. Abstract: 7:30 Registration / Inscription Room / Salle : Le Foyer 8:30 Announcements / Annonces Room / Salle : Ambassadeur A, B, C 8:45 Keynote Speaker / Conférencier invité Ronald F. Zernicke, University of Calgary, Alberta, Canada 57 Factors in Skeletal Adaptation Coauthors / Coauteurs : Wohl G.R., Boyd S.K., Judex S., Zernicke R.F. Chairman / Président : Hubert Labelle Room / Salle : Ambassadeur A, B, C 9:30 Debate / Débat The role of spine in locomotion / Le rôle de la colonne vertébrale dans la locomotion Serge Gracovetski, Concordia University, Montréal, Canada Jak P. Callaghan, University of Guelph, Guelph, Canada Moderator / Animateur : David Pearsall Room / Salle : Ambassadeur A, B, C 10:30 Poster Session / Session d'affichage Poster number corresponds to the abstract page number / Le numéro de l'affiche correspond au numéro de la page de l'abrégé Clinical Biomechanics / Biomécanique clinique Chairman / Président : Hubert Labelle Room / Salle : Salon Diplomate Analysis of Pressure Distribution at the Body-Seat Interface Using Image Processing Technique Aïssaoui R., Kauffmann C., Dansereau J., de Guise J.A. Bilateral and Three-Dimensional Analysis of Elderly Able-Bodied Gait Sadeghi H., Zabjek K.F., Prince F., Sadeghi S., Labelle H. Bilateral Rearfoot Asymmetry and Anterior Knee Pain Syndrome Livingston L., Mandigo J. Biomechanical Factors in Gait of Knee Osteoarthritis Patients Deluzio K.J., Wyss U.P., Costigan P.A., Zee B. Biomechanical Study of the Shoulder of Elderly Patients Using a Wheelchair Kheila I., Laboisse J.J., Pillu M., Lavaste F. Computer Keyboard Slope and Wrist Extension Angle on Individuals with Carpal Tunnel Syndrome Simoneau G.G., Marklin R.W., Berman J.E., Monroe J.F., Welsh S.E. Effet d'une AHMI sur les paramètres cinétiques et cinématiques lors d'une tâche dynamique Lafond D., Normand M.C. Energy Expenditure of Below-Knee Amputees as a Result of Prosthetic Weight Bateni H., Olney S.J. Experimental Protocol for the Kinematics Measurement of the Shoulder and of the Upper Limb Roux E., Bouilland S., Bouttens D., Istas D., Godillon-Maquinghen A.-P., Lepoutre F.-X. In Vivo Distance Between ACL Insertions of the Ovine Stifle Joint **During** Walking Ronsky J., Powers M., Tapper J., Majima T., Sutherland C., Shrive N., Frank C. Lower Limbs Deformities and Plantar Pressure Distribution in Cerebral Palsy Children Femery V., Moretto P., Thevenon A., Renaut H. Normal Values for Walking Base Measured **During** Clinical Gait Analysis DeGuzman A.B., Whittle M.W. Pressure Changes Under the Feet of Obese Adults After a Weight Reduction Program Bolte K., Hennig E.M., Hills A.P., McDonald M. Quasi Static Foot Compression Tests Masson C., Basile F., Cesari D., Bonnoit J. Resistance Versus Angular Movement Law of the Glenohumeral Joint Malak A., Fayet M., Maiffredy L., Bermond F., Bouquet R., Ramet M., Verriest J.P., Wang X., Voïglio E. Surface EMG of Tigh Muscles of

IPR2025-01313; Samsung
Ex. 1002 - Page 149

Transtibial Amputees Using Successively Ischial Bearing and PTB Socket Pillu M., Dechamps E., Dupré J.C. The Biomechanics of Foot Orthotics in People with Medial Compartment Knee Osteoarthritis Prasad M., Culham E., Rudan J. The Effect of Body Mass Index on Seat Interface Shape Patterns Li Y., Aïssaoui R., Brienza D.M., Dansereau J. The Effect of Bracing ACL Deficient Knees on Skeletal 3-D Kinematics Ramsey D.K., Lamontagne M., Wretenberg P.F., Németh G. The Effect of Chair Height on Selected Kinetic Parameters of the Sit-to-Stand Task in the Elderly Hughes L., Kozey J. Tibial Tubercle Anteromedialization Restores Patellar Force Distribution Wilson D., Apreleva M., Ramappa A., Harrold F., Steiner M. Motor Control / Contrôle moteur Chairman / Président : Anatholi Feldman Room / Salle : Salon Diplomate Changes in Gait Initiation Program Induced by an Heel-Off Posture Couillandre A., Brenière Y., Maton B. Coordination Changes Under Lower Leg Asymmetries Haddad J.M., van Emmerik R.E.A., Whittlesey S.N., Hamill J. Determination of Motor Control Variables in a Finite Element Model of the Trunk Using Artificial Neural Network Garceau P., Cheriet F., Beauséjour M., Labelle H., Aubin C.-É. Factors Limiting the Kinematics Parameters of Gait Initiation Michel V., Do M.-C. Les paramètres cinématiques d'un objet en chute libre sont-ils les seuls pris en compte lors de la planification de l'attraper? Prévost P., McIntyre J., Berthoz A. Modifications of Gait Velocity to Avoid Collisions Cinelli M.E., Patla A.E., Racco V. Phase-Delay Analysis of Interjoint Coordination **During** Reaching Movements Mitnitski A.B., Cirstea M.C., Feldman A.G., Levin M.F. Synchrony Between the Minimum in Global EMG Activity and the Point of Reversal in Sit-to-Stand Movements Archambault P.S., Feldman A.G. The Influence of Available Response Time on Centre of Mass Displacement **During** the Termination of Gait McGowan B.R., Patla A.E., Racco V. The Influence of Fatigue on Multi-Muscle and Multi-Joint Coordination **During** Hammering Côté J., Levin M.F., Feldman A.G. The Influence of Visual **Information** About the Lower Limbs on the Trajectory of the Centre of Mass and Time to Termination of Gait Racco V., Patla A.E., Cinelli M.E. The Relationship Between Gait Transition Speed and Dorsiflexor Force Production Hreljac A., Ferber R. Timing and Magnitude Changes of Muscle and Motion Dependent Torques with Practice Fast Arm Movements to Target Vardaxis V. Instrumentation Chairman / Président : Anne-Pascale Godillon Room / Salle : Salon Diplomate 3D Geometric Acquisition of the Human Body in Driving Posture for Modelling Purposes Serre T., Bidal S., Durand F., Behr M., Basile F., Brunet C. A Large Force Platform for Human Displacements Desjardins P., Gagnon M. A New **Dynamic** Transducer for In-Vitro Measurement of Human Knee Joint Contact Pressure Mun J.H., Choi W.S., Satomi T., Kim Y.S., Lim O.K., Freeman J., Rim K. A Robustness Study of Self-Calibration Technique for the Radiographic 3D Reconstruction of Human Spine Remaki L., Cheriet F., Beliefleur C., Labelle H., Dansereau J. Assessment of a Three-Dimensional Kinematic Robot for Biomechanics Studies of Human Movement Desjardins P., Plamondon A., Gagnon M.

IPR2025-01313; Samsung
Ex. 1002 - Page 150

Calibration of a Three Axis Force Cylindrical Sensor Used to Evaluate the Grasping Reflex Merrien A., Barbedette B., Mariot J.-P., Etcharry-Bouyx F., Le Gall D. Determination of the Effectiveness of Materials in Attenuating High Frequency Shock **During** Gait Using Filter-Bank Analysis Gillespie K.A., Dickey J.P. Development and Validation of a Mobile Video Capture System for Spatial Kinematics Lafontaine D., Lamontagne M. In-Vivo Anterior Cruciate Ligament Strain Behaviour **During** a Rapid Deceleration Movement Benoit D., Cerulli G., Caraffa A., Lamontagne M., Liti A., Brue S. Portable and Affordable: A Compact EMG Recorder Rambarran K.K., Robertson D.G.E. Quantification of In Vivo ACL Elongation **During Dynamic** Joint Movements: A New Methodology McLean S.G., van den Bogert A.J. Residual Errors of Three-Dimensional Coordinates by Comparing Filming Volumes and Num-ber of Cameras Lamontagne M., Kendall M., Murphy N., El Maach I. Simulation of Lift Truck Lateral Tipover to Improve Driver's Safety Koutchouk M., Aubin C.-É., Gou M., Olteanu M., Benoît R. Locomotion Chairman / Président : Denis Gravel Room / Salle : Salon Diplomate 3D Young Normal Knee Powers **During** Stair Climbing Oakley P.A., Costigan P.A. A Novel Machine for In Vitro Spinal Biomechanics Testing Gillespie K.A., Dickey J.P., Yang S.X. Automatic Determination of Lower Limb Segment Masses from M.R.I. Pinti A., Hédoux P., Kemoun G., Boluix B. Comparaison of Center of Mass Positions of Lower Body Segments Obtained from M.R.I. and Geometric Models Hédoux P., Pinti A., Waterlain E., Kemoun G., Boluix B. Effets de l'erreur du positionnement des axes lors de l'étude de la cinématique 3D du genou Parent G., de Guise J.A., Yahia L'H. Examining the Relationship Between the Mechanical and Metabolic Energy Expenditure of Walking at Various Velocities Semeniuk K.M., Robertson D.G.E. Gait Analysis on a Transversely Tilted Platform De Garie L., Pearsall D.J. Ground Reaction Force and EMG Responses **During** Gait in Treadmill Sacco I.C.N., Serrão J.C., Sá M.R., Amadio A.C. Interjoint Coordination in Lower Limbs **During** Different Movements in Humans St-Onge N., Yahia L'H., Feldman A.G. Kinematic Study of the Knee with a 3D Analyser Ganjikia S., Duval N., Yahia L'H., de Guise J.A. Local and Global Asymmetries in Able-Bodied Gait Sadeghi H., Allard P., Prince F., Duhaime M., Sadeghi S., Labelle H. Predicting Moment of Inertia of the Human Leg Requires the Use of an Elliptical Model Durkin J.L., Dowling J.J. Rigid Foot Segment Assumption: Effects of Mid-Foot Motion Tiberio D., Heiderscheit B.C., Hamill J. The Effect of Shank Soft Tissue Movement on Knee Moment Profiles **During** Natural Cadence Walking Manal K., McClay I., Richards J., Stanhope S. The Finite Helical Axis Distribution of the Ovine Stifle Joint **During** the Swing Phase of Normal Gait Tapper J., Powers M., Ronsky J., Shrive N., Majima T., Frank C. Two-Segment Model of the Foot: Reduction of Power Imbalance Cronin A., Robertson D.G.E. 12:00 Lunch / Déjeuner Room / Salle : Gouverneur 1, Gouverneur 2, Les Verrières, Sénateur 13:30 Keynote Speaker / Conférencier invité L'Hocine Yahia, École Polytechnique de Montréal, Montréal, Canada 121 Shape Memory Implants in Medicine:

IPR2025-01313; Samsung
Ex. 1002 - Page 151

Orthopaedics, Dental and Cardiovascular Applications Chairman / Président : Carl-Éric Aubin Room / Salle : Ambassadeur A, B, C 14:15 Poster Session / Session d'affichage Poster number corresponds to the abstract page number / Le numéro de l'affiche correspond au numéro de la page de l'abrégé Sport Biomechanics / Biomécanique du sport Chairman / Président : David Pearsall Room / Salle : Salon Diplomate Analyse mécanique des **conditions** d'accord d'un gymnaste avec un tremplin Kobbi Y., Duboy J., Lacouture P., Junqua A. Caractérisation d'un exercice de pédalage sur ergocycle par l'évaluation des travaux cumulés des forces internes Riquet A., Lacouture P., Duboy J. Carectérisation du phénomène transitoire entre deux états d'équilibre (A.T.R.) par l'évaluation de la quantité de rotation Jeddi R., Junqua A., Lacouture P., Duboy J. Comparison of Impact and Shock Attenuation Between Full-Suspension and Non-Rear Suspension Bicycles Roy J.P., Robertson D.G.E. Comparison of Lower Extremity Joint Angles, Moments and Powers Among Straight Ahead and Crossover Cutting Tasks Houck J., Yack H.J., Taibe K. Electromyographical and Mechanical Parameters Evolution on a Ever Changing Saddle Thiery C., Toumi H., Maitre S., Chandezon R., Vanneuville G., Terver S., Poumarat G. EMG Analysis of the Field Hockey Drive Murtaugh K. Evaluation of Human External Power in the Pedalling Task Using Air and Ground Friction Coefficientsidentification of a Bicycle Mariot J.-P., Barbedette B. Experimental Measurements of the Swimming Start Variations Bagesteiro L.B., Laranja R.A.C., Tamagna A. Initiating Rotation in Triple Somersaulting Armstand Dives Murtaugh K., Miller D.I. Intra-Step Belt Speed Variation and Horizontal Power Transfer **During** Treadmill Running Radstake T., Dowling J.J. Joint Angular Velocity Contributions to Clubhead Speed as Determined by Computer Simulation Sprigings E., Neal R. Joint Reaction Forces and Moments of the Ankle and Knee When Running Over Obstacles of Varying Height Hreljac A., Stergiou N., Scholten S.D. Kinetic and Kinematic Analysis of the Sprint Start Favérial J., Basset F., Azizah M.G., Teasdale N. Mathematical Model of the Sprint Relay Murphy S.D., Robertson D.G.E., Rambarran K.K. Modeling Tibial Accelerations in Running Chu J.J., Caldwell G.E. Modélisation expérimentale du coefficient de freinage aérodynamique en ski alpin Barelle C., Tavernier M. Motion of the Foot Inside a Hockey Skate: As Measured from Bone, Skin, and Boot Markers Al Hadi M., Lamontagne M. Relationship Between Impact and Rearfoot Motion **During** Running Countryman M., O'Connor K., Hamill J. The Effects of High vs. Low Stroke Rate on the Drive Phase in Rowing on a Rowing Ergometer Gervais P., Bell G. The Investigation of Cycling Position on Thoracic Spine - A Novel Method of Measureing Thoracic Kyphosis in the Standing Position Rajabi R., Freemont A.J., Doherty P. The Relationship Between Foot Velocity and Braking in the Horizontal Jumps Leblanc J.S. Trunk Muscle Endurance and Quadriceps Muscle Inhibition in Golfers with Low Back Pain Suter E., Lindsay D. Muscle (animal) Chairman / Président : Walter Herzog Room / Salle : Salon Diplomate Force Enhancement and Stability in Skeletal Muscle

IPR2025-01313; Samsung
Ex. 1002 - Page 152

Fibers Wakeling J., Herzog W., Syme D. Function of One- and Two-Joint Muscles **During** Cat Locomotion Based on Direct Measure-ment of In Vivo Muscle Forces Kaya M., Herzog W., Leonard T. In Vivo Fibre Length Changes in the Cat Soleus Herzog W., Leonard T.R. Stability and the Descending Limb of the Force-Length Relation in Mammalian Skeletal Muscle Schachar R., Herzog W., Leonard T. Muscle (human / humain) Chairman / Président : Robert Kearney Room / Salle : Salon Diplomate A Graphical Approach to Determine Synergistic Muscle Forces Using an Optimization Algorithm Ait-Haddou R., Jinha A., Herzog W. A Hybrid Formalism for Cross-Bridge Models Ait-Haddou R., Herzog W. A Robust Method for Estimating Fatigue Measures from Short Data Records Bateni H., Pearsall D.J. Changes in the Neural and Contractile Properties of the Quadriceps Muscle after a Prolonged Cycling Exercise Lepers R., Maffiuletti N.A., Martin A., van Hoecke J., Hausswirth C. Effects of Vibration Induced by Inline Skating on Neuromotor Functions Thompson C., Bélanger M. Effets prolongés d'un traitement de fibrolyse diacutanée Guissard N., Veszely M., Duchateau J. Functional Significance of Muscle Training by Electrical Stimulation Carpentier A., Decamp C., Duchateau J. High Pass Filtering Beyond 100Hz Improves Surface EMG-Based Force Predictions for the Biceps Brachii Potvin J., Brown S., Dowling J., Tolmie S. Muscular Modelling of the Lower Extremity: The Effect of Varying Joint Angles on Muscle Length St.Pierre T.A., Robertson D.G.E. Neuromuscular Recovery After a Strength Training Session Ferri A., Pousson M., van Hoecke J. Plantar-Flexor Twitch Contractile Properties Associated to Maximal Hoffmann Reflex in Three Different Populations Maffiuletti N.A., Martin A., Schieppati M. Quadriceps Femoris Activation and Accuracy Across the Perceptual Range Pincivero D.M., Suter E., Coelho A.J., Campy R.M. Repeatability of Electromyographic Profiles **During** Normal Walking in Young Adults Gavianes B., Goiriena J.J., Tobar C. The Soleus H-Reflex Modulation Pattern **During** Human Walking Is Not Based on Lower Limb Movements Schneider C., Lavoie B.A., Capaday C. 15:45 Oral presentation for the CSB Student and Young Investigator Award Competition / Présentations orales pour le concours SCB pour étudiants et jeunes chercheurs Chairman / Président : David Pearsall Room / Salle : Ambassadeur A, B, C 17:00 CSB General Meeting / Assemblée générale de la SCB Room / Salle : Ambassadeur A, B, C 19:30 SB-CSB Banquet / Banquet SB-SCB. [ABSTRACT FROM AUTHOR] DOI: 10.1076/apab.108.1.57.11511. (*AN: 5260868*), Database: Academic Search Complete

Subjects: BIOMECHANICS; CONFERENCES & conventions; Convention and Trade Show Organizers

PDF Full Text (3.3MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 153

EBSCO Connect | Privacy Policy | A/B Testing | Terms of Use | Copyright | Cookie Policy | Contact Us

powered by EBSCO*host*

© 2020 EBSCO Industries, Inc. All rights reserved.

IPR2025-01313; Samsung
Ex. 1002 - Page 154

Google performing communication with a second communication interface relati

Sign in

All News Images Videos More Settings Tools

About 79,200 results (0.67 seconds)

www.google.com/patents/EP3029590A1?cl=en

A computer system and an apparatus for use in a computer system

The computer system includes a first database containing the dynamic binary code ... The controller means performs, when receiving a code from the biometric ... receiving the first binary code, a second binary code by means of the dynamic ... as a parallel communication interface, a serial communication interface, an SPI, ...
App. - Filed Mar 15, 2004 - Published Jun 8, 2016 - Uffe Clemmensen - Quardlock ApS
Overview · Related · Discuss

www.google.com/patents/US8838071

Secure communications smartphone system



2 illustrates an exemplary graphical user interface of a first smartphone used to compose and send a secured communication and an ...
Grant - Filed Apr 30, 2014 - Issued Sep 16, 2014 - John Cronin - Oto Technologies Llc
Overview · Related · Discuss

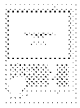
www.google.com/patents/US9288207

Secure communications smartphone system

Initial uses for biometrics (e.g., fingerprint, voice recognition, face recognition) are ... information entered into the communication interface may include, yet is not limited ... The digital communication may then be transmitted to the recipient over a ... a digital communication input by the sender, receiving one or more biometric ...
Grant - Filed Sep 4, 2014 - Issued Mar 15, 2016 - John Cronin - Grandios Technologies, Llc
Overview · Related · Discuss

www.google.com/patents/US8836473

Dynamic keypad and fingerprinting sequence authentication



The apparatus may further include a receiver. The receiver may receive information from the first fingerprint scanner, the information relating to user biometric ...
Grant - Filed Apr 5, 2012 - Issued Sep 16, 2014 - Rustam N. Wadia - Bank Of America Corporation
Overview · Related · Discuss

www.google.com/patents/US9342674

Man-machine interface for controlling access to electronic ...

After requesting the user authentication, the first device detects biometric information associated with the user with the one or more biometric sensors.
Grant - Filed Mar 5, 2015 - Issued May 17, 2016 - David S. Abdallah - Apple Inc.
Overview · Related · Discuss

www.google.com/patents/US9819675

Secure communications smartphone system

A sender of a secured communication may identify one or more biometrics ... initiate the transmission by selecting a part of the communication interface that ...
Grant - Filed Mar 15, 2016 - Issued Nov 14, 2017 - John Cronin - Grandios Technologies, Llc
Overview · Related · Discuss

www.google.com/patents/US20140157384

Biometric Authentication

A biometric authentication system is disclosed that provides a trusted third ... communication protocols for network security for supporting authentication of ...

After receiving the requested biometric data, first party system 104 may transmit the ... biometric information to the requesting second party via network interface 266.
App. - Filed May 3, 2013 - Published Jun 5, 2014 - Benjamin J. Stern - At&T Intellectual Property I, L.P.
Overview · Related · Discuss

www.google.com/patents/US9785763

Techniques for biometric authentication of user of mobile ...

A method for biometric authentication of a user of a mobile device, and a case for ... that was captured by the mobile device, storing the biometric data, receiving a request ... The first wireless communication sub system 530 and the second wireless ... transmits the converted audio data streams to the peripheral interface 523.
Grant - Filed Nov 24, 2015 - Issued Oct 10, 2017 - Paul SCULLY-POWER - Ncap Licensing, Llc
Overview · Related · Discuss

www.google.com/patents/US9530137

Method and apparatus for secure access payment and ...

The method comprises the acts of wirelessly transmitting from a first device, first encrypted authentication information of the first entity, receiving with a second ...
Grant - Filed Feb 9, 2016 - Issued Dec 27, 2016 - Kenneth P. Weiss - Universal Secure Registry, Llc
Overview · Related · Discuss

www.google.com/patents/US20030152254

User authenticating system and method using one-time ...



This invention relates to a user authenticating system and a method using aone-time fingerprint template. The system and the method according to ...
App. - Filed Jun 1, 2001 - Published Aug 14, 2003 - Tai-Dong Ha - Tai-Dong Ha
Overview · Related · Discuss

IPR2025-01313; Samsung
Ex. 1002 - Page 156

Google receiving the dynamic biometric information by the second device via co

Sign in

All News Shopping Videos More Settings Tools

About 119,000 results (0.53 seconds)

www.google.com/patents/US8326378

Communication between devices using tactile or visual ...



In some examples, the system provides two or more dedicated communication devices that communicate with one another without voice-based ...
Grant - Filed Feb 13, 2009 - Issued Dec 4, 2012 - Joseph Ungari - T-Mobile Usa, Inc.
Overview · Related · Discuss

www.google.com/patents/US9342674

Man-machine interface for controlling access to electronic ...

After requesting the user authentication, the first device detects biometric information associated with the user with the one or more biometric sensors.
Grant - Filed Mar 5, 2015 - Issued May 17, 2016 - David S. Abdallah - Apple Inc.
Overview · Related · Discuss

www.google.com/patents/US8627454

Dynamic quota-based entertainment manager



A system biometrically authenticates a user that intends to use an entertainment device. The system obtains, based on the biometric authentication, one or more ...
Grant - Filed Apr 1, 2009 - Issued Jan 7, 2014 - Yuriy Bolyukh - Verizon Patent And Licensing Inc.
Overview · Related · Discuss

www.google.com/patents/US9426150

Biometric authentication

After receiving the requested biometric data, first party system 104 may transmit the received biometric data to second party system 108 for authentication.
Grant - Filed May 3, 2013 - Issued Aug 23, 2016 - Benjamin J. Stern - At&T Intellectual Property Ii, L.P.
Overview · Related · Discuss

www.google.com/patents/US9426660

EHF secure communication device

A communication device employs a contactless secure communication interface to transmit and receive data with a computing device using close proximity ...
Grant - Filed Dec 19, 2013 - Issued Aug 23, 2016 - Gary Davis McCormack - Keyssa, Inc.
Overview · Related · Discuss

www.google.com/patents/US20110176667

Biometric identification in communication



The first calling party profile is provided to called party. A biometric information change from first calling party biometric information to a second calling party ...
App. - Filed Nov 18, 2008 - Published Jul 21, 2011 - Saurabh Kumar - At&T Intellectual Property Ii, L.P.
Overview · Related · Discuss

www.google.com/patents/US8836473

Dynamic keypad and fingerprinting sequence authentication



Each of the first fingerprint scanner and the second fingerprint scanner may capture at ... using modem 224, which may be any suitable communication device.
Grant - Filed Apr 5, 2012 - Issued Sep 16, 2014 - Rustam N. Wadia - Bank Of America Corporation
Overview · Related · Discuss

www.google.com/patents/EP3029590A1?cl=en

A computer system and an apparatus for use in a computer system

The controller means performs, when receiving a code from the biometric sensor ... receiving the first binary code, a second binary code by means of the dynamic ... In accordance with a first aspect of the present invention, the communication ... as a parallel communication interface, a serial communication interface, an SPI, ...

App. - Filed Mar 15, 2004 - Published Jun 8, 2016 - Uffe Clemmensen - Quardlock ApS

Overview · Related · Discuss

www.google.com/patents/US9288207

Secure communications smartphone system

A sender of a secured communication may identify one or more biometrics required ... financial information (e.g., with a bank requesting a transfer of funds between ... When a communication is received by a recipient computing device, the ... exemplary graphical user interface of a second smartphone that has received the ...

Grant - Filed Sep 4, 2014 - Issued Mar 15, 2016 - John Cronin - Grandios Technologies, Llc

Overview · Related · Discuss

www.google.com/patents/US20020174347

Authentication with variable biometric templates



In another embodiment, a module modifies a copy of the template of the reference ... This allows the client device 112 to interface with different types of biometric ...

App. - Filed May 17, 2002 - Published Nov 21, 2002 - David Ting - Imprivata, Inc.

Overview · Related · Discuss

IPR2025-01313; Samsung
Ex. 1002 - Page 158



IPR2025-01313; Samsung
Ex. 1002 - Page 159

1. ## Evaluation of stability of swipe gesture authentication across usage scenarios of mobile device.

By: Ellavarason, Elakkiya; Guest, Richard; Deravi, Farzin. *EURASIP Journal on Information Security* , 3/17/2020, Vol. 2020 Issue 1, p1-14, 14p Abstract: Background: User interaction with a mobile **device** predominantly consists of touch motions, otherwise known as swipe gestures, which are used as a behavioural **biometric** modality to verify the identity of a user. Literature reveals promising verification accuracy rates for swipe gesture authentication. Most of the existing studies have considered constrained environment in their experimental set-up. However, real-life usage of a mobile **device** consists of several unconstrained scenarios as well. Thus, our work aims to evaluate the stability of swipe gesture authentication across various usage scenarios of a mobile **device**. Methods: The evaluations were performed using state-of-the-art touch-based classification algorithms—support vector machine (SVM), k-nearest neighbour (kNN) and naive Bayes—to evaluate the robustness of swipe gestures across **device** usage scenarios. To simulate real-life behaviour, multiple usage scenarios covering stationary and dynamic modes are considered for the analysis. Additionally, we focused on analysing the stability of verification accuracy for time-separated swipes by performing intra-session (acquired on the same day) and inter-session (swipes acquired a week later) comparisons. Finally, we assessed the consistency of individual features for horizontal and vertical swipes using a statistical method. Results: Performance evaluation results indicate impact of body movement and environment (indoor and outdoor) on the user verification accuracy. The results reveal that for a **static** user scenario, the average equal error rate is 1%, and it rises significantly for the scenarios involving any body movement—caused either by user or the environment. The performance evaluation for time-separated swipes showed better verification accuracy rate for swipes acquired on the same day compared to swipes separated by a week. Finally, assessment on feature consistency reveal a set of consistent features such as maximum slope, standard deviation and mean velocity of **second** half of stroke for both horizontal and vertical swipes. Conclusions: The performance evaluation of swipe-based authentication shows variation in verification accuracy across different **device** usage scenarios. The obtained results challenge the adoption of swipe-based authentication on mobile **devices**. We have suggested ways to further achieve stability through specific template selection strategies. Additionally, our evaluation has established that at least 6 swipes are needed in enrolment to achieve acceptable accuracy. Also, our results conclude that features such as maximum slope and standard deviation are the most consistent features across scenarios. [ABSTRACT

IPR2025-01313; Samsung
Ex. 1002 - Page 160

FROM AUTHOR]; DOI: 10.1186/s13635-020-00103-0; (*AN 142293805*), Database: Applied Science & Technology Source

Subjects: Support vector machines; **Biometric** identification; Classification algorithms; Standard deviations; Biometry; Gesture; Body movement

HTML Full Text **PDF Full Text** (2MB) **USPTO Full Text Options**

2. Method for detecting **biometric information** and electronic **device** using same

By: Samsung Electronics Co., Ltd. US Patent: 10231,675. Filed: June 03, 2016. Issued: March 19, 2019. , Database: USPTO Patent Grants

Abstract: A **device** for detecting **biometric information** is provided. The **device** includes a housing, a fastener coupled to a part of the housing and detachably attached to a part of a user's body, at least one first **sensor** configured to detect the motion of the electronic **device**, at least one **second sensor** configured to detect a change in the user's body, a memory, and a processor electrically connected to the at least one first **sensor**, the at least one **second sensor**, and the memory. The memory may store instructions that configure the processor, when being executed, to determine whether the electronic **device** is worn on a part of the user's body using the at least one first **sensor**, acquire **information** on the motion of the electronic **device** using at least a part of the at least one first **sensor** for a **second** period of time shortly before and/or immediately after a first period of time selected passes from the time when the electronic **device** is worn on a part of the user's body, and activate the at least one **second sensor** based on at least a part of the **information** on the motion.

AN: edspgr.10231675

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 161

3. ## A survey on methods and challenges in EEG based authentication

By Jalaly Bidgoly, Amir; Jalaly Bidgoly, Hamed; Arezoumand, Zeynab. In *Computers & Security*. June 2020 93 Language: English. DOI: 10.1016/j.cose.2020.101788 Abstract: EEG is the recording of electrical activities of the brain, usually along the scalp surface, which are the results of synaptic activations of the brain's neurons. In recent years, it has been shown that EEG is an appropriate signal for the **biometric** authentication and has important features such as resistance to spoofing attacks and impossibility to use under pressure and coercion states. In this paper, the state-of-the-art methods in EEG based authentication are reviewed. This review includes a number of aspects such as the various tasks that the user required to perform during the authentication, **devices** and available datasets, the preprocessing procedures and the classification methods used in the EEG **biometric** authentication. Both shallow and deep classification methods are reviewed in this paper. The study shows that the deep learning approaches which are used in the past few years, although still require further research, have shown great results. Moreover, the paper summarizes the works to address the open challenges of this area. The EEG authentication challenges have been discussed from a variety of points of view, including privacy, user-friendliness, attacks, and authentication requirements such as universality, permanency, uniqueness, and collectability. This paper can be used as a preliminary plan and a roadmap for researchers interested in EEG **biometric**. (*AN: S0167404820300730*), Database: ScienceDirect

Subjects: EEG; **Biometric** factor; Authentication; User identification; Pattern recognition; Survey

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 162

4. Possibilities of dynamic **biometrics** for authentication and the circumstances for using dynamic **biometric** signature.

By: Hortai, Frantisek. *Journal of Systems Integration (1804-2724)* , 2018, Vol. 9 Issue 1, p3-18, 16p Abstract: New **information** technologies alongside their benefits also bring new dangers with themselves. It is difficult to decide which authentication tool to use and implement in the **information** systems and electronic documents. The final decision has to compromise among the facts that it faces several conflicting requirements: highly secure tool, to be a user-friendly and user simplicity method, ensure protection against errors and failures of users, speed of authentication and provide these features for a reasonable price. Even when the compromised solution is found it has to fulfill the given technology standards. For the listed reasons the paper argues one of the most natural **biometric** authentication method the dynamic **biometric** signature and lists its related standards. The paper also includes measurement evaluation which solves the independence between the person's signature and **device** on which it was created. [ABSTRACT FROM AUTHOR]; DOI: 10.20470/jsi.v9i1.326; (*AN 128354732*), Database: Applied Science & Technology Source

Subjects: Information technology; **Biometric** identification; Electronic authentication

PDF Full Text (3.2MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 163

5. METHOD FOR DETECTING **BIOMETRIC INFORMATION** AND ELECTRONIC **DEVICE** USING SAME

Patent Application: 15/173099. Filed: June 03, 2016. Published: February 16, 2017. , Database: USPTO Patent Applications

Abstract: A **device** for detecting **biometric information** is provided. The **device** includes a housing, a fastener coupled to a part of the housing and detachably attached to a part of a user's body, at least one first **sensor** configured to detect the motion of the electronic **device**, at least one **second sensor** configured to detect a change in the user's body, a memory, and a processor electrically connected to the at least one first **sensor**, the at least one **second sensor**, and the memory. The memory may store instructions that configure the processor, when being executed, to determine whether the electronic **device** is worn on a part of the user's body using the at least one first **sensor**, acquire **information** on the motion of the electronic **device** using at least a part of the at least one first **sensor** for a **second** period of time shortly before and/or immediately after a first period of time selected passes from the time when the electronic **device** is worn on a part of the user's body, and activate the at least one **second sensor** based on at least a part of the **information** on the motion.

