28. ## Continuous and transparent multimodal **authentication**: reviewing the state of the art.

By: Al Abdulwahid, Abdulwahid; Clarke, Nathan; Stengel, Ingo; Furnell, Steven; Reich, Christoph. *Cluster Computing* , Mar2016, Vol. 19 Issue 1, p455-474, 20p. Publisher: Springer Nature.; Abstract Individuals, businesses and governments undertake an ever-growing range of activities online and via various Internet-enabled digital devices. Unfortunately, these activities, services, **information** and devices are the targets of cybercrimes. Verifying the **user** legitimacy to use/access a digital device or service has become of the utmost importance. **Authentication** is the frontline countermeasure of ensuring only the authorized **user** is granted access; however, it has historically suffered from a range of issues related to the security and usability of the approaches. They are also still mostly functioning at the point of entry and those **performing** sort of re-**authentication** executing it in an intrusive manner. Thus, it is apparent that a more innovative, convenient and secure **user authentication** solution is vital. This paper reviews the **authentication** methods along with the current use of **authentication** technologies, aiming at developing a current state-of-the-art and identifying the open problems to be tackled and available solutions to be adopted. It also investigates whether these **authentication** technologies have the capability to fill the gap between high security and **user** satisfaction. This is followed by a literature review of the existing research on continuous and transparent multimodal **authentication**. It concludes that providing **users** with adequate protection and convenience requires innovative robust **authentication** mechanisms to be utilized in a universal level. Ultimately, a potential federated **biometric authentication** solution is presented; however it needs to be developed and extensively evaluated, thus operating in a transparent, continuous and **user**-friendly manner. [ABSTRACT FROM AUTHOR]; (*AN 114014182*), Database: Complementary Index

Subjects: COMPUTER access control; COMPUTER crimes; ELECTRONIC countermeasures; **BIOMETRIC** identification; ELECTRONIC **authentication**

Linked Full Text **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 320

29. ## Frame–**based** classification for cross-speed gait recognition.

By: Kovač, Jure; Štruc, Vitomir; Peer, Peter. *Multimedia Tools & Applications.* Mar2019, Vol. 78 Issue 5, p5621-5643. 23p. Abstract: The use of human gait as the means of **biometric** identification has gained a lot of attention in the past few years, mostly due to its enormous potential. Such **biometrics** can be captured at public places from a distance without subjects collaboration, awareness and even consent. However, there are still numerous challenges caused by influence of covariate factors like changes of walking speed, view, clothing, footwear etc., that have negative impact on recognition performance. In this paper we tackle walking speed changes with a skeleton model-**based** gait recognition system focusing on improving algorithm robustness and improving the performance at higher walking speed changes. We achieve these by proposing frame **based** classification method, which overcomes the main shortcoming of distance **based** classification methods, which are very sensitive to gait cycle starting point detection. The proposed technique is starting point invariant with respect to gait cycle starts and as such ensures independence of classification from gait cycle start positions. Additionally, we propose wavelet transform **based** signal approximation, which enables the analysis of feature signals on different frequency space resolutions and diminishes the need for using feature transformation that require training. With the evaluation on OU-ISIR gait dataset we demonstrate state of the art performance of proposed methods. [ABSTRACT FROM AUTHOR] DOI: 10.1007/s11042-017-5469-0. (*AN: 135822214*), Database: Engineering Source

Subjects: GAIT in humans; **BIOMETRIC** identification; WALKING speed; SIMULATION methods & models; SUPPORT vector machines

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

IPR2025-01313; Samsung
Ex. 1002 - Page 321

30. **Biometric User Authentication** for IT Security : From Fundamentals to Handwriting

By: Vielhauer, Claus. Series: Advances in **Information** Security, Vol. 18. New York : Springer. 2006. eBook. Description: **Biometric user authentication** techniques evoke an enormous interest by science, industry and society. Scientists and developers constantly pursue technology for automated determination or confirmation of the identity of subjects **based** on measurements of physiological or behavioral traits of humans. **Biometric User Authentication** for IT Security: From Fundamentals to Handwriting conveys general principals of passive (physiological traits such as fingerprint, iris, face) and active (learned and trained ... (*AN 150663*), 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; COMPUTERS / **User** Interfaces; **Biometric** identification

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 322

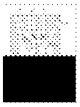
Google performing user authentication to obtain an authentication result based c Sign in

All News Videos Images More Settings Tools

About 36,300 results (0.46 seconds)

www.google.com/patents/US20150010215

Biometric authentication apparatus, biometric authentication ...



A biometric authentication apparatus includes a storage unit which stores first ... the registered biometric information based on a result of the matching process. ... biometric information of a registered user is performed (hereinafter referred to ... a shape of biometric information captured in a biometric image obtained at the ...
App. - Filed Sep 24, 2014 - Published Jan 8, 2015 - Mitsuaki Fukuda - Fujitsu Limited
Overview · Related · Discuss

www.google.com/patents/US8264325

Biometric authentication apparatus and biometric data ...



Biometric authentication requires a registration stage at which biometric features of a user are obtained in advance by a sensor and stored in a ...
Grant - Filed Mar 24, 2009 - Issued Sep 11, 2012 - Mitsuaki Fukuda - Fujitsu Limited
Overview · Related · Discuss

www.google.com/patents/US20150035643

Biometrics identification module and personal wearable ...



Biometrics identification module and personal wearable electronics network based authentication and transaction processing are disclosed. According to one ...
App. - Filed Nov 12, 2013 - Published Feb 5, 2015 - Eren Kursun - Jpmorgan Chase Bank, N.A.
Overview · Related · Discuss

www.google.com/patents/US7545962

Biometric authentication system



Moreover the authentication system is configured to authenticate the user on ... based on an analysis of the performance of the authentication system over a predefined ... algorithm and this can be considered a fixed static score threshold value. ... representation of the results obtained using a specific set of data parameters if ...
Grant - Filed Dec 22, 2005 - Issued Jun 9, 2009 - Michael Peirce - Daon Holdings Limited
Overview · Related · Discuss

www.google.com/patents/US6819219

Method for biometric-based authentication in wireless ...



Authentication based on fingerprint: One of the most common biometric techniques, wherein users scan in a copy of their fingerprint and a comparison is ...
Grant - Filed Oct 13, 2000 - Issued Nov 16, 2004 - Rudolf Maarten Bolle - International Business Machines Corporation
Overview · Related · Discuss

www.google.com/patents/CN102804200B?cl=en

Two-factor user authentication system, and method therefor

And the authentication request client generates a presentation pattern on the basis of the client identification information acquired from the authentication server ...
Grant - Filed Oct 5, 2010 - Issued Apr 1, 2015 - 玉井成知 - 株式会社希愛思昇
Overview · Related · Discuss

www.google.com/patents/US20130290229

Gripping-feature learning authentication system and ...

One example of the known user authentication means for mobile information terminals is fingerprint authentication means included in a mobile information ...

IPR2025-01313; Samsung
Ex. 1002 - Page 323



App. - Filed Feb 8, 2012 - Published Oct 31, 2013 - Masakatsu Tsukamoto - Ntt Docomo, Inc.
Overview · Related · Discuss

www.google.com/patents/CN102467663B?cl=en

Biometrics authentication device



The arithmetic unit extracts a vascular pattern from the authentication image, and ... vascular patterns photographed, more Biont information can be obtained from ... utilize display part 17 or loudspeaker 18 based on operation result, user can be ... in step S160 instruction make finger static, to suppress the variation of force
Grant - Filed Sep 9, 2011 - Issued May 20, 2015 - 松田友铺 - 株式会社日立制作所
Overview · Related · Discuss

www.google.com/patents/US8184866

Living body guidance control method for a biometrics ...



A biometrics authentication device identifies characteristics of the body from captured images of the body and performs individual authentication. The device ...
Grant - Filed Sep 13, 2007 - Issued May 22, 2012 - Kazuo Takaku - Fujitsu Limited
Overview · Related · Discuss

www.google.com/patents/US20120300992

Method and apparatus for authenticating swipe biometric ...



Authentication verifies the claim about the identity of an entity (e.g., a person or a ... transform the biometric information into signals for further use and processing. ... the submission of counterfeit images—obtained by using a different biometric ... integrity of the scanner by disassembling it, performing measurements inside of ...
App. - Filed May 24, 2012 - Published Nov 29, 2012 - Vladimir Iankov Ivanov - The University Of Maryland
Overview · Related · Discuss

IPR2025-01313; Samsung
Ex. 1002 - Page 324

Dynamic regulation of television **viewing** content **based** on viewer profile and **viewing** history

BJ Cragun, PR Day - US Patent 5,973,683, 1999 - Google Patents

... H04N21/478—Supplemental services, eg **displaying** phone caller identification, shopping application; H04N21/4782 ... rating sources and **viewing** time credits for desirable material and **viewing** time debits ... particular to a method and system for controlling the content **displayed** on ...

☆ 99 Cited by 833 Related articles All 2 versions »

User authentication for devices **with** touch sensitive elements, such as touch sensitive **display screens**

S Bayram, AE Dirik, N Memon, U Topkara - US Patent 8,941,466, 2015 - Google Patents

User authentication for devices **with** touch sensitive elements, such as touch sensitive **display screens**. Download PDF **Info** ... US 8941466 B2 US8941466 B2 US 8941466B2 Authority US United **States** Prior art keywords **user** signature finger touch **information** computer system ...

☆ 99 Cited by 150 Related articles All 4 versions »

Personalized **information** retrieval **using user-defined** profile

VS Dasan - US Patent 5,761,662, 1998 - Google Patents

... **Info** ... More specifically, the present invention relates to a client/server model for **information** retrieval **based** upon a **user-defined** profile, for example, for ... these resources is filtering the vast amount of **information** which is available in order that a **user** obtain that **information** which is ...

☆ 99 Cited by 893 Related articles All 2 versions »

Methods and systems for distributing **information** within a **dynamically defined** community

JP Bezos, W Adams, KL Dinovo, RJ Snodgrass... - US Patent ..., 2008 - Google Patents

... **displayed** in associated **with** the product, but the older review is automatically removed **from display** on the ... votes minus the not useful votes, the following or similar designations are **displayed** to viewers ... is in his or her opinions and preferences to those of the **viewing** customer ...

☆ 99 Cited by 324 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

... **Info** ... US 6148261 A US6148261 A US 6148261A Authority US United **States** Prior art keywords map processor map **information information** communicator Prior ... a legal analysis and makes no representation or warranty as to the accuracy of the list.) Silver **State** Intellectual Tech ...

☆ 99 Cited by 643 Related articles All 2 versions »

Method and apparatus for automatically **determining** and **dynamically** updating **user** preferences in an entertainment system

CD Williams, JMG Iki, AA Shah-Nazaroff... - US Patent ..., 1999 - Google Patents

... an apparatus comprises a storage medium to store **user** preference **information** corresponding to ... agent, communicatively coupled to the storage medium, is operative to **monitor user** interaction **with** ... 22, 1996, for a Television **Viewing** Behavior **Monitor by** Jean Goldschmidt, Tony ...