AN: edspap.20170042485

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 164

6. ## A context-aware system to secure enterprise content: Incorporating reliability specifiers

By Oluwatimi, Oyindamola; Damiani, Maria Luisa; Bertino, Elisa. In *Computers & Security*. August 2018 77:162-178 Language: English. DOI: 10.1016/j.cose.2018.04.001 Abstract: The **sensors** of a context-aware system extract contextual **information** from the environment and relay that **information** to higher-level processes of the system so to influence the system's control decisions. However, an adversary can maliciously influence such controls indirectly by manipulating the environment in which the **sensors** are monitoring, thereby granting privileges the adversary would otherwise not normally have. To address such context monitoring issues, we extend CASSEC by incorporating sentience-like constructs, which enable the emulation of "confidence", into our proximity-based access control model to grant the system the ability to make more inferable decisions based on the degree of reliability of extracted contextual **information**. In CASSEC 2.0, we evaluate our confidence constructs by implementing two new authentication mechanisms. Co-proximity authentication employs our time-based challenge-response protocol, which leverages Bluetooth Low Energy beacons as its underlying occupancy detection technology. **Biometric** authentication relies on the accelerometer and fingerprint **sensors** to measure behavioral and physiological user features to prevent unauthorized users from using an authorized user's **device**. We provide a feasibility study demonstrating how confidence constructs can improve the decision engine of context-aware access control systems. (*AN: S0167404818303018*), Database: ScienceDirect

Subjects: Access control; Context awareness; BYOD; Security; Mobility; **Biometric**; Authentication; Reliability; Proximity

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 165

7. ## Design of secure authentication protocol for dynamic user addition in distributed Internet-of-Things

By Trivedi, Hiral S.; Patel, Sankita J.. In *Computer Networks*. 4 September 2020 178 Language: English. DOI: 10.1016/j.comnet.2020.107335 Abstract: Rapid rise in adoption of smart **devices** in distributed Internet-of-things (IoT) has resulted in an exponential increase in volume of generated data. However, due to resource-constrained **sensor** nodes and vulnerable communication channels, **information** protection has become a key concern and prominent factor for improvement in IoT environment. Batch processing systems have several shortcomings as compared to distributed systems. Distributed systems enable dynamic changes in the potential number of **sensors**, actuators, RFID's, resources, users and subjects to tolerate unbounded interruptions in communication patterns. In this paper, we address the key challenges of communication security and scalability in IoT environment. We hypothesize distributed IoT approach between non-identical entities to communicate through secure authentication protocol for dynamically adding new user with partially involved trusted third party (TTP) as our module 1 and attribute based encryption scheme for non-identical smart entities to communicate securely as our module 2. We discuss module 1 in this paper. The existing approaches that focus on fully trusted central authority having full rights lead to serious weakness in violating security rules, while multi-authority based systems display revocation and compulsory user participation issues. As ideal functionalities we view TTP as honest-but-curious, honestly following the protocol while on the other hand curious to decrypt the cipher-text to breach the intention of encrypting parties. This motivates us to design an approach which jointly achieves effective authentication and partial trust management with scalability in distributed IoT environment. In accordance, we propose a novel authentication scheme with partially involved TTP nomenclatured Secure Dynamic User Addition Protocol (SDUAP) based on JWT (JSON Web Token) challenge and response game using symmetric key cryptography. The security of SDUAP is proved under real or random oracle model and its robustness against several attacks is verified using scyther security verification tool. We also compare performance of SDUAP with relatively similar modeled schemes in terms of communication, computation and storage overheads. The purpose of this paper is to mitigate the complications associated with scalability and curious/suspicious third party in distributed IoT approaches. (*AN: S1389128619316949*), Database: ScienceDirect

Subjects: Distributed IoT; Secure authentication; Partially involved TTP; Dynamic user addition; Scalability

IPR2025-01313; Samsung
Ex. 1002 - Page 166

Full Text Finder USPTO Full Text Options

8. A vision-based approach for fall detection using multiple cameras and convolutional neural networks: A case study using the UP-Fall detection dataset

By Espinosa, Ricardo; Ponce, Hiram; Gutiérrez, Sebastián; Martínez-Villaseñor, Lourdes; Brieva, Jorge; Moya-Albor, Ernesto. In *Computers in Biology and Medicine*. December 2019 115 Language: English. DOI: 10.1016/j.compbiomed.2019.103520 Abstract: The automatic recognition of human falls is currently an important topic of research for the computer vision and artificial intelligence communities. In image analysis, it is common to use a vision-based approach for fall detection and classification systems due to the recent exponential increase in the use of cameras. Moreover, deep learning techniques have revolutionized vision-based approaches. These techniques are considered robust and reliable solutions for detection and classification problems, mostly using convolutional neural networks (CNNs). Recently, our research group released a public multimodal dataset for fall detection called the UP-Fall Detection dataset, and studies on modality approaches for fall detection and classification are required. Focusing only on a vision-based approach, in this paper, we present a fall detection system based on a 2D CNN inference method and multiple cameras. This approach analyzes images in fixed time windows and extracts features using an optical flow method that obtains **information** on the relative motion between two consecutive images. We tested this approach on our public dataset, and the results showed that our proposed multi-vision-based approach detects human falls and achieves an accuracy of 95.64% compared to state-of-the-art methods with a simple CNN network architecture. (*AN: S0010482519303816*), Database: ScienceDirect

Subjects: Human activity recognition; Human fall detection; Machine learning; Healthcare; Computer vision

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 167

9. ## Handbook of Green **Information** and Communication Systems

By: Woungang, Isaac; Anpalagan, Alagan; Obaidat, Mohammad S. Amsterdam : Academic Press. 2013. eBook. Description: This book gives a comprehensive guide on the fundamental concepts, applications, algorithms, protocols, new trends and challenges, and research results in the area of Green **Information** and Communications Systems. It is an invaluable resource giving knowledge on the core and specialized issues in the field, making it highly suitable for both the new and experienced researcher in this area. Key Features: Core research topics of green **information** and communication systems are covered from a network ... (*AN 485200*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Signals & Signal Processing; SCIENCE / Environmental Science; Sustainable engineering--Handbooks, manuals, etc; Telecommunication--Environmental aspects--Handbooks, manuals, etc; Telecommunication--Energy conservation--Handbooks, manuals, etc

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 168

10. ## A survey on intrusion detection and prevention in wireless ad-hoc networks

By Khan, Khalid; Mehmood, Amjad; Khan, Shafiullah; Khan, Muhammad Altaf; Iqbal, Zeeshan; Mashwani, Wali Khan. In *Journal of Systems Architecture*. May 2020 105 Language: English. DOI: 10.1016/j.sysarc.2019.101701 Abstract: Ad hoc networks have been serving us in one way or the other, for two decades, through their vast variety of applications in majority fields. Due to their features such as hostile deployments, high level of mobility, limited resources and physical insecurity, they are in front line to attackers. First line of defense (cryptographic techniques, fire walls etc.) stops these attacks. But what would happen if the attacker break through this defense system? **Second** of line of defense also called intrusion detection system (IDS), would stop and mitigate these threats before they harm the network or its resources. Various schemes have been proposed to provide quality IDS that could mitigate the latest threats in ad hoc networks. In this review paper, we gave a detailed overview of ad hoc networks in the start. We explored ad hoc networks security followed by description about IDS. Next, we elaborated the taxonomy of IDS, containing types of IDS based on numerous parameters. In the trailing section, we compared wide variety of IDS schemes based on different methodology/techniques, to show their importance and performance in the field of intrusion detection. Finally, we concluded the paper with informative future research directions in the state of the art research fields that would open up ways for researchers in that area. (*AN: S1383762119305089*), Database: ScienceDirect

Subjects: Ad hoc networks; Intrusion detection system; IDS; MANETs; WSN; Security

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 169

11. ## A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT

By Sengupta, Jayasree; Ruj, Sushmita; Das Bit, Sipra. In *Journal of Network and Computer Applications*. 1 January 2020 149 Language: English. DOI: 10.1016/j.jnca.2019.102481 Abstract: In recent years, the growing popularity of Internet of Things (IoT) is providing a promising opportunity not only for the development of various home automation systems but also for different industrial applications. By leveraging these benefits, automation is brought about in the industries giving rise to the Industrial Internet of Things (IIoT). IoT is prone to several cyberattacks and needs challenging approaches to achieve the desired security. Moreover, with the emergence of IIoT, the security vulnerabilities posed by it are even more devastating. Therefore, in order to provide a guideline to researchers, this survey primarily attempts to classify the attacks based on the objects of vulnerability. Subsequently, each of the individual attacks is mapped to one or more layers of the generalized IoT/IIoT architecture followed by a discussion on the countermeasures proposed in literature. Some relevant real-life attacks for each of these categories are also discussed. We further discuss the countermeasures proposed for the most relevant security threats in IIoT. A case study on two of the most important industrial IoT applications is also highlighted. Next, we explore the challenges brought by the centralized IoT/IIoT architecture and how blockchain can effectively be used towards addressing such challenges. In this context, we also discuss in detail one IoT specific Blockchain design known as Tangle, its merits and demerits. We further highlight the most relevant Blockchain-based solutions provided in recent times to counter the challenges posed by the traditional cloud-centered applications. The blockchain-related solutions provided in the context of two of the most relevant applications for each of IoT and IIoT is also discussed. Subsequently, we design a taxonomy of the security research areas in IoT/IIoT along with their corresponding solutions. Finally, several open research directions relevant to the focus of this survey are identified. (*AN: S1084804519303418*), Database: ScienceDirect

Subjects: IIoT; Security; Privacy; Blockchain; Smart Factory; Smart Grid; Supply Chain; E-Healthcare; VANET

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 170

12. Energy-Efficient IoT-Health Monitoring System using Approximate Computing

By Ghosh, Avrajit; Raha, Arnab; Mukherjee, Amitava. In *Internet of Things*. March 2020 9 Language: English. DOI: 10.1016/j.iot.2020.100166 Abstract: Wireless Body **Sensor** Nodes (WBSN) are frequently used for real time IoT-based health monitoring of patients outside the hospital environment. These WBSNs involve bio-**sensors** to capture signals from a patient's body and wireless transmitters to transmit the collected signals to a server located in private/public cloud in real time. These WBSNs include hardware for processing of signals before being transmitted to the cloud. Simultaneous occurrence of all these processes inside energy constrained WBSNs results in considerable amount of power consumption, thus limiting their operational lifetime. Due to the inherent error-resilience in signal processing algorithms, most of these data reaching the servers are redundant in nature and hence of not much clinical importance. Transmission and storage of these excess data result in inefficient usages of transmission bandwidth and storage capabilities. In this paper, we develop a real time encoding scheme that performs iterative thresholding and approximation of wavelet coefficients for sparse encoding of bio-signals (ECG signals), thereby reducing the energy and bandwidth consumption of the WBSN. The encoding scheme compresses bio-signals (ECG signals), while still maintaining the clinically important features. We optimize various process parameters to model a low power hardware prototype for the implementation of our algorithm on a real time microcontroller based IoT platform that operates as an end-to-end WBSN system in real time. Experimental results show a system-level energy improvement of 96% with a negligible impact on signal quality (2%). (*AN: S2542660520300093*), Database: ScienceDirect

Subjects: Wireless Body **Sensor** Nodes; IoT-based Health Monitoring; Low Power Hardware Prototype; ECG Signal; Discrete Wavelet Transform; Sparse Encoding; Approximate Computing

 Full Text Finder **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 171

13. ## Apparatus and method for processing image

By: SAMSUNG ELECTRONICS CO., LTD. US Patent: 10469,742. Filed: June 27, 2017. Issued: November 05, 2019. , Database: USPTO Patent Grants

Abstract: An image processing apparatus and method for converting a frame rate are provided. According to the present disclosure, an electronic **device** includes a memory, a first black-and-white image **sensor**, a **second** image **sensor**, and a processor. The processor is configured to set different values as a first setting value for the first black-and-white image **sensor** and a **second** setting value for the **second** image **sensor**, if an illuminance value indicating an illuminance at an arbitrary time point does not satisfy a predetermined illuminance value, to acquire a black-and-white image of an object based on the first setting value using the first black-and-white image **sensor**, to acquire at least one color image of the object based on the **second** setting value using the **second** image **sensor**, to generate a color image by synthesizing the black-and-white image with a color determined based on at least part of color **information** of the at least one color image, and to store the generated color image as video data in the memory. The black-and-white image has a high resolution relative to a resolution of the at least one color image.

AN: edspgr.10469742

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 172

14. WEARABLE ELECTRONIC **DEVICE** AND OPERATING METHOD THEREFOR

Patent Application: 16/095999. Filed: June 02, 2017. Published: May 9, 2019. , Database: USPTO Patent Applications

Abstract: According to various examples of the present invention, a wearable electronic **device** comprises: an energy harvester for generating electric energy on the basis of a movement or a change in the shape of the wearable electronic **device**; a first processor for controlling the energy harvester; a first **sensor** and a **second sensor**; and a **second** processor for controlling the first **sensor** and the **second sensor**, wherein the first processor transmits, to the **second** processor, a control signal for transitioning the **second** processor into an activated state if the electric energy generated by the energy harvester satisfies a designated first condition, and the **second** processor can be set such that first **sensor** data is acquired through the first **sensor** and **second sensor** data is selectively acquired from the **second sensor** according to whether the first **sensor** data satisfies a designated **second** condition, when the **second** processor is transitioned from an inactivated state to the activated state by responding to the control signal.

AN: edspap.20190138068

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 173

15. **Biometrics** Systems and Technologies: A survey.

By: Buciu, I.; Gacsadi, A.. *International Journal of Computers, Communications & Control* , Jun2016, Vol. 11 Issue 3, p315-330, 16p

Abstract: In a nutshell, a **biometric** security system requires a user to provide some **biometric** features which are then verified against some stored **biometric** templates. Nowadays, the traditional password based authentication method tends to be replaced by advanced **biometrics** technologies. **Biometric** based authentication is becoming increasingly appealing and common for most of the human-computer interaction **devices**. To give only one recent example, Microsoft augmented its brand new Windows 10 OS version with the capability of supporting face recognition when the user login in. This chapter does not intend to cover a comprehensive and detailed list of **biometric** techniques. The chapter rather aims at briefly discussing **biometric** related items, including principles, definitions, **biometric** modalities and technologies along with their advantages, disadvantages or limitations, and **biometric** standards, targeting unfamiliar readers. It also mentions the attributes of a **biometric** system as well as attacks on **biometrics**. Important reference sources are pointed out so that the interested reader may gain deeper in-depth knowledge by consulting them. [ABSTRACT FROM AUTHOR]; DOI: 10.15837/ijccc.2016.3.2556; (*AN 114266005*), Database: Applied Science & Technology Source

Subjects: Security systems; Biometry software; **Biometric** identification software; Human-computer interaction; Human face recognition (Computer science); Security Systems Services (except Locksmiths); Microsoft Windows (Operating system)

PDF Full Text (621KB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 174

16. ## Artificial intelligence and ambient intelligence.

By: Gams, Matjaz; Gu, Irene Yu-Hua; Härmä, Aki; Muñoz, Andrés; Tam, Vincent. *Journal of Ambient Intelligence & Smart Environments* , 2019, Vol. 11 Issue 1, p71-86, 16p Abstract: Ambient intelligence (Aml) is intrinsically and thoroughly connected with artificial intelligence (AI). Some even say that it is, in essence, AI in the environment. AI, on the other hand, owes its success to the phenomenal development of the **information** and communication technologies (ICTs), based on principles such as Moore's law. In this paper we give an overview of the progress in AI and Aml interconnected with ICT through **information**-society laws, superintelligence, and several related disciplines, such as multi-agent systems and the Semantic Web, ambient assisted living and e-healthcare, Aml for assisting medical diagnosis, ambient intelligence for e-learning and ambient intelligence for smart cities. Besides a short history and a description of the current state, the frontiers and the future of Aml and AI are also considered in the paper. [ABSTRACT FROM AUTHOR]; DOI: 10.3233/AIS-180508; (*AN 134294074*), Database: Applied Science & Technology Source

Subjects: Artificial intelligence; **Information** & communication technologies; Multiagent systems; Mobile learning; Smart cities

HTML Full Text **PDF Full Text** (550KB)

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 175

17. Multimodal **Biometric** Person Authentication: A Review.

By: Sahoo, Soyuj Kumar; Choubisa, Tarun; Prasanna, S. R. Mahadeva. *IETE Technical Review* , Jan/Feb2012, Vol. 29 Issue 1, p54-75, 22p, 7 Diagrams

Abstract: This paper provides a review of multimodal **biometric** person authentication systems. The paper begins with an introduction to **biometrics**, its advantages, disadvantages, and authentication system using them. A brief discussion on the selection criteria of different **biometrics** is also given. This is followed by a discussion on the classification of **biometric** systems, their strengths, and limitations. Detailed descriptions on the multimodal **biometric** person authentication system, different modes of operation, and integration scenarios are also provided. Considering the importance of **information** fusion in multi-**biometric** approach, a separate section is dedicated on the different levels of fusion, which include **sensor**-level, feature-level, score-level, rank-level, and abstract-level fusions, and also different rules of fusion. This paper also presents an overview of some performance parameters and error rates for **biometric** person authentication systems. A separate section is devoted to the recent trends in **biometrics** field, namely, adaptive **biometric** system, analysis of complementary and supplementary **information**, and physiological **biometrics**. The paper concludes with a discussion on the issues that are currently holding the deployment of multimodal **biometric** person authentication systems and a possible scope for future work. [ABSTRACT FROM AUTHOR]; DOI: 10.4103/0256-4602.93139; (*AN 73183333*), Database: Applied Science & Technology Source

Subjects: Biometric identification; Error rates; Biometry; Digital signatures; **Information** & communication technologies; Computer network resources; Authentication (Law)

Show all 7 Images






PDF Full Text (1.2MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 176

18. ## Security of smart manufacturing systems

By Tuptuk, Nilufer; Hailes, Stephen. In *Journal of Manufacturing Systems*. April 2018 47:93-106 Language: English. DOI: 10.1016/j.jmsy.2018.04.007 Abstract: Highlights •Current state of security in smart manufacturing.•Survey of important reported attacks against smart manufacturing systems.•The fundamental differences between the IT and smart manufacturing security; discussion of existing vulnerabilities, types of attacks and adversaries.•Survey of existing active and passive countermeasures with their limitations.•Recommendations for future research directions. (*AN: S0278612518300463*), Database: ScienceDirect

Subjects: Smart manufacturing; Sustainable manufacturing; Design for manufacturing; Internet of Things; **Information** security; Cyber-physical systems

Full Text Finder USPTO Full Text Options

19. ## Computer and **Information** Security Handbook

By: Vacca, John R. Series: The Morgan Kaufmann Series in Computer Security. Amsterdam : Morgan Kaufmann. 2009. eBook. Description: Presents **information** on how to analyze risks to your networks and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to physical and network threats. Also imparts the skills and knowledge needed to identify and counter some fundamental security risks and requirements, including Internet security threats and measures (audit trails IP sniffing/spoofing etc.) and how to implement security policies and procedures. In addition, this book covers security and network ... (*AN 248988*), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Networking / General; COMPUTERS / Security / General; Computer networks--Security measures

PDF Full Text EPUB Full Text USPTO Full Text Options

Full Download

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 177

20. Dictionary of **Information** Science and Technology

By: Khosrowpour, Mehdi. Hershey, PA : IGI Global, 2007. eBook.
Description: 'This book is the premier comprehensive reference source for the latest terms, acronyms and definitions related to all aspects of **information** science and technology. It provides the most current **information** to researchers on every level'--Provided by publisher. (*AN 173395*), Database: eBook Collection (EBSCOhost)

Subjects: LANGUAGE ARTS & DISCIPLINES / Library & **Information** Science / General; **Information** science--Dictionaries; **Information** technology--Dictionaries

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 178

21. Writer identification using machine learning approaches: a comprehensive review.

By: Rehman, Arshia; Naz, Saeeda; Razzak, Muhammad Imran. *Multimedia Tools & Applications* , Apr2019, Vol. 78 Issue 8, p10889-10931, 43p

Abstract: Handwriting is one of the most common types of questioned writing encountered and frequently attracts the attention in litigation. Contrary to the physiological characteristics, handwriting is a behavioral characteristic thus no two individuals with mature handwriting are exactly alike or an individual cannot produce the others writing exactly. Writing behavior and individualities are examined for similarities for both specimen and questioned document, thus, it is very efficient and effective strategy for **biometrics**. In this paper, we present a comprehensive review of writer identification methods and intend to provide taxonomy of dataset, feature extraction methods, as well as classification (conventional and deep learning based) for writer identification. For ease of reader, we grouped the discussion into English, Arabic, Western and Other languages from script prospective, whereas, from algorithm and methods perspective, we grouped the discussion with respect to implementation steps sequence. In the end, we highlighted the challenges and open research issues in the field of writer identification. Finally, we also suggest future direction. [ABSTRACT FROM AUTHOR]; DOI: 10.1007/s11042-018-6577-1; (*AN 136338569*), Database: Applied Science & Technology Source

Subjects: Machine learning; **Biometric** identification; Algorithms; Writing; English language

HTML Full Text **PDF Full Text** (1.7MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 179

22. ## Advances in Enterprise **Information** Technology Security

By: Herrmann, Francine; Khadraoui, Djamel. Hershey [Pa.] : IGI Global. 2007. eBook. Description: 'This book provides a broad working knowledge of all the major security issues affecting today's enterprise IT activities. Multiple techniques, strategies, and applications are thoroughly examined, presenting the tools to address opportunities in the field.It is an all-in-one reference for IT managers, network administrators, researchers, and students'--Provided by publisher. (*AN 185367*), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Security / General; COMPUTERS / Security / Network Security; COMPUTERS / Internet / Online Safety & Privacy; Computer security; Data protection; Business enterprises--Computer networks--Security measures; **Information** technology--Security measures

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 180

23. ## Optimization of signal quality over comfortability of textile electrodes for ECG monitoring in fog computing based medical applications

By Wu, Wanqing; Pirbhulal, Sandeep; Sangaiah, Arun Kumar; Mukhopadhyay, Subhas Chandra; Li, Guanglin. In *Future Generation Computer Systems*. September 2018 86:515-526 Language: English. DOI: 10.1016/j.future.2018.04.024 Abstract: Fog computing is the backbone of modern healthcare systems, it not only cut-downs the associated treatment and medicine costs but also decreases the logistics requirements. Recently, both stationary and wearable systems are utilized for long-term monitoring of Electrocardiogram (ECG) signals in fog computing based medical applications. However, the comfort of monitored patients is not at a satisfactory level and therefore, a well-designed textile electrode with excellent signal quality and comfortability (SQC) plays a significant role in collecting ECG signals. In this study, in order to provide SQC optimization, a textile electrode with knitted structure and conductive material comprising cotton /nylon fiber coated silver is investigated. This textile composite is integrated to a wearable carrier (T-Shirt) with a miniaturized wireless sensing platform to collect ECG signals from the human. As a design strategy to acquire dimensional stability, the fabric was knitted with two layers that form the same technical face on both fabric surfaces. The conducted experiment elaborate that to find out a balance between the quality of signal and wearable comfort level by finely adjusting the composition of fiber type, yarn density, fabric pattern, fabric density, and thickness. From our experimental results, it is observed that textile electrodes having cotton (30) /nylon fiber coated silver (70) provides less air resistance (0.17 KPa•s/m), optimized tactile comfort (9/10), reasonable signal to noise ratio (SNR) value of 30.78dB, and better thermal conductivity (0.018W/m•K) than compared electrodes. Thus, it can be concluded that developed textile electrode can be useful for future research to offer the balance for SQC ratio for ECG measurement in fog computing based healthcare systems. (*AN: S0167739X18300621*), Database: ScienceDirect

Subjects: Fog computing; Textile electrode; Wearable sensing; ECG measurement; Signal quality and comfortability (SQC); Medical applications

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 181

24. ## Genomic and Personalized Medicine : V1-2

By: Willard, Huntington F.; Ginsburg, Geoffrey S. Edition: **2nd** ed. London : Academic Press. 2013. eBook. Description: Genomic and Personalized Medicine, **Second** Edition — winner of a 2013 Highly Commended BMA Medical Book Award for Medicine — is a major discussion of the structure, history, and applications of the field, as it emerges from the campus and lab into clinical action. As with the first edition, leading experts review the development of the new science, the current opportunities for genome-based analysis in healthcare, and the potential of genomic medicine in future healthcare. The inclusion of the latest ... (*AN 485475*), Database: eBook Collection (EBSCOhost)

Subjects: SCIENCE / Life Sciences / Genetics & Genomics; MEDICAL / Pharmacology; Proteomics; Genomics; Medical genetics

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 182

25. ## Gait-based Person Re-identification.

By: Nambiar, Athira; Bernardino, Alexandre; Nascimento, Jacinto C. *ACM Computing Surveys.* Mar2019, Vol. 52 Issue 2, p1-34. 34p. Abstract: The way people walk is a strong correlate of their identity. Several studies have shown that both humans and machines can recognize individuals just by their gait, given that proper measurements of the observed motion patterns are available. For surveillance applications, gait is also attractive, because it does not require active collaboration from users and is hard to fake. However, the **acquisition** of good-quality measures of a person's motion patterns in unconstrained environments, (e.g., in person re-identification applications) has proved very challenging in practice. Existing technology (video cameras) suffer from changes in viewpoint, daylight, clothing, accessories, and other variations in the person's appearance. Novel three-dimensional **sensors** are bringing new promises to the field, but still many research issues are open. This article presents a survey of the work done in gait analysis for re-identification in the past decade, looking at the main approaches, datasets, and evaluation methodologies. We identify several relevant dimensions of the problem and provide a taxonomic analysis of the current state of the art. Finally, we discuss the levels of performance achievable with the current technology and give a perspective of the most challenging and promising directions of research for the future. [ABSTRACT FROM AUTHOR] DOI: 10.1145/3243043. (*AN: 137310282*), Database: Computers & Applied Sciences Complete

Subjects: Camcorders; Evaluation methodology; Video surveillance; Computer vision; Daylight

HTML Full Text **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 183

26. ## A Novel Approach to Improve the **Biometric** Security using Liveness Detection.

By: Devi, Mamta; GurmeetKaur; Kant, Chander. *International Journal of Advanced Research in Computer Science* , May/Jun2017, Vol. 8 Issue 5, p1415-1420, 6p Abstract: A **biometric** system automatically authenticate individuals based on their physical and behavioral features like face, iris retina, ear, voice, signature keystroke dynamics etc. A **biometric** system which uses only a single trait for recognition is known as unimodal system. In Unimodal **biometric** system contains some limitation such as high error rate, non-universality, noise in sensed data, and spoof attacks etc. These problems could be overcome by multimodal approaches which combine more than one trait of user for authentication. The main purpose of using liveness detection with multimodal **biometric** is that we can use this approach in highly secured application such as defense, labs, pharmacies and bank applications. So in this paper liveness detection technique is used with multimodal approach. Initially, it checks the liveness of the person. If the person is found alive, only then the further calculations are performed. The main purpose of the purposed scheme is to reduce the FAR (false acceptance rate), FRR (false reject rate) and provide protection against spoof attacks. Proposed scheme was implemented using MUBI (Multimodal **Biometrics** Integration) software. [ABSTRACT FROM AUTHOR]; (*AN 124636607*), Database: Applied Science & Technology Source

Subjects: Biometric identification; Computer access control; Error rates; Computer security; Pattern recognition systems

PDF Full Text (518KB) **USPTO Full Text Options**

27. ## Wireless Technologies : Concepts, Methodologies, Tools and Applications

By: **Information** Resources Management Association. Hershey, PA : IGI Global. 2012. eBook. (*AN 396408*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Mobile & Wireless Communications; TECHNOLOGY & ENGINEERING / Radio; Wireless communication systems; Telecommunication

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 184

28. ## Computer Engineering : Concepts, Methodologies, Tools and Applications

By: **Information** Resources Management Association. Hershey, Pa : IGI Global. 2012. eBook. Description: Features perspectives on the fundamental aspects, tools and technologies, methods and design, applications, managerial impact, social/behavioral perspectives, critical issues, and emerging trends in the field of computer engineering. (*AN 431988*), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Computer Engineering; COMPUTERS / Machine Theory; COMPUTERS / Hardware / General; Computer engineering

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 185

29. A 3-D hand gesture signature based **biometric** authentication system for smartphones.

By: Sun, Ziwen; Wang, Yao; Qu, Gang; Zhou, Zhiping. *Security & Communication Networks* , 7/25/2016, Vol. 9 Issue 11, p1359-1373, 15p
Abstract: The authentication mechanism being equipped in most of the smartphones, by detecting a 4-digit password or a simple pattern, are easy to be hacked and impersonated. In this paper, a 3-D hand gesture signature (HGS) based **biometric** authentication system is designed and implemented by taking advantage of the on-phone accelerometer to capture the 3-D acceleration **information** when user makes a gesture to gain access to the phone. The captured data will be processed through a sequence of signal processing such as data smooth, gesture spotting, sequence alignment, and interpolation, and then a match rule will be used to compare the processed data and the genuine user's registered pattern to determine whether granting the access to the phone to the user. And an automatic template updating strategy based on cluster analysis is proposed to improve the stability of the system. The 3-D HGS authentication system has been implemented on real smartphones, and the results tested for a total of 76 520 times by 19 users show very low false acceptance (0.27%) and false rejection rates (4.65%). Furthermore, comparison tests have been carried out among the 3-D HGS and two similar authentication systems by exporting the real gesture samples from the phones to a desktop PC, the simulation results reveal the 3-D HGS system has the best authentication accuracy. Copyright © 2016 John Wiley & Sons, Ltd. [ABSTRACT FROM AUTHOR]; DOI: 10.1002/sec.1422; (*AN 116123722*), Database: Applied Science & Technology Source

Subjects: Computer access control; Passwords (Computers); Computer hacking; **Biometric** identification; Accelerometers; Signal processing; Other Measuring and Controlling **Device** Manufacturing

PDF Full Text (992KB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 186

30. 3D **Biometrics** : Systems and Applications

By: Zhang, David; Lu, Guangming. New York, NY : Springer. 2013. eBook.
Description: Automatic personal authentication using **biometric information** is becoming more essential in applications of public security, access control, forensics, banking, etc. Many kinds of **biometric** authentication techniques have been developed based on different **biometric** characteristics. However, most of the physical **biometric** recognition techniques are based on two dimensional (2D) images, despite the fact that human characteristics are three dimensional (3D) surfaces. Recently, 3D techniques have been ... (*AN 590691*), Database: eBook Index

Subjects: COMPUTERS / Artificial Intelligence / Computer Vision & Pattern Recognition; TECHNOLOGY & ENGINEERING / Electronics / General; **Biometric** identification--Technological innovations; Three-dimensional imaging

Full Text Finder USPTO Full Text Options

EBSCO Connect | Privacy Policy | A/B Testing | Terms of Use | Copyright | Cookie Policy | Contact Us

powered by EBSCO*host*

© 2020 EBSCO Industries, Inc. All rights reserved.

IPR2025-01313; Samsung
Ex. 1002 - Page 187

Google acquiring the dynamic biometric information from the dynamic biometric

Sign in

All News Images Videos More Settings Tools

About 9,460 results (0.51 seconds)

www.google.com/patents/US7020308

Personal authentication system using biometrics information



In this case, when the biometrics information inputting section is of a type ... using biometrics information according to the first embodiment of the invention; ... or to acquire and use time series data such as voice, keystroke or dynamic signature. ... Precision Technology, Inc Real time fingerprint sensor and verification system.
Grant - Filed Aug 15, 2000 - Issued Mar 28, 2006 - Takashi Shinzaki - Fujitsu Limited
Overview · Related · Discuss

www.google.com/patents/US20160217310

System and method for partial fingerprint enrollment and ...