☆ 99 Cited by 777 Related articles All 2 versions »

Soliciting **information based** on a computer **user's** context

KH Abbott, JO Robarts, D Newell - US Patent 6,968,333, 2005 - Google Patents

Soliciting **information based** on a computer **user's** context. Download PDF **Info** ... G—PHYSICS; G06—COMPUTING; CALCULATING; COUNTING; G06F—ELECTRIC DIGITAL DATA PROCESSING; G06F16/00—**Information** retrieval; Database structures therefor; File system ...

☆ 99 Cited by 588 Related articles All 4 versions »

Dynamic information management system and method for content delivery and sharing in content-, metadata-and viewer-**based**, live social networking among **users** ...

J Robinson, P Muller, T Noke, TL Lim, W Glausi... - US Patent ..., 2014 - Google Patents

Dynamic information management system and method for content delivery and sharing in content-, metadata- and viewer-**based**, live social networking among **users** concurrently engaged in the same and/or similar content. Download PDF **Info** ...

☆ 99 Cited by 466 Related articles All 4 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 325

Determining advertisements **using user** interest **information** and map-**based** location **information**

S Glassman, J Joseph, B Kilday... - US Patent App. 11 ..., 2008 - Google Patents

... For example, the ads may be **displayed** in an area adjacent to a map ... 1 is a high-level diagram **showing** parties or entities that can interact **with** an advertising ... 17-19 depict exemplary **display screens**, each including a map, advertisements, and marker icons, and each being ...

☆ 99 Cited by 286 Related articles All 2 versions »

Using location data to **determine** traffic **information**

RC Fan, X Yang, JD Fay - US Patent 6,594,576, 2003 - Google Patents

Using location data to **determine** traffic **information**. Download PDF **Info** ... US6594576B2 US 6594576 B2 US6594576 B2 US 6594576B2 US 89868201 A US89868201 A US 89868201A US 6594576 B2 US6594576 B2 US 6594576B2 Authority US United **States** Prior art ...

☆ 99 Cited by 484 Related articles All 4 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 326

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 16/535,574	Filing Date 08/08/2019	☐ To be Mailed

ENTITY: ☑ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $100 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $460 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	05/21/2020	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 29	Minus	** 29	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 4	Minus	*** 4	= 0		x $460 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	SLIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/DESHONNE T. MARTINO/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. 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 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc Code: DIST.E.FILE **Document Description: Electronic Terminal Disclaimer - Filed**	PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	16535574
Filing Date	08-Aug-2019
First Named Inventor	Masayuki HIRABAYASHI
Attorney Docket Number	SEI-10740-02
Title of Invention	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
Maxell, Ltd.	100%

The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

10423769

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

◉ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.

○ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.	
Applicant claims the following fee status: ○ Small Entity ○ Micro Entity ◉ Regular Undiscounted I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.	
THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES I certify, in accordance with 37 CFR 1.4(d)(4) that I am: ◉ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application Registration Number 30293 ○ A sole inventor ○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application ○ A joint inventor; all of whom are signing this request	
Signature	/John R. Mattingly/
Name	John R. Mattingly

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

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
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:				
STATUTORY OR TERMINAL DISCLAIMER	1814	1	160	160
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**160**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 16535574

Filing Date: 08-Aug-2019

Applicant/Patent under Reexamination: HIRABAYASHI

Electronic Terminal Disclaimer filed on May 21, 2020

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt	
EFS ID:	39507660
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
Filer Authorized By:	
Attorney Docket Number:	SEI-10740-02
Receipt Date:	21-MAY-2020
Filing Date:	08-AUG-2019
Time Stamp:	15:10:11
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$160
RAM confirmation Number	E20205KF10050883
Deposit Account	501417
Authorized User	John Mattingly
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	Terminal Disclaimer-Filed (Electronic)	eTerminal-Disclaimer.pdf	33553 6bfec5d7a662ffc601effd3ab0560094bab93000	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30715 baace0000a80196e53cf244fde6950f9c9902df2	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	64268		

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.

Attorney Docket No. SEI-10740-02

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	MAXELL, LTD.	Confirmation No.: 5886
Serial No.:	16/535,574	
Filed:	August 8, 2019	
For:	INFORMATION PROCESSING DEVICE, APPLICATION SOFTWARE START-UP SYSTEM, AND APPLICATION SOFTWARE START-UP METHOD	
Group:	2498	
Examiner:	Thanhnga B. TRUONG	

AMENDMENT

Mail Stop: Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

May 21, 2020

Sir:

In response to the Office Action dated February 21, 2020, reconsideration and withdrawal of the outstanding rejections and allowance of the present application are respectfully requested in view of the following remarks.

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

Remarks begin on page 14 of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Original) A system, comprising:

a first information processing device including:

a dynamic biometric information acquisition sensor that acquires dynamic biometric information from a body of a user; and

a first communication interface that transmits the acquired dynamic biometric information; and

a second information processing device including:

a static biometric information acquisition sensor that acquires static biometric information;

a processor that performs user authentication based on the acquired static biometric information and obtains an authentication result;

a second communication interface that performs communication relating to the authentication result with the first communication interface and receives the dynamic biometric information transmitted from the first communication interface; and

a display screen,

wherein the first information processing device:

performs communication relating to the authentication result between the first communication interface and the second communication interface and executes an unlock operation to unlock itself in response to the communication relating to the authentication result,

acquires the dynamic biometric information from the dynamic biometric information acquisition sensor after unlocking, and

maintains the unlocked state during a condition that the dynamic biometric information can be acquired,

wherein the second information processing device receives the dynamic biometric information via communication between the first communication interface and the second communication interface and the display screen displays information based on a state of the user that is determined using the received dynamic biometric information.

2. (Original) The system according to claim 1,

wherein the first communication interface and the second communication interface are Bluetooth interfaces and communication between the first communication interface and the second communication interface is Bluetooth wireless communication.

3. (Original) The system according to claim 1,

wherein the first communication interface and the second communication interface are Wi-Fi interfaces and communication between the first communication interface and the second communication interface includes establishing a Wi-Fi Direct connection.

4. (Original) The system according to claim 1,

wherein the dynamic biometric information is one of heart rate, pulse, blood pressure, body temperature, amount of sweating, or brain wave and the static biometric information is one of finger print information, facial recognition information, retina information, vein information, or iris information.

5. (Original) The system according to claim 1,

wherein the first information processing device is a wearable device that acquires the dynamic biometric information at least by being physically in contact with the body.

6. (Original) The system according to claim 1,

wherein the first information processing device is a smartwatch and the second information processing device is a smartphone or tablet.

7. (Original) The system according to claim 1,

wherein the first information processing device continuously acquires the dynamic biometric information after being unlocked and the second information processing device receives the dynamic biometric information transmitted from the first communication device continuously or based on starting of an application on the second information processing device.

8. (Original) The system according to claim 1,

wherein the second information processing device gets position information denoting a position of the second information processing device and automatically transmits the position information to a predetermined address based on reception of a user input that is determined to be a predetermined type of user input during a time period, wherein the predetermined address is not inputted by the user during the time period.

9. (Original) The system according to claim 8,

wherein the position information is automatically transmitted in response to the user input and without requiring additional user input that explicitly requires approval of the automatic transmission of the position information during the time period.

10. (Original) The system according to claim 1,

wherein upon determining that the user is in a state matching predetermined criteria, the second information processing device limits an operation of the second

information processing device by displaying a screen seeking confirmation from the user that the user intended to execute the operation.

11. (Original) The system according to claim 10,

wherein the operation is executed on the second information processing device after the user provides confirmation in response to displaying of the screen.

12. (Withdrawn) An information processing device, comprising:

a dynamic biometric information acquisition sensor that acquires dynamic biometric information from a body of a user;

a wireless communication interface is configured to:

transmits the acquired dynamic biometric information to another information processing device; and

perform communication relating to an authentication result based on static biometric information with the other information processing device;

a processor that:

executes an unlock operation to unlock the information processing device in response to the communication relating the authentication result;

acquires the dynamic biometric information from the dynamic biometric information acquisition sensor after unlocking; and

maintains the unlocked state during a condition that the dynamic biometric information can be acquired,

wherein the wireless communication interface is configured to transmit the dynamic biometric information to the other information processing device via wireless communications such that the dynamic biometric information is used to determine a state of the user and generate information for display on the other information processing device, and

wherein the dynamic biometric information is continuously acquired after the information processing device is unlocked and the wireless communication interface is configured to transmit the dynamic biometric information to the other information processing device continuously or based on starting of an application on the other information processing device.

13. (Withdrawn) The information processing device according to claim 12,

wherein the wireless communication interface is one of a Bluetooth interface for executing Bluetooth wireless communication or a Wi-Fi interface for executing Wi-Fi wireless communication.

14. (Withdrawn) The information processing device according to claim 12,

wherein the dynamic biometric information is one of heart rate, pulse, blood pressure, body temperature, amount of sweating, or brain wave and the static biometric information is one of finger print information, facial recognition information, retina information, vein information, or iris information.

15. (Withdrawn) The information processing device according to claim 12,

wherein the processor is programmed to switch from the unlocked state to locked state when in a condition that the dynamic biometric information cannot be acquired.

16 . (Withdrawn) A method being executed by a first information processing device, comprising:

acquiring, by a dynamic biometric information acquisition sensor, dynamic biometric information from a body of a user;

wirelessly transmitting the acquired dynamic biometric information to a second information processing device;

performing communication relating to an authentication result based on static biometric information with the second information processing device;

executing an unlock operation to unlock the first information processing device in response to the communication relating to the authentication result;

acquiring the dynamic biometric information from the dynamic biometric information acquisition sensor after the unlocking; and

maintaining the unlocked state during a condition that the dynamic biometric information can be acquired,

wherein the dynamic biometric information is transmitted to the second information processing device via wireless communications such that the dynamic biometric information is used to determine a state of the user and generate information for display on the second information processing device, and

wherein the dynamic biometric information is continuously acquired after the first information processing device is unlocked and the dynamic biometric information is transmitted to the second information processing device continuously or based on starting of an application on the second information processing device.

17. (Withdrawn) The method according to claim 16,

wherein the wireless communication is one of Bluetooth wireless communication or Wi-Fi wireless communication.

18. (Withdrawn) The method according to claim 16,

wherein the dynamic biometric information is one of heart rate, pulse, blood pressure, body temperature, amount of sweating, or brain wave and the static biometric information is one of finger print information, facial recognition information, retina information, vein information, or iris information.

19. (Original) A method, comprising:

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.

20. (Original) The method according to claim 19,

wherein the first communication interface and the second communication interface are Bluetooth interfaces and the communication performed between the first

communication interface and the second communication interface is Bluetooth wireless communication.

21. (Original) The method according to claim 19,

wherein the first communication interface and the second communication interface are Wi-Fi interfaces and the communication performed between the first communication interface and the second communication interface includes establishing a Wi-Fi Direct connection.

22. (Original) The method according to claim 19,

wherein the acquiring of dynamic biometric information acquires one of heart rate, pulse, blood pressure, body temperature, amount of sweating, or brain wave and the static biometric information is one of finger print information, facial recognition information, retina information, vein information, or iris information.

23. (Original) The method according to claim 19,

wherein the acquiring of dynamic biometric information by the acquisition sensor of the first device acquires the dynamic biometric information with a wearable device at least by being physically in contact with the body.

24. (Original) The method according to claim 19,

wherein the dynamic biometric information is acquired by a smartwatch as the first device and the dynamic biometric information acquired by a smartphone or tablet as the second device.

25. (Original) The method according to claim 19,

wherein the dynamic biometric information is continuously acquired by the first device after being unlocked and the second device receives the dynamic biometric information transmitted from the first device continuously or based on starting of an application on the second device.

26. (Original) The method according to claim 19,

wherein the second device gets position information denoting a position of the second device and automatically transmits the position information to a predetermined address based on reception of a user input that is determined to be a predetermined type of user input during a time period, wherein the predetermined address is not inputted by the user during the time period.

27. (Original) The method according to claim 26,

wherein the position information is automatically transmitted in response to the user input and without requiring additional user input that explicitly requires approval of the automatic transmission of the position information during the time period.

28. (Original) The method according to claim 19,

wherein upon determining that the user is in a state matching predetermined criteria, the second device limits an operation of the second device by displaying on the display screen a message seeking confirmation from the user that the user intended to execute the operation.

29. (Original) The method according to claim 28,

wherein the operation is executed on the second device after the user provides confirmation in response to the displaying of the message on the display screen.

REMARKS

Claims 1-29 are pending in this application. Claims 12-18 are withdrawn. No new matter has been added.

Information Disclosure Statement

Applicants appreciate the Examiner's consideration of the references submitted in the Information Disclosure Statement filed August 8, 2019.

Double Patenting Rejections

Claims 1-11 and 19-29 stand rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-15 of U.S. Patent No. 10,423,769 B2. Without admitting to the propriety of the rejection, an e-Terminal Disclaimer is being submitted with this Reply to overcome the rejection.

Conclusion

In view of the foregoing remarks, Applicants request reconsideration of the rejection and allowance of the claims.

To the extent necessary, the Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Mattingly & Malur, PC, Deposit Account No. 50-1417 (referencing attorney docket no. SEI-10740-02).

Respectfully submitted,

MATTINGLY & MALUR, PC

/John R. Mattingly/
John R. Mattingly
Registration No. 30,293

Electronic Acknowledgement Receipt

EFS ID:	39507613
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
Filer Authorized By:	
Attorney Docket Number:	SEI-10740-02
Receipt Date:	21-MAY-2020
Filing Date:	08-AUG-2019
Time Stamp:	15:07:32
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		10740-02-AMDwithjustTERMDIS.pdf	58459 7ac4e73e2c04cadb5b461e0791285e5f4a544c3b	yes	15

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	13
	Applicant Arguments/Remarks Made in an Amendment	14	15
Warnings:			
Information:			
	Total Files Size (in bytes):	58459	

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

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 02/21/2020

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

EXAMINER	
TRUONG, THANHNGA B	

ART UNIT	PAPER NUMBER
2498	

NOTIFICATION DATE	DELIVERY MODE
02/21/2020	ELECTRONIC

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

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

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

ptomail@mmiplaw.com

Office Action Summary	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 --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 12/16/19.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ 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.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-29 is/are pending in the application.

5a) Of the above claim(s) 12-18 is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-11 and 19-29 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, 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.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 8/8/19 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ 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)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to the communication filed on December 16, 2019. Claims 1-29 are pending. At this time, claims 1-11 and 19-29 are rejected.

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.

Election/Restrictions

3. Applicant's election of Invention I, claims 1-11 and 19-29, in the reply filed on December 16, 2019 is acknowledged.

Claims 12-18 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to nonelected Invention II, there being no allowable generic or linking claim. Election was made **with traverse** in the reply filed on December 16, 2019. However, Examiner has noticed that there are no arguments included in the Response to Election that filed on December 16, 2019. Therefore, the election will be treated as **without traverse.**

Double Patenting

4. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a

nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-11 and 19-29 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-15 of U.S. Patent No. 10, 423, 769 B2. Although the conflicting claims are not identical, they are not patentably distinct from each other because the two inventions have similar subject matter, especially 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 (see Abstract).

Allowable Subject Matter

5. Claims 1-11 and 19-29 would be allowable if a terminal disclaimer will be filed with the next amendment to overcome the Double Patenting rejection above.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

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 at 571-272-8593. The fax and phone numbers 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

February 17, 2020

Notice of References Cited	Application/Control No. 16/535,574	Applicant(s)/Patent Under Reexamination HIRABAYASHI et al.	
	Examiner THANHNGA B TRUONG	Art Unit 2498	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-9373047-B2	06-2016	Aoki; Takahiro	G06K9/00926	1/1
*	B	US-20100131414-A1	05-2010	Tame; Gavin Randall	G06F21/32	705/67
*	C	US-9314193-B2	04-2016	Haddad; Waleed Sami	G06F3/011	1/1
*	D	US-8218459-B1	07-2012	Stucker; Brian	H04L63/0407	370/261
*	E	US-8667562-B2	03-2014	LeBeau; Michael J	G06F3/048	726/2
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

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	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	TBT
TEXT Searched; EAST Searched; NPL Searched - Google/Patents and Scholar	02/17/2020	TBT

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

IPR2025-01313; Samsung
Ex. 1002 - Page 358

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

IPR2025-01313; Samsung
Ex. 1002 - Page 359

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

BIB DATA SHEET

CONFIRMATION NO. 5886

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
16/535,574	08/08/2019	726	2498	SEI-10740-02

APPLICANTS
Maxell, Ltd., Kyoto, JAPAN;

INVENTORS
Masayuki HIRABAYASHI, Osaka, JAPAN;
Yasunobu HASHIMOTO, Osaka, JAPAN;
Kazuhiko YOSHIZAWA, Osaka, JAPAN;

**** CONTINUING DATA ***************************
This application is a CON of 15/315,735 12/02/2016 PAT 10423769
which is a 371 of PCT/JP2014/065644 06/12/2014

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****
08/20/2019

Foreign Priority claimed	☐ Yes ☑ No	☐ Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119(a-d) conditions met	☐ Yes ☑ No		JAPAN	19	29	4
Verified and Acknowledged	/THANHNGA B TRUONG/ Examiner's Signature	Initials				

ADDRESS

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

TITLE

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

FILING FEE RECEIVED	FEES: Authority has been given in Paper	☐ All Fees
3080	No._____ to charge/credit DEPOSIT ACCOUNT	☐ 1.16 Fees (Filing)
	No._____ for following:	☐ 1.17 Fees (Processing Ext. of time)
		☐ 1.18 Fees (Issue)
		☐ Other _____
		☐ Credit

Remote device **authentication**

S Svensson - US Patent App. 10/028,583, 2003 - Google Patents

... [0018]. Where **authentication** is always **performed** via a ... The network 14 **performs** the same calculation, using RAND and the SSD associated with the ... claim 1 wherein calculating an **authentication** response based on said **authentication** key comprises **performing** a mathematical ...

☆ 99 Cited by 51 Related articles All 2 versions »

Authentication mechanism for wireless **communication** devices

K Ma - US Patent App. 10/460,969, 2005 - Google Patents

... To **perform** this, he must acquire another SIM card from his carrier ... The method of claim 11 wherein said receiving is **performed** by a user inputting on a ... Abandoned US20050021940A1 (en), 2003-06-13, 2003-06-13, **Authentication** mechanism for wireless **communication** devices ...

☆ 99 Cited by 34 Related articles All 2 versions »

ID check device, ID generation device, and **authentication** system

K Ohkubo - US Patent App. 10/924,578, 2005 - Google Patents

... (8) In the preferred embodiment, the ID generation circuits 34 and 36, which **perform** the same ... Thus, confidentiality is ensured and the identification process is properly **performed** ... device receiving the ID acquisition code from the ID check device, **performing** a predetermined ...

☆ 99 Cited by 31 Related articles All 2 versions »

Method and apparatus for **performing** enhanced time-based **authentication**

JG Brainard, BS Kaliski Jr, RL Rivest - US Patent 7,363,494, 2008 - Google Patents

Method and apparatus for **performing** enhanced time-based **authentication**. Download PDF ... **Authentication** can **result** in the **performance** of one or more actions including, without limitation ... to as an iteration count, can be used to indicate how many times to **perform** an underlying ...

☆ 99 Cited by 387 Related articles All 4 versions »

... 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 109 Related articles All 2 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 46 Related articles All 4 versions »

Power line **communication** apparatus, registration status confirmation method, and power line **communication** system

H Koga - US Patent App. 12/030,778, 2008 - Google Patents

... the foregoing **authentication** process method, it is possible to reliably **perform** an **authentication** ... to confirm that an **authentication** process has been reliably **performed** between desired ... 1. A power line **communication** apparatus capable of **performing** power line **communications** ...

☆ 99 Cited by 175 Related articles All 2 versions »

Flexible **interface** to **authentication** services in a distributed data processing environment

LK Loucks, TA Smith - US Patent 5,481,720, 1996 - Google Patents

... killed, restarted, and scheduled as a regular program without affecting the **performance** of the ... The only operations that the requesting process needs to **perform** with these elements are ... permission to request an operation 420 of the service, conditionally **performing** the requested ...

☆ 99 Cited by 185 Related articles All 2 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 361

… using a single **authentication** device to **authenticate** a user to a service provider among a plurality of service providers and device for **performing** such a method

B Wendling, J Wenger - US Patent 9,338,163, 2016 - Google Patents

... 27 for managing all the components of the service provider and for **performing** cryptographic and ... This way of **doing** can be also be improved by using a modulo function applied to ... It should be understood that the account registration phase is **performed** only one time with each ...

☆ 99 Cited by 26 Related articles All 4 versions »

Use of **communication** equipment and method for **authenticating** an item, unit and system for **authenticating** items, and **authenticating** device

MA Amon, A Bleikolm, O Rozumek, E Müller... - US Patent ..., 2010 - Google Patents

... of the invention, the **authenticating** device is a micro-spectrometer for **performing** spectral analysis ... protect the sensor from dirt and mechanical damage, without degrading its optical resolution **performance** ... Said remote server may also **perform authenticating** operations centrally ...

☆ 99 Cited by 137 Related articles All 4 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 362

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

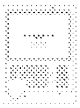
Sign in

All Images News Videos More Settings Tools

About 128,000 results (0.52 seconds)

www.google.com/patents/US8836473

Dynamic keypad and fingerprinting sequence authentication



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

The receiver may **receive information from** the first **fingerprint** scanner, ... **States** ... digit **displayed by** the first **display** during the receipt of the first **biometric** ... for **user** authentication to be used in conjunction **with** a **dynamic display** of inputs ... The ATM may also include one **display screen** or a plurality of **display** ... **determined** ...

Overview · Related · Discuss

www.google.com/patents/US20150324564

Dynamic activation of user profiles based on biometric ...

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

The apparatus may compare the detected **biometric information with** stored ... may then **determine** whether to **display** the stored **user** profile **based** on ... United **States** ... At step 222, the **user** device **displays** a default **user** profile after a ... a locked **screen** that prevents the unknown **user from** further accessing ...

Overview · Related · Discuss

www.google.com/patents/US20160327922

A control device and control method for performing an ...

App. - Filed Jun 22, 2016 - Published Nov 10, 2016 - Masakazu SEKIGUCHI - Nikon Corporation

There has been a desire for proactively adding more detailed embodiments relating to the acquisition and use of **biometric information**. Therefore, according to ...