The mobile device includes a fingerprint registration unit configured to receive at least one first image of a fingerprint input in a first orientation, receive at least ...
App. - Filed Jan 27, 2016 - Published Jul 28, 2016 - Jidnya Samir SHAH - Samsung Electronics Co., Ltd.
Overview · Related · Discuss

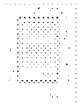
www.google.com/patents/US9471765

Fingerprint authentication with template updating

When it is determined that a first match between a present fingerprint image representation and the stored template fulfills a first template ...
Grant - Filed Mar 10, 2016 - Issued Oct 18, 2016 - Eric Setterberg - Fingerprint Cards Ab
Overview · Related · Discuss

www.google.com/patents/US20110267298

Fingerprint sensor and integratable electronic display



A fingerprint sensor which includes a conductive layer which is ... based on information acquired by an integratable sensor such as those ...
App. - Filed May 3, 2011 - Published Nov 3, 2011 - Richard Alexander Erhart - Validity Sensors, Inc.
Overview · Related · Discuss

www.google.com/patents/US9590984

Smartphone fingerprint pass-through system

After validating a biometric input that corresponds with a code that locks or unlocks a remote lock, the code may be sent to a remote electronic device in a ...
Grant - Filed Feb 13, 2015 - Issued Mar 7, 2017 - John Cronin - Grandios Technologies, Llc
Overview · Related · Discuss

www.google.com/patents/US9373047

Biometric authentication device, biometric authentication ...

A biometric authentication device includes a photographing unit configured to photograph a biological body and acquire biological body information; .
Grant - Filed Mar 9, 2012 - Issued Jun 21, 2016 - Takahiro Aoki - Fujitsu Limited
Overview · Related · Discuss

www.google.com/patents/US9329771

Embedded authentication systems in an electronic device

An electronic device with a display and a fingerprint sensor may authenticate a ... element indicating a first direction of finger movement that enables unlocking of ... the input meets unlock criteria based at least in part on fingerprint information of ... Upon authenticating the user, the electronic device may provide the user with ...

Grant - Filed Jun 20, 2014 - Issued May 3, 2016 - Anthony Fadell - Apple Inc
Overview · Related · Discuss

www.google.com/patents/US9721142

Multi-resolution fingerprint sensor



The multi-resolution fingerprint sensors each include a portion of the imaging area or ... stack, which expects a uniform resolution for the entire image acquired. ... of the first image and the second image to determine biometric information of ... as random access memories (RAM), dynamic random access memories (DRAM), ...
Grant - Filed Jun 26, 2015 - Issued Aug 1, 2017 - Anthony P. Russo - Synaptics Incorporated
Overview · Related · Discuss

www.google.com/patents/US8797140

Biometric authentication method and biometric authentication ...



The first group is a group of registrants whose biometric information previously acquired for the high-speed authentication method is high in quality, i.e., a group ...
Grant - Filed Mar 3, 2008 - Issued Aug 5, 2014 - Takashi Shinzaki - Fujitsu Limited
Overview · Related · Discuss

www.google.com/patents/US20140359757

User authentication biometrics in mobile devices



The control system may be capable of acquiring biometric information from the digit when the digit is positioned in an area corresponding to the biometric sensor ...
App. - Filed Feb 11, 2014 - Published Dec 4, 2014 - Muhammed Ibrahim Sezan - Qualcomm Incorporated
Overview · Related · Discuss

Help Send feedback Privacy Terms

A survey on touch **dynamics** authentication in mobile **devices**

PS Teh, N Zhang, ABJ Teoh, K Chen - Computers & Security, 2016 - Elsevier
... with other **biometrics** features, such as face and voice **biometrics**, the feature **acquisition of** touch **dynamics** ... This is because the **acquiring** and processing of touch **dynamics** patterns can be carried ... suited to this mode, as touch **dynamics** data can be **acquired** transparently over a ...
☆ 99 Cited by 91 Related articles All 6 versions

Automatic gain amplifier for **biometric sensor device**

HLJ Yeh, EW Cheng, AP Russo - US Patent 6,518,560, 2003 - Google Patents
... printed or written characters or for recognising patterns, eg fingerprints; G06K9/00006—**Acquiring** or recognising ... **Dynamic** finger detection mechanism for a **fingerprint sensor** ... 1999-11-16, Lucent Technologies, Apparatus for correcting fixed column noise in images **acquired** by a ...
☆ 99 Cited by 43 Related articles All 2 versions »

Combined **fingerprint acquisition** and control **device**

AW Senior - US Patent 6,400,836, 2002 - Google Patents
... would be scanned at 410 and then immediately stored in a **dynamically** accessible memory ... in computer 100, could enable or disable transmission of **acquired fingerprint** image data ... for combined **fingerprint acquisition** for user authentication and for **acquiring** control parameters ...
☆ 99 Cited by 233 Related articles All 4 versions »

Information processing **device**, application software start-up system, and application software start-up method

M Hirabayashi, Y Hashimoto ... - US Patent App. 16 ..., 2019 - Google Patents
... **Info** ... US 201916535574 A US201916535574 A US 201916535574A US 2019362061 A1 US2019362061 A1 US 2019362061A1 Authority US United States Prior art keywords **biometric information information** user processing **device dynamic biometric** Prior art date 2019 ...
☆ 99 All 2 versions »

Authentication gets personal with **biometrics**

J Ortega-Garcia, J Bigun, D Reynolds ... - IEEE signal ..., 2004 - ieeexplore.ieee.org
... in which signal processing methodology is applied to the **dynamically acquired** time sequences ... ii) feature-based approaches, in which statistical parameters are derived from the **acquired information** ... aspect ratio, center of mass, or horizontal span ratio), global **dynamic** (ie, total ...
☆ 99 Cited by 216 Related articles All 15 versions

Information processing **device**, application software start-up system, and application software start-up method

M Hirabayashi, Y Hashimoto, K Yoshizawa - US Patent 10,423,769, 2019 - Google Patents
... **Info** ... B2 US10423769 B2 US 10423769B2 US 201415315735 A US201415315735 A US 201415315735A US 10423769 B2 US10423769 B2 US 10423769B2 Authority US United States Prior art keywords **biometric information device** user state **dynamic biometric** Prior art ...
☆ 99 Related articles All 4 versions »

To a combined **fingerprint acquisition** and control **device**

RM Bolle, NK Ratha, A Senior - US Patent 6,941,001, 2005 - Google Patents
... **fingerprint** image **acquisition** scanner incorporated into a pointing **device** for **acquiring** at least ... computing means for computing image correlations between the **acquired fingerprint** images; an image processor ... verifying an **acquisition of** data in real time from a live user based on ...
☆ 99 Cited by 149 Related articles All 2 versions »

Secure network and networked **devices** using **biometrics**

A Russo, P McCoy, T Roske - US Patent App. 10/194,949, 2003 - Google Patents
Secure network and networked **devices** using **biometrics**. Download PDF **Info** ... US 19494902 A US19494902 A US 19494902A US 2003115490 A1 US2003115490 A1 US 2003115490A1 Authority US United States Prior art keywords **biometric biometric** data **device** data secure ...
☆ 99 Cited by 155 Related articles All 2 versions »

Context aware ubiquitous **biometrics** in edge of military things

A Castiglione, KKR Choo, M Nappi ... - IEEE Cloud ..., 2017 - ieeexplore.ieee.org

... combat suit, instrumented helmets, weapon systems, etc.) are capable of **acquiring** a variety ... puting **devices**, such as Android and iOS **devices**, facilitate the **acquisition of** context dependent ... J. Hu and AC Weaver, "A **Dynamic**, Context- Aware Security Infrastructure for Distributed ...

☆ 99 Cited by 28 Related articles All 3 versions

Dynamic Biometric Signature-an Effective Alternative for Electronic Authentication

V Smejkal, J Kodl - Advances in Technology Innovation, 2018 - researchgate.net

... **When acquiring** signature data, **biometric** data [mostly x(t ... In this way, we **acquire** authentication data for the signer with subsequent securing against forgery ... experiments have shown that a handwritten signature **acquired** through long practice and the compaction of the **dynamic** ...

☆ 99 Cited by 1 Related articles All 3 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 191

STIC
Scientific and Technical Information Center

1. Patent Application Titled '**Information** Processing **Device**, Application Software Start-Up System, And Application Software Start-Up Method' Published Online (USPTO 20190362061)

In: **Information** Technology Newsweekly, Dec 17, 2019, 2279; NewsRX LLC
Language: English. Abstract: 2019 DEC 17 (VerticalNews) -- By a News Reporter-Staff News Editor at **Information** Technology Newsweekly -- According to news reporting originating from Washington, D.C., by VerticalNews journalists, a patent application [...] (*AN: edsgcl.608720217*), Database: Gale General OneFile

Subjects: Japan; Software quality; Software -- Methods; Software -- Intellectual property; Control equipment -- Methods; Control equipment -- Intellectual property

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 192

2. Electronic **device** for providing VR image based on polyhedron and image providing method thereof

By: SAMSUNG ELECTRONICS CO., LTD. US Patent: 10650,596. Filed: January 12, 2018. Issued: May 12, 2020. , Database: USPTO Patent Grants

Abstract: An electronic **device** is provided. The electronic **device** includes a **communication** module comprising **communication** circuitry, a memory configured to store **first information** indicating **first** image data generated using a **first** rendering scheme based on a **first** polyhedron configured with a **first** number of surfaces and **second information** indicating **second** image data generated using a **second** rendering scheme based on a **second** polyhedron configured with a **second** number of surfaces, and a processor. The processor is configured to verify state **information** of the electronic **device**, to select one of the **first information** and the **second information** based on the at least state **information**, to transmit a request corresponding to the selected **information** to an external electronic **device via** the **communication** module, to receive image data corresponding to the selected **information between** the **first** image data and the **second** image data from the external electronic **device** in response to the request, and to control playback of the received image data.

AN: edspgr.10650596

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 193

3. ## Context-aware access control and anonymous authentication in WBAN

By Arfaoui, Amel; Boudia, Omar Rafik Merad; Kribeche, Ali; Senouci, Sidi-Mohammed; Hamdi, Mohamed. In *Computers & Security*. January 2020 88 Language: English. DOI: 10.1016/j.cose.2019.03.017 Abstract: The emergence of the Internet of Things (IoT) as the next generation megatrend has paved the way for pervasive, ubiquitous and proficient healthcare monitoring systems. In the diverse kinds of networks, Wireless Body Area Network (WBAN) has been perceived as one of the most promising wireless sensor technologies for improving healthcare services thanks to its potential for continuous and real-time monitoring of health conditions. However, the open nature of wireless **communication** introduces wide security and privacy concerns as personal health **information** could be exposed to unauthorized parties or even malicious adversaries. Furthermore, in such a **dynamic** and heterogeneous environment where the context conditions continuously and frequently change, adaptive and context-aware solutions become mandatory to satisfy burgeoning security and privacy requirements. Therefore, it is indispensable to adaptively secure the extra-body **communication between** the smart portable **device** held by the WBAN client and the healthcare providers while considering the **dynamic** context changes. In this paper, we propose a context-aware access control and anonymous authentication approach based on a secure and efficient Hybrid Certificateless Signcryption (H-CLSC) scheme. Particularly, it incorporates the merits of Ciphertext-Policy Attribute-Based Signcryption (CP-ABSC) and Identity-Based Broadcast Signcryption (IBBSC) in order to meet the security requirements and provide adaptive contextual privacy. From a security perspective, the proposed mechanism achieves confidentiality, integrity, anonymity, context-aware privacy, key escrow resistance, public verifiability, and ciphertext authenticity. Performance analysis proves the efficiency and the effectiveness of the H-CLSC scheme compared to benchmark schemes in terms of functional security, storage, **communication**, and computational cost. (*AN: S0167404818304802*), Database: ScienceDirect

Subjects: IoT; WBAN; Certificateless signcryption; Anonymous authentication; Context-aware authorization

Full Text Finder **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 194

4. ## Cybersecurity challenges in vehicular **communications**

By El-Rewini, Zeinab; Sadatsharan, Karthikeyan; Selvaraj, Daisy Flora; Plathottam, Siby Jose; Ranganathan, Prakash. In *Vehicular Communications*. June 2020 23 Language: English. DOI: 10.1016/j.vehcom.2019.100214 Abstract: As modern vehicles are capable to connect to an external infrastructure and Vehicle-to-Everything (V2X) **communication** technologies mature, the necessity to secure **communications** becomes apparent. There is a very real risk that today's vehicles are subjected to cyber-attacks that target vehicular **communications**. This paper proposes a three-layer framework (sensing, **communication** and control) through which automotive security threats can be better understood. The sensing layer is made up of vehicle **dynamics** and environmental sensors, which are vulnerable to eavesdropping, jamming, and spoofing attacks. The **communication** layer is comprised of both in-vehicle and V2X **communications** and is susceptible to eavesdropping, spoofing, man-in-the-middle, and sybil attacks. At the top of the hierarchy is the control layer, which enables autonomous vehicular functionality, including the automation of a vehicle's speed, braking, and steering. Attacks targeting the sensing and **communication** layers can propagate upward and affect the functionality and can compromise the security of the control layer. This paper provides the state-of-the-art review on attacks and threats relevant to the **communication** layer and presents countermeasures. (*AN: S221420961930261X*), Database: ScienceDirect

Subjects: Cyber-physical systems; Security; Vehicle safety; Cyber-attacks; Vehicle-to-vehicle

Full Text Finder **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 195

5. ## Design of secure authentication protocol for **dynamic** user addition in distributed Internet-of-Things

By Trivedi, Hiral S.; Patel, Sankita J.. In *Computer Networks*. 4 September 2020 178 Language: English. DOI: 10.1016/j.comnet.2020.107335 Abstract: Rapid rise in adoption of smart **devices** in distributed Internet-of-things (IoT) has resulted in an exponential increase in volume of generated data. However, due to resource-constrained sensor nodes and vulnerable **communication** channels, **information** protection has become a key concern and prominent factor for improvement in IoT environment. Batch processing systems have several shortcomings as compared to distributed systems. Distributed systems enable **dynamic** changes in the potential number of sensors, actuators, RFID's, resources, users and subjects to tolerate unbounded interruptions in **communication** patterns. In this paper, we address the key challenges of **communication** security and scalability in IoT environment. We hypothesize distributed IoT approach **between** non-identical entities to communicate through secure authentication protocol for dynamically adding new user with partially involved trusted third party (TTP) as our module 1 and attribute based encryption scheme for non-identical smart entities to communicate securely as our module 2. We discuss module 1 in this paper. The existing approaches that focus on fully trusted central authority having full rights lead to serious weakness in violating security rules, while multi-authority based systems display revocation and compulsory user participation issues. As ideal functionalities we view TTP as honest-but-curious, honestly following the protocol while on the other hand curious to decrypt the cipher-text to breach the intention of encrypting parties. This motivates us to design an approach which jointly achieves effective authentication and partial trust management with scalability in distributed IoT environment. In accordance, we propose a novel authentication scheme with partially involved TTP nomenclatured Secure **Dynamic** User Addition Protocol (SDUAP) based on JWT (JSON Web Token) challenge and response game using symmetric key cryptography. The security of SDUAP is proved under real or random oracle model and its robustness against several attacks is verified using scyther security verification tool. We also compare performance of SDUAP with relatively similar modeled schemes in terms of **communication**, computation and storage overheads. The purpose of this paper is to mitigate the complications associated with scalability and curious/suspicious third party in distributed IoT approaches. (*AN: S1389128619316949*), Database: ScienceDirect

Subjects: Distributed IoT; Secure authentication; Partially involved TTP; **Dynamic** user addition; Scalability

IPR2025-01313; Samsung
Ex. 1002 - Page 196

Full Text Finder USPTO Full Text Options

6. LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment

By Wazid, Mohammad; Das, Ashok Kumar; Bhat K, Vivekananda; Vasilakos, Athanasios V.. In *Journal of Network and Computer Applications*. 15 January 2020 150 Language: English. DOI: 10.1016/j.jnca.2019.102496 Abstract: Internet of Things (IoT) becomes a new era of the internet, which consists of several connected physical smart objects (i.e., sensing **devices**) through the Internet. IoT has different types of applications, such as smart home, wearable **devices**, smart connected vehicles, industries, and smart cities. Therefore, IoT based applications become the essential parts of our day-to-day life. In a cloud-based IoT environment, cloud platform is used to store the data accessed from the IoT sensors. Such an environment is greatly scalable and it supports real-time event processing which is very important in several scenarios (i.e., IoT sensors based surveillance and monitoring). Since some applications in cloud-based IoT are very critical, the **information** collected and sent by IoT sensors must not be leaked during the **communication**. To accord with this, we design a new lightweight authentication mechanism in cloud-based IoT environment, called LAM-CIoT. By using LAM-CIoT, an authenticated user can access the data of IoT sensors remotely. LAM-CIoT applies efficient "one-way cryptographic hash functions" along with "bitwise XOR operations". In addition, fuzzy extractor mechanism is also employed at the user's end for local **biometric** verification. LAM-CIoT is methodically analyzed for its security part through the formal security using the broadly-accepted "Real-Or-Random (ROR)" model, formal security verification using the widely-used "Automated Validation of Internet Security Protocols and Applications (AVISPA)" tool as well as the informal security analysis. The performance analysis shows that LAM-CIoT offers better security, and low **communication** and computation overheads as compared to the closely related authentication schemes. Finally, LAM-CIoT is evaluated using the NS2 network simulator for the measurement of network performance parameters that envisions the impact of LAM-CIoT on the network performance of LAM-CIoT and other schemes. (*AN: S108480451930356X*), Database: ScienceDirect

Subjects: Internet of Things (IoT); Cloud computing; Authentication; Key agreement; Security; AVISPA simulation

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 197

7. ## Securing internet of medical things systems: Limitations, issues and recommendations

By Yaacoub, Jean-Paul A.; Noura, Mohamad; Noura, Hassan N.; Salman, Ola; Yaacoub, Elias; Couturier, Raphaël; Chehab, Ali. In *Future Generation Computer Systems*. April 2020 105:581-606 Language: English. DOI: 10.1016/j.future.2019.12.028 Abstract: Traditional health-care systems suffer from new challenges associated with the constant increase in the number of patients. In order to address this issue, and to increase the accuracy, reliability, efficiency, and effectiveness of the health-care domain, the Internet of Medical Things (IoMT) was proposed. IoMT can be considered as an enhancement and investment to respond more effectively and efficiently to patients' needs. However, IoMT suffers from different issues and challenges such as the lack of security and privacy measures, in addition to the necessary training and awareness. In this paper, we highlight the importance of implementing the right security measures and the required training skills, in order to enhance the immunity of IoMT against cyber-attacks. Moreover, we review the main IoMT security and privacy issues, and the existing security solutions. These solutions are classified as cryptographic or non-cryptographic. Then, the different solutions are analyzed and compared in terms of computational complexity and required resources. It is important to note that the security measures for IoMT exhibit a trade-off **between** the security level and the system performance, especially in the rise of digital healthcare v4.0 era. Next, we discuss the appropriate security solutions such as lightweight cryptographic algorithms, and protocols that attempt to reduce the overhead in terms of computations and resources. This leads to the conclusion that there is a need to design an efficient intrusion detection/prevention system that cooperates with **dynamic** shadow honeypots. Finally, we propose a security solution, which is divided into five different layers to detect and prevent attacks, in addition to reducing/correcting the damage of these known attacks and preserving the patients' privacy. However, it should be noted that zero-day attacks and exploits are still the main challenging issue that surrounds IoMT. (*AN: S0167739X19305680*), Database: ScienceDirect

Subjects: Healthcare; IoMT; Medical cyber physical systems; Medical **devices**

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 198

8. ## Bio-AKA: An efficient fingerprint based two factor user authentication and key agreement scheme

By Bian, Weixin; Gope, Prosanta; Cheng, Yongqiang; Li, Qingde. In *Future Generation Computer Systems*. August 2020 109:45-55 Language: English. DOI: 10.1016/j.future.2020.03.034 Abstract: The fingerprint has long been used as one of the most important biological features in the field of **biometrics**. It is person-specific and remain identical though out one's lifetime. Physically uncloneable functions (PUFs) have been used in authentication protocols due to the unique physical feature of it. In this paper, we take full advantage of the inherent security features of user's fingerprint **biometrics** and PUFs to design a new user authentication and key agreement scheme, namely Bio-AKA, which meets the desired security characteristics. To protect the privacy and strengthen the security of **biometric** data and to improve the robustness of the proposed scheme, the fuzzy extractor is employed. The scheme proposed in the paper can protect user's anonymity without the use of password and allow mutual authentication with key agreement. The experimental results show superior robustness and the simplicity of our proposed scheme has been validated **via** our performance and security analysis. The scheme can be an ideal candidate for real life applications that requires remote user authentication. (*AN: S0167739X19332467*), Database: ScienceDirect

Subjects: Mutual authentication; Key agreement; Physical unclonable functions; Fuzzy extractor; **Biometric** security and privacy

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 199

9. ## Handbook of Green **Information** and **Communication** Systems

By: Woungang, Isaac; Anpalagan, Alagan; Obaidat, Mohammad S. Amsterdam : Academic Press. 2013. eBook. Description: This book gives a comprehensive guide on the fundamental concepts, applications, algorithms, protocols, new trends and challenges, and research results in the area of Green **Information** and **Communications** Systems. It is an invaluable resource giving knowledge on the core and specialized issues in the field, making it highly suitable for both the new and experienced researcher in this area. Key Features: Core research topics of green **information** and **communication** systems are covered from a network ... (*AN 485200*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Signals & Signal Processing; SCIENCE / Environmental Science; Sustainable engineering--Handbooks, manuals, etc; Telecommunication--Environmental aspects--Handbooks, manuals, etc; Telecommunication--Energy conservation--Handbooks, manuals, etc

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 200

10. ## Blockchain envisioned UAV networks: Challenges, solutions, and comparisons

By Mehta, Parimal; Gupta, Rajesh; Tanwar, Sudeep. In *Computer Communications.* 1 February 2020 151:518-538 Language: English. DOI: 10.1016/j.comcom.2020.01.023 Abstract: Unmanned Aerial Vehicles (UAV) or drones is a technology with a huge potential for proving different efficient solutions in the smart city. It has been mostly adopted by military, aviation, civil, and commercial sectors for audio and video surveillance. The **communication** and security challenges of UAV is well mentioned by researchers and organizations (defense) around the world, although many of the challenges remain unresolved (especially for sensitive and consumer-related applications). Moreover, the conventional network systems may not be very efficient in dealing with the **dynamic** requirements of UAVs. As the UAVs are generally deployed in tough environments and terrains, therefore it is quite essential to provide a strong and secure network. Motivated from these facts, this paper presents an extensive survey on security issues in 5G-enabled UAV networks as per the literature published till the fourth quarter of 2019. It also presents the taxonomy of existing security issues in 5G-enabled UAV networks. Based on the findings from the survey, we present a Blockchain (BC)-based security solution and a summary of research challenges in the integration of BC with 5G-enabled UAV. Then, we present a case study of implementing BC with UAVs to secure industrial applications. (*AN: S0140366419318675*), Database: ScienceDirect

Subjects: Blockchain; Industry 4.0; Latency; Reliability; 5G; IoT; Unmanned aerial vehicles

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 201

11. ## Intelligence and security in big 5G-oriented IoNT: An overview

By Al-Turjman, Fadi. In *Future Generation Computer Systems*. January 2020 102.357-368 Language: English. DOI: 10.1016/j.future.2019.08.009 Abstract. Internet of Nano-Things (IoNT) overcomes critical difficulties and additionally open doors for wearable sensor based huge **information** examination. Conventional computing and/or **communication** systems do not offer enough flexibility and adaptability to deal with the gigantic amount of assorted **information** nowadays. This creates the need for legitimate components that can efficiently investigate and communicate the huge data while maintaining security and quality of service. In addition, while developing the ultra-wide Heterogeneous Networks (HetNets) associated with the ongoing Big Data project and 5G-based IoNT, it is required to resolve the emerging difficulties as well. Accordingly, these difficulties and other relevant design issues have been comprehensively reported in this survey. It mainly focuses on security issues and associated intelligence to be considered while managing these issues. (*AN: S0167739X19301074*), Database: ScienceDirect

Subjects: IoNT; Security; Big data; Design factors

Full Text Finder **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 202

12. WIRELESS ROUTER, INTERNET OF THINGS **DEVICE** AND SYSTEM FOR SUPPORTING CONNECTION TO WIRELESS ROUTER OF INTERNET OF THINGS **DEVICE**

Patent Application: 15/876679. Filed: January 22, 2018. Published: September 13, 2018. , Database: USPTO Patent Applications

Abstract: An electronic **device** for supporting a connection to a wireless router of an internet of things (IoT) **device** is provided. The electronic **device** includes a transceiver, a **communication interface**, a processor, and a memory. The processor connects a **first** external **device** by using a **first** service set identifier (SSID), receives **first information** about the **first** external **device** from the **first** external **device**, transmits at least part of the **first information** and **second information** about the electronic **device** to a **second** external **device**, forwards connection **information** from the **second** external **device**, which includes a **second** SSID for wireless connection **between** the **first** external **device** and the electronic **device**, or receives a transmission request of the connection **information** from the **second** external **device** and transmits the connection **information** to the **first** external **device**, and wirelessly connects to the **first** external **device** by using the connection **information**.

AN: edspap.20180263071

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 203

13. ## Optimized in-network authentication against pollution attacks in software-defined-named data networking

By Boussaha, Ryma; Challal, Yacine; Bouabdallah, Abdelmadjid; Bessedik, Malika. In *Journal of Information Security and Applications*. February 2020 50 Language: English. DOI: 10.1016/j.jisa.2019.102409 Abstract: The exponential growth of multimedia content in today's internet traffic and the increasing need of bandwidth-consuming or location-independent services motivated the research community to design a viable replacement for the current IP-based Internet architecture. Named Data Networking or NDN is a novel network architecture that uses universal in-network caching and routing by name functionalities to deliver content efficiently and to improve service quality. Network coding benefits named data networking with its inherent algebraic structure and the maximum flow rates performance it achieves in multicast. With network coding, the content can be requested via multiple interfaces thus improving significantly content delivery efficiency. However, it is vulnerable to pollution attacks, which can cause a crucial degradation of network bandwidth. In this paper, we propose an efficient and optimized authentication technique for a content distribution NDN architecture based on network coding. Our solution uses homomorphic signature mechanism, which allows intermediate nodes to verify the authenticity of flows to overcome the pollution problem without having access to content. We formulate NDNAuth, an optimal coding and homomorphic signature scheme as a MIP problem. Furthermore, we show how to leverage Software Defined Networking to provide seamless implementation of the proposed solution. We measure the processing overhead and the dynamic system security state based on three metrics: (1) defence power; (2) threat severity and (3) system vulnerability. Finally, we discuss how to minimize the computational cost of coding and signature scheme operations. Experimentation results prove the efficiency of the proposed coding scheme, which achieves better performance than conventional NDN with random coding especially in terms of transmission cost and security. (*AN: S2214212619302790*), Database: ScienceDirect

Subjects: Named data networking; Network coding; Software defined networking; Homomorphic signature

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 204

14. Mind your privacy: Privacy leakage through BCI applications using machine learning methods

By Landau, Ofir; Cohen, Aviad; Gordon, Shirley; Nissim, Nir. In *Knowledge-Based Systems*. 21 June 2020 198 Language: English. DOI: 10.1016/j.knosys.2020.105932 Abstract: With the digitization of almost every aspect of our lives, privacy leakage in cyber space has become a pressing concern. Brain–Computer **interface** (BCI) systems have become more popular in recent years and are now being used for a variety of applications. BCI data represents an individual's brain activity at a given time. Like many other kinds of data, BCI data can be utilized for malicious purposes. Electroencephalography (EEG) is one of the most popular brain activity acquisition methods of BCI applications. More specifically, BCI games, represent one of the main EEG applications. However, a malicious BCI application (e.g. game) could allow an attacker to take advantage of an unsuspecting user happily enjoying a game and record the user's brain activity; by analyzing this data, the attacker can infer private **information** and characteristics regarding the user, without his/her consent or awareness. This study is the **first** to demonstrate the ability to predict and infer meaningful personality traits and cognitive abilities by analyzing resting-state EEG (rsEEG) recordings o&an individual's brain activity using a variety of machine learning methods. A comprehensive set of raw rsEEG scans, along with the dissociation level and executive function (EF) performance measures, for the 162 subjects were used in our evaluation. The best results we achieved were an accuracy of 73% for dissociation classification and less than 16% mean absolute error in predicting performance for all examined EFs. These encouraging results are better than those presented in prior research, both in terms of accuracy and data-validity and dataset size. (*AN: S0950705120302641*), Database: ScienceDirect

Subjects: Privacy leakage; Brain–computer **interface**; BCI; EEG; BCI games

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 205

15. ## Authentication Techniques and Methodologies used in Wireless Body Area Networks

By Hussain, Munir; Mehmood, Amjad; Khan, Shafiullah; Khan, M. Altaf; Iqbal, Zeeshan. In *Journal of Systems Architecture*. December 2019 101 Language: English. DOI: 10.1016/j.sysarc.2019.101655 Abstract: Wireless body area network (WBAN), got the IEEE standard in February 2012, is the most significant and highly focused research area among researchers, academicians, and practitioners; applied to the patient's body for monitoring various physiological parameters and then the sensitive measured data is passed to the concerned medical doctor or server for taking the necessary actions. In order to pass the sensitive data securely, authentication is the **first** step towards it. The authentication schemes help network to reduce unwanted users and prevent from deceptions effectively since the authentication process identifies the user's identity that he or she claims to be. In connection to the safe **communication**, authentication is one of the key aspects. So, it is important to design novel authentication schemes; those offer secure authentication and prevent various security attacks in WBANs. A lot of methods and techniques have been proposed for authentication in WBANs. In this survey paper for improving the authentication process in WBANs, an overview of WBAN and their characteristics, various authentication types and classification of authentication schemes has been done. It further provides a complete comparison of different authentication schemes and highlights their pros, cons, limitations, challenges, performance evaluation and their robustness against different security attacks which open doors of new opportunities. This finally ends with the most significant open issues, future research directions and draw interesting conclusions. (*AN: S138376211930462X*), Database: ScienceDirect

Subjects: Authentication; **Biometric**; Security; Wireless body area network; Smart card

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 206

16. ## Location of three-dimensional movement for a human using a wearable multi-node instrument implemented by wireless body area networks

By Wang, Dong; Huang, Qingcheng; Chen, Xin; Ji, Lijuan. In *Computer Communications*. 1 March 2020 153:34-41 Language: English. DOI: 10.1016/j.comcom.2020.01.070 Abstract: A wireless human body local area network is a wireless network composed of lightweight, wearable or implantable sensor nodes that sense various physiological parameters of the human body. This paper introduces the key technologies and characteristics of wireless sensor networks and the research status of node localization, analyzes the wireless sensor network localization algorithms and their performance evaluation indicators, and conducts in-depth research on wearable 3D node localization algorithms. The 3D positioning algorithm uses static beacon nodes to achieve the 3D positioning of public nodes. The positioning accuracy and positioning rate depend on the number of beacon nodes, and the number of beacon nodes increases, which increases network costs and energy consumption. Aiming at the spatiotemporal correlation **between** motion data collected by multiple sensors in a wireless human local area network, an RSSI-based multi-node 3D motion monitoring auxiliary algorithm is used, including the planning of wearable **device** motion trajectories. Throughout the positioning process, the workflow belongs to the public node and involves the format of the relevant **information** packet. The 3D wearable multi-node positioning algorithm based on RSSI is a distance-dependent distributed positioning algorithm. The public node uses the RSSI ranging method to obtain the distance during the two-stage positioning process, and then uses the three-dimensional multilateral positioning method to perform its own calculation. (*AN: S014036641931477X*), Database: ScienceDirect

Subjects: Wireless body area network; Motion recognition; Wearable **device**; Three-dimensional motion monitoring; Multi-node

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 207

17. A survey on QoE-oriented wireless resources scheduling

By Sousa, Ivo; Queluz, Maria Paula; Rodrigues, António. In *Journal of Network and Computer Applications*. 15 May 2020 158 Language: English. DOI: 10.1016/j.jnca.2020.102594 Abstract: Future wireless systems are expected to provide a wide range of services to more and more users. Advanced scheduling strategies thus arise not only to perform efficient radio resource management, but also to provide fairness among the users. On the other hand, the users' perceived quality, i.e., Quality of Experience (QoE), is becoming one of the main drivers within the schedulers design. In this context, this paper starts by providing a comprehension of what is QoE and an overview of the evolution of wireless scheduling techniques. Afterwards, a survey on the most recent QoE-based scheduling strategies for wireless systems is presented, highlighting the application/service of the different approaches reported in the literature, as well as the parameters that were taken into account for QoE optimization. Therefore, this paper aims at helping readers interested in learning the basic concepts of QoE-oriented wireless resources scheduling, as well as getting in touch with its current research frontier. (*AN: S1084804520300680*), Database: ScienceDirect

Subjects: Quality of experience (QoE); Scheduling; Radio resource management; Wireless networks

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 208

18. ## A three-factor anonymous user authentication scheme for Internet of Things environments

By Lee, Hakjun; Kang, Dongwoo; Ryu, Jihyeon; Won, Dongho; Kim, Hyoungshick; Lee, Youngsook. In *Journal of Information Security and Applications*. June 2020 52 Language: English. DOI: 10.1016/j.jisa.2020.102494 Abstract: To accelerate the deployment of fifth-generation (5G) cellular networks, millions of **devices** are being connected to massive Internet of Things (IoT) networks. However, advances in the scale of connectivity on 5G networks may increase the attack surface of these **devices**, thereby increasing the number of attack opportunities. To address the potential security risks in IoT systems, one feasible security practice involves the development of secure and efficient user authentication schemes. In 2017, Dhillon and Kalra proposed a three-factor user authentication scheme for IoT. We noted that their scheme suffers from several security weaknesses. In this study, we specifically demonstrate that the scheme proposed by Dhillon and Kalra (1) is not secured from a stolen mobile **device** attack; (2) does not prevent a user impersonation attack; (3) does not provide a session key agreement; (4) does not have a contingency plan (e.g., a revocation phase) for situations where a user's private key is compromised, or a mobile **device** is stolen or lost. We propose an improved three-factor user authentication scheme to resolve these security issues. Furthermore, we demonstrate that the proposed scheme provides desirable attributes for IoT environments and that its computation and **communication** costs are suitable for extremely low-cost IoT **devices**. (*AN: S2214212619308051*), Database: ScienceDirect

Subjects: Authentication; Key agreement; Wireless sensor network; Internet of things

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 209

19. ## Security breach notification

By: Wells Fargo Bank, N.A. US Patent: 10542,018. Filed: December 27, 2016. Issued: January 21, 2020. , Database: USPTO Patent Grants

Abstract: Systems and methods are disclosed for security breach notification. In one implementation, an indication of a security breach is received, at a **first device** with respect to a user account. Based on the indication of the security breach, a processing **device** generates a security breach notification, the security breach notification including an instruction to initiate at an account repository one or more actions with respect to the user account. An attempt is made to transmit the security breach notification to the account repository **via** a **first communication interface** of the **first device**. In response to a determination that the security breach notification was not successfully transmitted to the account repository, the security breach notification is transmitted to a **second device via** a **second communication interface** of the **first device**.