Overview · Related · Discuss

www.google.com/patents/US9235733

Mobile biometrics information collection and identification

Grant - Filed Feb 23, 2012 - Issued Jan 12, 2016 - J. Douglas Birdwell - J. Douglas Birdwell

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 ...

Overview · Related · Discuss

www.google.com/patents/US20140182952

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



App. - Filed Mar 7, 2014 - Published Jul 3, 2014 - Shelten Gee Jao Yuen - Fitbit, Inc.

US9084538B2 2011-01-09 2015-07-21 Fitbit, Inc. **Biometric** monitoring ... Fitness monitoring device **with user** engagement metric functionality ... US9005129B2 2012-06-22 2015-04-14 Fitbit, Inc. Wearable heart rate **monitor** ... methods for acquisition of sensorial **information from** smart devices.

Overview · Related · Discuss

www.google.com/patents/US7994898

Portable access device



Grant - Filed Jun 16, 2009 - Issued Aug 9, 2011 - Helmars E. Ozolins - Bloomberg Finance L.P.

Information from the person seeking access and the system is then used at ... **received** ... As mentioned, the **information** representing a **biometric** characteristic of a ... for **use** in **determining** whether to grant the person **from** whom the **information** is ... the life of large **screen** liquid crystal **display** components, and can operate in ...

Overview · Related · Discuss

www.google.com/patents/US9304624

Embedded authentication systems in an electronic device

Grant - Filed Sep 5, 2014 - Issued Apr 5, 2016 - Anthony Fadell - Apple Inc.

The device **receives** input **based** on the **displayed** irregular arrangement of the ... In accordance **with** a **determination** that the input meets input pattern criteria, ... device **with** a **display** and a **fingerprint** sensor may authenticate a **user** for a ... United **States** ... Info: Patent citations (616); Non-patent citations (228); Cited by (466) ...

Overview · Related · Discuss

www.google.com/patents/US20130057573

Smart Display with Dynamic Face-Based User Preference Settings

IPR2025-01313; Samsung
Ex. 1002 - Page 363



App. - Filed Nov 11, 2011 - Published Mar 7, 2013 - Hari Chakravarthula - DigitalOptics Corporation Europe Limited
The **display** can include a processor configured to adjust a **user** preference or ... an age of the **user**, a distance of the **user** from the **screen**, a head angle of the **user**, ... Application **status** is Abandoned. Info: Patent citations (30); Cited ... In one embodiment, the age of the **user** can be **determined based** on the size ... **biometric** ...
Overview · Related · Discuss

www.google.com/patents/US8463003
Biometric information acquisition apparatus, biometric ...



Grant - Filed Dec 2, 2009 - Issued Jun 11, 2013 - Hiroyasu Otsubo - Hitachi Maxell, Ltd.
A **biometric information** acquisition apparatus includes: a light guide that guides a ... from other individuals **based** on a **determination** as to whether the **biometric** ...
Overview · Related · Discuss

www.google.com/patents/EP2743873A1?cl=en
Dynamic authentication technology



App. - Filed Dec 13, 2013 - Published Jun 18, 2014 - Nataraj Subbaraya Kuntagod - Accenture Global Services Limited
Based on to authenticating the **user** that requested performance of the ... related to an ability to authenticate the **user using biometric** authentication techniques.
Overview · Related · Discuss

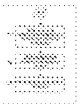
Help Send feedback Privacy Terms

IPR2025-01313; Samsung
Ex. 1002 - Page 364

Google performing user authentication to obtain an authentication result based c Sign in

All News Videos Images More Settings Tools

About 39,100 results (0.54 seconds)

www.google.com/patents/US8548206
Multifactor multimedia biometric authentication

Grant - Filed Apr 30, 2012 - Issued Oct 1, 2013 - Paul T. Schultz - Verizon Patent And Licensing Inc.
A device may **receive** a request to **authenticate** a **user**, automatically ... The device may further **perform** a group of **biometric authentication** ... **user** is properly **authenticated based** on the group of **authentication** scores, ... **authentication information** consistent with exemplary embodiments. ... **static** ... **obtained** ...
Overview · Related · Discuss

www.google.com/patents/US7545962
Biometric authentication system

Grant - Filed Dec 22, 2005 - Issued Jun 9, 2009 - Michael Peirce - Daon Holdings Limited
Moreover the **authentication** system is configured to **authenticate** the **user** on ... score is provided **based** on an analysis of the **performance** of the **authentication** system over a ... **Info**: Patent citations (10); Non-patent citations (3); Cited by (55) ... **static** ... As the ROC is a statistical representation of the **results obtained** using a ...
Overview · Related · Discuss

www.google.com/patents/US20160162673
Technologies for learning body part geometry for use in ...
App. - Filed Dec 5, 2014 - Published Jun 9, 2016 - Gershom Kutliroff - Gershom Kutliroff
The **Biometric authentication** processes utilizing the technologies are ... In some instances the extraction is **performed** with the aid of a ... **static** ... denote **biometric information** of the **user** that is not **obtained** from the first body part. ... The **result** of such comparison may be the generation of calibration ... **based** ...
Overview · Related · Discuss

www.google.com/patents/US9355234
Authentication involving selection among different biometric ...
Grant - Filed Sep 27, 2013 - Issued May 31, 2016 - Trilnu Magi Shaashua - Emc Corporation
The **authentication** technique further involves **performing**, **based** on the set of suitability factors and by the ... **Info** ... methods includes: (i) **based** on the set of suitability factors **obtained** from the **user** device of the **user**, ... As a **result**, the control circuitry is now able to select which **biometric** method (or ... **static** ...
Overview · Related · Discuss

www.google.com/patents/US8264325
Biometric authentication apparatus and biometric data ...

Grant - Filed Mar 24, 2009 - Issued Sep 11, 2012 - Mitsuaki Fukuda - Fujitsu Limited
in accordance with input **user** ID, a personal template fetcher reads ... A verification sensor extracts **biometric** feature **information** from an ... verifies the **biometric** feature data **obtained** by the verification sensor in ... **static** ... **Biometric authentication** technologies for **performing authentication based** on ... **result** ...
Overview · Related · Discuss

www.google.com/patents/US20130290229
Gripping-feature learning authentication system and ...

App. - Filed Feb 8, 2012 - Published Oct 31, 2013 - Masakatsu Tsukamoto - Ntt Docomo, Inc.
A server includes a template receiver receiving a **user authentication** ... and a determination **result** sending part sending a determination **result**. ... a mobile **information** terminal is gripped and **performs user authentication**. ... **user authentication** means for mobile **information** terminals is **fingerprint** ... **depending** ... **obtained** ...
Overview · Related · Discuss

www.google.com/patents/US8649569
Authentication apparatus, image capture apparatus, ...

Grant - Filed Jul 19, 2011 - Issued Feb 11, 2014 - Tatsuo Shindo - Fujitsu Frontech Limited
In an **authentication** apparatus, an input section **acquires** a living body image ... The output section outputs guidance **information** for prompting a reduction in the ... an **authentication** apparatus for **performing biometrics authentication** including: ... **obtained** as a **result** of positioning by the comparison unit 135, the positioning ...
Overview · Related · Discuss

IPR2025-01313; Samsung
Ex. 1002 - Page 365

www.google.com/patents/WO2007071288A1?cl=en

Biometric authentication system

App. - Filed Dec 22, 2005 - Published Jun 28, 2007 - Michael Peirce - Daon Holdings Limited
A **biometric authentication** engine is described. The engine includes components which are configured to **authenticate** a **user based** on one or ...
Overview · Related · Discuss

www.google.com/patents/US9223955

User-authentication gestures

Grant - Filed Jan 30, 2014 - Issued Dec 29, 2015 - Dimitrios Lymberopoulos - Microsoft Corporation
This document relates to **user-authentication** gestures. ... **performance** ... threshold for the **user based** upon the sensor data **obtained** during the training session.
Overview · Related · Discuss

www.google.com/patents/US8930709

Method and apparatus for sequential authentication using one ...

Grant - Filed Mar 28, 2008 - Issued Jan 6, 2015 - Jiri Navratil - International Business Machines Corporation
The intermediate **authentication result** is **based**, for example, on one or more of false accept ... or known **information** about a given challenge. ... include the **use** of a **biometric** feature as the verification object, e.g., a **fingerprint**. ... **obtained** ... used to **perform** simple verification steps that operate in a predefined **static** manner, ...
Overview · Related · Discuss

IPR2025-01313; Samsung
Ex. 1002 - Page 366

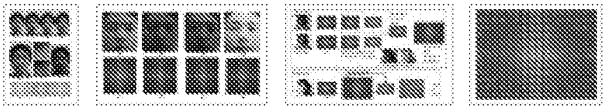
STIC
Scientific and Technical Information Center

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 367

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 368

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 369

4. ## 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 370



PDF Full Text (7.9MB) USPTO Full Text Options

5. 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

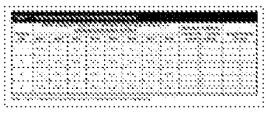
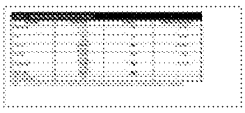
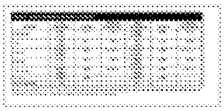
IPR2025-01313; Samsung
Ex. 1002 - Page 371

6. ## 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 372

7. ## 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 373

8. 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 374

9. ## 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 375

10. ## 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 376

11. 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

12. 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 377

13. 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

14. 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 378

15. ## 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

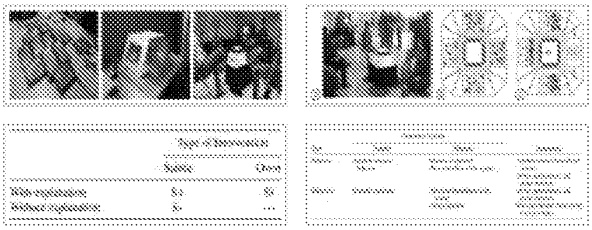
IPR2025-01313; Samsung
Ex. 1002 - Page 379

16. ## 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 380

17. Abstract.

Basic & Clinical Pharmacology & Toxicology. Jan2019 Supplement S, p3-119. 117p. DOI: 10.1111/bcpt.13173. (*AN: 134091944*), Database: Academic Search Complete

Subjects: NON-insulin-dependent diabetes; AIR pollution; DEEP learning; MAGNETIC resonance imaging of the brain; SKIN disease diagnosis; REHABILITATION

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

18. Abstract.

Basic & Clinical Pharmacology & Toxicology. Dec2018 Supplement S2, Vol. 124, p3-119. 117p. DOI: 10.1111/bcpt.13173. (*AN: 133465006*), Database: Academic Search Complete

Subjects: NON-insulin-dependent diabetes; AIR pollution; SKIN injuries; MAGNETIC nanoparticles; MAGNETIC resonance imaging; Diagnostic Imaging Centers

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

IPR2025-01313; Samsung
Ex. 1002 - Page 381

19. ## 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

20. ## 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 382

21. 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 383

22. ## 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 384

23. ## 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

IPR2025-01313; Samsung
Ex. 1002 - Page 385

24. An Offensive and Defensive Exposition of Wearable Computing.

By: SHRESTHA, PRAKASH; SAXENA, NITESH. *ACM Computing Surveys* , Nov2017, Vol. 50 Issue 6, p1-39, 39p Abstract: Wearable computing is rapidly getting deployed in many—commercial, medical, and personal—domains of day-to-day life. Wearable devices appear in various forms, shapes, and sizes and facilitate a wide variety of applications in many domains of life. However, wearables raise unique security and privacy concerns. Wearables also hold the promise to help enhance the existing security, privacy, and safety paradigms in unique ways while preserving the system's usability. The contribution of this research literature survey is threefold. First, as a background, we identify a wide range of existing as well as upcoming wearable devices and investigate their broad applications. Second, we provide an exposition of the security and privacy of wearable computing, studying dual aspects, that is, both attacks and defenses. Third, we provide a comprehensive study of the potential security, privacy, and safety enhancements to existing systems **based** on the emergence of wearable technology. Although several research works have emerged exploring different offensive and defensive uses of wearables, there is a lack of a broad and precise literature review systematizing all those security and privacy aspects and the underlying threat models. This research survey also analyzes current and emerging research trends and provides directions for future research. [ABSTRACT FROM AUTHOR]; DOI: 10.1145/3133837; (*AN 129932537*), Database: Applied Science & Technology Source

Subjects: Wearable technology; Computer security; Computer privacy; Technological innovations; Standards; Computer software; Software publishers (except video game publishers); Computer and software stores; Computer and Computer Peripheral Equipment and Software Merchant Wholesalers; Computer, computer peripheral and pre-packaged software merchant wholesalers

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

IPR2025-01313; Samsung
Ex. 1002 - Page 386

25. ## Testing the primary and convergent retrieval model of recall: Recall practice produces faster recall success but also faster recall failure.

By: Hopper, William J.; Huber, David E. *Memory & Cognition*. May2019, Vol. 47 Issue 4, p816-841. 26p. Abstract: The primary and convergent retrieval (PCR) model assumes that the act of successful recall not only boosts associations between the item and retrieval cues but additionally strengthens associations within the item (i.e., between the features of an item), speeding the rate of **information** retrieval from memory. The latter effect is termed intra-item learning and is a unique benefit of recall practice (i.e., the "testing effect"). Prior work confirmed the prediction that recall practice produces faster subsequent recall than restudy practice even if accuracy is higher following restudy. The current study replicated this result, but also examined the downside of recall practice: that after a failure to recall during practice, participants will be faster in their failure to recall on a subsequent recall test. This prediction was confirmed in a multisession cued recall experiment that collected accuracy and recall latency measurements for no practice, recall practice, or restudy, with an immediate or delayed final test. The linear ballistic accumulator model was fit to latency distributions, and model comparison **determined** that these effects reflect differences in drift rates, as predicted by the PCR model. [ABSTRACT FROM AUTHOR] DOI: 10.3758/s13421-019-00903-x. (*AN: 136445174*), Database: Business Source Complete

Subjects: Mathematical models; Task performance; Cognitive testing; Learning; Memory; Psychology; Research evaluation; Prompts (Psychology)

HTML Full Text **PDF Full Text** (1.9MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 387

26. ## 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

27. ## 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

IPR2025-01313; Samsung
Ex. 1002 - Page 388

28. ## Encyclopedia of Portal Technologies and Applications

By: Tatnall, Arthur. Hershey, PA : IGI Global. 2007. eBook. Description: 'This book offers complete coverage of the nature, characteristics, advantages, limitations, design, and evolution of Web portals. Other topics include semantic portals, philosophical portal issues, and personal portals. This authoritative encyclopedia encompasses the economics of setting up and **using** personal portals, knowledge management, strategic planning, **user** acceptance, security and the law'--Provided by publisher. (*AN 181467*), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / System Administration / Storage & Retrieval; COMPUTERS / Online Services / Resource Directories; Web portals--Encyclopedias; World Wide Web--Encyclopedias; Knowledge management--Encyclopedias; Online **information** services--Encyclopedias; Computer network resources--Encyclopedias

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

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 389

29. ## Profiling of the plasma proteome across different stages of human heart failure.

By: Egerstedt, Anna; Berntsson, John; Smith, Maya Landenhed; Gidlöf, Olof; Nilsson, Roland; Benson, Mark; Wells, Quinn S.; Celik, Selvi; Lejonberg, Carl; Farrell, Laurie; Sinha, Sumita; Shen, Dongxiao; Lundgren, Jakob; Rådegran, Göran; Ngo, Debby; Engström, Gunnar; Yang, Qiong; Wang, Thomas J.; Gerszten, Robert E.; Smith, J. Gustav. *Nature Communications* , 12/20/2019, Vol. 10 Issue 1, p1-13, 13p. Publisher: Springer Nature.:

Abstract Heart failure (HF) is a major public health problem characterized by inability of the heart to maintain sufficient output of blood. The systematic characterization of circulating proteins across different stages of HF may provide pathophysiological insights and identify therapeutic targets. Here we report application of aptamer-**based** proteomics to identify proteins associated with prospective HF incidence in a population-**based** cohort, implicating modulation of immunological, complement, coagulation, natriuretic and matrix remodeling pathways up to two decades prior to overt disease onset. We observe further divergence of these proteins from the general population in advanced HF, and regression after heart transplantation. By leveraging coronary sinus samples and transcriptomic tools, we describe likely cardiac and specific cellular origins for several of the proteins, including Nt-proBNP, thrombospondin-2, interleukin-18 receptor, gelsolin, and activated C5. Our findings provide a broad perspective on both cardiac and systemic factors associated with HF development. Heart failure is a major health issue worldwide. Here, Egerstedt et al. perform proteomic profiling of human plasma at different stages of heart failure, providing a comprehensive analysis of changes in the plasma proteome during disease progression. [ABSTRACT FROM AUTHOR]; (*AN 140453779*), Database: Complementary Index

Subjects: PROTEOMICS; HEART failure treatment; PATHOLOGICAL physiology; COHORT analysis; IMMUNOLOGY

Full Text Finder **USPTO Full Text Options**

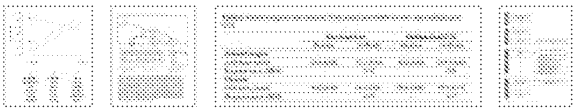
IPR2025-01313; Samsung
Ex. 1002 - Page 390

30. 25th Annual Conference of the International Society for Quality of Life Research.

Quality of Life Research. Oct2018 Supplement 1, Vol. 27 Issue 1, p1-190. 190p. 1 Color Photograph, 2 Black and White Photographs, 16 Diagrams, 47 Charts, 22 Graphs. DOI: 10.1007/s11136-018-1946-9. (*AN: 131927674*), Database: Academic Search Complete

Subjects: DATA analysis; BIG data; BLADDER cancer; ONCOLOGIC surgery; BURDEN of care; CANCER in children; LUNG cancer

Show all 88 images



PDF Full Text (11.8MB) **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 391

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	40920	("HITACHI MAXELL" or "MAXELL")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/02/17 12:22
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	2020/02/17 12:27
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	2020/02/17 12:28
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	2020/02/17 12:28
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	2020/02/17 12:28
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	2020/02/17 12:29
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	2020/02/17 12:29
L8	1	l1 and (((perform$3 with	US-PGPUB;	OR	OFF	2020/02/17

IPR2025-01313; Samsung
Ex. 1002 - Page 392

		communication) with (relat$3 with authentication with result)) with (between with ((first with communication with interface) and (second with communication with interface))))	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			12:29
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	2020/02/17 12:30
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	2020/02/17 12:30
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	2020/02/17 12:30
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	2020/02/17 12:30
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	2020/02/17 12:30
L14	222974	(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	2020/02/17 12:56
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	2020/02/17 12:56
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	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	OFF	2020/02/17 13:00

		device))))	IBM_TDB			
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	2020/02/17 13:01
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	2020/02/17 13:01
L19	3	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	2020/02/17 13:01
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	2020/02/17 13:01
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	2020/02/17 13:01
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	2020/02/17 13:02
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	2020/02/17 13:02
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	2020/02/17 13:02
L25	1	l14 and (((receiv$3 with (dynamic with biometric with information)) with (second with device)) with ((communication with "between") with	US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	OFF	2020/02/17 13:02

		((first with communication with interface) and (second with communication with interface))))	JPO; DERWENT; IBM_TDB			
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	2020/02/17 13:03

EAST Search History (Interference)

< This search history is empty>

2/ 17/ 2020 1:07:21 PM
C:\ Users\ ttruong4\ Documents\ EAST\ Workspaces\ Case-16535574-080819.wsp

IPR2025-01313; Samsung
Ex. 1002 - Page 395

Google transmitting the acquired dynamic biometric information through a first communicati Sign in

All News Shopping Images More Settings Tools

About 108,000 results (0.57 seconds)

www.google.com/patents/US20150379322

Method and apparatus for communication using fingerprint input

App. - Filed Jun 30, 2015 - Published Dec 31, 2015 - Suha Yoon - Samsung Electronics Co., Ltd.
The method includes detecting a **fingerprint information** input, changing a ... Image **acquisition** by non-optical methods, e.g. by ultrasonic or capacitive sensing ... recent electronic **devices** can perform **communication** between **devices** by ... For example, a **first** component may be referred to as a **second** component ... **interface** ...
Overview · Related · Discuss

www.google.com/patents/EP2920731A1?cl=en

Biometric system with body coupled communication interface

App. - Filed Nov 5, 2013 - Published Sep 23, 2015 - Johan-Paul Marie Gerard LINNARTZ - Koninklijke Philips N.V.
Info: Patent citations (26); Non-patent citations (2); Cited by (4) ... Removing noise from the **obtained biometric** data using the helper data allows the ... **from** a computing **device**, but this poses the problem of which wireless signal ... in use, the **first** body coupled **communication interface** would be arranged for ... **dynamically** ...
Overview · Related · Discuss

www.google.com/patents/US9342674

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

Grant - Filed Mar 5, 2015 - Issued May 17, 2016 - David S. Abdallah - Apple Inc.
For example, while the **first device** is proximate to a **second device**, the **first device** ... In response to detecting the **biometric information** associated with the user, ... **communication** ... GAW screens **transmit** a wave **through** the glass panel (**using** the glass as a ... **Fingerprint acquisition** assembly **using** prism and camera.
Overview · Related · Discuss

www.google.com/patents/US20150071502

Noise Reduction in Biometric Images

App. - Filed Sep 8, 2013 - Published Mar 12, 2015 - Michal Breznicky - Apple Inc.
The processing **device** can be configured to remove noise **from** a ... **dynamic** ... by the **biometric** sensing **device using** a **first** calibration image and a **second** ... of the **biometric** image can be **acquired** by a single sensing element. ... For example, a network **communication interface** can **transmit** ... **information** ...
Overview · Related · Discuss

www.google.com/patents/US20090328159

Systems and Methods for Secure Printing



App. - Filed Jun 30, 2008 - Published Dec 31, 2009 - Qi Luo - Konica Minolta Systems Laboratory, Inc.
The **first** security data is matched with **second** security data **obtained from** an ... may be **dynamically** assigned to different security levels corresponding to the ... **using** conventional **communication** protocols and/or data **port interfaces**. ... as the **biometric information obtained by biometric** identification **device** ...
Overview · Related · Discuss

www.google.com/patents/US20070198436

Method and apparatus for secure access payment and ...