AN: edspgr.10542018

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 210

20. ## Secure IoT **communications** for smart healthcare monitoring system

By El Zouka, Hesham A.; Hosni, Mustafa M.. In *Internet of Things*. January 2018 Language: English. DOI: 10.1016/j.iot.2019.01.003 Abstract: Healthcare monitoring systems in hospitals and other health centers have witnessed throughout the last decade a tremendous growth and wireless healthcare monitoring **devices** with various technologies have become of great interest in many nations around the world. The proposed paper aims at integrating artificial intelligence technology, such as the neural networks and fuzzy system in a secure healthcare monitoring system in order to enable the system to work as a smart healthcare model that decides the priority by itself depending on the collected health parameters from the senor nodes. The proposed model consists of a trust environment that is responsible for collecting authenticated physiological data from patient's body which is then sent through GSM module to Azure IoT Hub where raw data is converted into linguistic representation, with the help of logic-based algorithm, which is trained in fuzzy-based inference system (FBIS) to get the status of the patient. The proposed system, then, provides reliable, accurate, secure and real-time patient monitoring. The following sections describe how the FBIS can be integrated with a secure healthcare monitoring system to get the states of the patient and send it to the medical advisory for the preliminary precautions. (*AN: S254266051830088X*), Database: ScienceDirect

Subjects: Internet of Things (IoT); health monitoring; sensors; security; trust; fuzzy

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 211

21. ## Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment

By Bera, Basudeb; Chattaraj, Durbadal; Das, Ashok Kumar. In *Computer Communications*. 1 March 2020 153:229-249 Language: English. DOI: 10.1016/j.comcom.2020.02.011 Abstract: In recent years, the Internet of Drones (IoD) has emerged as an important research topic in the academy and industry because it has several potential applications ranging from the civilian to military. In IoD environment, several drones, called Unmanned Aerial Vehicles (UAVs), are deployed in different flying zones that communicate each other to exchange crucial **information**, and then the **information** are collected by the Ground Station Server (GSS). All the drones and the GSS are registered with a central trusted authority, Control Room (CR) prior to their deployment. Since the drones and the GSS communicate over open channel (e.g., wireless medium), there are security and privacy issues in the IoD environment. To handle such issues, in this paper we introduce a blockchain-based access control scheme in the IoD environment that allows secure **communication** among the drones, and also among the drones and the GSS. Secure data gathered by the GSS form transactions, and those transactions are made into the blocks. The blocks are finally added in the blockchain by the cloud servers connected with the GSS **via** the Ripple Protocol Consensus Algorithm (RPCA) in a peer-to-peer cloud server network. Once the blocks are added into the blockchain, the transactions containing in the blocks cannot be altered, modified or even removed. We provide all sorts of security analysis including formal security under the random oracle model, informal security and simulation-based formal security verification to assure that the proposed scheme can resist various potential attacks with high probability needed in an IoD environment. In addition, a meticulous comparative analysis among the proposed scheme and other closely related existing schemes shows that our scheme offers more functionality attributes and better security, and also low **communication** and computation costs as compared to other schemes. (*AN: S0140366419318377*), Database: ScienceDirect

Subjects: Internet of Drones (IoD); Access control; Blockchain; Consensus; Security; AVISPA

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 212

22. ## An approach to develop the smart health using Internet of Things and authentication based on **biometric** technology

By Hamidi, Hodjat. In *Future Generation Computer Systems*. February 2019 91:434-449 Language: English. DOI: 10.1016/j.future.2018.09.024 Abstract: Internet of things is a new pattern in wireless **communications** of things. The basic theory of IoT is the comprehensive presence of different kinds of things in surrounding environment. The three main dimensions of data security in the Internet are integration, privacy and availability. One of the major tools for maintaining the security of Internet medical things is **biometric** technology. **Biometric** systems are used in different fields of the smart healthcare. In this regard, we also need a means for identifying people's identity based on their physical characteristics; the use of **biometric** data is absolutely critical for IoT functions. Considering this emerging pattern, everything integrated will connect to a virtual chain of connected things with address in the **dynamic** world of networks. Given the importance of secure connections of things to the Internet and access to them, **biometric** features are used as identifiers; because they cannot be borrowed, bought, forgotten and they are very difficult to forge or copy. The smart healthcare and IoT resulted in the emergence of a new standard in the applications of **biometric** data. In this paper, we present a new standard for applying **biometric** technology to develop smart healthcare using IoT which includes high capacity to access data in addition to being easy to use. In this paper, we reached a more secure way of accessing IoT based on **biometrics** and fast identity standard by which we can expect significant advances in smart healthcare systems. (*AN: S0167739X18313517*), Database: ScienceDirect

Subjects: Internet of Things (IoT); **Biometric**; Data protection standard; Identifiers; Smart healthcare

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 213

23. ## A privacy-preserving scheme with identity traceable property for smart grid

By Wu, Fan; Li, Xiong; Xu, Lili; Kumari, Saru. In *Computer Communications*. 1 May 2020 157:38-44 Language: English. DOI: 10.1016/j.comcom.2020.03.047 Abstract: Smart city is a hot aim, and is organized gradually in many developed countries. People can understand the variation of city clearly via the collected data from sensors and RFID chips all over the city. As one of the most important applications for smart city, smart grid is a popular technology which has been already used in some developed countries. Wireless circumstance is the main way for the transmission data in collection process, and it is undoubtedly insecure. The problems that protecting the consumption data in smart grid and tracking some special users simultaneously are still open issues. We propose a novel scheme for smart grid involving three kinds of entities: Smart Meters (SMs), Electricity Utilities (EUs), and a Trustful Anchor (TA). In this scheme, SM encrypts the periodical consumptions and its identity, and sends the **information** to the relative electricity utility, and then EU can get the consumptions of smart meters in its scope. If necessary, TA may disclose the identities of the special smart meters. The security of this scheme is illustrated by formal proof and security property analysis. After expressions of performance and network simulation, it is easy to see that our scheme is suitable for practicality. (*AN: S0140366419319668*), Database: ScienceDirect

Subjects: Smart grid; NS-3; Traceability; Anonymity; Unlinkability

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 214

24. Blockchain leveraged decentralized IoT eHealth framework

By Uddin, Md. Ashraf; Stranieri, Andrew; Gondal, Iqbal; Balasubramanian, Venki. In *Internet of Things*. March 2020 9 Language: English. DOI: 10.1016/j.iot.2020.100159 Abstract: Blockchain technologies recently emerging for eHealth, can facilitate a secure, decentralized and patient-driven, record management system. However, Blockchain technologies cannot accommodate the storage of data generated from IoT **devices** in remote patient management (RPM) settings as this application requires a fast consensus mechanism, careful management of keys and enhanced protocols for privacy. In this paper, we propose a Blockchain leveraged decentralized eHealth architecture which comprises three layers: (1) The Sensing layer – Body Area Sensor Networks include medical sensors typically on or in a patient body transmitting data to a smartphone. (2) The NEAR processing layer – Edge Networks consist of **devices** at one hop from data sensing IoT **devices**. (3) The FAR processing layer – Core Networks comprise Cloud or other high computing servers). A Patient Agent (PA) software replicated on the three layers processes medical data to ensure reliable, secure and private **communication**. The PA executes a lightweight Blockchain consensus mechanism and utilizes a Blockchain leveraged task-offloading algorithm to ensure patient's privacy while outsourcing tasks. Performance analysis of the decentralized eHealth architecture has been conducted to demonstrate the feasibility of the system in the processing and storage of RPM data. (*AN: S2542660520300020*), Database: ScienceDirect

Subjects: Internet of Things; Blockchain; Consensus mechanism; Proof of stake; Patient agent; Fog computing; Edge computing; Cloud; Patient monitoring; eHealth; Fuzzy inference process; Task offloading

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 215

25. ## Taxonomy and analysis of security protocols for Internet of Things

By Das, Ashok Kumar; Zeadally, Sherali; He, Debiao. In *Future Generation Computer Systems*. December 2018 89:110-125 Language: English. DOI: 10.1016/j.future.2018.06.027 Abstract: The Internet of Things (IoT) is a system of physical as well as virtual objects (each with networking capabilities incorporated) that are interconnected to exchange and collect **information** locally or remotely over the Internet. Since the **communication** often takes place over the Internet, it is vulnerable to various security threats in an IoT environment. We **first** discuss essential security requirements that are needed to secure IoT environment. We also discuss the threat model and various attacks related to the IoT environment. We then present a taxonomy of security protocols for the IoT environment which includes important security services such as key management, user and **device** authentication, access control, privacy preservation, and identity management. We also present a comparative study of recently proposed IoT-related state-of-art security protocols in terms of various security and functionality features they support. Finally, we discuss some future challenges for IoT security protocols that need to be addressed in the future. (*AN: S0167739X18308112*), Database: ScienceDirect

Subjects: Access control; Authentication; Identity management; IoT; Key management; Security; Privacy; Sensing **devices**

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 216

26. ## BTNC: A blockchain based trusted network connection protocol in IoT

By Zhang, Junwei; Wang, Zhuzhu; Shang, Lei; Lu, Di; Ma, Jianfeng. In *Journal of Parallel and Distributed Computing*. September 2020 143:1-16 Language: English. DOI: 10.1016/j.jpdc.2020.04.004 Abstract: Along with the rapid growth of the size and complexity of Internet of Things (IoT), the security of terminal **devices** has increasingly become a focus. In order to ensure the security of terminals, the trusted network connect (TNC) could realize not only the user authentication but also the platform attestation during the network access process. However, the existing TNC infrastructure is based on a centralized architecture, which is not suitable for distributed services. To address this problem, we present a blockchain-based TNC protocol named BTNC to ensure the reliability of terminals in IoT. Due to the decentralization, trustlessness, trackability, and immutability features of blockchain, BTNC is able to verify the security of terminal **devices** in IoT networks. **First**, we come up with some threats, including unauthorized user, illegal platform and platform replacement attack, then correspondingly define the security goals of our scheme. **Second**, combining key exchange protocol based on blockchain and D–H PN protocol included in TNC specification, we propose a blockchain-based trusted network connection protocol, which realizes mutual user authentication, platform attestation and trust network access by cryptography among terminals in IoT. Third, we make a security analysis in the PCL mode and conclude that our protocol can resist the attacks above. Finally, the performance overheads caused by our scheme are evaluated and the experiments show that it is efficient and feasible for different kinds of terminals in IoT. (*AN: S0743731519308457*), Database: ScienceDirect

Subjects: Blockchain; IoT; Key exchange; Platform measurement; Trusted network connection

Full Text Finder **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 217

27. ESEAP: ECC based secure and efficient mutual authentication protocol using smart card

By Kumari, Adesh; Jangirala, Srinivas; Abbasi, M. Yahya; Kumar, Vinod; Alam, Mansaf. In *Journal of Information Security and Applications*. April 2020 51 Language: English. DOI: 10.1016/j.jisa.2019.102443 Abstract: Highlights •We have reviewed Wang et al.'s scheme in two-factor based remote user authentication environment.•Wang et al.'s scheme has security issues such as impersonation attack, stolen-verifier attack, off-line password guessing attack and fails to secure session key.•We have designed an enhanced and secure elliptic curve cryptography(ECC) assisted authentication framework for same environment.•The proposed protocol resists various kinds of malicious attacks such as security attributes and features like as off-line password guessing attack, no password verifier-table, smart card loss attack, anonymity, mutual authentication, replay attack, impersonation attack, server spooling attack, no clock-synchronization attack, forward secrecy, insider attack, message authentication, provision of key agreement, parallel attack, sound repairability, no password exposure, timely typo detection, resistance to know attacks, password friendly, user unlinkability and server unlinkability and hence secure for real life applications.•The proposed protocol presents better results and proven to be secure and efficient which can be practically applicable for the real life applications. (*AN: S221421261930482X*), Database: ScienceDirect

Subjects: Mutual authentication; Elliptic curve cryptography; Smart card; Random oracle model; Security and privacy

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 218

28. ## A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT

By Sengupta, Jayasree; Ruj, Sushmita; Das Bit, Sipra. In *Journal of Network and Computer Applications*. 1 January 2020 149 Language: English. DOI: 10.1016/j.jnca.2019.102481 Abstract: In recent years, the growing popularity of Internet of Things (IoT) is providing a promising opportunity not only for the development of various home automation systems but also for different industrial applications. By leveraging these benefits, automation is brought about in the industries giving rise to the Industrial Internet of Things (IIoT). IoT is prone to several cyberattacks and needs challenging approaches to achieve the desired security. Moreover, with the emergence of IIoT, the security vulnerabilities posed by it are even more devastating. Therefore, in order to provide a guideline to researchers, this survey primarily attempts to classify the attacks based on the objects of vulnerability. Subsequently, each of the individual attacks is mapped to one or more layers of the generalized IoT/IIoT architecture followed by a discussion on the countermeasures proposed in literature. Some relevant real-life attacks for each of these categories are also discussed. We further discuss the countermeasures proposed for the most relevant security threats in IIoT. A case study on two of the most important industrial IoT applications is also highlighted. Next, we explore the challenges brought by the centralized IoT/IIoT architecture and how blockchain can effectively be used towards addressing such challenges. In this context, we also discuss in detail one IoT specific Blockchain design known as Tangle, its merits and demerits. We further highlight the most relevant Blockchain-based solutions provided in recent times to counter the challenges posed by the traditional cloud-centered applications. The blockchain-related solutions provided in the context of two of the most relevant applications for each of IoT and IIoT is also discussed. Subsequently, we design a taxonomy of the security research areas in IoT/IIoT along with their corresponding solutions. Finally, several open research directions relevant to the focus of this survey are identified. (*AN: S1084804519303418*), Database: ScienceDirect

Subjects: IIoT; Security; Privacy; Blockchain; Smart Factory; Smart Grid; Supply Chain; E-Healthcare; VANET

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 219

29. ## A survey on methods and challenges in EEG based authentication

By Jalaly Bidgoly, Amir; Jalaly Bidgoly, Hamed; Arezoumand, Zeynab. In *Computers & Security*. June 2020 93 Language: English. DOI: 10.1016/j.cose.2020.101788 Abstract: EEG is the recording of electrical activities of the brain, usually along the scalp surface, which are the results of synaptic activations of the brain's neurons. In recent years, it has been shown that EEG is an appropriate signal for the **biometric** authentication and has important features such as resistance to spoofing attacks and impossibility to use under pressure and coercion states. In this paper, the state-of-the-art methods in EEG based authentication are reviewed. This review includes a number of aspects such as the various tasks that the user required to perform during the authentication, **devices** and available datasets, the preprocessing procedures and the classification methods used in the EEG **biometric** authentication. Both shallow and deep classification methods are reviewed in this paper. The study shows that the deep learning approaches which are used in the past few years, although still require further research, have shown great results. Moreover, the paper summarizes the works to address the open challenges of this area. The EEG authentication challenges have been discussed from a variety of points of view, including privacy, user-friendliness, attacks, and authentication requirements such as universality, permanency, uniqueness, and collectability. This paper can be used as a preliminary plan and a roadmap for researchers interested in EEG **biometric**. (*AN: S0167404820300730*), Database: ScienceDirect

Subjects: EEG; **Biometric** factor; Authentication; User identification; Pattern recognition; Survey

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 220

30. Proximal spatial vector and affinity coefficient for multimodal **biometric** secured social network **communication**.

By: Sivasubramaniam, Jayanthi; Chandrasekar, C.. *World Wide Web* , Jul2019, Vol. 22 Issue 4, p1751-1764, 14p. Publisher: Springer Nature.; Abstract Using multimodalities, the field of **biometric** is **receiving** widespread acceptance for efficient **communication between** users in social network. Hence, suitable designing of authentication and access control is highly required to perform analysis of system in social network domain. In this work, a Proximal Spatial Vector and Affinity Coefficient (PSV-AC) framework is designed with the objective of ensuring authentic **communication between** users in social network using face and fingerprint. Initially, multimodal user **biometric** features with proximal feature pixel stored in spatial vector are gene encoded to obtain **biometric** identity keys. User authenticity is authorized by decoding gene encoded **biometric** features using **biometric** identity keys. User Affinity Coefficient is calculated **via** antecedent instances shared **between** different social users. The social network user's affinity coefficient is ordered in a matrix. Matrix ranking is then performed to identify whether authentic user social **communication** happened in network. Experiments have been carried out using BioSecure datasets to measure the performance in terms of number of social users, social network authentication time, access control time, multimodal **biometric** feature template size, and true positive rate. [ABSTRACT FROM AUTHOR]; (*AN 136915010*), Database: Complementary Index

Subjects: Satellite Telecommunications; TELECOMMUNICATION systems; SOCIAL network analysis; ACCESS control

Linked Full Text **USPTO Full Text Options**

EBSCO Connect | Privacy Policy | A/B Testing | Terms of Use | Copyright | Cookie Policy | Contact Us

powered by EBSCO*host*

© 2020 EBSCO Industries, Inc. All rights reserved.

IPR2025-01313; Samsung
Ex. 1002 - Page 221

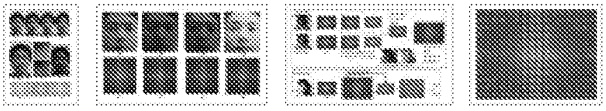
STIC
Scientific and Technical Information Center

1. Face Spoofing Attack Detection **Using** Spatial Frequency and Gradient-**Based** Descriptor.

By: Ali, Zahid; Park, Unsang. *KSII Transactions on Internet & **Information** Systems* , Feb2019, Vol. 13 Issue 2, p892-911, 20p Abstract: **Biometric** recognition systems have been widely used for **information** security. Among the most popular **biometric** traits, there are fingerprint and face due to their high recognition accuracies. However, the security system that uses face recognition as the login method are vulnerable to face-spoofing attacks, from **using** printed photo or video of the valid **user**. In this study, we propose a fast and robust method to detect face-spoofing attacks **based** on the analysis of spatial frequency differences between the real and fake videos. We found that the effect of a spoofing attack stands out more prominently in certain regions of the 2D Fourier spectra and, therefore, it is adequate to use the **information** about those regions to classify the input video or image as real or fake. We adopt a divide-conquer-aggregate approach, where we first divide the frequency domain image into local blocks, classify each local block independently, and then aggregate all the classification results by the weighted-sum approach. The effectiveness of the methodology is demonstrated **using** two different publicly available databases, namely: 1) Replay Attack Database and 2) CASIA-Face Anti-Spoofing Database. Experimental results show that the proposed method provides **state**-of-the-art performance by processing fewer frames of each video. [ABSTRACT FROM AUTHOR]; DOI: 10.3837/tiis.2019.02.022; (*AN 135231624*), Database: Applied Science & Technology Source

Subjects: Biometric identification; Pattern recognition systems; **Information** storage & retrieval system security measures; Human face recognition (Computer science); Robust control

Show all 7 Images



PDF Full Text (533KB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 222

2. Patent Application Titled '**Information** Processing Device, Application Software Start-Up System, And Application Software Start-Up Method' Published Online (USPTO 20190362061)

In: **Information** Technology Newsweekly, Dec 17, 2019, 2279; NewsRX LLC
Language: English. Abstract: 2019 DEC 17 (VerticalNews) -- By a News Reporter-Staff News Editor at **Information** Technology Newsweekly -- According to news reporting originating from Washington, D.C., by VerticalNews journalists, a patent application [...] (*AN: edsgcl.608720217*), Database: Gale General OneFile

Subjects: Japan; Software quality; Software -- Methods; Software -- Intellectual property; Control equipment -- Methods; Control equipment -- Intellectual property

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 223

3. ## Securing internet of medical things systems: Limitations, issues and recommendations

By Yaacoub, Jean-Paul A.; Noura, Mohamad; Noura, Hassan N.; Salman, Ola; Yaacoub, Elias; Couturier, Raphaël; Chehab, Ali. In *Future Generation Computer Systems*. April 2020 105:581-606 Language: English. DOI: 10.1016/j.future.2019.12.028 Abstract: Traditional health-care systems suffer from new challenges associated with the constant increase in the number of patients. In order to address this issue, and to increase the accuracy, reliability, efficiency, and effectiveness of the health-care domain, the Internet of Medical Things (IoMT) was proposed. IoMT can be considered as an enhancement and investment to respond more effectively and efficiently to patients' needs. However, IoMT suffers from different issues and challenges such as the lack of security and privacy measures, in addition to the necessary training and awareness. In this paper, we highlight the importance of implementing the right security measures and the required training skills, in order to enhance the immunity of IoMT against cyber-attacks. Moreover, we review the main IoMT security and privacy issues, and the existing security solutions. These solutions are classified as cryptographic or non-cryptographic. Then, the different solutions are analyzed and compared in terms of computational complexity and required resources. It is important to note that the security measures for IoMT exhibit a trade-off between the security level and the system performance, especially in the rise of digital healthcare v4.0 era. Next, we discuss the appropriate security solutions such as lightweight cryptographic algorithms, and protocols that attempt to reduce the overhead in terms of computations and resources. This leads to the conclusion that there is a need to design an efficient intrusion detection/prevention system that cooperates with dynamic shadow honeypots. Finally, we propose a security solution, which is divided into five different layers to detect and prevent attacks, in addition to reducing/correcting the damage of these known attacks and preserving the patients' privacy. However, it should be noted that zero-day attacks and exploits are still the main challenging issue that surrounds IoMT. (*AN: S0167739X19305680*), Database: ScienceDirect

Subjects: Healthcare; IoMT; Medical cyber physical systems; Medical devices

Full Text Finder USPTO Full Text Options

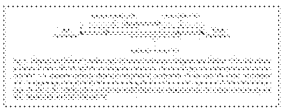
IPR2025-01313; Samsung
Ex. 1002 - Page 224

4. ## Security and Privacy Approaches in Mixed Reality: A Literature Survey.

By: DE GUZMAN, JAYBIE A.; THILAKARATHNA, KANCHANA; SENEVIRATNE, ARUNA. *ACM Computing Surveys*. Jan2020, Vol. 52 Issue 6, p1-37. 37p. Abstract: Mixed reality (MR) technology development is now gaining momentum due to advances in computer vision, sensor fusion, and realistic **display** technologies. With most of the research and development focused on delivering the promise of MR, the privacy and security implications of this technology are yet to be thoroughly investigated. This survey article aims to put in to light these risks and to look into the latest security and privacy work on MR. Specifically, we list and review the different protection approaches that have been proposed to ensure **user** and data security and privacy in MR. We extend the scope to include work on related technologies such as augmented reality, virtual reality, and human-computer interaction as crucial components, if not the origins, of MR, as well as numerous related work from the larger area of mobile devices, wearables, and Internet-of-Things. We highlight the lack of investigation, implementation, and evaluation of data protection approaches in MR. Further challenges and directions on MR security and privacy are also discussed. [ABSTRACT FROM AUTHOR] DOI: 10.1145/3359626. (*AN: 142465075*), Database: Computers & Applied Sciences Complete

Subjects: Mixed reality; Computer vision; Data security; Privacy; Human-computer interaction; Augmented reality

Show all 12 Images






PDF Full Text (4.8MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 225

5. ## Systems and methods for customizing **display** modes for a touch-sensitive secondary **display**

By: Apple Inc. US Patent: 10635,134. Filed: September 26, 2018. Issued: April 28, 2020. , Database: USPTO Patent Grants

Abstract: Disclosed herein are systems and methods that enable **users** to customize operation of a touch-sensitive secondary **display**. An example method includes: **displaying**, on primary **display**, a first UI for a first application; while secondary **display** is operating in an adaptive **display** mode: (i) **displaying**, on a respective portion of the touch-sensitive secondary **display**, application-specific **user** interface elements selected **based** on current **state** of the first UI; and (ii) receiving a request to operate the secondary **display** in a persistent mode; in response to receiving the request, operating the touch-sensitive secondary **display** in the persistent **display** mode; and after changing focus to a second UI for a second application: **displaying**, on the primary **display**, the second UI; and maintaining **display**, on the respective portion of the secondary **display**, of UI elements associated with the persistent **display** mode.

AN: edspgr.10635134

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 226

6. ## Data-driven vibrotactile rendering of digital buttons on touchscreens

By Sadia, Bushra; Emgin, Senem Ezgi; Sezgin, T. Metin; Basdogan, Cagatay. In *International Journal of Human - Computer Studies*. March 2020 135 Language: English. DOI: 10.1016/j.ijhcs.2019.09.005 Abstract: Highlights •We proposed a methodology to **display** vibrotactile feedback on a touchscreen that imitates the feeling of physical buttons.•We recorded and analyzed the force, acceleration, and voltage data from three different types of physical buttons to identify their distinct characteristics.•A button-specific vibrotactile stimulus was generated for each physical button **based** on the recorded data.•We then conducted two experimental studies with 20 subjects to investigate how the buttons were perceived by the **user**.•The results showed that subjects could match digital buttons to their physical counterparts with a success rate of 83%. (*AN: S107158191930120X*), Database: ScienceDirect

Subjects: Data-Driven rendering; Surface haptics; Vibrotactile feedback; Digital buttons

Full Text Finder USPTO Full Text Options

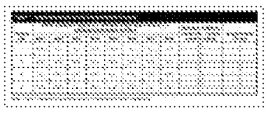
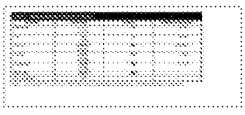
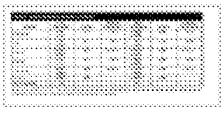
IPR2025-01313; Samsung
Ex. 1002 - Page 227

7. THE DARK SIDE OF REVIEWS: THE SWAYING EFFECTS OF ONLINE PRODUCT REVIEWS ON ATTRIBUTE PREFERENCE CONSTRUCTION.

By: Liu, Qianqian Ben; Karahanna, Elena. *MIS Quarterly.* Jun2017, Vol. 41 Issue 2, p427-A6. 28p. 7 Charts, 2 Graphs. Abstract: **Based** on the "wisdom of the crowd" effect, consumer-generated online reviews are supposed to help consumers make more accurate product evaluations. However, the large amount of **information** in the reviews, coupled with conflicting opinions, can make it difficult for consumers to identify and consider those attributes relevant to their decision. Thus, while online product reviews are generally believed to empower consumers, we suggest that they may have "swaying" effects in that attribute preferences (i.e., the relative importance consumers place on various product attributes in product evaluation) are more heavily influenced by characteristics of the online reviews rather than by the relevance of the attributes to the consumers' decision context. We propose that three characteristics of online reviews affect the assessment of attribute preferences: (1) the amount of **information** about attribute-level performance, which is often unevenly distributed across attributes, (2) the degree of **information** conflict about attribute-level performance, and (3) the relationship between the overall numeric rating and the attribute-level performance **information** in the reviews. We test our hypotheses in two randomized experiments and a free simulation study. Results from the three studies show that the three review characteristics influence attribute preferences and that their effects are strong enough such that attribute preferences are influenced more by these online review characteristics than by the relevance of the attributes to the consumers' decision context. Our work, which illustrates a dark side to online reviews, has implications for both online word-of-mouth and preference construction research. [ABSTRACT FROM AUTHOR] (*AN: 123148195*), Database: Engineering Source

Subjects: USER-generated content; EVALUATION; ONLINE comments; WORD of mouth advertising; CONSUMER preferences

Show all 9 images

HTML Full Text **PDF Full Text** (2MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 228

8. ## Designing Social Nudges for Enterprise Recommendation Agents: An Investigation in the Business Intelligence Systems Context.

By: Kretzer, Martin; Maedche, Alexander. *Journal of the Association for Information Systems*. 2018, Vol. 19 Issue 12, p1145-1186. 42p. 1 Color Photograph, 2 Diagrams, 20 Charts, 4 Graphs. Abstract: According to behavioral economists, a "nudge" is an attempt to steer individuals toward making desirable choices without affecting their range of choices. We draw on this concept, and design and examine nudges that exploit social influence's effects to control individuals' choices. Although recommendation agent research provides numerous insights into extending **information** systems and assisting end consumers, it lacks insights into extending enterprise **information** systems to assist organizations' internal employees. We address this gap by demonstrating how enterprise recommendation agents (ERAs) and social nudges can be used to tackle a common challenge that enterprise **information** systems face. That is, we use an ERA to facilitate **information** (i.e., reports) retrieval in a business intelligence system. In addition, we use social nudges to steer **users** toward reusing specific recommended reports rather than choosing between recommended reports randomly. To test the effects of the ERA and the four social nudges, we conduct a within-subject lab experiment **using** 187 participants. We also conduct gaze analysis ("eye tracking") to examine the impact of participants' elaboration. The results of our logistic mixed-effects model show that the ERA and the proposed social nudges steer individuals toward certain choices. Specifically, the ERA steers **users** toward reusing certain reports. These theoretical findings also have high practical relevance and applicability: In an enterprise setting, the ERA allows employees to reuse existing resources (such as existing reports) more effectively across their organizations because employees can more easily find the reports they actually need. This, in turn, prevents the development of duplicate reports. [ABSTRACT FROM AUTHOR] DOI: 10.17705/1jais.00523. (*AN: 133966693*), Database: Computer Source

Subjects: NUDGE theory; BUSINESS intelligence; BEHAVIORAL economics; SOCIAL influence; ECONOMICS -- Laboratory experiments

Show all 27 Images

IPR2025-01313; Samsung
Ex. 1002 - Page 229



PDF Full Text (7.9MB) USPTO Full Text Options

9. Near-Eye **Display** and Tracking Technologies for Virtual and Augmented Reality.

By: Koulieris, G. A.; Akşit, K.; Stengel, M.; Mantiuk, R. K.; Mania, K.; Richardt, C. *Computer Graphics Forum*. May2019, Vol. 38 Issue 2, p493-519. 27p. 2 Color Photographs, 4 Diagrams, 1 Chart, 4 Graphs. Abstract: Virtual and augmented reality (VR/AR) are expected to revolutionise entertainment, healthcare, communication and the manufacturing industries among many others. Near-eye **displays** are an enabling vessel for VR/AR applications, which have to tackle many challenges related to ergonomics, comfort, visual quality and natural interaction. These challenges are related to the core elements of these near-eye **display** hardware and tracking technologies. In this **state**-of-the-art report, we investigate the background theory of perception and vision as well as the latest advancements in **display** engineering and tracking technologies. We begin our discussion by describing the basics of light and image formation. Later, we recount principles of visual perception by relating to the human visual system. We provide two structured overviews on **state**-of-the-art near-eye **display** and tracking technologies involved in such near-eye **displays**. We conclude by outlining unresolved research questions to inspire the next generation of researchers. [ABSTRACT FROM AUTHOR] DOI: 10.1111/cgf.13654. (*AN: 136857003*), Database: Academic Search Complete

Subjects: VIRTUAL reality; AUGMENTED reality; COMPUTER vision; VISUAL perception; ENGINEERING technicians

Show all 11 Images



HTML Full Text PDF Full Text (14.3MB)

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 230

10. Systems and Methods for Customizing **Display** Modes for a Touch-Sensitive Secondary **Display**

Patent Application: 16/142633. Filed: September 26, 2018. Published: November 14, 2019. , Database: USPTO Patent Applications

Abstract: Disclosed herein are systems and methods that enable **users** to customize operation of a touch-sensitive secondary **display**. An example method includes: **displaying**, on primary **display**, a first UI for a first application; while secondary **display** is operating in an adaptive **display** mode: (i) **displaying**, on a respective portion of the touch-sensitive secondary **display**, application-specific **user** interface elements selected **based** on current **state** of the first UI; and (ii) receiving a request to operate the secondary **display** in a persistent mode; in response to receiving the request, operating the touch-sensitive secondary **display** in the persistent **display** mode; and after changing focus to a second UI for a second application: **displaying**, on the primary **display**, the second UI; and maintaining **display**, on the respective portion of the secondary **display**, of UI elements associated with the persistent **display** mode.

AN: edspap.20190346884

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 231

11. **State** of the Art of Sports Data Visualization.

By: Perin, C.; Vuillemot, R.; Stolper, C. D.; Stasko, J. T.; Wood, J.; Carpendale, S. *Computer Graphics Forum.* Jun2018, Vol. 37 Issue 3, p663-686. 24p. Abstract: Abstract: In this report, we organize and reflect on recent advances and challenges in the field of sports data visualization. The exponentially-growing body of visualization research **based** on sports data is a prime indication of the importance and timeliness of this report. Sports data visualization research encompasses the breadth of visualization tasks and goals: exploring the design of new visualization techniques; adapting existing visualizations to a novel domain; and conducting design studies and evaluations in close collaboration with experts, including practitioners, enthusiasts, and journalists. Frequently this research has impact beyond sports in both academia and in industry because it is i) grounded in realistic, highly heterogeneous data, ii) applied to real-world problems, and iii) designed in close collaboration with domain experts. In this report, we analyze current research contributions through the lens of three categories of sports data: box score data (data containing statistical summaries of a sport event such as a game), tracking data (data about in-game actions and trajectories), and meta-data (data about the sport and its participants but not necessarily a given game). We conclude this report with a high-level discussion of sports visualization research informed by our analysis—identifying critical research gaps and valuable opportunities for the visualization community. More **information** is available at the STAR's website: https://sportsdataviz.github.io/. [ABSTRACT FROM AUTHOR] DOI: 10.1111/cgf.13447. (*AN: 130628179*), Database: Academic Search Complete

Subjects: INFORMATION visualization; SPORTS; COMPUTER visualization; VISUAL analytics; COMPUTER graphics; Fitness and Recreational Sports Centers

PDF Full Text (12.1MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 232

12. ## Enhancing Security on Touch-**Screen** Sensors with Augmented Handwritten Signatures.

By: Abazid, Majd; Houmani, Nesma; Garcia-Salicetti, Sonia. *Sensors (14248220)*. Feb2020, Vol. 20 Issue 3, p933-933. 1p. Abstract. We aim at enhancing personal identity security on mobile touch-**screen** sensors by augmenting handwritten signatures with specific additional **information** at the enrollment phase. Our former works on several available and private data sets acquired on different sensors demonstrated that there are different categories of signatures that emerge automatically with clustering techniques, **based** on an entropy-**based** data quality measure. The behavior of such categories is totally different when confronted to automatic verification systems in terms of vulnerability to attacks. In this paper, we propose a novel and original strategy to reinforce identity security by enhancing signature resistance to attacks, assessed per signature category, both in terms of data quality and verification performance. This strategy operates upstream from the verification system, at the sensor level, by enriching the **information** content of signatures with personal handwritten inputs of different types. We study this strategy on different signature types of 74 **users**, acquired in uncontrolled mobile conditions on a largely deployed mobile touch-**screen** sensor. Our analysis per writer category revealed that adding alphanumeric (date) and handwriting (place) **information** to the usual signature is the most powerful augmented signature type in terms of verification performance. The relative improvement for all **user** categories is of at least 93% compared to the usual signature. [ABSTRACT FROM AUTHOR] DOI: 10.3390/s20030933. (*AN: 141759215*), Database: Academic Search Complete

Subjects: AUGMENTED reality; DETECTORS; SELF; DATA quality; PERSONAL security; DATABASES

HTML Full Text **PDF Full Text** (3.2MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 233

13. ## Homogeneous Physio-Behavioral Visual and Mouse-**Based Biometric**.

By: HAMDY, OMAR; TRAORÉ, ISSA. *ACM Transactions on Computer-Human Interaction (TOCHI)* , Jul2011, Vol. 18 Issue 3, p12-12:30, 30p

Abstract: In this research, we propose a novel **biometric** system for static **user** authentication that homogeneously combines mouse **dynamics**, visual search capability and short-term memory effect. The proposed system introduces the visual search capability, and short-term memory effect to the **biometric-based** security world for the first time. The use of a computer mouse for its **dynamics**, and as an input sensor for the other two **biometrics**, means no additional hardware is required than the standard mouse. Experimental evaluation showed the system effectiveness **using** variable or one-time passwords. All of these attributes qualify the proposed system to be effectively deployed as a static authentication mechanism. Extensive experimentation was done **using** 2740 sessions collected from 274 **users**. To measure the performance, a computational statistics model was specially designed and used; a statistical classifier **based** on Weighted-Sum produced an Equal Error Rate (EER) of 2.11%. [ABSTRACT FROM AUTHOR]; DOI: 10.1145/1993060.1993062; (*AN 64873423*), Database: Applied Science & Technology Source

Subjects: Electronic **information** resource searching; **Biometric** identification; Computer network security; Computer input-output equipment; Human-computer interaction; Errors; Computer and peripheral equipment manufacturing; Computer Terminal and Other Computer Peripheral Equipment Manufacturing; Short-term memory; Performance evaluation

PDF Full Text (2.6MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 234

14. ## Genomic and Personalized Medicine : V1-2

By: Willard, Huntington F.; Ginsburg, Geoffrey S. Edition: 2nd ed. London : Academic Press. 2013. eBook. Description: Genomic and Personalized Medicine, Second Edition —— winner of a 2013 Highly Commended BMA Medical Book Award for Medicine —— is a major discussion of the structure, history, and applications of the field, as it emerges from the campus and lab into clinical action. As with the first edition, leading experts review the development of the new science, the current opportunities for genome-based analysis in healthcare, and the potential of genomic medicine in future healthcare. The inclusion of the latest ... (*AN 485475*), Database: eBook Collection (EBSCOhost)

Subjects: SCIENCE / Life Sciences / Genetics & Genomics; MEDICAL / Pharmacology; Proteomics; Genomics; Medical genetics

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 235

15. A Comprehensive Survey of Indoor Localization Methods **Based** on Computer Vision.

By: Morar, Anca; Moldoveanu, Alin; Mocanu, Irina; Moldoveanu, Florica; Radoi, Ion Emilian; Asavei, Victor; Gradinaru, Alexandru; Butean, Alex. *Sensors (14248220)*. May2020, Vol. 20 Issue 9, p2641. 1p. Abstract: Computer vision **based** indoor localization methods use either an infrastructure of static cameras to track mobile entities (e.g., people, robots) or cameras attached to the mobile entities. Methods in the first category employ object tracking, while the others map images from mobile cameras with images acquired during a configuration stage or extracted from 3D reconstructed models of the space. This paper offers an overview of the computer vision **based** indoor localization domain, presenting application areas, commercial tools, existing benchmarks, and other reviews. It provides a survey of indoor localization research solutions, proposing a new classification **based** on the configuration stage (use of known environment data), sensing devices, type of detected elements, and localization method. It groups 70 of the most recent and relevant image **based** indoor localization methods according to the proposed classification and discusses their advantages and drawbacks. It highlights localization methods that also offer orientation **information**, as this is required by an increasing number of applications of indoor localization (e.g., augmented reality). [ABSTRACT FROM AUTHOR] DOI: 10.3390/s20092641. (*AN: 143235608*), Database: Academic Search Complete

Subjects: LOCALIZATION (Mathematics); OBJECT tracking (Computer vision); COMPUTER vision

HTML Full Text **PDF Full Text** (525KB)

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 236

16. Computer and **Information** Security Handbook

By: Vacca, John R. Series: The Morgan Kaufmann Series in Computer Security. Amsterdam : Morgan Kaufmann, 2009. eBook. Description: Presents **information** on how to analyze risks to your networks and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to physical and network threats. Also imparts the skills and knowledge needed to identify and counter some fundamental security risks and requirements, including Internet security threats and measures (audit trails IP sniffing/spoofing etc.) and how to implement security policies and procedures. In addition, this book covers security and network ... (*AN 248988*), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Networking / General; COMPUTERS / Security / General; Computer networks--Security measures

PDF Full Text **EPUB Full Text** **USPTO Full Text Options**

Full Download

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 237

17. ## Sparking conversations on Facebook brand pages: Investigating fans' reactions to rhetorical brand posts

By van Hooijdonk, Charlotte; van Charldorp, Tessa. In *Journal of Pragmatics*. October 2019 151:30-44 Language: English. DOI: 10.1016/j.pragma.2019.07.013 Abstract: On Facebook brands create pages to facilitate interaction with their (potential) customers, or fans. Brands publish content on these pages which often contain rhetorical figures. Facebook's technological affordances allow fans to respond to these posts leading to multiple participation framework levels that were initiated and can be seen by the brand, but may -- at some point -- no longer involve the brand. In this study, we uncovered how brands initiate interaction by posting content in an artfully divergent way by collecting 62 Dutch Facebook posts from 12 brands and fans' reactions they evoked. **Using** a mixed-methods approach, the posts' rhetorical figures and how fans responded to them were analyzed. The results showed that brands' posts often contain a deviation in meaning which enabled fans to respond in various ways: they responded to the actions posts generated, such as answering questions, but also responded by evaluating the brands. Despite the post's rhetorical type (trope or scheme), format (visual, verbal, or verbo-pictorial), or relevant next action projected, rhetorical posts on brand pages secure responses and thus participation from fans. (*AN: S0378216618308877*), Database: ScienceDirect

Subjects: Facebook; Technological affordances; Digital conversation analysis; Rhetorical figures; Brands

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 238

18. ## Consumer Grade EEG Measuring Sensors as Research Tools: A Review.

By: Sawangjai, Phattarapong; Hompoonsup, Supanida; Leelaarporn, Pitshaporn; Kongwudhikunakorn, Supavit; Wilaiprasitporn, Theerawit. *IEEE Sensors Journal* , 4/15/2020, Vol. 20 Issue 8, p3996-4024, 29p. Publisher: IEEE.; Abstract Since the launch of the first consumer grade EEG measuring sensors 'NeuroSky Mindset' in 2007, the market has witnessed an introduction of at least one new product every year by competing manufacturers, which include NeuroSky, Emotiv, interaXon and OpenBCI. There are numerous variations in the make and versions, but these products clearly share the key selling points of affordability, portability, and ease of use. These features are patently well placed provided one of the main objectives for their development is to attract a new target group of commercial **users**. Nevertheless, with several decades of traditional EEG usage in clinical and experimental settings, the shift toward commercial and engineering sides has not been achieved without skepticism. With this in mind, researchers in related fields have been tirelessly working to ensure that these putatively novel features were not introduced at the expense of efficiency and accuracy by conducting validation studies to compare the performance of data derived from consumer grade EEG devices with ones from standard research grade counterparts. In this review, we seek to provide the detail of the products supplied by the major players, summarize studies that evaluate consumer product's performance against research grade devices, the key areas of applications that these consumer grade devices have been employed in over the past five years or so, and finally give our perspectives on the limitations and what these innovative tools could offer going forward in terms of research and commercial applications. [ABSTRACT FROM AUTHOR]; (*AN 142343142*), Database: Complementary Index

Linked Full Text **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 239

19. Dictionary of **Information** Science and Technology

By: Khosrowpour, Mehdi. Hershey, PA : IGI Global, 2007. eBook. Description: 'This book is the premier comprehensive reference source for the latest terms, acronyms and definitions related to all aspects of **information** science and technology. It provides the most current **information** to researchers on every level'--Provided by publisher. (*AN 173395*), Database: eBook Collection (EBSCOhost)

Subjects: LANGUAGE ARTS & DISCIPLINES / Library & **Information** Science / General; **Information** science--Dictionaries; **Information** technology--Dictionaries

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

20. Emery and Rimoin's Essential Medical Genetics

By: Korf, Bruce R.; Pyeritz, Reed E.; Rimoin, David L. Amsterdam : Academic Press, 2013. eBook. Description: For decades, Emery and Rimoin's Principles and Practice of Medical Genetics has provided the ultimate source for practicing clinicians to learn how the study of genetics can be integrated into practice. Developed in parallel to the sixth edition, and featuring 174 original contributions from the many authors of the full set, this one volume work expertly condenses and synthesizes the most clinically relevant content, for convenient desk reference. Helping to bridge the gap between high-level molecular ... (*AN 587933*), Database: eBook Collection (EBSCOhost)

Subjects: SCIENCE / Life Sciences / Genetics & Genomics; SCIENCE / Life Sciences / General; Medical genetics

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 240

21. ## Advances in Enterprise **Information** Technology Security

By: Herrmann, Francine; Khadraoui, Djamel. Hershey [Pa.] : IGI Global. 2007. eBook. Description: 'This book provides a broad working knowledge of all the major security issues affecting today's enterprise IT activities. Multiple techniques, strategies, and applications are thoroughly examined, presenting the tools to address opportunities in the field.It is an all-in-one reference for IT managers, network administrators, researchers, and students'--Provided by publisher. (*AN 185367*), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Security / General; COMPUTERS / Security / Network Security; COMPUTERS / Internet / Online Safety & Privacy; Computer security; Data protection; Business enterprises--Computer networks--Security measures; **Information** technology--Security measures

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

22. ## Driver rest recommendation

By: LG ELECTRONICS INC. US Patent: 9,789,878. Filed: April 20, 2015. Issued: October 17, 2017. , Database: USPTO Patent Grants
Abstract: Methods and systems for monitoring a driver of a vehicle **using** a driver **state** monitoring (DSM) system. The DSM system includes a sensing unit that senses biological **information** of a **user** of a vehicle. The DSM system also includes a controller that determines a drowsy **state** of the **user based** on the sensed biological **information**. The controller also determines a current condition of traffic and outputs **information** recommending rest for the **user based** on the **determined** drowsy **state** of the **user** and the **determined** current condition of traffic. The controller monitors the traffic and determines a rest **state** of the **user**, and outputs an alarm **based** on monitoring the traffic and the **determined** rest **state** of the **user**.
AN: edspgr.09789878

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 241

23. ## Wireless Technologies : Concepts, Methodologies, Tools and Applications

By: **Information** Resources Management Association. Hershey, PA : IGI Global. 2012. eBook. (*AN 396408*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Mobile & Wireless Communications; TECHNOLOGY & ENGINEERING / Radio; Wireless communication systems; Telecommunication

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

24. ## Computer Engineering : Concepts, Methodologies, Tools and Applications

By: **Information** Resources Management Association. Hershey, Pa : IGI Global. 2012. eBook. Description: Features perspectives on the fundamental aspects, tools and technologies, methods and design, applications, managerial impact, social/behavioral perspectives, critical issues, and emerging trends in the field of computer engineering. (*AN 431988*), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Computer Engineering; COMPUTERS / Machine Theory; COMPUTERS / Hardware / General; Computer engineering

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

25. ## Abstracts.

Basic & Clinical Pharmacology & Toxicology. Apr2019 Supplement S3, Vol. 124, p3-379. 377p. DOI: 10.1111/bcpt.13217. (*AN: 135934828*), Database: Academic Search Complete

Subjects: MEDICAL textiles; SPECTROMETRY; POLYMERASE chain reaction; BLOOD glucose monitoring; DNA separation

HTML Full Text **PDF Full Text** (11.2MB)

USPTO Full Text Options

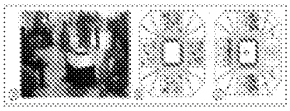
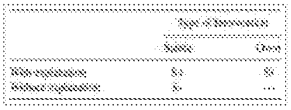
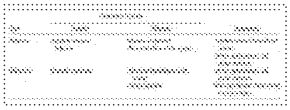
IPR2025-01313; Samsung
Ex. 1002 - Page 242

26. Influencing Participation in Group Brainstorming Through Ambient Intelligence.

By: Schiavo, Gianluca; Cappelletti, Alessandro; Mencarini, Eleonora; Stock, Oliviero; Zancanaro, Massimo. *International Journal of Human-Computer Interaction.* 2016, Vol. 32 Issue 3, p258-276. 19p. 2 Color Photographs, 1 Diagram, 6 Charts, 4 Graphs. Abstract: Drawing on concepts from theories on persuasion, social psychology, and philosophy of language, this article presents the design of an ambient persuasive system that acts as an automatic facilitator by supporting a balanced flow of communication in group conversational activity. The system includes two main components: (a) a context-awareness system that monitors group member non-verbal behavior, and (b) a visualization component that promotes balanced participation, providing targeted directives to participants through peripheral **displays**. In two empirical studies, a strategy for influencing participant social **dynamics based** on subtle directives in the form of aesthetically pleasant visual animations was assessed. The findings provide insight on the effect, the acceptability, and the perceived influence of subtle peripheral persuasive messages for ambient **displays**. The studies indicate that when the participants understand the message intention, the subtle directives have a positive influence on group behavior, and are considered more appealing and less intrusive than overt, language-**based** messages. Furthermore, it was found that personality traits influenced attitudes towards the system. [ABSTRACT FROM AUTHOR] DOI: 10.1080/10447318.2016.1136179. (*AN: 113304631*), Database: Computer Source

Subjects: PERSUASIVE technology; SOCIAL psychology; BRAINSTORMING; AMBIENT intelligence; PHILOSOPHY of language; VISUALIZATION; SOCIAL **dynamics**

Show all 13 Images

HTML Full Text **PDF Full Text** (909KB)

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 243

27. ## Emery and Rimoin's Principles and Practice of Medical Genetics

By: Korf, Bruce R.; Pyeritz, Reed E.; Rimoin, David L. Edition: 6th ed. Oxford : Academic Press. 2013. eBook. Description: For decades, Emery and Rimoin's Principles and Practice of Medical Genetics has provided the ultimate source for practicing clinicians to learn how the study of genetics can be integrated into practice. With almost 5,000 pages of detailed coverage, this fully online sixth edition of the classic reference adds the latest **information** on prenatal diagnosis, genetic screening, genetic counseling, and treatment strategies to complete its coverage of the growing field for medical students, residents and ... (*AN 485154*), Database: eBook Collection (EBSCOhost)

Subjects: HEALTH & FITNESS / Diseases / Genetic; MEDICAL / Genetics; Medical genetics

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

28. ## Statistical Signal Processing for Neuroscience and Neurotechnology

By: Oweiss, Karim G. Burlington, MA : Academic Press. 2010. eBook. Description: This is a uniquely comprehensive reference that summarizes the **state** of the art of signal processing theory and techniques for solving emerging problems in neuroscience, and which clearly presents new theory, algorithms, software and hardware tools that are specifically tailored to the nature of the neurobiological environment. It gives a broad overview of the basic principles, theories and methods in statistical signal processing for basic and applied neuroscience problems.Written by experts in ... (*AN 344981*), Database: eBook Collection (EBSCOhost)

Subjects: SCIENCE / Life Sciences / Neuroscience; TECHNOLOGY & ENGINEERING / Signals & Signal Processing; Signal processing--Digital techniques; Electroencephalography; Brain mapping

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 244

29. ## Fuzzy-System-**Based** Detection of Pupil Center and Corneal Specular Reflection for a Driver-Gaze Tracking System **Based** on the Symmetrical Characteristics of Face and Facial Feature Points.

By: Dong Eun Lee; Hyo Sik Yoon; Hyung Gil Hong; Kang Ryoung Park.
Symmetry (20738994). Nov2017, Vol. 9 Issue 11, p267. 31p. Abstract: Recently, many studies have actively dealt with the issue of driver-gaze tracking for monitoring the forward gaze and physical condition. Driver-gaze tracking is an effective method of measuring a driver's inattention that is one of the major causes of traffic accidents. Among many gaze-tracking methods, the corneal specular reflection (SR)-**based** method becomes ineffective, unlike in an indoor environment, when a driver's head rotates, which makes SR disappear from input images or disperses SR in the lachrymal gland or eyelid, thereby increasing the gaze-tracking error. Besides, since a driver's eyes in a vehicle environment need to be captured in a wide range covering his head rotation, the eye region is captured in a relatively low resolution compared to face-only images taken in indoor environments at the same resolution, making pupil and corneal SR difficult to detect accurately. To solve these problems, we propose a fuzzy-system-**based** method for detecting a driver's pupil and corneal SR for gaze tracking in a vehicle environment. Unlike existing studies detecting pupil and corneal SR in both eyes, the method proposed in this research uses the results of a fuzzy system **based** on two features considering the symmetrical characteristics of face and facial feature points to determine the status of a driver's head rotation. **Based** on the output of the fuzzy system, the proposed method excludes the eye region, which is very likely to have a high error rate of detection due to excessive head rotation, from the detection process of the pupil and corneal SR. Accordingly, the proposed method detects pupil and corneal SR only in the eye region that apparently has a low detection error rate, thereby achieving accurate detection. We use 20,654 images capturing 15 subjects (including subjects wearing glasses), who gaze at pre-set fifteen regions in a vehicle, to measure the detection accuracy of the pupil and corneal SR for each region and the gaze tracking accuracy. Our experimental results show that the proposed method performs better than existing methods. [ABSTRACT FROM AUTHOR] DOI: 10.3390/sym9110267. (*AN: 126425065*), Database: Academic Search Complete

Subjects: PUPIL (Eye); **BIOMETRIC** eye scanning systems; **BIOMETRIC** identification; IRIS recognition; FUZZY systems

PDF Full Text (7.4MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 245

30. ## On Computing : The Fourth Great Scientific Domain

By: Rosenbloom, Paul S. Cambridge, Mass : The MIT Press. 2013. eBook. Description: A proposal that computing is not merely a form of engineering but a scientific domain on a par with the physical, life, and social sciences.Computing is not simply about hardware or software, or calculation or applications. Computing, writes Paul Rosenbloom, is an exciting and diverse, yet remarkably coherent, scientific enterprise that is highly multidisciplinary yet maintains a unique core of its own. In On Computing, Rosenbloom proposes that computing is a great scientific domain on a par with ... (*AN 504117*), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Computer Science; COMPUTERS / Social Aspects; Computer science--Research; Computer science; Computer science--Philosophy

PDF Full Text **EPUB Full Text** **USPTO Full Text Options**

Full Download

Table of Contents Most Relevant Pages From This eBook

EBSCO Connect | Privacy Policy | A/B Testing | Terms of Use | Copyright | Cookie Policy | Contact Us

powered by EBSCO*host*

© 2020 EBSCO Industries, Inc. All rights reserved.

IPR2025-01313; Samsung
Ex. 1002 - Page 246

STIC
Scientific and Technical Information Center

1. **INFORMATION** PROCESSING METHOD AND **DEVICE** BASED ON INTERNET OF THINGS

Patent Application: 16/586796. Filed: September 27, 2019. Published: January 23, 2020. , Database: USPTO Patent Applications

Abstract: Embodiments of the application provide **information** processing systems, methods and **devices** based on Internet of Things. An **information** processing system comprises a server **device**, a **first device** and a second **device**. The **first device** and second **device** are both an Internet of Things **device**. The **first device** is configured to: in response to detecting that a **first acquisition** instruction is triggered, acquire **biometric** feature **information**, and send the acquired **biometric** feature **information** to the server **device**. The server **device** is configured to identify a user corresponding to the **biometric** feature **information**. The second **device** is configured to: in response to detecting that a second **acquisition** instruction is triggered, acquire body movement **information** associated with the user, and send the acquired body movement **information** to the server **device**. The server **device** is further configured to perform an operation for the user according to the body movement **information**.

AN: edspap.20200026839

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 247

2. Patent Application Titled '**Information** Processing **Device**, Application Software Start-Up System, And Application Software Start-Up Method' Published Online (USPTO 20190362061)

In: **Information** Technology Newsweekly, Dec 17, 2019, 2279; NewsRX LLC
Language: English. Abstract: 2019 DEC 17 (VerticalNews) -- By a News Reporter-Staff News Editor at **Information** Technology Newsweekly -- According to news reporting originating from Washington, D.C., by VerticalNews journalists, a patent application [...] (*AN: edsgcl.608720217*), Database: Gale General OneFile

Subjects: Japan; Software quality; Software -- Methods; Software -- Intellectual property; Control equipment -- Methods; Control equipment -- Intellectual property

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 248

3. UNIVERSAL ID SYSTEM AND METHODS AND **BIOMETRIC INFORMATION**

Patent Application: 16/164822. Filed: October 19, 2018. Published: March 28, 2019. , Database: USPTO Patent Applications

Abstract: A method is provided of conducting an interaction between a **first** entity and a second entity. A Universal ID system includes a front end with a transmitter, a receiver coupled to the transmitter and at least one passive filter coupled to the transmitter. The front-end is coupled to at least one of a back-end or a cloud system. Each of the back-end and the cloud system includes: storage; server; a Universal ID character generator **device** that generates portions of the Universal ID. In response to an interaction between the **first** entity and a second entity he transmitter transmits a signal for all or a portion of a **first** entity Universal ID that includes non-permanent IDs and permanent IDs. The Universal ID includes and/or is layered with **biometric** identifiers of the **first** entity. The signal includes a plurality of authentications with identifiers. Each of an authentication associated with a different second entity. The **first** party Universal ID is used with a plurality of electronic **devices** that each have a different **first** entity authentication from the Universal ID with each of a different electronic **device** requiring a **first** entity authentication to gain access to each of an electronic **device** of the plurality of electronic **devices**. The signal provides an authentication of the Universal ID to a second entity and is done passivity where the **first** entity takes no action for the **first** entity Universal ID signal to be emitted, and for an interaction to be sensed and acted on by an action, in response to the interaction the second entity creates an action that causes a physical change in a hardware component of a second entity electronic **device**.

AN: edspap.20190098004

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 249

4. ELECTRONIC **DEVICE** AND METHOD OF OPERATING SAME

Patent Application: 15/397074. Filed: January 03, 2017. Published: July 6, 2017. , Database: USPTO Patent Applications

Abstract: Disclosed are an electronic **device** and a method of operating the same. The electronic **device** may include a touch screen; a communication interface comprising communication circuitry; and a processor functionally connected to the communication circuitry of the communication interface, wherein the processor may be configured to receive execution **information** usable for authenticating at least one resource of a second external **device** from a **first** external **device** through the communication circuitry of the communication interface, to display a user interface configured to acquire **biometric information** of a user through the touch screen in response to receiving the execution **information**, to generate virtual **biometric information** based on the acquired **biometric information**, and to transmit the virtual **biometric information** to the second external **device** through the communication circuitry of the communication interface wherein the virtual **biometric information** is usable for authenticating the at least one resource.

AN: edspap.20170193314

USPTO Full Text Options

5. ELECTRONIC **DEVICE** AND METHOD FOR CONTROLLING DISPLAY UNIT INCLUDING A **BIOMETRIC SENSOR**

Patent Application: 15/862720. Filed: January 05, 2018. Published: July 12, 2018. , Database: USPTO Patent Applications

Abstract: The present disclosure relates to an electronic **device** and a method for controlling a display that includes a **biometric sensor**. The electronic **device** may include: a display including a **first** area having a **first** pixel controlled by a **first** signal and powered by a **first** power supply and a second area having a second pixel controlled by a second signal and powered by a second power supply; and a **biometric sensor** disposed in the **first** area and configured to acquire **biometric information**.

AN: edspap.20180196931

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 250

6. Selfie **Biometrics** : Advances and Challenges

By: Ajita Rattani; Reza Derakhshani; Arun Ross. Series: Advances in Computer Vision and Pattern Recognition. Edition: **1st** ed. 2019. Cham : Springer, 2019. eBook. Description: This book highlights the field of selfie **biometrics**, providing a clear overview and presenting recent advances and challenges. It also discusses numerous selfie authentication techniques on mobile **devices**. **Biometric** authentication using mobile **devices** is becoming a convenient and important means of verifying identity for secured access and services such as telebanking and electronic transactions. In this context, face and ocular **biometrics** in the visible spectrum has gained increased attention from ... (*AN 2255532*), Database: eBook Index

Subjects: COMPUTERS / Artificial Intelligence / Computer Vision & Pattern Recognition; COMPUTERS / User Interfaces

Full Text Finder **USPTO Full Text Options**

7. AUTHENTICATION METHOD USING **BIOMETRIC INFORMATION** AND ELECTRONIC **DEVICE** THEREFOR

Patent Application: 14/969074. Filed: December 15, 2015. Published: June 16, 2016. , Database: USPTO Patent Applications
Abstract: An authentication method using **biometric information** and an electronic **device**. An authentication method using **biometric information** in an electronic **device** includes: receiving **biometric information** from an external electronic **device**. An authentication is performed for the received **biometric information** by comparing the received **biometric information** with **biometric information** stored in the electronic **device**. An authentication result us transmitted to the external electronic **device** such that the external electronic **device** performs a predesignated operation.
AN: edspap.20160173492

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 251

8. ## Consumer Grade EEG Measuring **Sensors** as Research Tools: A Review.

By: Sawangjai, Phattarapong; Hompoonsup, Supanida; Leelaarporn, Pitshaporn; Kongwudhikunakorn, Supavit; Wilaiprasitporn, Theerawit. *IEEE **Sensors** Journal* , 4/15/2020, Vol. 20 Issue 8, p3996-4024, 29p. Publisher: IEEE.; Abstract Since the launch of the **first** consumer grade EEG measuring **sensors** 'NeuroSky Mindset' in 2007, the market has witnessed an introduction of at least one new product every year by competing manufacturers, which include NeuroSky, Emotiv, interaXon and OpenBCI. There are numerous variations in the make and versions, but these products clearly share the key selling points of affordability, portability, and ease of use. These features are patently well placed provided one of the main objectives for their development is to attract a new target group of commercial users. Nevertheless, with several decades of traditional EEG usage in clinical and experimental settings, the shift toward commercial and engineering sides has not been achieved without skepticism. With this in mind, researchers in related fields have been tirelessly working to ensure that these putatively novel features were not introduced at the expense of efficiency and accuracy by conducting validation studies to compare the performance of data derived from consumer grade EEG **devices** with ones from standard research grade counterparts. In this review, we seek to provide the detail of the products supplied by the major players, summarize studies that evaluate consumer product's performance against research grade **devices**, the key areas of applications that these consumer grade **devices** have been employed in over the past five years or so, and finally give our perspectives on the limitations and what these innovative tools could offer going forward in terms of research and commercial applications. [ABSTRACT FROM AUTHOR]; (*AN 142343142*), Database: Complementary Index

Linked Full Text **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 252

9. ## Genomic and Personalized Medicine : V1-2

By: Willard, Huntington F.; Ginsburg, Geoffrey S. Edition: 2nd ed. London : Academic Press. 2013. eBook. Description: Genomic and Personalized Medicine, Second Edition —— winner of a 2013 Highly Commended BMA Medical Book Award for Medicine —— is a major discussion of the structure, history, and applications of the field, as it emerges from the campus and lab into clinical action. As with the **first** edition, leading experts review the development of the new science, the current opportunities for genome-based analysis in healthcare, and the potential of genomic medicine in future healthcare. The inclusion of the latest ... (*AN 485475*), Database: eBook Collection (EBSCOhost)

Subjects: SCIENCE / Life Sciences / Genetics & Genomics; MEDICAL / Pharmacology; Proteomics; Genomics; Medical genetics

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

10. ## Mobile **Biometrics**

By: Guo, Guodong; Wechsler, Harry. Series: The IET Book Series on Advances in **Biometrics**, Vol. 03. London : The Institution of Engineering and Technology. 2017. eBook. Description: Mobile **biometrics** - the use of physical and/or behavioral characteristics of humans to allow their recognition by mobile/smart phones - aims to achieve conventional functionality and robustness while also supporting portability and mobility, bringing greater convenience and opportunity for its deployment in a wide range of operational environments from consumer applications to law enforcement. But achieving these aims brings new challenges such as issues with power consumption, algorithm complexity, ... (*AN 1623761*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; **Biometric** identification; Computer security; Mobile computing

View record at Knovel **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 253

11. **Biometric**-Based Physical and Cybersecurity Systems

By: Obaidat, Mohammad S.; Traore, Issa; Woungang, Isaac. Cham, Switzerland : Springer. 2019. eBook. Description: This book presents the latest developments in **biometrics** technologies and reports on new approaches, methods, findings, and technologies developed or being developed by the research community and the industry. The book focuses on introducing fundamental principles and concepts of key enabling technologies for **biometric** systems applied for both physical and cyber security. The authors disseminate recent research and developing efforts in this area, investigate related trends and challenges, and present ... (*AN 1921993*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Electronics / General; COMPUTERS / Artificial Intelligence / Computer Vision & Pattern Recognition; COMPUTERS / Security / General; TECHNOLOGY & ENGINEERING / Engineering (General); **Biometric** identification

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 254

12. ## Press touch code: A finger press based screen size independent authentication scheme for smart devices.