App. - Filed Feb 21, 2007 - Published Aug 23, 2007 - Kenneth Weiss - Weiss Kenneth P
... **information**; and a secure system in **communication** with the **second device**. ... of a memorized PIN number or code, **biometric** identification such as a **fingerprint**, ... **transmitting from** a **first device**, **first** encrypted authentication **information** of the ... is configured to **communicate** with the magnetic card reader via the data **port**.
Overview · Related · Discuss

www.google.com/patents/US8151334

Communication card for mobile network devices and ...



Grant - Filed Oct 7, 2005 - Issued Apr 3, 2012 - Eric Lauper - Swisscom Ag
A removable **communication** card for mobile network **devices**, respectively a ... a network **interface** module for bidirectional **transmission** of data with a network, ... by a user is **transmitted** to **devices** of the network for user authentication. ... **dynamic** ... **first biometric** feature of the one user with the stored **biometric information** ...

IPR2025-01313; Samsung
Ex. 1002 - Page 396

Google transmitting the acquired dynamic biometric information through a first communicati Sign in

Grant · Filed Dec 3, 2007 · Issued Jan 27, 2015 · Luke Smith · Luke Smith

Biometric data is generated from such information and stored in a ... First, the user communication device, typically a cell phone, is powered up and allowed to ...

Overview · Related · Discuss

www.google.com/patents/US20100131414

Personal identification device for secure transactions



App. - Filed Mar 14, 2008 - Published May 27, 2010 - Gavin Randall Tame - Gavin Randall Tame

A processor compares acquired biometric data with the stored biometric ... data in the identification information transmitted via the communication terminal. ... The device has two wireless communication interfaces, in the form of a Blue ... The device to be issued is first interrogated using the pre-registered ...

Overview · Related · Discuss

www.google.com/patents/EP3035243A1?cl=en

Method of updating biometric feature pattern and electronic ...

App. - Filed Dec 14, 2015 - Published Jun 22, 2016 - Young-Eun Han - Samsung Electronics Co., Ltd

The method includes acquiring a plurality of biometric images. ... Among the various pieces of biometric information, a security method using the ... For example, a first user device and a second user device indicate different user ... an input/output interface 150, a display 160, and a communication interface 170. ... Dynamic ...

Overview · Related · Discuss

IPR2025-01313; Samsung
Ex. 1002 - Page 397

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 398

2. 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 399

3. ## 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 400

4. 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 401

5. ## 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 402

6. ## 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 focuse3 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 403

7. ## Cybersecurity challenges in vehicular **communications**

By El-Rewini, Zeinab; Sadatsharan, Karthikeyan; Selvaraj, Daisy Flora; Plathottam, Siby Jose; Ranganathan, Prakash. In *Vehicular Communications*. January 2019 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 404

8. ## 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 405

9. ## 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 406

10. ## 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 407

11. ## 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 408

12. ## 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 409

13. ## 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 410

14. 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 411

15. ## 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 412

16. ## 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 413

17. ## 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 414

18. ## 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**

IPR2025-01313; Samsung
Ex. 1002 - Page 415

19. ## 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 416

20. ## 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 417

21. ## 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 418

22. ## Recent progress in tactile sensors and their applications in intelligent systems

By Liu, Yue; Bao, Rongrong; Tao, Juan; Li, Jing; Dong, Ming; Pan, Caofeng. In *Science Bulletin.* 15 January 2020 65(1):70-88 Language: English. DOI: 10.1016/j.scib.2019.10.021 Abstract: With the rapid development of intelligent technology, tactile sensors as sensing **devices** constitute the core foundation of intelligent systems. Biological organs that can sense various stimuli play vital roles in the interaction **between** human beings and the external environment. Inspired by this fact, research on skin-like tactile sensors with multifunctionality and high performance has attracted extensive attention. An overview of the development of high-performance tactile sensors applied in intelligent systems is systematically presented. **First**, the development of tactile sensors endowed with stretchability, self-healing, biodegradability, high resolution and self-powered capability is discussed. Then, for intelligent systems, tactile sensors with excellent application prospects in many fields, such as wearable **devices**, medical treatment, artificial limbs and robotics, are presented. Finally, the future prospects of tactile sensors for intelligent systems are discussed. (*AN: S2095927319306164*), Database: ScienceDirect

Subjects: Tactile sensor; Intelligent system; Self-powered capability; Biodegradability; Self-healing

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 419

23. ELECTRONIC **DEVICE** FOR PROVIDING VR IMAGE BASED ON POLYHEDRON AND IMAGE PROVIDING METHOD THEREOF

Patent Application: 15/869399. Filed: January 12, 2018. Published: August 9, 2018. , Database: USPTO Patent Applications

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: edspap.20180225876

USPTO Full Text Options

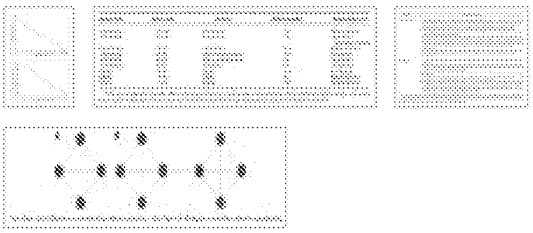
IPR2025-01313; Samsung
Ex. 1002 - Page 420

24. Friends, Gifts, and Cliques: Social Proximity and Recognition in Peer-Based Tournament Rituals.

By: Aadland, Erik; Cattani, Gino; Ferriani, Simone. *Academy of Management Journal.* Jun2019, Vol. 62 Issue 3, p883-917. 35p. 1 Diagram, 6 Charts, 5 Graphs. Abstract: Two main accounts of the effect of social proximity **between** candidates competing for recognition and members of the evaluating audience can be extrapolated from extant literature on peer-based tournament rituals and cultural fields. Following a Bourdieusian tradition, one account—which we label "self-reproduction"—points to the catalyzing effect of social proximity in shaping recognition along relational lines. Drawing from recent scholarship on social evaluation, a **second** account—which we call "intellectual distance"—suggests that social proximity deters recognition. We probe the influence of different articulations of social proximity (i.e., direct ties, cliquishness, and reciprocity) on recognition by studying awarding decisions within the context of the Norwegian advertising industry. Interviews with key informants as well as econometric results suggest that, while self-reproduction tends to prevail over intellectual distance, these effects coexist and their relative influence varies across levels of recognition. We gauge the relative saliency of the two accounts by using a mixed methods approach. Important implications for research on social evaluation and recognition in peer-based tournament rituals are drawn. [ABSTRACT FROM AUTHOR] DOI: 10.5465/amj.2016.0437. (*AN: 136916064*), Database: Business Source Complete

Subjects: Advertising; Other Services Related to Advertising; Outdoor Advertising; Awards; Social distance; Peers; Social perception

Show all 12 images



HTML Full Text **PDF Full Text** (529KB)

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 421

25. ## 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 422

26. ## Design of secure key management and user authentication scheme for fog computing services

By Wazid, Mohammad; Das, Ashok Kumar; Kumar, Neeraj; Vasilakos, Athanasios V.. In *Future Generation Computer Systems*. February 2019 91:475-492 Language: English. DOI: 10.1016/j.future.2018.09.017 Abstract: Fog computing (fog networking) is known as a decentralized computing infrastructure in which data, applications, compute as well as data storage are scattered in the most logical and efficient place among the data source (i.e., smart **devices**) and the cloud. It gives better services than cloud computing because it has better performance with reasonably low cost. Since the cloud computing has security and privacy issues, and fog computing is an extension of cloud computing, it is therefore obvious that fog computing will inherit those security and privacy issues from cloud computing. In this paper, we design a new secure key management and user authentication scheme for fog computing environment, called SAKA-FC. SAKA-FC is efficient as it only uses the lightweight operations, such as one-way cryptographic hash function and bitwise exclusive-OR (XOR), for the smart **devices** as they are resource-constrained in nature. SAKA-FC is shown to be secure with the help of the formal security analysis using the broadly accepted Real-Or-Random (ROR) model, the formal security verification using the widely-used Automated Validation of Internet Security Protocols and Applications (AVISPA) tool and also the informal security analysis. In addition, SAKA-FC is implemented for practical demonstration using the widely-used NS2 simulator. (*AN: S0167739X18303959*), Database: ScienceDirect

Subjects: Fog computing; Key management; Authentication; Services; Security; AVISPA; NS2 simulation

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

IPR2025-01313; Samsung
Ex. 1002 - Page 423

27. ## Mapping the rise of digital mental health technologies: Emerging issues for law and society

By Gooding, Piers. In *International Journal of Law and Psychiatry*. November-December 2019 67 Language: English. DOI: 10.1016/j.ijlp.2019.101498 Abstract: The use of digital technologies in mental health initiatives is expanding, leading to calls for clearer legal and regulatory frameworks. However, gaps in knowledge about the scale and nature of change impede efforts to develop responsible public governance in the early stages of what may be the mass uptake of 'digital mental health technologies'. This article maps established and emerging technologies in the mental health context with an eye to locating major socio-legal issues. The paper discusses various types of technology, including those designed for **information** sharing, **communication**, clinical decision support, 'digital therapies', patient and/or population monitoring and control, bio-informatics and personalised medicine, and service user health informatics. The discussion is organised around domains of use based on the actors who use the technologies, and those on whom they are used. These actors go beyond mental health service users and practitioners/service providers, and include health and social system or resource managers, data management services, private companies that collect personal data (such as major technology corporations and data brokers), and multiple government agencies and private sector actors across diverse fields of criminal justice, education, and so on. The mapping exercise offers a starting point to better identify cross-cutting legal, ethical and social issues at the convergence of digital technology and contemporary mental health practice. (*AN: S0160252719300950*), Database: ScienceDirect

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 424

28. A meta-analysis of virtual reality training programs for social skill development

By Howard, Matt C.; Gutworth, Melissa B.. In *Computers & Education*. January 2020 144 Language: English. DOI: 10.1016/j.compedu.2019.103707
Abstract: Recent years have seen an increase in the number of researchers and practitioners applying virtual reality (VR) to develop social skills, but varying levels of success have been observed when applying these VR training programs. Due to these disparities, review and summary work is needed to determine (a) whether these programs are effective and (b) the attributes of these programs that lead to success. In the current article, we perform a meta-analysis to determine the overall effectiveness of VR training programs for developing social skills, and we also study the effect of several moderating variables that may influence the effectiveness of these programs. We test whether certain aspects of the applied hardware (e.g. input devices, output devices), applied software (e.g. game elements, Second Life), participant population (e.g. general/specialized), and study design (e.g. type of control group, type of measure, others) influence the success of these programs. Sources were identified using EBSCO and Google Scholar, and, after our inclusion criteria were applied, 23 samples were included in our meta-analysis. Using a random-effects approach, we show that VR training programs, on average, perform better than alternative training programs for developing social skills, but almost all the other findings contradict current notions regarding these programs. Of note, gamified programs produced slightly worse outcomes than non-gamified programs, and programs utilizing immersive technologies (e.g. head-mounted displays) produced slightly worse outcomes than programs utilizing non-immersive displays (e.g. monitors). We provide suggestions regarding the effectiveness of VR training for social skills in comparison to alternative training approaches, the attributes of VR training programs that produce better outcomes, and directions for future research and practice. (*AN: S036013151930260X*), Database: ScienceDirect

Subjects: Virtual reality; Social skills; Learning; Training and development; Simulation

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 425

29. ## Emodash: a Dashboard Supporting Retrospective Awareness of Emotions in Online Learning

By Ezzaouia, Mohamed; Tabard, Auré lien; Lavoué, Elise. In *International Journal of Human - Computer Studies*. January 2018 Language: English. DOI: 10.1016/j.ijhcs.2020.102411 Abstract: Highlights •Design and in the wild study of an interactive dashboard called Emodash for retrospective awareness of learners emotions in a video-conferencing language learning environment.•Tutors mostly appreciate the overview elements of the dashboard, and used the detailed session view mostly to navigate through the session recording.•Emodash led tutors to write more formative and less summative feedback reports than without the dashboard.•Emodash led tutors to write more affective feedback reports than without the dashboard.•Visualizing learners emotions led to an increase in tutors self-awareness and reflection. (*AN: S1071581918305585*), Database: ScienceDirect

Subjects: Visualization; Dashboard; Awareness; Emotion; Online learning; Feedback

Full Text Finder **USPTO Full Text Options**

30. ## 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

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 426

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

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

... **Devices** with touch screens and/or applications **running** on such **devices** may be **unlocked** by ... aforementioned methods may be included in a computer program product configured for **execution** by one ... of a **device** at various points in the performance of an **unlock** action gesture ...