By: Ranak, M. S. A. Noman; Azad, Saiful; Nor, Nur Nadiah Hanim Binti Mohd; Zamli, Kamal Z. *PLoS ONE.* 10/30/2017, Vol. 12 Issue 10, p1-20. 20p.

Abstract: Due to recent advancements and appealing applications, the purchase rate of smart **devices** is increasing at a higher rate. Parallely, the security related threats and attacks are also increasing at a greater ratio on these **devices**. As a result, a considerable number of attacks have been noted in the recent past. To resist these attacks, many password-based authentication schemes are proposed. However, most of these schemes are not screen size independent; whereas, smart **devices** come in different sizes. Specifically, they are not suitable for miniature smart **devices** due to the small screen size and/or lack of full sized keyboards. In this paper, we propose a new screen size independent password-based authentication scheme, which also offers an affordable defense against shoulder surfing, brute force, and smudge attacks. In the proposed scheme, the Press Touch (PT)—a.k.a., Force Touch in Apple's MacBook, Apple Watch, ZTE's Axon 7 phone; 3D Touch in iPhone 6 and 7; and so on—is transformed into a new type of code, named Press Touch Code (PTC). We design and implement three variants of it, namely mono-PTC, multi-PTC, and multi-PTC with Grid, on the Android Operating System. An in-lab experiment and a comprehensive survey have been conducted on 105 participants to demonstrate the effectiveness of the proposed scheme. [ABSTRACT FROM AUTHOR] DOI: 10.1371/journal.pone.0186940. (*AN: 125953219*), Database: Academic Search Complete

Subjects: BIOMETRIC identification; PASSWORDS (Computers); COMPUTER security; CYBERTERRORISM; ANDROID (Operating system)

PDF Full Text (8.3MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 255

13. ## Computer Engineering : Concepts, Methodologies, Tools and Applications

By: **Information** Resources Management Association. Hershey, Pa : IGI Global. 2012. eBook. Description: Features perspectives on the fundamental aspects, tools and technologies, methods and design, applications, managerial impact, social/behavioral perspectives, critical issues, and emerging trends in the field of computer engineering. *(AN 431988)*, Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Computer Engineering; COMPUTERS / Machine Theory; COMPUTERS / Hardware / General; Computer engineering

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

14. ## Handbook of Multimedia **Information** Security: Techniques and Applications

By: Singh, Amit Kumar; Mohan, Anand. Cham : Springer. 2019. eBook. Description: This handbook is organized under three major parts. The **first** part of this handbook deals with multimedia security for emerging applications. The chapters include basic concepts of multimedia tools and applications, biological and behavioral **biometrics**, effective multimedia encryption and secure watermarking techniques for emerging applications, an adaptive face identification approach for android mobile **devices**, and multimedia using chaotic and perceptual hashing function. The second part of this ... *(AN 2202581)*, Database: eBook Index

Subjects: COMPUTERS / Security / General; COMPUTERS / **Information** Technology; COMPUTERS / Interactive & Multimedia; COMPUTERS / Networking / Hardware; Computer security; Multimedia systems

Full Text Finder **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 256

15. Advances in Network-Based **Information** Systems : The 20th International Conference on Network-Based **Information** Systems (NBiS-2017)

By: Leonard Barolli; Tomoya Enokido; Makoto Takizawa. Series: Lecture Notes on Data Engineering and Communications Technologies. Cham, Switzerland : Springer, 2018. eBook. Description: This book highlights the latest research findings, innovative research results, methods and development techniques from both theoretical and practical perspectives related to the emerging areas of **information** networking and their applications. It includes the Proceedings of the 20th International Conference on Network-Based **Information** Systems (NBiS-2017), held on August 24 –26, 2017 in Toronto, Canada.Today's networks and **information** systems are evolving rapidly. Further, there are **dynamic** new trends ... (*AN 1583616*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Engineering (General); COMPUTERS / Artificial Intelligence / General; TECHNOLOGY & ENGINEERING / Telecommunications; **Information** networks--Congresses; Computer networks--Congresses; Network computers--Congresses

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 257

16. **Information** Governance : Concepts, Strategies and Best Practices

By: Smallwood, Robert F. Series: The Wiley CIO Series. Edition: Second edition. Hoboken, New Jersey : Wiley. 2019. eBook. Description: The essential guide to effective IG strategy and practice **Information** Governance is a highly practical and deeply informative handbook for the implementation of effective **Information** Governance (IG) procedures and strategies. A critical facet of any mid- to large-sized company, this "super-discipline" has expanded to cover the management and output of **information** across the entire organization; from email, social media, and cloud computing to electronic records and documents, the IG umbrella now ... (*AN 2319528*), Database: eBook Index

Subjects: BUSINESS & ECONOMICS / **Information** Management; **Information** technology--Management; Management **information** systems; Electronic records--Management

Full Text Finder USPTO Full Text Options

17. Elementary **Information** Security

By: SMITH, RICHARD E. [Place of publication not identified] : Jones & Bartlett Learning. 2019. eBook. Description: An ideal text for introductory **information** security courses, the third edition of Elementary **Information** Security provides a comprehensive yet easy-to-understand introduction to the complex world of cyber security and technology. Thoroughly updated with an increased emphasis on mobile **devices** and technologies, this essential text enables students to gain direct experience by analyzing security problems and practicing simulated security activities. Emphasizing learning through experience, Elementary ... (*AN 2227834*), Database: eBook Index

Subjects: COMPUTERS / Security / Network Security; Computer networks--Security measures; Computer security

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 258

18. ## Iris and Periocular **Biometric** Recognition

By: Rathgeb, Christian. Series: IET Security Series, Vol. 05. Stevenage, UNKNOWN : The Institution of Engineering and Technology. 2017. eBook. Description: Iris recognition technologies for identity management are already deployed globally in several large-scale nationwide **biometric** projects and are currently entering the mobile market. More recently, periocular recognition has been employed to augment the **biometric** performance of the iris in unconstrained environments where only the ocular region is present in the image.Iris and Periocular **Biometric** Recognition provides an overview of scientific fundamentals and principles of iris and periocular **biometric** ... (*AN 1585200*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; **Biometric** identification

View record at Knovel **USPTO Full Text Options**

19. ## Deep Learning in **Biometrics**

By: Vatsa, Mayank; Singh, Richa; Majumdar, Angshul. Edition: **First** edition. Boca Raton, FL : CRC Press. 2018. eBook. Description: Deep Learning is now synonymous with applied machine learning. Many technology giants (e.g. Google, Microsoft, Apple, IBM) as well as start-ups are focusing on deep learning-based techniques for data analytics and artificial intelligence. This technology applies quite strongly to **biometrics**. This book covers topics in deep learning, namely convolutional neural networks, deep belief network and stacked autoencoders. The focus is also on the application of these techniques to various **biometric** modalities: ... (*AN 1728832*), Database: eBook Index

Subjects: COMPUTERS / Data Science / Data Analytics; COMPUTERS / Machine Theory; TECHNOLOGY & ENGINEERING / Imaging Systems; TECHNOLOGY & ENGINEERING / Biomedical; **Biometric** identification

Full Text Finder **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 259

20. The Science of **Biometrics** : Security Technology for Identity Verification

By: Das, Ravindra. New York, NY : Routledge. 2018. eBook. Description: The Science of **Biometrics**: Security Technology for Identity Verification covers the technical aspects of iris and facial recognition, focusing primarily on the mathematical and statistical algorithms that run the verification and identification processes in these two modalities. Each chapter begins with a review of the technologies, examining how they work, their advantages and disadvantages, as well as some of their established market applications. Numerous approaches are examined. Facial recognition ... (*AN 1776879*), Database: eBook Index

Subjects: COMPUTERS / Software Development & Engineering / General; COMPUTERS / Security / General; POLITICAL SCIENCE / Security (National & International); SOCIAL SCIENCE / Criminology; **Biometric** identification

Full Text Finder USPTO Full Text Options

21. **Biometrics** in Identity Management : Concepts to Applications

By: Modi, Shimon K. Series: Artech House **Information** Security and Privacy Series. Boston : Artech House. 2011. eBook. Description: In today's digital infrastructure we have to interact with an increasing number of systems, both in the physical and virtual world. Identity management (IdM) -- the process of identifying an individual and controlling access to resources based on their associated privileges -- is becoming progressively complex. This has brought the spotlight on the importance of effective and efficient means of ascertaining an individual's identity. **Biometric** technologies like fingerprint recognition, face recognition, ... (*AN 416001*), Database: eBook Index

Subjects: NATURE / Reference; SCIENCE / Life Sciences / Biology; SCIENCE / Life Sciences / General; **Biometric** identification; **Biometric** identification--Technological innovations; Identification--Data processing

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 260

22. **Biometric** Security

By: Ling Ngo, David Chek; Jin Teoh, Andrew Beng; Hu, Jiankun. Newcastle upon Tyne, England : Cambridge Scholars Publishing. 2015. eBook. Description: Modern **biometrics** delivers an enhanced level of security by means of a "proof of property". The design and deployment of a **biometric** system, however, hide many pitfalls, which, when underestimated, can lead to major security weaknesses and privacy threats. Issues of concern include **biometric** identity theft and privacy invasion because of the strong connection between a user and his identity. This book showcases a collection of comprehensive references on the advances of **biometric** security technology. ... (*AN 960122*), Database: eBook Index

Subjects: NATURE / Reference; SCIENCE / Life Sciences / Biology; SCIENCE / Life Sciences / General; **Biometric** identification; Security systems

Full Text Finder USPTO Full Text Options

23. Human Recognition in Unconstrained Environments : Using Computer Vision, Pattern Recognition and Machine Learning Methods for **Biometrics**

By: De Marsico, Maria; Nappi, Michele; Proença, Hugo. London : Academic Press. 2017. eBook. Description: Human Recognition in Unconstrained Environments provides a unique picture of the complete 'in-the-wild'**biometric** recognition processing chain, from data **acquisition** through to detection, segmentation, encoding, and matching reactions against security incidents. Coverage includes: Data hardware architecture fundamentalsBackground subtraction of humans in outdoor scenes Camera synchronizationBiometric traits: Real-time detection and data segmentationBiometric traits: Feature encoding / matching Fusion ... (*AN 1144731*), Database: eBook Index

Subjects: COMPUTERS / Image Processing; COMPUTERS / Artificial Intelligence / Computer Vision & Pattern Recognition; Machine learning; Computer vision; **Biometric** identification; Pattern recognition systems

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 261

24. ## Pulse mode of operation – A new booster of TEG, improving power up to X2.7 – to better fit IoT requirements

By Haras, Maciej; Markiewicz, Michał; Monfray, Stéphane; Skotnicki, Thomas. In *Nano Energy*. February 2020 68 Language: English. DOI: 10.1016/j.nanoen.2019.104204 Abstract: Internet of Things (IoT) is becoming the new driver for semiconductor industry and the largest electronic market ever seen. The number of IoT nodes is already many times larger than the human population and is continuously growing. It is thus mandatory that IoT nodes become self-supplying with energy harvested from environment since periodic exchange of batteries in such a huge number of units (often located in inaccessible places e.g. industrial environment or elements of constructions) is impractical and soon will be simply impossible. Photovoltaic generators may easily harvest energy where light is available, but the IoT nodes often work in dark, hidden locations where the only available energy sources are heat losses. There, ThermoElectric Generators (TEGs) could be the best candidate, if not that if we speak of exploiting heat losses it often means very low temperature differences. This means conditions where TEGs power production drops down dramatically. In this paper we put forward a new idea of TEG's pulse operation that boosts the power production up to X2.7. This extends the domain of applicability of TEGs to lower temperature differences, where conventional TEGs are out of the game. Next, we show that the improvement X2.7 maintains also at larger temperature differences that presents obvious advantages. (*AN: S2211285519309115*), Database: ScienceDirect

Subjects: Internet of things (IoT); Heat energy harvesting; Thermoelectricity; Power boost; Pulse operation; Bimetal

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 262

25. **Information** and Communication Technology : Proceedings of ICICT 2016

By: Mishra, Durgesh Kumar; Azar, Ahmad Taher; Joshi, Amit. Series: Advances in Intelligent Systems and Computing, volume 625. Singapore : Springer. 2018. eBook. Description: This book volume contains 31 papers presented at ICICT 2016: Second International Congress on **Information** and Communication Technology. The conference was held during 12-13 December 2016, Bangkok, Thailand and organized communally by G R Foundation, and Computer Society of India Division IV – Communication and Division V – Education and Research. This volume contains papers mainly focused on ICT for computation, algorithms and data analytics, and IT security. (*AN 1614958*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; COMPUTERS / Data Science / Data Analytics; COMPUTERS / Security / General; Computer networks--Congresses; **Information** technology--Congresses

Full Text Finder USPTO Full Text Options

26. Managing Medical **Devices** Within a Regulatory Framework

By: Fiedler, Beth Ann. Amsterdam : Elsevier. 2018. eBook. Description: Managing Medical **Devices** within a Regulatory Framework helps administrators, designers, manufacturers, clinical engineers, and biomedical support staff to navigate worldwide regulation, carefully consider the parameters for medical equipment patient safety, anticipate problems with equipment, and efficiently manage medical **device acquisition** budgets throughout the total product life cycle. This contributed book contains perspectives from industry professionals and academics providing a comprehensive ... (*AN 1144633*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Biomedical; LAW / Commercial / General; Medical instruments and apparatus--Management

View record at Knovel USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 263

27. ## Handbook of **Biometrics**

By: Ross, Arun A.; Flynn, Patrick J.; Jain, Anil K. New York : Springer. 2008. eBook. Description: **Biometrics** is a rapidly evolving field with applications ranging from accessing one's computer to gaining entry into a country. The deployment of large-scale **biometric** systems in both commercial and government applications has increased public awareness of this technology. Recent years have seen significant growth in **biometric** research resulting in the development of innovative **sensors**, new algorithms, enhanced test methodologies and novel applications. This book addresses this void by inviting some ... (*AN 254816*), Database: eBook Index

Subjects: COMPUTERS / Artificial Intelligence / Computer Vision & Pattern Recognition; COMPUTERS / Software Development & Engineering / Computer Graphics; COMPUTERS / **Information** Theory; COMPUTERS / Interactive & Multimedia; COMPUTERS / Security / General; Identification--Automation; Pattern recognition systems; **Biometric** identification

Full Text Finder **USPTO Full Text Options**

28. ## Strengths, weaknesses and recommendations in implementing **biometrics** in mobile **devices**.

By: Sanchez-Reillo, Raul; Sierra-Ramos, Daniel; Estrada-Casarrubios, Roberto; Amores-Duran, Jose A.. *2014 International Carnahan Conference on Security Technology (ICCST)* , 2014, p1-6, 6p. Publisher: IEEE. (*AN 101243179*), Database: Complementary Index

Get Full Text at IEEE *Xplore*® **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 264

29. ## Proceedings of International Conference on Computer Vision and Image Processing : CVIP 2016, Volume 1

By: Raman, Balasubramanian; Kumar, Sanjeev; Roy, Partha Pratim; Sen, Debashis. Series: Proceedings of International Conference on Computer Vision and Image Processing, Volume 1. Singapore : Springer. 2017. eBook. Description: This edited volume contains technical contributions in the field of computer vision and image processing presented at the First International Conference on Computer Vision and Image Processing (CVIP 2016). The contributions are thematically divided based on their relation to operations at the lower, middle and higher levels of vision systems, and their applications. The technical contributions in the areas of **sensors**, **acquisition**, visualization and enhancement are classified as related to low-level ... (*AN 1443961*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Electronics / General; COMPUTERS / Software Development & Engineering / Computer Graphics; COMPUTERS / Artificial Intelligence / Computer Vision & Pattern Recognition; Image processing--Digital techniques--Congresses; Computer vision--Congresses; Engineering; Biometry; Image processing

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 265

30. Inventive Communication and Computational Technologies : Proceedings of ICICCT 2019

By: G. Ranganathan; Joy Chen; Álvaro Rocha. Series: Lecture Notes in Networks and Systems, Vol. 89. Edition: 1st ed. 2020. Singapore : Springer. 2020. eBook. Description: This book gathers selected papers presented at the Inventive Communication and Computational Technologies conference (ICICCT 2019), held on 29–30 April 2019 at Gnanamani College of Technology, Tamil Nadu, India. The respective contributions highlight recent research efforts and advances in a new paradigm called ISMAC (IoT in Social, Mobile, Analytics and Cloud contexts). Topics covered include the Internet of Things, Social Networks, Mobile Communications, Big Data Analytics, Bio-inspired Computing ... (*AN 2364338*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; BUSINESS & ECONOMICS / Industries / Computers & **Information** Technology; COMPUTERS / Artificial Intelligence / General; TECHNOLOGY & ENGINEERING / Mobile & Wireless Communications; COMPUTERS / Programming / Mobile **Devices**

Full Text Finder USPTO Full Text Options

EBSCO Connect | Privacy Policy | A/B Testing | Terms of Use | Copyright | Cookie Policy | Contact Us

powered by EBSCO*host*

© 2020 EBSCO Industries, Inc. All rights reserved.

IPR2025-01313; Samsung
Ex. 1002 - Page 266

STIC
Scientific and Technical Information Center

1. Patent Application Titled '**Information** Processing Device, Application Software Start-Up System, And Application Software Start-Up Method' Published Online (USPTO 20190362061)

In: **Information** Technology Newsweekly, Dec 17, 2019, 2279; NewsRX LLC
Language: English. Abstract: 2019 DEC 17 (VerticalNews) -- By a News Reporter-Staff News Editor at **Information** Technology Newsweekly -- According to news reporting originating from Washington, D.C., by VerticalNews journalists, a patent application [...] (*AN: edsgcl.608720217*), Database: Gale General OneFile

Subjects: Japan; Software quality; Software -- Methods; Software -- Intellectual property; Control equipment -- Methods; Control equipment -- Intellectual property

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 267

2. ## Cybersecurity challenges in vehicular **communications**

By El-Rewini, Zeinab; Sadatsharan, Karthikeyan; Selvaraj, Daisy Flora; Plathottam, Siby Jose; Ranganathan, Prakash. In *Vehicular Communications*. June 2020 23 Language: English. DOI: 10.1016/j.vehcom.2019.100214 Abstract: As modern vehicles are capable to connect to an external infrastructure and Vehicle-to-Everything (V2X) **communication** technologies mature, the necessity to secure **communications** becomes apparent. There is a very real risk that today's vehicles are subjected to cyber-attacks that target vehicular **communications**. This paper proposes a three-layer framework (sensing, **communication** and control) through which automotive security threats can be better understood. The sensing layer is made up of vehicle **dynamics** and environmental sensors, which are vulnerable to eavesdropping, jamming, and spoofing attacks. The **communication** layer is comprised of both in-vehicle and V2X **communications** and is susceptible to eavesdropping, spoofing, man-in-the-middle, and sybil attacks. At the top of the hierarchy is the control layer, which enables autonomous vehicular functionality, including the automation of a vehicle's speed, braking, and steering. Attacks targeting the sensing and **communication** layers can propagate upward and affect the functionality and can compromise the security of the control layer. This paper provides the state-of-the-art review on attacks and threats relevant to the **communication** layer and presents countermeasures. (*AN: S221420961930261X*), Database: ScienceDirect

Subjects: Cyber-physical systems; Security; Vehicle safety; Cyber-attacks; Vehicle-to-vehicle

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 268

3. ## Design of secure **authentication** protocol for **dynamic** user addition in distributed Internet-of-Things

By Trivedi, Hiral S.; Patel, Sankita J.. In *Computer Networks*. 4 September 2020 178 Language: English. DOI: 10.1016/j.comnet.2020.107335 Abstract: Rapid rise in adoption of smart devices in distributed Internet-of-things (IoT) has resulted in an exponential increase in volume of generated data. However, due to resource-constrained sensor nodes and vulnerable **communication** channels, **information** protection has become a key concern and prominent factor for improvement in IoT environment. Batch processing systems have several shortcomings as compared to distributed systems. Distributed systems enable **dynamic** changes in the potential number of sensors, actuators, RFID's, resources, users and subjects to tolerate unbounded interruptions in **communication** patterns. In this paper, we address the key challenges of **communication** security and scalability in IoT environment. We hypothesize distributed IoT approach between non-identical entities to communicate through secure **authentication** protocol for dynamically adding new user with partially involved trusted third party (TTP) as our module 1 and attribute based encryption scheme for non-identical smart entities to communicate securely as our module 2. We discuss module 1 in this paper. The existing approaches that focus on fully trusted central authority having full rights lead to serious weakness in violating security rules, while multi-authority based systems display revocation and compulsory user participation issues. As ideal functionalities we view TTP as honest-but-curious, honestly following the protocol while on the other hand curious to decrypt the cipher-text to breach the intention of encrypting parties. This motivates us to design an approach which jointly achieves effective **authentication** and partial trust management with scalability in distributed IoT environment. In accordance, we propose a novel **authentication** scheme with partially involved TTP nomenclatured Secure **Dynamic** User Addition Protocol (SDUAP) based on JWT (JSON Web Token) challenge and response game using symmetric key cryptography. The security of SDUAP is proved under real or random oracle model and its robustness against several attacks is verified using scyther security verification tool. We also compare performance of SDUAP with relatively similar modeled schemes in terms of **communication**, computation and storage overheads. The purpose of this paper is to mitigate the complications associated with scalability and curious/suspicious third party in distributed IoT approaches. (*AN: S1389128619316949*), Database: ScienceDirect

Subjects: Distributed IoT; Secure **authentication**; Partially involved TTP; **Dynamic** user addition; Scalability

IPR2025-01313; Samsung
Ex. 1002 - Page 269

Full Text Finder USPTO Full Text Options

4. Handbook of Green **Information** and **Communication** Systems

By: Woungang, Isaac; Anpalagan, Alagan; Obaidat, Mohammad S. Amsterdam : Academic Press, 2013. eBook. Description: This book gives a comprehensive guide on the fundamental concepts, applications, algorithms, protocols, new trends and challenges, and research **results** in the area of Green **Information** and **Communications** Systems. It is an invaluable resource giving knowledge on the core and specialized issues in the field, making it highly suitable for both the new and experienced researcher in this area. Key Features: Core research topics of green **information** and **communication** systems are covered from a network ... (*AN 485200*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Signals & Signal Processing; SCIENCE / Environmental Science; Sustainable engineering--Handbooks, manuals, etc; Telecommunication--Environmental aspects--Handbooks, manuals, etc; Telecommunication--Energy conservation--Handbooks, manuals, etc

PDF Full Text USPTO Full Text Options Full Download

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 270

5. ## Optimized in-network **authentication** against pollution attacks in software-defined-named data networking

By Boussaha, Ryma; Challal, Yacine; Bouabdallah, Abdelmadjid; Bessedik, Malika. In *Journal of Information Security and Applications*. February 2020 50 Language: English. DOI: 10.1016/j.jisa.2019.102409 Abstract: The exponential growth of multimedia content in today's internet traffic and the increasing need of bandwidth-consuming or location-independent services motivated the research community to design a viable replacement for the current IP-based Internet architecture. Named Data Networking or NDN is a novel network architecture that uses universal in-network caching and routing by name functionalities to deliver content efficiently and to improve service quality. Network coding benefits named data networking with its inherent algebraic structure and the maximum flow rates performance it achieves in multicast. With network coding, the content can be requested via multiple **interfaces** thus improving significantly content delivery efficiency. However, it is vulnerable to pollution attacks, which can cause a crucial degradation of network bandwidth. In this paper, we propose an efficient and optimized **authentication** technique for a content distribution NDN architecture based on network coding. Our solution uses homomorphic signature mechanism, which allows intermediate nodes to verify the authenticity of flows to overcome the pollution problem without having access to content. We formulate NDNAuth, an optimal coding and homomorphic signature scheme as a MIP problem. Furthermore, we show how to leverage Software Defined Networking to provide seamless implementation of the proposed solution. We measure the processing overhead and the **dynamic** system security state based on three metrics: (1) defence power; (2) threat severity and (3) system vulnerability. Finally, we discuss how to minimize the computational cost of coding and signature scheme operations. Experimentation **results** prove the efficiency of the proposed coding scheme, which achieves better performance than conventional NDN with random coding especially in terms of transmission cost and security. (*AN: S2214212619302790*), Database: ScienceDirect

Subjects: Named data networking; Network coding; Software defined networking; Homomorphic signature

Full Text Finder USPTO Full Text Options

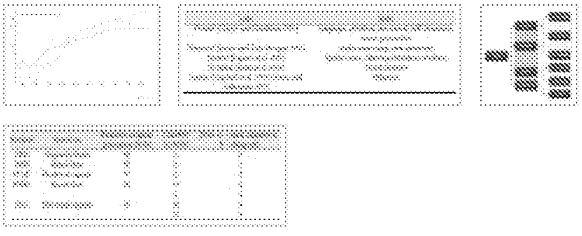
IPR2025-01313; Samsung
Ex. 1002 - Page 271

6. ## Mind Your Mind: EEG-Based Brain-Computer **Interfaces** and Their Security in Cyber Space.

By: LANDAU, OFIR; PUZIS, RAMI; NISSIM, NIR. *ACM Computing Surveys* , Feb2020, Vol. 53 Issue 1, p1-38, 38p Abstract. A brain-computer **interface** (BCI) system is a system that leverages brainwave **information** acquired by a designated brain monitoring device to interact with a computerized system. Over the past 40 years, many BCI applications have been developed in a variety of domains, from entertainment to medical field and even to computer securitymechanisms. Until now, the development of BCI systems has focused on improving their accuracy, functionality, and ease of use, and not enough effort and attention has been invested in securing these systems and the sensitive data they acquire. In this article, we present the principles of brain activity data acquisition, with a special focus on EEG, and we present a taxonomy of BCI applications and domains. We also provide a comprehensive survey that covers eight possible attacks aimed at BCI systems. For each BCI application, we created an ecosystem and data and attack flow-diagram, which comprehensively describes the roles and interactions of the players associated with the BCI application and presents the most vulnerable vectors and components within its ecosystem; we identified gaps between existing security solutions and the presented attacks and vulnerabilities. Finally, we provide several concrete suggestions for improving the security of BCI systems in cyber-space. [ABSTRACT FROM AUTHOR]; DOI: 10.1145/3372043; (*AN 141670891*), Database: Applied Science & Technology Source

Subjects: Brain-computer **interfaces**; Internet security; Acquisition of data; Security systems; Systems development; Electroencephalography; Wired Telecommunications Carriers; Internet Publishing and Broadcasting and Web Search Portals; Security Systems Services (except Locksmiths); Brain

Show all 16 Images



PDF Full Text (6.2MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 272

7. ## Efficient and Secure **Biometric**-Based User Authenticated Key Agreement Scheme with Anonymity.

By: Kang, Dongwoo; Jung, Jaewook; Kim, Hyoungshick; Lee, Youngsook; Won, Dongho. *Security & **Communication** Networks* , 6/20/2018, p1-14, 14p

Abstract: At present, a number of users employ an **authentication** protocol so as to enjoy protected electronic transactions in wireless networks. In order to establish an efficient and robust the transaction system, numerous researches have been conducted **relating** to **authentication** protocols. Recently, Kaul and Awasthi presented an user **authentication** and key agreement scheme, arguing that their scheme is able to resist various types of attacks and preserve diverse security properties. However, this scheme possesses critical vulnerabilities. **First**, the scheme cannot prevent two kinds of attacks, including off-line password guessing attacks and user impersonation attacks. **Second**, user anonymity rule cannot be upheld. Third, session key can be compromised by an attacker. Fourth, there is high possibility that the time synchronization trouble occurs. Therefore, we suggest an upgraded version of the user authenticated key agreement method that provides enhanced security. Our security and performance analysis shows that compared, to other associated protocols, our method not only improves the security level but also ensures efficiency. [ABSTRACT FROM AUTHOR]; DOI: 10.1155/2018/9046064; (*AN 130253394*), Database: Applied Science & Technology Source

Subjects: Biometric identification; Computer access control; **Information** & **communication** technologies; Cryptography; Passwords (Computers)

HTML Full Text **PDF Full Text** (2.9MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 273

8. ## Securing internet of medical things systems: Limitations, issues and recommendations

By Yaacoub, Jean-Paul A.; Noura, Mohamad; Noura, Hassan N.; Salman, Ola; Yaacoub, Elias; Couturier, Raphaël; Chehab, Ali. In *Future Generation Computer Systems*. April 2020 105:581-606 Language: English. DOI: 10.1016/j.future.2019.12.028 Abstract: Traditional health-care systems suffer from new challenges associated with the constant increase in the number of patients. In order to address this issue, and to increase the accuracy, reliability, efficiency, and effectiveness of the health-care domain, the Internet of Medical Things (IoMT) was proposed. IoMT can be considered as an enhancement and investment to respond more effectively and efficiently to patients' needs. However, IoMT suffers from different issues and challenges such as the lack of security and privacy measures, in addition to the necessary training and awareness. In this paper, we highlight the importance of implementing the right security measures and the required training skills, in order to enhance the immunity of IoMT against cyber-attacks. Moreover, we review the main IoMT security and privacy issues, and the existing security solutions. These solutions are classified as cryptographic or non-cryptographic. Then, the different solutions are analyzed and compared in terms of computational complexity and required resources. It is important to note that the security measures for IoMT exhibit a trade-off between the security level and the system performance, especially in the rise of digital healthcare v4.0 era. Next, we discuss the appropriate security solutions such as lightweight cryptographic algorithms, and protocols that attempt to reduce the overhead in terms of computations and resources. This leads to the conclusion that there is a need to design an efficient intrusion detection/prevention system that cooperates with dynamic shadow honeypots. Finally, we propose a security solution, which is divided into five different layers to detect and prevent attacks, in addition to reducing/correcting the damage of these known attacks and preserving the patients' privacy. However, it should be noted that zero-day attacks and exploits are still the main challenging issue that surrounds IoMT. (*AN: S0167739X19305680*), Database: ScienceDirect

Subjects: Healthcare; IoMT; Medical cyber physical systems; Medical devices

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 274

9. ELECTRONIC DEVICE AND METHOD FOR PROVIDING PAYMENT **INFORMATION**

Patent Application: 16/086393. Filed: March 23, 2017. Published: April 4, 2019. , Database: USPTO Patent Applications

Abstract: The present invention relates to a method for providing payment **information**, for example, to a device for providing payment **information** by using a sensor, and a method therefor. To this end, an electronic device, of the present invention, comprising a **first communication** circuit, a **second communication** circuit, a sensor, and a processor, can comprise the operations of: **receiving** a user input by using the sensor; **performing authentication** on the user input; **receiving** payment **information** from an external electronic device by using the **first communication** circuit when the **authentication** has been successful; and outputting the payment **information** through the **second communication** circuit when a complete event for the user input has been received from the sensor by using the processor.

AN: edspap.20190102770

USPTO Full Text Options

10. **Communication** service operating method and electronic device supporting the same

By: Samsung Electronics Co., Ltd. US Patent: 10038,790. Filed: October 29, 2015. Issued: July 31, 2018. , Database: USPTO Patent Grants

Abstract: An electronic device includes: a **first communication** module configured to perform a call signal based **communication** and a **second communication** module configured to perform a short range **communication** or wired **communication**; and a processor configured to control call signal reception processing of the **first communication** module, wherein when an operation change of a **communication** channel established based on the **second communication** module, based on at least one of a movement of an electronic device and a movement of a **second** electronic device that is connected through the **second communication** module or has a connection history, the processor allows the electronic device or the **second** electronic device to receive the call signal.