☆ 99 Cited by 1165 Related articles All 4 versions »

Wireless **device** enabled locking system

GL Myers, A Hirpara, JD Veleris, A Zimny... - US Patent ..., 2015 - Google Patents

... to the shape pattern received from the web portal 106 and successfully **executes** a parameter ... 500-502, the lock 100 begins its own **authentication** process by **executing** an encryption ... Alternatively or in addition, as part of the **authentication** process **executed** by the encryption ...

☆ 99 Cited by 113 Related articles All 4 versions »

... for **unlocking** a lock by a lock **device** enabled for short-range wireless data **communication** in compliance with a **communication** standard and associated **device**

O Bliding, J Hörberg - US Patent 8,593,249, 2013 - Google Patents

... lock decrypts the signal and compares it to the original to determine if the lock should be **unlocked** ... the delay that a user may experience waiting in front of the lock for it to **unlock** ... the **unlocking** method according to the **first** aspect is much faster than the **unlocking** method known ...

☆ 99 Cited by 35 Related articles All 4 versions »

Method for intermediate **unlocking** of a keypad on a mobile electronic **device**

K Simelius - US Patent 7,414,613, 2008 - Google Patents

... eg a predetermined number of input **operations** and/or to a defined number of **executed operations** ... Multi-purpose **devices** benefit the most from the ability to **execute** the previously ... Preferably, the electronic **device** further comprises a timer, for **executing** timer **related** detecting of ...

☆ 99 Cited by 70 Related articles All 4 versions »

Input to locked computing **device**

MJ Lebeau, JN Jitkoff, RP Guy - US Patent 8,402,533, 2013 - Google Patents

... The command, which is distinct from a command to **unlock** the **device**, can be **executed** while the ... for the full **unlocked** display of the **device** to be shown, and then **execute** a command ... command, it can **unlock** normally and notify the user when the **results** of **executing** the voice ...

☆ 99 Cited by 302 Related articles All 4 versions »

Extending user **authentication** across a trust group of smart **devices**

FM Tharappel, SS Shah, L Krishnamurthy... - US Patent ..., 2017 - Google Patents

... block diagram illustrating example logic that may be used to **execute** activities associated with the ... biometric credentials have been provided, the accessed smart **device** can **unlock** its **operating** ... through the wearable **device** to a Personal Assistant (PA) application **running** on the ...

☆ 99 Cited by 111 Related articles All 4 versions »

Method of **unlocking** a mobile electronic **device**

RAA Hainzl - US Patent 8,385,885, 2013 - Google Patents

... SONY MOBILE **COMMUNICATIONS** AB CORRECTIVE ASSIGNMENT TO CORRECT THE **EXECUTION** DATE PREVIOUSLY ... Microprocessor 109 may **execute** programs stored in memory 110 ... filters 116 and 117 may also be implemented as software **running** on microprocessor ...

☆ 99 Cited by 112 Related articles All 4 versions »

Cryptography and **authentication** on RFID passive tags for apparel products

KHM Wong, PCL Hui, ACK Chan - Computers in industry, 2006 - Elsevier

... P i be a k-bit PIN for tag i. Let r ← **Unlock**(P) denote the **execution** of "**unlock** ... function on T i . When an EPC tag replies with A = "ack", the "**unlock**" command is **executed** successfully ... Table 1. Two hundred measurements were made to **execute** cipher **operations** on a 64-bit string ...

☆ 99 Cited by 95 Related articles All 9 versions

Unlock screen

SE Teng, J Shi, A Shen, RM Haning, P Guntaur... - US Patent ..., 2013 - Google Patents

... B2 US 8355698B2 Authority US United States Prior art keywords mobile **communications** **communications** **device** **device** display **unlock** screen Prior art date ... 230000004044 **response** Effects 0 claims description 4; 230000002618 waking Effects 0 claims description 4; ...

☆ 99 Cited by 238 Related articles All 4 versions »

Mobile terminal, method of controlling the same, and computer program of the same

H Nagata - US Patent 7,366,497, 2008 - Google Patents

... 2 is a flowchart showing a control processing **executed** in the mobile telephone 1 according to ... the processing **procedure** of the software program which the CPU 101 **executes** in the ... function 302) instructs the opening/closing detection and lock mechanism 50 to **unlock** the upper ...

☆ 99 Cited by 226 Related articles All 4 versions »

STIC
Scientific and Technical Information Center

1. 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 429

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 430

3. 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 431

4. ## 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 432

5. ## 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 433

6. 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 434

7. ## 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 435

8. ## 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 436

9. ## 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 437

10. ## Multimodal Gait Recognition With Inertial **Sensor** Data and Video Using Evolutionary Algorithm.

By: Kumar, Pradeep; Mukherjee, Subham; Saini, Rajkumar; Kaushik, Pallavi; Roy, Partha Pratim; Dogra, Debi Prosad. *IEEE Transactions on Fuzzy Systems* , May2019, Vol. 27 Issue 5, p956-965, 10p. Publisher: IEEE.; Abstract Evolutionary decision fusion has applications in **biometric** authentication and verification. Gray wolf optimizer (GWO) is one such evolutionary decision fusion approach that can be used to tune the fusion parameters in a multimodal data **acquisition** system. Human gait is a proven **biometric** trait with applications in security and authentication. However, **acquiring** human-gait data can be erroneous due to various factors and multimodal fusion of such erroneous gait data can be challenging. In this paper, we propose a new decision fusion-based approach to solve the above problem. Gait data is recorded simultaneously using motion **sensors** and visible-light camera. The signals of the motion **sensors** are modeled using a long short-term memory neural network and corresponding video recordings are processed using a three-dimensional convolutional neural network. GWO has been used to optimize the parameters during fusion. It has been chosen based on the underlying hunting strategy that leads to better approximation of the solution. Interestingly, in our case it converges quicker than other optimization techniques such as genetic algorithm or particle swarm optimization. To test the model, a dataset involving 23 males and females has been recorded while they perform four different types of walks, including, normal walk, fast walk, walking while listening to music, and walking while watching multimedia content on a mobile. An overall accuracy of 91.3% has been recorded across all test scenarios. Results reveal that the proposed study can further be explored to design robust gait **biometric** systems. [ABSTRACT FROM AUTHOR]; (*AN 136253980*), Database: Complementary Index

Subjects: MULTIMODAL user interfaces; EVOLUTIONARY algorithms; GAIT in humans; PARTICLE swarm optimization; MOTION detectors; DATA **acquisition** systems

Get Full Text at IEEE *Xplore*® **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 438

11. 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 439

12. Bio-Inspired Presentation Attack Detection for Face **Biometrics**.

By: Tsifiridis, Aristeidis; Conde, Cristina; Gomez Ayllon, Beatriz; Cabello, Enrique. *Frontiers in Computational Neuroscience* , 5/28/2019, pN.PAG-N.PAG, 17p. Publisher: Frontiers Media S.A..; Abstract Today, face **biometric** systems are becoming widely accepted as a standard method for identity authentication in many security settings. For example, their deployment in automated border control gates plays a crucial role in accurate document authentication and reduced traveler flow rates in congested border zones. The proliferation of such systems is further spurred by the advent of portable **devices**. On the one hand, modern smartphone and tablet cameras have in-built user authentication applications while on the other hand, their displays are being consistently exploited for face spoofing. Similar to **biometric** systems of other physiological **biometric** identifiers, face **biometric** systems have their own unique set of potential vulnerabilities. In this work, these vulnerabilities (presentation attacks) are being explored via a biologically-inspired presentation attack detection model which is termed "BIOPAD." Our model employs Gabor features in a feedforward hierarchical structure of layers that progressively process and train from visual **information** of people's faces, along with their presentation attacks, in the visible and near-infrared spectral regions. BIOPAD's performance is directly compared with other popular biologically-inspired layered models such as the "Hierarchical Model And X" (HMAX) that applies similar handcrafted features, and Convolutional Neural Networks (CNN) that discover low-level features through stochastic descent training. BIOPAD shows superior performance to both HMAX and CNN in all of the three presentation attack databases examined and these results were consistent in two different classifiers (Support Vector Machine and k -nearest neighbor). In certain cases, our findings have shown that BIOPAD can produce authentication rates with 99% accuracy. Finally, we further introduce a new presentation attack database with visible and near-infrared **information** for direct comparisons. Overall, BIOPAD's operation, which is to fuse **information** from different spectral bands at both feature and score levels for the purpose of face presentation attack detection, has never been attempted before with a biologically-inspired algorithm. Obtained detection rates are promising and confirm that near-infrared visual **information** significantly assists in overcoming presentation attacks. [ABSTRACT FROM AUTHOR]; (*AN 136695700*), Database: Complementary Index

Subjects: BIOLOGICALLY inspired computing; SUPPORT vector machines; BORDER security; FACE

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 440

13. 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 441

14. **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 442

15. ## 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 443

16. ## 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 444

17. 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

18. 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 445

19. ## 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 446

20. Iris liveness detection for next generation smartphones.

By: Thavalengal, Shejin; Nedelcu, Tudor; Bigioi, Petronel; Corcoran, Peter. *IEEE Transactions on Consumer Electronics* , May2016, Vol. 62 Issue 2, p95-102, 8p. Publisher: IEEE.; Abstract This paper presents a novel liveness detection method that exploits the **acquisition** workflow for iris **biometrics** on smartphones using a hybrid visible (RGB)/near infra-red (NIR) **sensor**. These **devices** are able to capture both RGB and NIR images of the eye and iris region in synchronization. This multi-spectral **information** is mapped into a discrete feature space. An intermediate classifier which uses a distance metric close to Jenson-Shannon divergence is employed to classify the incoming image. Further, a fast, multi-frame pupil localization technique using one-dimensional processing of the eye region is proposed and evaluated. This is used to analyze the pupil characteristics of the images classified as 'live' in the previous stage. It is shown that such an analysis could detect presentation attacks, even with a 3-D face model made of materials that has properties similar to human skin and the ocular region1. [ABSTRACT FROM AUTHOR]; (*AN 116975157*), Database: Complementary Index

Subjects: SMARTPHONES; **BIOMETRIC** identification; IRIS (**Information** retrieval system); NEAR infrared spectroscopy; SPECTRAL imaging; EQUIPMENT & supplies

Linked Full Text **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 447

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

IPR2025-01313; Samsung
Ex. 1002 - Page 448

22. 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**

IPR2025-01313; Samsung
Ex. 1002 - Page 449

23. 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 450

24. ## Enhanced Sparse Representation-Based Device-Free Localization with Radio Tomography Networks.