AN: edspgr.10038790

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 275

11. **Communication** service operating method and electronic device supporting the same

By: Samsung Electronics Co., Ltd. US Patent: 10009,470. Filed: October 29, 2015. Issued: June 26, 2018. , Database: USPTO Patent Grants

Abstract: An electronic device includes: a **first communication** module configured to perform a call signal based **communication** and a **second communication** module configured to perform a short range **communication** or wired **communication**; and a processor configured to control call signal reception processing of the **first communication** module, wherein when an operation change of a **communication** channel established based on the **second communication** module, based on at least one of a movement of an electronic device and a movement of a **second** electronic device that is connected through the **second communication** module or has a connection history, the processor allows the electronic device or the **second** electronic device to receive the call signal.

AN: edspgr.10009470

USPTO Full Text Options

12. Wireless Technologies : Concepts, Methodologies, Tools and Applications

By: **Information** Resources Management Association. Hershey, PA : IGI Global. 2012. eBook. (*AN 396408*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Mobile & Wireless **Communications**; TECHNOLOGY & ENGINEERING / Radio; Wireless **communication** systems; Telecommunication

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 276

13. ## Electronic device having loop antenna

By: SAMSUNG ELECTRONICS CO., LTD. US Patent: 10468,746. Filed: September 28, 2017. Issued: November 05, 2019. , Database: USPTO Patent Grants

Abstract: An electronic device includes a housing including a **first** surface facing in a **first** direction, a **second** surface facing in a **second** direction to the **first** direction, and a side member enclosing at least a portion of a space between the **first** surface and the **second** surface; a **first** metal plate positioned between the **first** surface and the **second** surface; a conductive coil positioned within the housing, having a shaft substantially perpendicular to the **first** direction or the **second** direction, and that winds around the **first** metal plate; a **first communication** circuit positioned within the housing and electrically connected to the conductive coil; a **second communication** circuit positioned within the housing and electrically connected to the **first** metal plate; a display exposed through at least a portion of the **first** surface; and a processor positioned within the housing and electrically connected to the **first communication** circuit, the **second communication** circuit, and the display. The **second** surface may include a **first** portion made of a conductive material and including a **first** opening and a **second** portion made of a non-conductive material and that fills the **first** opening. The conductive coil may be positioned under the **first** portion when viewed from above the **second** surface. A portion of the **first** metal plate may be wound with the conductive coil, and another portion of the **first** metal plate may be electrically connected to the **second communication** circuit. The another portion may extend to the **first** opening when viewed from above the **second** surface, a **first** magnetic flux may be generated in the conductive coil by the **first communication** circuit, and a **second** magnetic flux advancing in a direction perpendicular to an advancing direction of the **first** magnetic flux may be generated by the **second communication** circuit in the another portion of the **first** metal plate.

AN: edspgr.10468746

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 277

14. ## Wireless Multi-access Environments and Quality of Service Provisioning : Solutions and Application

By: Trestian, Ramona; Muntean, Gabriel-Miro. Hershey, Pa : IGI Global. 2012. eBook. Description: 'This book serves as a vital resource for practitioners to learn about the latest research and methodology within the field of wireless technology, covering important aspects of emerging technologies in the heterogeneous next generation network environment with a focus on wireless **communications** and their quality'--Provided by publisher. (*AN 420165*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Mobile & Wireless **Communications**; Wireless **communication** systems

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

15. ## Applied Signal and Image Processing : Multidisciplinary Advancements

By: Hines, Evor; Green, Roger; Qahwaji, Rami. Hershey, PA : IGI Global. 2011. eBook. Description: 'This book highlights the growing multidisciplinary nature of signal and image processing by focusing on emerging applications and recent advances in well-established fields, covering state-or-the-art applications in both signal and image processing, which include optical **communication** and sensing, wireless **communication** management, face recognition and facial imaging, solar imaging and feature detection, fractal analysis, and video processing'-- (*AN 362372*), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / **Information** Theory; TECHNOLOGY & ENGINEERING / Signals & Signal Processing; Wireless **communication** systems; Image processing; Signal processing; Image analysis

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 278

16. SYSTEMS AND METHODS FOR DATA **COMMUNICATION** OVER A PLURALITY OF DATA PATHS

Patent Application: 16/236061. Filed: December 28, 2018. Published: June 20, 2019. , Database: USPTO Patent Applications

Abstract: Systems and methods for data **communication** over a plurality of data paths are disclosed. Messages between a **first** node and a **second** node may be **transmitted**, wherein some of the messages are **transmitted** over a **first** data path using a **first communication** protocol, and some of the messages are **transmitted** over a **second** data path using a **second communication** protocol. A determination may be made that the **first** data path is altering a flow of messages due to the messages being **transmitted** using the **first communication** protocol and a number of messages sent over the different data paths adjusted in response, wherein adjusting comprises decreasing a number of the messages **transmitted** over the **first** data path and increasing a number of messages **transmitted** over the **second** data path, wherein altering the flow of messages is performed automatically under control of an expert system.

AN: edspap.20190187690

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 279

17. **Second** International Conference on Computer Networks and **Communication** Technologies : ICCNCT 2019

By: S. Smys; Tomonobu Senjyu; Pavel Lafata. Series: Lecture Notes on Data Engineering and **Communications** Technologies, Vol. 44. Edition: **1st** ed. 2020. Cham : Springer, 2020. eBook. Description: This book presents new **communication** and networking technologies, an area that has gained significant research attention from both academia and industry in recent years. It also discusses the development of more intelligent and efficient **communication** technologies, which are an essential part of current day-to-day life, and reports on recent innovations in technologies, architectures, and standards **relating** to these technologies. The book includes research that spans a wide range of **communication** ... (*AN 2358922*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; TECHNOLOGY & ENGINEERING / Engineering (General)

Full Text Finder **USPTO Full Text Options**

18. METHOD AND ELECTRONIC DEVICE FOR PROVIDING **COMMUNICATION** FUNCTION

Patent Application: 15/469791. Filed: March 27, 2017. Published: September 28, 2017. , Database: USPTO Patent Applications

Abstract: An electronic device is provided. The electronic device includes a **first communication** module configured to communicate with an external device through a **first communication** scheme, a **second communication** module configured to communicate with the external device through a **second communication** scheme, and a processor configured to identify a state of the **second communication** module, generate availability **information** indicating whether the **second communication** module is available to perform a same function with the **first communication** module, based on the state of the **second communication** module, and control the **first communication** module or the **second communication** module to transmit the availability **information** of the **second communication** module to the external device.

AN: edspap.20170280506

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 280

19. ## Applied Cryptography : Protocols, Algorithms and Source Code in C

By: Schneier, Bruce. Edition: **Second** edition, 20th anniversary edition. Indianapolis, IN : Wiley. 2015. eBook. Description: From the world's most renowned security technologist, Bruce Schneier, this 20th Anniversary Edition is the most definitive reference on cryptography ever published and is the seminal work on cryptography. Cryptographic techniques have applications far beyond the obvious uses of encoding and decoding **information.** For developers who need to know about capabilities, such as digital signatures, that depend on cryptographic techniques, there's no better overview than Applied Cryptography, the definitive ... (*AN 1535854*), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Security / Cryptography & Encryption; Cryptography; C (Computer program language)

EPUB Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 281

20. ## Proceedings of **First** International Conference on **Information** and **Communication** Technology for Intelligent Systems: Volume 2

By: Satapathy, Suresh Chandra; Das, Swagatam. Series: Proceedings of **First** International Conference on **Information** and **Communication** Technology for Intelligent Systems, Volume 2. Switzerland : Springer. 2016. eBook. Description: This volume contains 60 papers presented at ICTIS 2015: International Conference on **Information** and **Communication** Technology for Intelligent Systems. The conference was held during 28th and 29th November, 2015, Ahmedabad, India and organized communally by Venus International College of Technology, Association of Computer Machinery, Ahmedabad Chapter and Supported by Computer Society of India Division IV – **Communication** and Division V – Education and Research. This volume contains papers mainly focused ... (*AN 1181944*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Engineering (General); COMPUTERS / Artificial Intelligence / General; **Information** technology--Congresses; Computer networks--Congresses; Artificial intelligence--Congresses

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 282

21. Proceedings of **First** International Conference on **Information** and **Communication** Technology for Intelligent Systems: Volume 1

By: Satapathy, Suresh Chandra; Das, Swagatam. Series: Proceedings of **First** International Conference on **Information** and **Communication** Technology for Intelligent Systems, Volume 1. Switzerland : Springer. 2016. eBook. Description: This volume contains 59 papers presented at ICTIS 2015: International Conference on **Information** and **Communication** Technology for Intelligent Systems. The conference was held during 28th and 29th November, 2015, Ahmedabad, India and organized communally by Venus International College of Technology, Association of Computer Machinery, Ahmedabad Chapter and Supported by Computer Society of India Division IV – **Communication** and Division V – Education and Research. This volume contains papers mainly focused ... (*AN 1181945*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Engineering (General); COMPUTERS / Artificial Intelligence / General; **Information** technology--Congresses; Computer networks--Congresses; Artificial intelligence--Congresses

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 283

22. ## Technological aspects of WBANs for health monitoring: a comprehensive review.

By: Punj, Roopali; Kumar, Rakesh. *Wireless Networks (10220038)* , Apr2019, Vol. 25 Issue 3, p1125-1157, 33p Abstract: According to the World Health Organization, most of the world population is affected by chronic diseases, obesity, cardiovascular diseases and diabetes while another dominant problem is of aging population. Thus, it is desirable to have cost effective solutions for health monitoring, especially for countries that have minimum conventionally trained healthcare staff and infrastructure. Healthcare has shifted from hospital dominant services to patient dominant services which has thrived WBANs to provide ubiquitous health monitoring by virtue of wearable or implantable sensor nodes that commonly monitor biological signals. As the society becomes more health conscious, WBANs have the potential to revolutionize the way people integrate their health and **information** technology. Hence, WBANs are desired to strengthen conventional healthcare systems. Notwithstanding the current achievements, technological advances, proposed solutions and commercialized products, WBANs still experience many obstacles in their foolproof adoption. This paper surveys the plethora of WBAN applications and network architecture in detail used for data collection, data transmission and data analysis that form sensor analyst system in the realm of Internet of Things. Wireless communicational technologies are also discussed in this paper. Also, we have categorized the routing protocols and have provided with their critical qualitative analysis. Towards the end we discuss several projects in the field of WBANs and some open research areas. These findings on how the sensor nodes, newest routing protocols and data analysis techniques influence ubiquitous health monitoring sets this survey apart from the already existing surveys on WBANs. [ABSTRACT FROM AUTHOR]; DOI: 10.1007/s11276-018-1694-3; (*AN 134870254*), Database: Applied Science & Technology Source

Subjects: Medical informatics; Wireless sensor networks; Wireless sensor nodes; **Information** technology; World Health Organization

HTML Full Text **PDF Full Text** (1.4MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 284

23. CLOUD-BASED TRANSACTIONS METHODS AND SYSTEMS

Patent Application: 16/438178. Filed: June 11, 2019. Published: September 26, 2019. , Database: USPTO Patent Applications

Abstract: Systems and methods provide for **communication** of transaction data that is formatted according to a transaction type that is support by an access device. **First** transaction data may be formatted according to a **first** type of transaction supported by a **first** access device and **second** transaction data may be formatted according to a **second** type of transaction supported by a **second** access device. The **first** transaction data may be **transmitted** over a **first communication** link to the **first** access device and the **second** transaction data may be **transmitted** to the **second** access over a **second communication** link.

AN: edspap.20190295063

USPTO Full Text Options

24. **Information** and **Communication** Technology : Proceedings of ICICT 2016

By: Mishra, Durgesh Kumar; Azar, Ahmad Taher; Joshi, Amit. Series: Advances in Intelligent Systems and Computing, volume 625. Singapore : Springer. 2018. eBook. Description: This book volume contains 31 papers presented at ICICT 2016: **Second** International Congress on **Information** and **Communication** Technology. The conference was held during 12-13 December 2016, Bangkok, Thailand and organized communally by G R Foundation, and Computer Society of India Division IV -- **Communication** and Division V -- Education and Research. This volume contains papers mainly focused on ICT for computation, algorithms and data analytics, and IT security. (*AN 1614958*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; COMPUTERS / Data Science / Data Analytics; COMPUTERS / Security / General; Computer networks--Congresses; **Information** technology--Congresses

Full Text Finder **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 285

25. ## Proceedings of the **First** International Conference on Intelligent Computing and **Communication**

By: Mandal, Jyotsna Kumar; Satapathy, Suresh Chandra; Sanyal, Manas Kumar; Bhateja, Vikrant. Series: Advances in Intelligent Systems and Computing, v. 458. Singapore : Springer, 2017. eBook. Description: The book covers a wide range of topics in Computer Science and **Information** Technology including swarm intelligence, artificial intelligence, evolutionary algorithms, and bio-inspired algorithms. It is a collection of papers presented at the **First** International Conference on Intelligent Computing and **Communication** (ICIC2) 2016. The prime areas of the conference are Intelligent Computing, Intelligent **Communication**, Bio-informatics, Geo-informatics, Algorithm, Graphics and Image Processing, Graph Labeling, ... (*AN 1281875*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Engineering (General); COMPUTERS / Artificial Intelligence / General; COMPUTERS / Security / General; TECHNOLOGY & ENGINEERING / Telecommunications; Artificial intelligence--Congresses

Full Text Finder USPTO Full Text Options

26. ## **Communication** Service Operating Method and Electronic Device Supporting the Same

Patent Application: 14/927176. Filed: October 29, 2015. Published: May 5, 2016. , Database: USPTO Patent Applications

Abstract: An electronic device includes: a **first communication** module configured to perform a call signal based **communication** and a **second communication** module configured to perform a short range **communication** or wired **communication**; and a processor configured to control call signal reception processing of the **first communication** module, wherein when an operation change of a **communication** channel established based on the **second communication** module, based on at least one of a movement of an electronic device and a movement of a **second** electronic device that is connected through the **second communication** module or has a connection history, the processor allows the electronic device or the **second** electronic device to receive the call signal.

AN: edspap.20160127559

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 286

27. Recent Trends in **Information** and **Communication** Technology : Proceedings of the **2nd** International Conference of Reliable **Information** and **Communication** Technology (IRICT 2017)

By: Saeed, Faisal; Gazem, Nadhmi; Patnaik, Srikanta; Saed Balaid, Ali Saleh; Mohammed, Fathey. Series: Lecture Notes on Data Engineering and **Communications** Technologies, v. 5. Cham : Springer. 2018. eBook. Description: This book presents 94 papers from the **2nd** International Conference of Reliable **Information** and **Communication** Technology 2017 (IRICT 2017), held in Johor, Malaysia, on April 23–24, 2017. Focusing on the latest ICT innovations for data engineering, the book presents several hot research topics, including advances in big data analysis techniques and applications; mobile networks; applications and usability; reliable **communication** systems; advances in computer vision, artificial intelligence and soft ... (*AN 1526117*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Engineering (General); TECHNOLOGY & ENGINEERING / Telecommunications; Artificial intelligence--Congresses; **Information** technology--Congresses

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 287

28. Proceedings of the **2nd** Workshop on **Communication** Security : Cryptography and Physical Layer Security

By: Baldi, Marco; Quaglia, Elizabeth A.; Tomasin, Stefano. Series: Lecture Notes in Electrical Engineering, Vol. 447. Cham : Springer. 2018. eBook. Description: This book focuses on techniques that can be applied at the physical and data-link layers of **communication** systems in order to secure transmissions against eavesdroppers. It discusses topics ranging from **information** theory-based security to coding for security and cryptography, and presents cutting-edge research and innovative findings from leading researchers. The characteristic feature of all the contributions in this book is their relevance for the practical application of security principles to ... (*AN 1555253*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; COMPUTERS / Programming / Algorithms; COMPUTERS / Security / General; Data encryption (Computer science)--Congresses; Telecommunication systems--Security measures--Congresses; Computer networks--Security measures--Congresses

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 288

29. Proceedings of the Mediterranean Conference on **Information** & **Communication** Technologies 2015 : MedCT 2015 Volume 1

By: Oualkadi, Ahmed El; Choubani, Fethi; Moussati, Ali El. Series: Proceedings of the Mediterranean Conference on **Information** & **Communication** Technologies 2015, Volume 1. Switzerland : Springer, 2016. eBook. Description: This volume presents the **first** part of the proceedings of the Mediterranean Conference on **Information** & **Communication** Technologies (MedICT 2015), which was held at Saidia, Morocco during 7–9 May, 2015. MedICT provides an excellent international forum to the researchers and practitioners from both academia as well as industry to meet and share cutting-edge development. The conference has also a special focus on enabling technologies for societal challenges, and seeks to address multidisciplinary challenges ... (*AN 1175990*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; COMPUTERS / **Information** Technology; TECHNOLOGY & ENGINEERING / Engineering (General); Wireless **communication** systems--Congresses; **Communication** in demography--Congresses; **Information** technology--Social aspects--Congresses; **Information** technology--Security measures--Congresses

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 289

30. Genomic and Personalized Medicine : V1-2

By: Willard, Huntington F.; Ginsburg, Geoffrey S. Edition: **2nd** ed. London : Academic Press. 2013. eBook. Description: Genomic and Personalized Medicine, **Second** Edition — winner of a 2013 Highly Commended BMA Medical Book Award for Medicine — is a major discussion of the structure, history, and applications of the field, as it emerges from the campus and lab into clinical action. As with the **first** edition, leading experts review the development of the new science, the current opportunities for genome-based analysis in healthcare, and the potential of genomic medicine in future healthcare. The inclusion of the latest ... (*AN 485475*), Database: eBook Collection (EBSCOhost)

Subjects: SCIENCE / Life Sciences / Genetics & Genomics; MEDICAL / Pharmacology; Proteomics; Genomics; Medical genetics

PDF Full Text **USPTO Full Text Options** **Full Download**

Table of Contents Most Relevant Pages From This eBook

EBSCO Connect | Privacy Policy | A/B Testing | Terms of Use | Copyright | Cookie Policy | Contact Us

powered by EBSCO*host*

© 2020 EBSCO Industries, Inc. All rights reserved.

IPR2025-01313; Samsung
Ex. 1002 - Page 290

Biological **information acquisition device**, method for **acquiring** biological **information**, and **biometrics device**

K Amano, K Shimizu - US Patent 8,144,938, 2012 - Google Patents
... be achieved as well as biological **information** to be highly accurately and reliably **acquired** ... 7. A method for **acquiring information** of a biological **body** by irradiating the biological ... A **biometrics device**, comprising: a biological **information acquisition** part to **acquire information** of a ...
☆ 99 Cited by 8 Related articles All 4 versions »

Dynamic bio-**sensing** process design in mobile wellness **information** system for smart healthcare

T Lee, SH Lee - Wireless Personal Communications, 2016 - Springer
... **user** should be able to select various healthcare services and **acquire information** necessary for ... proposed **dynamic** process configuration can select each computing station **dynamically** depending on ... access times of both the proposed local and global **dynamic** sequences show ...
☆ 99 Cited by 15 Related articles All 6 versions »

Heart **biometrics**: Theory, methods and applications

F Agrafioti, J Gao, D Hatzinakos, J Yang - **Biometrics**, 2011 - books.google.com
... Another observation was that even though **dynamic** features such as the RR interval ... During enrollment, ECG **sensors** located on the smart **phone**, **first acquire** an ECG sample from a ... Similarly, during verification a newly **acquired** sample is matched against the store template ...
☆ 99 Cited by 68 Related articles All 6 versions »

A survey on touch **dynamics** authentication in mobile **devices**

PS Teh, N Zhang, ABJ Teoh, K Chen - Computers & Security, 2016 - Elsevier
... This is because the **acquiring** and processing of touch **dynamics** patterns can be carried out in ... is to identify and extract distinctive features common to a **user** from the **acquired** raw data ... The focus of this paper is on authentication using touch **dynamic biometrics**, so hereafter our ...
☆ 99 Cited by 91 Related articles All 6 versions

Information fusion in **biometrics**

AA Ross, AK Jain, K Nandakumar - Handbook of Multibiometrics, 2006 - Springer
... the cost of adding new **sensors** and the additional time required for **acquiring** and processing ... the average processing time since a decision can be made without having to **acquire** all the ... Note that the evidence pertaining to the multiple sources may be **acquired** in a sequential ...
☆ 99 Cited by 264 Related articles All 20 versions »

Biometric information acquisition apparatus and **biometric** authentication apparatus

H Otsubo, A Sakemoto - US Patent App. 12/402,292, 2009 - Google Patents
... Further, the components necessary for **acquiring biometric information** (the light source 21, the light guide 22, the ... between optical channels, thereby enabling the image pickup **device** 31 to **acquire** clearer vein ... the **fingerprint** image of the finger 96 can be thereby **acquired** by the ...
☆ 99 Cited by 14 Related articles All 2 versions »

Multivariate **Dynamic Biometrics** System

D Palti-Wasserman, Y Wasserman - US Patent App. 11/792,318, 2008 - Google Patents
... Eye Tracking **Sensors**; Several technologies may be used for measuring and **acquiring** different types ... The **acquired** data is amplified and digitized (110), and then processed and analyzed (111 ... The track ball can include additional **sensors**, which may **acquire** parameters such as ...
☆ 99 Cited by 73 Related articles All 2 versions »

Fingerprint silicon replicas: static and **dynamic** features for vitality detection using an optical capture **device**

P Coli, GL Marcialis, F Roli - International Journal of Image and ..., 2008 - World Scientific
... The system **acquires** consecutive frames during the rotation of the fingertip ... In order to investigate static and **dynamic** features, we collected a multiple- frames/multiple-impressions ... Images were **acquired** from 82 different fingerprints from 50 people aged between 20 and 70 and ...
☆ 99 Cited by 47 Related articles All 6 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 291

To a combined **fingerprint acquisition** and control **device**

RM Bolle, NK Ratha, A Senior - US Patent 6,941,001, 2005 - Google Patents

... G06F21/31—**User** authentication; G06F21/32—**User** authentication using **biometric** data, eg ... control **information** for an electronic **device**, said method comprising: **acquiring** through a ... correlations between a multiplicity of small regions of the **acquired fingerprint** images; extracting ...

☆ 99 Cited by 149 Related articles All 2 versions »

Biometric monitoring **device** having a **body** weight **sensor**, and methods of operating same

SGJ Yuen, J Park, EN Friedman - US Patent 8,475,367, 2013 - Google Patents

Biometric monitoring **device** having a **body** weight **sensor**, and ... A US201213346275 A US 201213346275A US 8475367 B1 US8475367 B1 US 8475367B1 Authority US United States Prior art keywords data monitoring **device user biometric** monitoring example Prior art ...

☆ 99 Cited by 238 Related articles All 2 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 292

STIC
Scientific and Technical Information Center

1. **User Authentication** Method **Based** on MKL for Keystroke and Mouse Behavioral Feature Fusion.

By: Wang, Xiujuan; Zheng, Qianqian; Zheng, Kangfeng; Wu, Tong. *Security & Communication Networks* , 5/20/2020, p1-14, 14p Abstract: In order to improve the recognition rate of **users** with single behavioral feature and prevent impostors from restricting an input device to avoid detection, a dual-index **user authentication** method **based** on Multiple Kernel Learning (MKL) for keystroke and mouse behavioral feature fusion was proposed in this paper. Due to the heterogeneity between the keystroke features and the mouse features, we argue that each type of features is mapped to a suitable kernel and the weights of each kernel are obtained through computing and then summed to **obtain** a compound kernel that implements the multifeature fusion. The dataset used in this paper was collected under complete uncontrolled condition from some volunteers by using our data collection program. The experimental **results** show that the proposed method can **obtain** the best recognition accuracy of 89.6%. Compared to the traditional methods of single feature, the dual-index method can get more stable and effective **authentication**. Therefore, the proposed method in this paper fully demonstrates the reliability of dual-index **user authentication**. [ABSTRACT FROM AUTHOR]; DOI: 10.1155/2020/9282380; (*AN 143347067*), Database: Applied Science & Technology Source

Subjects: Acquisition of data; All Other Animal Production; Mice

HTML Full Text **PDF Full Text** (1.8MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 293

2. ## A survey on methods and challenges in EEG **based authentication**

By Jalaly Bidgoly, Amir; Jalaly Bidgoly, Hamed; Arezoumand, Zeynab. In *Computers & Security*. June 2020 93 Language: English. DOI: 10.1016/j.cose.2020.101788 Abstract: EEG is the recording of electrical activities of the brain, usually along the scalp surface, which are the **results** of synaptic activations of the brain's neurons. In recent years, it has been shown that EEG is an appropriate signal for the **biometric authentication** and has important features such as resistance to spoofing attacks and impossibility to use under pressure and coercion states. In this paper, the state-of-the-art methods in EEG **based authentication** are reviewed. This review includes a number of aspects such as the various tasks that the **user** required to perform during the **authentication**, devices and available datasets, the preprocessing procedures and the classification methods used in the EEG **biometric authentication**. Both shallow and deep classification methods are reviewed in this paper. The study shows that the deep learning approaches which are used in the past few years, although still require further research, have shown great **results**nMoreover, the paper summarizes the works to address the open challenges of this area. The EEG **authentication** challenges have been discussed from a variety of points of view, including privacy, **user**-friendliness, attacks, and **authentication** requirements such as universality, permanency, uniqueness, and collectability. This paper can be used as a preliminary plan and a roadmap for researchers interested in EEG **biometric**. (*AN: S0167404820300730*), Database: ScienceDirect

Subjects: EEG; **Biometric** factor; **Authentication**; **User** identification; Pattern recognition; Survey

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 294

3. ELECTRONIC DEVICE AND METHOD FOR CONTROLLING THE SAME

Patent Application: 16/116790. Filed: August 29, 2018. Published: November 14, 2019. , Database: USPTO Patent Applications

Abstract: The present disclosure relates to an electronic device capable of **performing** complex **biometric authentication**, and the electronic device may include a plurality of **biometric** sensors configured to sense different **biometric information**, a security module configured to calculate a matching score for each of the different **biometric information** through a comparison between the different **biometric information** and previously registered **user information**, and calculate fake probability **information** for each of the different **biometric information** in consideration of a fake factor of the different **biometric information**, and perform **user authentication** using the matching score and the fake probability **information** calculated for each of the different **biometric information**, and a controller configured to control the electronic device **based** on a **user authentication result** performed by the security module.

AN: edspap.20190347390

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 295

4. A New **Biometric-Based** Remote **User Authentication** Scheme in Hierarchical Wireless Body Area Sensor Networks.

By: DAS, ASHOK KUMAR; CHATTERJEE, SANTANU; SING, JAMUNA KANTA. *Adhoc & Sensor Wireless Networks* , 2015, Vol. 28 Issue 3/4, p221-256, 45p Abstract: **User authentication** is a primary concern in a resource constrained wireless sensor network (WSN) before accessing real-time data from the nodes inside WSN. In this paper, we propose a novel **biometric-based user authentication** scheme suitable for hierarchical wireless body area networks (WBANs). The proposed scheme makes use of **biometric** verification along with password verification, which enables any authorized **user** to access real-time data from any cluster head in the sensor network. The proposed scheme is light-weight because it only requires the efficient cryptographic hash function, and symmetric key encryption and decryption algorithms. The strengths of the proposed protocol are that it provides strong **authentication** as compared to traditional related password-**based authentication** schemes in WSNs and achieves some good properties such as it works without synchronized clock, it supports freely password change by the legitimate **users** at any time, and it provides low computation costs and mutual **authentication**. In addition, the proposed scheme provides unconditional security against node capture attack and also prevents other attacks such as denial-of-service attack, stolen-verifier attack, many logged-in **users** with the same login-id attack, masquerade attack, replay attack, privileged-insider attack, smart card breach attack, and man-in-the-middle attack. Through the formal security verification using AVISPA (Automated Validation of Internet Security Protocols and Applications) tool we show that our scheme is secure against passive and active attacks. Furthermore, the formal security analysis under the random oracle models proves that our scheme is provably secure against different known attacks. [ABSTRACT FROM AUTHOR]; (*AN 109451129*), Database: Applied Science & Technology Source

Subjects: Biometric identification; Computer access control; Wireless sensor networks; Real-time control; Passwords (Computers); Data encryption

PDF Full Text (797KB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 296

5. ## Continuous **Authentications** Using Frequent English Terms.

By: Darabseh, Alaa; Siami-Namini, Sima; Siami Namin, Akbar. *Applied Artificial Intelligence*. 2018, Vol. 32 Issue 1, p13-47. 35p. Abstract: Most of the current computer systems authenticate a **user**'s identity only at the point of entry to the system (i.e., login). However, an effective **authentication** system includes continuous or frequent monitoring of the identity of a **user** already logged into a system to ensure the validity of the identity of the **user** throughout a session. Such a system is called a "<italic>continuous or active **authentication** system</italic>." An **authentication** system equipped with such a security mechanism protects the system against certain attacks including session hijacking that can be performed later by a malicious **user**. The aim of this research is to advance the state-of-the-art of the **user**-active **authentication** research using keystroke dynamics. Through this research, we assess the performance and influence of various keystroke features on keystroke dynamics **authentication** systems. In particular, we investigate the performance of keystroke features on a subset of most frequently used English words. The performance of four features including key duration, flight time latency, diagraph time latency, and word total time duration are analyzed. A series of experiments is performed to measure the performance of each feature individually as well as the **results** from the combinations of these features. More specifically, four machine learning techniques are adapted for the purpose of assessing keystroke **authentication** schemes. The selected classification methods are Support Vector Machine (SVM), Linear Discriminate Classifier (LDC), K-Nearest Neighbors (K-NN), and Naive Bayesian (NB). Moreover, this research proposes a novel approach **based** on sequential change-point methods for early detection of an imposter in computer **authentication** without the needs for any modeling of **users** in advance, that is, no need for a-priori **information** regarding changes. The proposed approach **based** on sequential change-point methods provides the ability to detect the impostor in early stages of attacks. The study is performed and evaluated **based** on data collected for 28 **users**. The experimental **results** indicate that the word total time feature offers the best performance **result** among all four keystroke features, followed by diagraph time latency. Furthermore, the **results** of the experiments also show that the combination of features enhances the performance accuracy. In addition, the nearest neighbor method performs the best among the four machine learning techniques. [ABSTRACT FROM AUTHOR] DOI: 10.1080/08839514.2018.1447535. (*AN: 128928131*), Database: Computer Source

Subjects: COMPUTER systems; COMPUTER access control; COMPUTER **users**; MALWARE; GRAPH theory

IPR2025-01313; Samsung
Ex. 1002 - Page 297

HTML Full Text PDF Full Text (2.8MB) USPTO Full Text Options

6. PGFit: **Static** permission analysis of health and fitness apps in IoT programming frameworks

By Nobakht, Mehdi; Sui, Yulei; Seneviratne, Aruna; Hu, Wen. In *Journal of Network and Computer Applications*. 15 February 2020 152 Language: English. DOI: 10.1016/j.jnca.2019.102509 Abstract: Popular Internet of Things (IoT) programming frameworks, such as Google Fit, enable third-party developers to build apps that store and retrieve **user** data from a variety of data sources such as wearable devices. Most of these apps, particularly those that are health and fitness-related, collect potentially sensitive personal data and send it to cloud servers. Analogous to Android OS, IoT programming frameworks often follow similar permission model; third-party apps on IoT platforms prompt **users** to grant the apps the access to their private data stored on cloud servers of IoT programming frameworks. Most **users** have a poor understanding of why these permissions are being asked. This can often lead to unnecessary permissions being granted, which in turn grant these apps with excessive privileges. Over-privileged apps might not be harmful to **users** when they are used as designed, however, they can potentially be exploited by a malicious actor in a cyber security attack. This is of particular concern with health and fitness apps, which may be exploited to leak highly sensitive personal **information**. This paper presents PGFit, a **static** permission analysis tool that precisely and efficiently identifies privilege escalation in third-party apps built on top of a popular IoT programming framework, Google Fit. PGFit extracts the set of requested permission scopes and the set of used data types in Google Fit-enabled apps to determine whether the requested permission scopes are actually necessary. PGFit performs graph reachability analysis on inter-procedural control flow graph. PGFit serves as a quality assurance tool for developers and a privacy checker for app **users**. We evaluated PGFit using a set of 20 popular Google Fit-enabled apps downloaded from Google Play. Our tool successfully identified the unnecessary permission scopes granted in our data set apps and found that 6 (30%) of the 20 apps are over-privileged. (*AN: S1084804519303698*), Database: ScienceDirect

Subjects: Permissions; Principle of least privilege; **Static** program analysis; IoT programming frameworks; Google Fit; Health and fitness data

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 298

7. Patent Application Titled '**Information** Processing Device, Application Software Start-Up System, And Application Software Start-Up Method' Published Online (USPTO 20190362061)

In: **Information** Technology Newsweekly, Dec 17, 2019, 2279; NewsRX LLC Language: English. Abstract: 2019 DEC 17 (VerticalNews) -- By a News Reporter-Staff News Editor at **Information** Technology Newsweekly -- According to news reporting originating from Washington, D.C., by VerticalNews journalists, a patent application [...] (*AN: edsgcl.608720217*), Database: Gale General OneFile

Subjects: Japan; Software quality; Software -- Methods; Software -- Intellectual property; Control equipment -- Methods; Control equipment -- Intellectual property

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 299

8. Continuous **authentication** for VANET

By Palaniswamy, Basker; Camtepe, Seyit; Foo, Ernest; Simpson, Leonie; Rezazadeh Baee, Mir Ali; Pieprzyk, Josef. In *Vehicular Communications*. October 2020 25 Language: English. DOI: 10.1016/j.vehcom.2020.100255 Abstract: Vehicular Ad-hoc Network (VANET) services use a range of **information**, such as traffic conditions and location **information**, for safe and convenient driving. **Information** exchange in VANET happens in Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communication modes. Several V2I and V2V **authentication** protocol suites are proposed to protect the **information** from attacks, namely replay, masquerading and man-in-the-middle. This paper identifies critical weaknesses in the protocols proposed for V2I and V2V communication modes and proposes a new protocol suite as a countermeasure. Our protocol suite is composed of driver **authentication**, V2I and V2V key exchanges, **information** exchange, offline password change and vehicle complain protocols. Our V2I key exchange protocol facilitates handoff capability to ensure continuous **authentication** when vehicles move from the coverage of one roadside unit (RSU) to another. The protocol also assures detectability to denial-of-service (DoS). Our V2V key exchange protocol enables vehicles to verify the time-bounded validity of certificates of vehicles and integrity of keys. We use the random oracle model to prove the security of our key exchange protocols and prove various security attributes of the protocols informally. Tamarin tool is used to formally verify the security properties of our driver **authentication** and key exchange protocols. Performance comparisons show that our driver **authentication** and key exchange protocols assure lesser computation overhead and more functional attributes than the existing protocols. Simulation performance ensures the fast key dissemination capability of our protocol suite. (*AN: S2214209620300267*), Database: ScienceDirect

Subjects: Secure-vehicular-communication; Security and privacy; VANET **authentication**; V2I and V2V key exchange; Handoff **authentication**; Formal verification

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 300

9. ## Enhanced Tacit Secrets: System-assigned passwords you can't write down, but don't need to.

By: Joudaki, Zeinab; Thorpe, Julie; Vargas Martin, Miguel. *International Journal of Information Security*. Apr2019, Vol. 18 Issue 2, p239-255. 17p. Abstract: We explore the feasibility of Tacit Secrets: system-assigned passwords that you can remember, but cannot write down or otherwise communicate. We design an approach to creating Tacit Secrets based on contextual cueing, an implicit learning method previously studied in the cognitive psychology literature. Our feasibility study indicates that our approach has strong security properties: resistance to brute-force attacks, online attacks, phishing attacks, some coercion attacks, and targeted impersonation attacks. It also offers protection against leaks from other verifiers as the secrets are system-assigned. Our approach also has some interesting usability properties, a high login success rate, and low false positive rates. We explore enhancements to our approach and find that incorporating eye-tracking data offers substantial improvements. We also explore the trade-offs of different configurations of our design and provide insight into valuable directions for future work. [ABSTRACT FROM AUTHOR] DOI: 10.1007/s10207-018-0408-2. (*AN: 135326762*), Database: Computer Source

Subjects: PASSWORDS (Computers); COMPUTER access control; FALSE personation; INTERNET security; PHISHING

HTML Full Text **PDF Full Text** (1.1MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 301

10. ## A new **authentication** protocol for healthcare applications using wireless medical sensor networks with **user** anonymity.

By: Li, Xiong; Niu, Jianwei; Kumari, Saru; Liao, Junguo; Liang, Wei; Khan, Muhammad Khurram. *Security & Communication Networks* , Oct2016, Vol. 9 Issue 15, p2643-2655, 13p Abstract: ABSTRACT With the development and maturation of the wireless communication technologies, the wireless sensor networks have been widely applied in different environments to acquire specific **information**. The wireless medical sensor networks (WMSNs), as a professional application of the wireless sensor networks in medicine, have attracted more and more attention because of its potential in improving the quality of healthcare services. Through the WMSNs, the parameters of patients' vital signs can be gathered from the sensor nodes equipped on the body of the patients and then can be accessed by the healthcare professionals by using a mobile device. By reason of the open feature of wireless communication, how to guarantee secure communication becomes an important issue. On the other hand, because the vital signs parameters are sensitive to the patients' health status and no one wants to reveal it to the others except the healthcare professionals, the protection of patients' privacy becomes another key issue for WMSNs applications. **User authentication** protocol with anonymity is the most basic and commonly used method to resolve the security and privacy issues of WMSNs. Recently, He et al. proposed an enhanced **authentication** protocol for healthcare applications using WMSNs to protect the security and privacy problems. However, we find that their scheme is incorrect in **authentication** and session key agreement phase. Besides, their scheme has no wrong password detection mechanism, which will not only waste the unnecessary computation and communication costs, but also may deduce the denial of service problem. In this paper, the **biometric** is introduced as the third **authentication** factor, and a new **user** anonymous **authentication** protocol **based** on WMSNs is designed so as to remove the drawbacks of the protocol of He et al. Compared with previous protocols, the new presented protocol enhances the security and also keeps the computation efficiency. Copyright © 2015 John Wiley & Sons, Ltd. [ABSTRACT FROM AUTHOR]; DOI: 10.1002/sec.1214; (*AN 118222100*), Database: Applied Science & Technology Source

Subjects: Computer access control; Computer network protocols; Wireless sensor networks; Wireless communications security; Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing; Wireless Telecommunications Carriers (except Satellite); Health **information** exchanges

PDF Full Text (595KB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 302

11. ## Opportunistic sensing for inferring in-the-wild human contexts **based** on activity pattern recognition using smart computing

By Ehatisham-ul-Haq, Muhammad; Azam, Muhammad Awais. In *Future Generation Computer Systems*. May 2020 106:374-392 Language: English. DOI: 10.1016/j.future.2020.01.003 Abstract: In recent years, with the evolution of internet-of-things and smart sensing technologies, sensor-**based** physical activity recognition has gained substantial prominence, and numerous research works have been conducted in this regard. However, the accurate recognition of in-the-wild human activities and the associated contexts remains an open research challenge to be addressed. This research work presents a novel activity-aware human context recognition scheme that explicitly learns human activity patterns in diverse behavioral contexts and infers in-the-wild **user** contexts **based** on physical activity recognition. In this aspect, five daily living activities, e.g., lying, sitting, standing, walking, and running, are associated with overall fourteen different behavioral contexts, including phone positions. A public domain dataset, i.e., ExtraSensory, is used for evaluating the proposed scheme using a series of machine learning classifiers. Random Forest classifier achieves the best recognition rate of 88.4% and 89.8% in recognizing five physical activities and the associated behavioral contexts, respectively, which demonstrates the efficacy of the proposed method. (*AN: S0167739X19314967*), Database: ScienceDirect

Subjects: Activity recognition; Human context recognition; In-the-wild; Machine learning; Pervasive computing; Smart sensing

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 303

12. ## Building an efficient intrusion detection system **based** on feature selection and ensemble classifier

By Zhou, Yuyang; Cheng, Guang; Jiang, Shanqing; Dai, Mian. In *Computer Networks*. 19 June 2020 174 Language: English. DOI: 10.1016/j.comnet.2020.107247 Abstract: Intrusion detection system (IDS) is one of extensively used techniques in a network topology to safeguard the integrity and availability of sensitive assets in the protected systems. Although many supervised and unsupervised learning approaches from the field of machine learning have been used to increase the efficacy of IDSs, it is still a problem for existing intrusion detection algorithms to achieve good performance. First, lots of redundant and irrelevant data in high-dimensional datasets interfere with the classification process of an IDS. Second, an individual classifier may not perform well in the detection of each type of attacks. Third, many models are built for stale datasets, making them less adaptable for novel attacks. Thus, we propose a new intrusion detection framework in this paper, and this framework is **based** on the feature selection and ensemble learning techniques. In the first step, a heuristic algorithm called CFS-BA is proposed for dimensionality reduction, which selects the optimal subset **based** on the correlation between features. Then, we introduce an ensemble approach that combines C4.5, Random Forest (RF), and Forest by Penalizing Attributes (Forest PA) algorithms. Finally, voting technique is used to combine the probability distributions of the base learners for attack recognition. The experimental **results**, using NSL-KDD, AWID, and CIC-IDS2017 datasets, reveal that the proposed CFS-BA-Ensemble method is able to exhibit better performance than other related and state of the art approaches under several metrics. (*AN: S1389128619314203*), Database: ScienceDirect

Subjects: Cyber security; Intrusion detection system; Data mining; Feature selection; Ensemble classifier

Full Text Finder **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 304

13. ## Exploring the cognitive process for service task in smart home: A robot service mechanism

By Zhang, Ying; Tian, Guohui; Chen, Huanzhao. In *Future Generation Computer Systems*. January 2020 102:588-602 Language: English. DOI: 10.1016/j.future.2019.09.020 Abstract: Smart home (SH) has been widely viewed as a promising paradigm to enhance the quality of life by providing context-aware services. Although the remarkable progress in SH has been made, it still remains a challenging problem to actively discover and provide complex service tasks in a proper way, especially bridging the gap between the complex tasks and the executable task descriptions by robot. To address this problem, this paper explores a robot service mechanism **based** on system cooperation in SH. Through the combination of intelligent space and robot, a system architecture of SH is presented, where the abilities of environmental perception and service execution can be effectively improved. For supporting the proposed system architecture and service task, a knowledge-**based** context model is proposed to address the data heterogeneity issue. Then the robot service mechanism of how to actively discover and provide the service task in the right way is fully revealed, the purpose of which is to provide a feasible solution for improving the quality of life. In particular, the comprehensive cognitive process of service task, including task cognition, task inference, task planning and task assessment, and autonomous navigation of service robot are exposed. The comprehensive experimental evaluations are conducted in the real-world, and the **results** demonstrate the feasibility and effectiveness of the presented schemes. (*AN: S0167739X19311197*), Database: ScienceDirect

Subjects: Smart home; Robot service mechanism; System cooperation; Knowledge representation; Cognitive process; Active service

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 305

14. ## Trustworthiness and a Zero Leakage OTMP-P2L Scheme **Based** on NP Problems for Edge Security Access †.

By: Han, Daoqi; Du, Xiaofeng; Lu, Yueming. *Sensors (14248220)*. Apr2020, Vol. 20 Issue 8, p2231. 1p. Abstract: Resource constraints have prevented comprehensive cryptography and multifactor **authentication** in numerous Internet of Things (IoT) connectivity scenarios. Existing IoT systems generally adopt lightweight security protocols that lead to compromise and privacy leakage. Edge computing enables better access control and privacy protection, furthermore, blockchain architecture has achieved a trusted store of value by open-source and distributed consensus mechanisms. To embrace these new paradigms, we propose a scheme that employs one-time association multitasking proofs for peer to local **authentication** (OTMP-P2L). The scheme chooses relevant nondeterministic polynomial (NP) problem tasks, and manages localized trust and anonymity by using smart devices such as phones and pads, thereby enabling IoT devices to autonomously perform consensus validation with an enhanced message **authentication** code. This nested code is a one-time zero-knowledge proof that comprises multiple logic verification arguments. To increase diversity and reduce the workload of each one, these arguments are chained by a method that establishes some of the inputs of the following task from the output of previous tasks. We implemented a smart lock system and confirmed that the scheme outperforms IoT **authentication** methods. The **result** demonstrates superior flexibility through dynamic difficulty strategies and succinct non-interactive peer-to-peer (P2P) verification. [ABSTRACT FROM AUTHOR] DOI: 10.3390/s20082231. *(AN: 143076745)*, Database: Academic Search Complete

Subjects: MESSAGE **authentication** codes; CONFIRMATION (Logic); PEER-to-peer architecture (Computer networks); MULTI-factor **authentication**; COMPUTER network architectures; CRYPTOSYSTEMS; SMARTPHONES; LEAKAGE

HTML Full Text **PDF Full Text** (2MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 306

15. A **biometric authentication** model using hand gesture images.

By: Simon Fong; Yan Zhuang; Fister, Iztok; Fister Jr, Iztok. *BioMedical Engineering OnLine*. 2013, Vol. 12 Issue 1, p2-27. 26p. Abstract: A novel hand **biometric authentication** method **based** on measurements of the **user's** stationary hand gesture of hand sign language is proposed. The measurement of hand gestures could be sequentially **acquired** by a low-cost video camera. There could possibly be another level of contextual **information**, associated with these hand signs to be used in **biometric authentication**. As an analogue, instead of typing a password 'iloveu' in text which is relatively vulnerable over a communication network, a signer can encode a **biometric** password using a sequence of hand signs, 'i', 'l', 'o', 'v', 'e', and 'u'. Subsequently the features from the hand gesture images are extracted which are integrally fuzzy in nature, to be recognized by a classification model for telling if this signer is who he claimed himself to be, by examining over his hand shape and the postures in doing those signs. It is believed that everybody has certain slight but unique behavioral characteristics in sign language, so are the different hand shape compositions. Simple and efficient image processing algorithms are used in hand sign recognition, including intensity profiling, color histogram and dimensionality analysis, coupled with several popular machine learning algorithms. Computer simulation is conducted for investigating the efficacy of this novel **biometric authentication** model which shows up to 93.75% recognition accuracy. [ABSTRACT FROM AUTHOR] DOI: 10.1186/1475-925X-12-111. (*AN: 91845977*), Database: Academic Search Complete

Subjects: BIOMETRIC identification; GESTURE; HAND signals; MACHINE learning; SIGN language; Translation and Interpretation Services

PDF Full Text (2.5MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 307

16. ## A survey on security issues of 5G NR: Perspective of artificial dust and artificial rain

By Shafi, Misbah; Jha, Rakesh Kumar; Sabraj, Manish. In *Journal of Network and Computer Applications*. 15 June 2020 160 Language: English. DOI: 10.1016/j.jnca.2020.102597 Abstract: 5G NR (New Radio) incorporates concepts of novel technologies such as spectrum sharing, D2D communication, UDN, and massive MIMO. However, providing security and identifying the security threats to these technologies occupies the prime concern. This paper intends to provide an ample survey of security issues and their countermeasures encompassed in the technologies of 5G NR. Further, security concerns of each technology are defined mathematically. Thereby defining the impact on the factors of security. Moreover, a methodology is developed in which the influence on security due to artificially generated rain and artificially generated dust on the wireless communication network is studied. By doing so, an attacking scenario is identified, where a half-duplex attack in D2D communication is attained. Half-duplex attack specifies the attack solely on the downlink to spoof the allocated resources, with reduced miss-rate. Thus, ultra-reliable and adequate advances are required to be addressed to remove the obstacles that create a hindrance in achieving the secured and authenticated communicating network. (*AN: S1084804520300710*), Database: ScienceDirect

Subjects: 5G NR; Security; Artificial rain; Artificial dust; D2D; Miss-rate; Half-duplex attack

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 308

17. ## Security analysis of drones systems: Attacks, limitations, and recommendations

By Yaacoub, Jean-Paul; Noura, Hassan; Salman, Ola; Chehab, Ali. In *Internet of Things*. September 2020 11 Language: English. DOI: 10.1016/j.iot.2020.100218 Abstract: Recently, the world witnessed a significant increase in the number of used drones, with a global and continuous rise in the demand for their multi-purpose applications. The pervasive aspect of these drones is due to their ability to answer people's needs. Drones are providing **users** with a bird's eye that can be activated and used almost anywhere and at any time. However, recently, the malicious use of drones began to emerge among criminals and cyber-criminals alike. The probability and frequency of these attacks are both high and their impact can be very dangerous with devastating effects. Therefore, the need for detective, protective and preventive counter-measures is highly required. The aim of this survey is to investigate the emerging threats of using drones in cyber-attacks, along the countermeasures to thwart these attacks. The different uses of drones for malicious purposes are also reviewed, along the possible detection methods. As such, this paper analyzes the exploitation of drones vulnerabilities within communication links, as well as smart devices and hardware, including smart-phones and tablets. Moreover, this paper presents a detailed review on the drone/Unmanned Aerial Vehicle (UAV) usage in multiple domains (i.e civilian, military, terrorism, etc.) and for different purposes. A realistic attack scenario is also presented, which details how the authors performed a simulated attack on a given drone following the hacking cycle. This review would greatly help ethical hackers to understand the existing vulnerabilities of UAVs in both military and civilian domains. Moreover, it allows them to adopt and come up with new techniques and technologies for enhanced UAV attack detection and protection. As a **result**, various civilian and military anti-drones/UAVs (detective and preventive) countermeasures will be reviewed. (*AN: S2542660519302112*), Database: ScienceDirect

Subjects: UAV; UAS; UUV; Armed drones; Drone/UAV warfare; Terrorism/counter-Terrorism; Drones security; Drones threats and vulnerabilities; Drones attacks; Drones security countermeasures techniques; Drones forensics

Full Text Finder **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 309

18. Motion-**based** countermeasure against photo and video spoofing attacks in face recognition

By Edmunds, Taiamiti; Caplier, Alice. In *Journal of Visual Communication and Image Representation*. January 2018 50:314-332 Language: English. DOI: 10.1016/j.jvcir.2017.12.004 Abstract: Highlights •A novel motion-**based** countermeasure **based** on rigid and non-rigid face movements is introduced.•Identification and characterization of discriminant motion cues: natural motions from real faces and peculiar fake face motions such as the absence of motion, hand-shaking movements and simulated movements.•Extensive experiments are conducted on the latest public spoof databases, namely CASIA-FASD, ReplayAttack-DB, MSU-MFSD and MSU databases.•Generalization issues are investigated via cross-database evaluations in particular.•A detailed review of dynamic face anti-spoofing countermeasures is provided. (*AN: S1047320317302365*), Database: ScienceDirect

Subjects: Motion cues; Face anti-spoofing; Fisher kernel; Replay attacks

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 310

19. A fingerprint **based** bio-cryptographic security protocol designed for client/server **authentication** in mobile computing environment.

By: Xi, Kai; Ahmad, Tohari; Han, Fengling; Hu, Jiankun. *Security & Communication Networks* , May2011, Vol. 4 Issue 5, p487-499, 13p Abstract: With fast evolution of mobile devices and mobile network, the need of protecting **user** sensitive **information** locally and **performing** secure **user authentication** remotely become evermore increasing. Bio-cryptography is emerging as a powerful solution which can combine the advantages of conventional cryptography and **biometric** security. In this paper, we present an efficient bio-cryptographic security protocol designed for client/server **authentication** in current mobile computing environment, with a reasonable assumption that server is secure. In this protocol, fingerprint **biometric** is used in **user** verification, protected by a computationally efficient Public Key Infrastructure (PKI) scheme, Elliptic Curve Cryptography (ECC). The genuine fingerprint **information** is hidden in the feature vault which is the mixture of genuine and chaff features. Fingerprint features are not only used for **biometric** verification but also for cryptographic key generation. Our security analysis shows that the proposed protocol can provide a secure and trustworthy **authentication** of remote mobile **users** over insecure network. Experimental **results** on public domain database show an acceptable verification performance. We also tested the computational costs and efficiency of our protocol on the CLDC emulator using Java ME (previous J2ME) programming technology. The simulation **results** prove that the proposed protocol suits current mobile environment. Copyright © 2010 John Wiley & Sons, Ltd. In this protocol, fingerprint **biometric** is used in **user** verification, protected by a computationally efficient Public Key Infrastructure (PKI) scheme, Elliptic Curve Cryptography (ECC). The genuine fingerprint **information** is hidden in the feature vault which is the mixture of genuine and chaff features. Fingerprint features are not only used for **biometric** verification but also for cryptographic key generation. [ABSTRACT FROM AUTHOR]; DOI: 10.1002/sec.225; (*AN 60026563*), Database: Applied Science & Technology Source

PDF Full Text (997KB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 311

20. ## Analysis of interaction trace maps for active **authentication** on smart devices.

By: Ahmad, Jamil; Sajjad, Muhammad; Jan, Zahoor; Mehmood, Irfan; Rho, Seungmin; Baik, Sung. *Multimedia Tools & Applications* , Feb2017, Vol. 76 Issue 3, p4069-4087, 19p Abstract: The availability and affordability of handheld smart devices have made life easier by enabling us to do work on the go. Their widespread use brings with it concerns relating to data security and privacy. The rising demand to secure private and highly confidential data found on smart devices has motivated researchers to devise means for ensuring privacy and security at all times. This kind of continuous **user authentication** scheme would add an additional layer of much needed security to smart devices. In this context, touch screen interactions have recently been studied as an effective modality to perform active **user authentication** on mobile devices. In this paper, a visual analysis **based** active **authentication** framework has been presented. Considering the touch screen as a canvas, interaction trace maps are constructed as a **result** of **user** interactions within various applications. The **user** touch gestures are captured and represented as drawing strokes on the canvas. The behavioral and physiological characteristics of **users** are modeled as signatures by combining texture and shape features from the interaction trace maps. A two-step mechanism with support vector machines exploit this signature to perform active **user authentication**. Experiments conducted with various datasets show that the proposed framework compares favorably with other state-of-the-art methods. [ABSTRACT FROM AUTHOR]; DOI: 10.1007/s11042-016-3450-y; (*AN 121442576*); Database: Applied Science & Technology Source

Subjects: Computer access control; Data security; Support vector machines; Cell phones; Tablet computers; Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing; Electronic components, navigational and communications equipment and supplies merchant wholesalers; Electronics Stores; Wireless Telecommunications Carriers (except Satellite); Other Computer Related Services; Computer systems design and related services (except video game design and development); Privacy

PDF Full Text (2.8MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 312

21. ## Data security in mobile cloud computing paradigm: a survey, taxonomy and open research issues.

By: Bhatia, Tarunpreet; Verma, A. *Journal of Supercomputing*. Jun2017, Vol. 73 Issue 6, p2558-2631. 74p. Abstract: The incessant spurt of research activities to augment capabilities of resource-constrained mobile devices by leveraging heterogeneous cloud resources has created a new research impetus called mobile cloud computing. However, this rapid relocation to the cloud has fueled security and privacy concerns as users' data leave owner's protection sphere and enter the cloud. Significant efforts have been devoted by academia and research community to study and build secure frameworks in cloud environment, but there exists a research gap for comprehensive study of security frameworks in mobile cloud computing environment. Therefore, we aim to conduct a comprehensive survey to analyze various cryptographic, **biometric** and multifactor lightweight solutions for data security in mobile cloud. This survey highlights the current security issues in mobile cloud environment and infrastructure, investigates various data security frameworks and provides a taxonomy of the state-of-the-art data security frameworks and deep insight into open research issues for ensuring security and privacy of data in mobile cloud computing platform. [ABSTRACT FROM AUTHOR] DOI: 10.1007/s11227-016-1945-y. (*AN: 123190258*), Database: Academic Search Complete

Subjects: DATA security; CLOUD computing; MOBILE computing; ACCESS control of databases; **INFORMATION** technology surveys; TAXONOMY; Computer systems design and related services (except video game design and development); Other Computer Related Services; Data Processing, Hosting, and Related Services

PDF Full Text (2.4MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 313

22. ## Privacy-Constrained **Biometric** System for Non-Cooperative **Users**.

By: S. Jahromi, Mohammad N.; Buch-Cardona, Pau; Avots, Egils; Nasrollahi, Kamal; Escalera, Sergio; Moeslund, Thomas B.; Anbarjafari, Gholamreza. *Entropy*. Nov2019, Vol. 21 Issue 11, p1033-1033. 1p. Abstract: With the consolidation of the new data protection regulation paradigm for each individual within the European Union (EU), major **biometric** technologies are now confronted with many concerns related to **user** privacy in **biometric** deployments. When individual **biometrics** are disclosed, the sensitive **information** about his/her personal data such as financial or health are at high risk of being misused or compromised. This issue can be escalated considerably over scenarios of non-cooperative **users**, such as elderly people residing in care homes, with their inability to interact conveniently and securely with the **biometric** system. The primary goal of this study is to design a novel database to investigate the problem of automatic people recognition under privacy constraints. To do so, the collected data-set contains the subject's hand and foot traits and excludes the face **biometrics** of individuals in order to protect their privacy. We carried out extensive simulations using different baseline methods, including deep learning. Simulation **results** show that, with the spatial features extracted from the subject sequence in both individual hand or foot videos, state-of-the-art deep models provide promising recognition performance. [ABSTRACT FROM AUTHOR] DOI: 10.3390/e21111033. (*AN: 139863108*), Database: Academic Search Complete

Subjects: OLDER people; DATABASE design; PERSONALLY identifiable **information**; DATA protection; DEEP learning; MULTIMODAL **user** interfaces; EUROPEAN Union

HTML Full Text **PDF Full Text** (8.9MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 314

23. **User** perspective and security of a new mobile **authentication** method.

By: Laka, Pawel; Mazurczyk, Wojciech. *Telecommunication Systems.* Nov2018, Vol. 69 Issue 3, p365-379. 15p. Abstract: This paper describes a new mobile **authentication** method which is **based** on an Open ID Connect standard and subscriber identity module card. The proposed solution enables **users** to access websites, services and applications without the need to remember passwords, responses or support of any equipment. The proposed method is evaluated from the **users'** perspective as well as from the security viewpoint. Moreover, we compare it with the two most popular existing **authentication** schemes i.e. **static** passwords and SMS OTP (one time password). In order to evaluate **user's** view on various **authentication** methods a questionnaire was prepared and distributed among 40 participants. Obtained **results** revealed that the new **authentication** scheme yielded better **results** than the existing methods. Finally, we also performed a security analysis with respect to all abovementioned **authentication** solutions to assess whether there are any major risks related to the proposed method. [ABSTRACT FROM AUTHOR] DOI: 10.1007/s11235-018-0437-1. (*AN: 132044390*), Database: Engineering Source

Subjects: SMART cards; COMPUTER access control; CYBERCRIMINALS; COMPUTER crime prevention; COMPUTER network architectures

HTML Full Text **PDF Full Text** (1.6MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 315

24. ## Artificial Immune Systems approaches to secure the internet of things: A systematic review of the literature and recommendations for future research

By Aldhaheri, Sahar; Alghazzawi, Daniyal; Cheng, Li; Barnawi, Ahmed; Alzahrani, Bandar A.. In *Journal of Network and Computer Applications*. 1 May 2020 157 Language: English. DOI: 10.1016/j.jnca.2020.102537

Abstract: As the Internet of Things (IoT) recently attains tremendous popularity, this promising technology leads to a variety of security challenges. The traditional solutions do not fit the new challenges brought by the IoT ecosystem. Although the development's area of Artificial Immune Systems (AIS) provides an opportunity to improve security issues and create a fertile and exciting environment for further research and experiments, there is not any systematic and comprehensive study about analyzing its importance for IoT environment. Therefore, this work aims to identify, evaluate, and perform a comprehensive study of empirical research on the studies of AIS approaches to secure the IoT environment. The relevant and high-quality studies are addressing using three research questions about the main research motivations, existing solutions, and future gaps and directions. The AIS approaches have been divided into three main categories **based** on IoT layers, and detailed classifications have also been included **based** on different parameters. To achieve this aim, the authors use a systematic literature review (SLR) as a powerful method to collect and critically analyze the research papers. Also, the authors discuss the selected studies and their main techniques, as well as their benefits and drawbacks in general. This research process strives to build a knowledge base for AIS solutions under the umbrella of IoT security and suggest directions for future research. (*AN: S1084804520300114*), Database: ScienceDirect

Subjects: Artificial intelligence; Artificial immune system; Artificial immune networks; Clonal selection; Cyber security; Danger theory; Dendritic cell; Internet of things; IoT; Negative selection; Network security

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 316

25. ## Multimodal **Biometric** Person **Authentication**: A Review.

By: Sahoo, Soyuj Kumar; Choubisa, Tarun; Prasanna, S. R. Mahadeva. *IETE Technical Review.* Jan/Feb2012, Vol. 29 Issue 1, p54-75. 22p. 7 Diagrams.

Abstract: This paper provides a review of multimodal **biometric** person **authentication** systems. The paper begins with an introduction to **biometrics**, its advantages, disadvantages, and **authentication** system using them. A brief discussion on the selection criteria of different **biometrics** is also given. This is followed by a discussion on the classification of **biometric** systems, their strengths, and limitations. Detailed descriptions on the multimodal **biometric** person **authentication** system, different modes of operation, and integration scenarios are also provided. Considering the importance of **information** fusion in multi-**biometric** approach, a separate section is dedicated on the different levels of fusion, which include sensor-level, feature-level, score-level, rank-level, and abstract-level fusions, and also different rules of fusion. This paper also presents an overview of some performance parameters and error rates for **biometric** person **authentication** systems. A separate section is devoted to the recent trends in **biometrics** field, namely, adaptive **biometric** system, analysis of complementary and supplementary **information**, and physiological **biometrics**. The paper concludes with a discussion on the issues that are currently holding the deployment of multimodal **biometric** person **authentication** systems and a possible scope for future work. [ABSTRACT FROM AUTHOR] DOI: 10.4103/0256-4602.93139. (*AN: 73183333*)

Database: Academic Search Complete

Subjects: BIOMETRIC identification; **AUTHENTICATION** (Law); ERROR rates; BIOMETRY; DIGITAL signatures; **INFORMATION** & communication technologies; COMPUTER network resources

Show all 7 Images






PDF Full Text (1.2MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 317

26. ## Time/Space **based Biometric** Handwritten Signature Verification.

By: Gonçalves, Ricardo P.; Augusto, Alexandre B.; Correia, Manuel E.. *CISTI (Iberian Conference on **Information** Systems & Technologies / Conferência Ibérica de Sistemas e Tecnologias de Informação) Proceedings* , 2015, Vol. 1, p934-939, 6p Abstract: Handwritten signature recognition is still the most widely accepted method to validate paper **based** documents. However, in the digital world, there is no readymade way to distinguish a real handwritten signature on a scanned document from a forged copy of another signature made by the same person on another document that is simply "pasted" into the forged document. In this paper we describe how we are using the touch screen of smartphones or tablets to collect handwritten signature images and associated **biometric** markers derived from the motion direction of handwritten signatures that are made directly into the device touchscreen. These time base **biometric** markers can then be converted into signaling time waves, by using the dragging or lifting movements the **user** makes with a touch screen omnidirectional tip stylus, when he handwrites is signature at the device touchscreen. These time/space signaling time waves can then be converted into a **biometric** bit stream that can be matched with previously enrolled **biometric** markers of the **user's** handwritten signature. In this paper we contend that the collection of these simple **biometric** features is sufficient to achieve a level of **user** recognition and **authentication** that is sufficient for the majority of online **user authentication** and digital documents authenticity. [ABSTRACT FROM AUTHOR]; (*AN 114061177*), Database: Applied Science & Technology Source

Subjects: Biometric identification; Digital signatures; Touch screens; Computer Terminal and Other Computer Peripheral Equipment Manufacturing; Computer and peripheral equipment manufacturing; Signatures (Writing); Identification documents

PDF Full Text (8.6MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 318

27. Three-Factor Anonymous **Authentication** and Key Agreement Scheme for Telecare Medicine **Information** Systems.

By: Arshad, Hamed; Nikooghadam, Morteza. *Journal of Medical Systems.* Dec2014, Vol. 38 Issue 12, p1-12. 12p. 2 Diagrams, 3 Charts. Abstract: The article discusses the research on preventing computer network security failures in telecare medicine **information** systems using a three-factor anonymous **authentication** and key agreement scheme. Topics discussed include how computer network are vulnerable to replay attacks and Denial-of-Service attacks and the **results** of the security and performance analysis of the proposed computer security scheme. DOI: 10.1007/s10916-014-0136-8. (*AN: 115925535*), Database: Engineering Source

Subjects: BIOMETRY; **INFORMATION** storage & retrieval systems -- Medical care; INTERNET; MEDICAL ethics; PRIVACY; SMART cards; TELEMEDICINE; DATA security

PDF Full Text (906KB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 319