By: Liu, Tong; Luo, Xiaomu; Liang, Zhuoqian. *Journal of Sensor & Actuator Networks* , Mar2018, Vol. 7 Issue 1, p7, 16p Abstract: The sparse distribution of targets in monitored areas is an important prior for device-free localization (DFL) with radio tomography networks. In this article, our goal is to develop an enhanced sparse representation-based DFL method that takes the full potential of sparsity for location reconstruction. An expanded sensing matrix spanning the concatenation of a sampling matrix and a unit error-correcting base is proposed for modelling the measurement process. The sampling matrix can either be composed of the ellipse model from calibrated networks or the received signal strength (RSS) fingerprint-based model induced by training samples with one person at predefined locations. Thus, the sparsity of targets is enhanced under the expanded sensing matrix and the ℓ_1-minimization-based approximations are derived for the recovery of locations. Experimental studies in an open outdoor scenario, in a line-of-sight (LOS) indoor scenario, and in a non-line-of-sight (NLOS) indoor scenario, are conducted to verify the efficacy of the proposed method. [ABSTRACT FROM AUTHOR]; DOI: 10.3390/jsan7010007; (*AN 128764158*), Database: Applied Science & Technology Source

Subjects: Radio networks; Tomography; Sparse matrices; Wireless sensor networks; Signal processing; Radio Networks

HTML Full Text **PDF Full Text** (3.5MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 451

25. ## Implementing Levels of Security using Multimodal Architecture.

By: Sinha, Kinnri; Kharge, Prachi; Pandey, Ajit; Sathyaraj R.. *International Journal of Advanced Research in Computer Science* , Mar/Apr2017, Vol. 8 Issue 3, p899-905, 7p Abstract: Following the announcement of Demonetization in India, there has been a heightened need for online payments which calls for increased security measures. The following paper analyses the different techniques that Cn be used for user authentication before transactions. This includes the incorporation of barcodes/ QR codes, behavioural **biometrics** and physical **biometrics** in the security measures. It then proposes a multimodal security model which suggests a combination of these techniques to make transactions safer and more secure. [ABSTRACT FROM AUTHOR]; (*AN 122961349*), Database: Applied Science & Technology Source

Subjects: Online data processing; Payment systems; Multimodal user interfaces; **Biometric** identification; Two-dimensional bar codes; Security systems; Security Systems Services (except Locksmiths); Financial Transactions Processing, Reserve, and Clearinghouse Activities

PDF Full Text (529KB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 452

26. 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 453

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

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 454

29. ## Toward decentralized intelligence in manufacturing: recent trends in automatic identification of things.

By: Liukkonen, Mika; Tsai, Tsung-Nan. *International Journal of Advanced Manufacturing Technology*. Dec2016, Vol. 87 Issue 9-12, p2509-2531. 23p.

Abstract: Development of decentralized solutions for managing individual products in manufacturing and postmanufacturing applications makes it possible to embed automation in the product flow, which is more efficient compared to the conventional approach based on automating individual unit processes. The decentralized approach can be enabled using manufacturing objects that are capable of negotiating with their environment, observing it, making decisions according to these observations, and sharing **information** on their status and needs. For these purposes, automatic identification (auto-ID) technology is required. Automatic identification involves techniques for automatically identifying things by using tokens with individual codes, collecting **information** on them, and transferring that **information** automatically into computer systems. In general, not only techniques such as barcode, optical character recognition (OCR), and Radio Frequency Identification (RFID) are associated with auto-ID but also other techniques that are less used in manufacturing can be highlighted. The present study seeks to map the existing techniques for automatic identification of objects and to determine their most potential targets of use in manufacturing. [ABSTRACT FROM AUTHOR] DOI: 10.1007/s00170-016-8628-y. (*AN: 119597148*), Database: Engineering Source

Subjects: DECENTRALIZATION in management; MANUFACTURING industries; **INFORMATION** sharing; OPTICAL character recognition **devices**; POTENTIAL theory (Physics)

Show all 11 images



PDF Full Text (2.8MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 455

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 456

Google performing communication relating to the authentication result between t Sign in

All News Images Shopping More Settings Tools

About 971,000 results (0.40 seconds)

www.google.com/patents/CN103647577B?cl=en
通信系统、通信设备和通信设备的控制方法 Method of controlling a communication ...

Grant - Filed Jun 2, 2009 - Issued Jan 20, 2016 - 森友和夫 - 佳能株式会社
The present invention includes the **communication** system with DSC and printer. ... connection status in the **first communication** layers, **perform** the **authentication** ... and **second communication** equipment via **communication interface**, wherein, ... status in **second communication** layer **between** described **first communication** ...
Overview · Related · Discuss

www.google.com/patents/US20130267205
Communication apparatus, communication system, notification ...

App. - Filed Jun 6, 2013 - Published Oct 10, 2013 - Kazuo Takada - Sony Corporation
CROSS REFERENCES TO RELATED APPLICATIONS ... Then, after the **second communication** unit receives a **result** of **authentication** based ... a notification unit which carries out a notification for a user, to **perform** a function as a ... as a proximity **communication** method which is for **communicating between** very ... **interface** ...
Overview · Related · Discuss

www.google.com/patents/US9622088
Communication system, communication device, program and ...

Grant - Filed Dec 18, 2015 - Issued Apr 11, 2017 - Ryo Sawai - Sony Corporation
There is provided a **communication** system comprising: a **first communication** device ... **authentication** node is **performed** as a **communication between** logical ...
Overview · Related · Discuss

www.google.com/patents/US20130124651
File-based application programming interface providing ...

App. - Filed Nov 11, 2011 - Published May 16, 2013 - Michael T. Kain - Michael T. Kain
In particular, the present disclosure **relates** to a file-based API providing ... In a **second** aspect, a method of securing data at a **communication interface** of a ...
Overview · Related · Discuss

www.google.com/patents/US20020126845
Method for performing short-range wireless transactions ...

App. - Filed Jul 27, 2001 - Published Sep 12, 2002 - Cyril Hue - Alcatel
The invention **relates** notably to a method for **performing** a short-range wireless ... The hybrid terminal is able to **communicate** over a **first interface** with a radio ...
Overview · Related · Discuss

www.google.com/patents/US8218459
Topology hiding of a network for an administrative interface ...

Grant - Filed Dec 20, 2007 - Issued Jul 10, 2012 - Brian Stucker - Genbrand US LLC
An administrative **interface** is provided **between** a **first** network and a ... At least one of authorization, **authentication**, and accounting ... **interface** is provided to **perform** topology hiding of the **first** network ... Priority and **Related** Applications ... **between first** and **second** networks through the **communications** ...
Overview · Related · Discuss

www.google.com/patents/WO2014122076A2?cl=en
Body coupled communication system

App. - Filed Jan 31, 2014 - Published Aug 14, 2014 - Sotir Filipov OUZOUNOV - Koninklijke Philips N.V.
The **first** and **second** body coupled **communication interfaces** (114, 134) ... **communication** (BCC) allows exchange of information **between** devices that are ... This basically means that the physical **communication** is **performed** via the ... **resulting** ... it is only **relevant** that the authenticator at least needs the key to **authenticate** ...
Overview · Related · Discuss

www.google.com/patents/US6836814
Mobile communication terminal device

IPR2025-01313; Samsung
Ex. 1002 - Page 457



Grant - Filed Mar 19, 2001 - Issued Dec 28, 2004 - Toshiaki Takaoka - Kabushiki Kaisha Toshiba
According to the present invention, a serial control signal **interface** and a serial ... CROSS-REFERENCE TO **RELATED** APPLICATIONS ... external connector **between** the mobile **communication** terminal device itself ... of the **first** and the **second interfaces** on the basis of the determination **result** of ... **performs** ... **authentication** ...
Overview · Related · Discuss

www.google.com/patents/US20070191056

Controlling alternative communication pathway utilization in ...



App. - Filed May 24, 2006 - Published Aug 16, 2007 - Jeyhan Karaoguz - Jeyhan Karaoguz
A system and method for controlling alternative **communication** pathway ... **perform** a plurality of types of **communication** over the **second communication** network. ... a user to choose **between** a plurality of **communication** networks through which ... In an exemplary configuration where the **first communication interface** module ...
Overview · Related · Discuss

www.google.com/patents/EP2843973A1?cl=en

Information processing device, information processing ...



App. - Filed Mar 26, 2013 - Published Mar 4, 2015 - Katsuya Shimoji - Sony Corporation
... **first communication** path from at least one of a **first** and **second** control target device which are target devices to be caused to **perform** wireless **communication** ...
Overview · Related · Discuss

IPR2025-01313; Samsung
Ex. 1002 - Page 458

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

All News Videos Images More Settings Tools

About 12,200 results (0.53 seconds)

www.google.com/patents/US7020306
Personal authentication system using biometrics information

Grant - Filed Aug 15, 2000 - Issued Mar 28, 2006 - Takashi Shinzaki - Fujitsu Limited
A personal authentication system using **biometrics information**, which ... **acquired** through said **biometrics information** inputting section, into a **state** to be ... **condition under** which the registered **biometric information** was **acquired**, and ... **dynamic** ... registering section **for** previously **preserving** auxiliary **biometrics** characteristic ...
Overview · Related · Discuss

www.google.com/patents/US9329771
Embedded authentication systems in an electronic device
Grant - Filed Jun 20, 2014 - Issued May 3, 2016 - Anthony Fadell - Apple Inc
While a respective function of the device is in a locked **state**, the device ... the input meets **unlock** criteria based at least in part on **fingerprint information** of the ... criteria, the device **maintains** the respective function in the locked **state**. ... In some embodiments, input/output circuitry **can** also convert digital data into ... **condition**.
Overview · Related · Discuss

www.google.com/patents/EP3101868A1?cl=en
Device, method, and graphical user interface for ...
App. - Filed Sep 9, 2014 - Published Dec 7, 2016 - Byron Han - Apple Inc.
While a device is in a locked mode of operation in which access to a ... the **fingerprint** sensor: determining whether the first input meets one of **unlock** ... the first **unlock**-failure criteria, **maintaining** the device in the locked mode and ... **acquisition** ... display **state**, indicating what applications, views or other **information** occupy ...
Overview · Related · Discuss

www.google.com/patents/US20130287272
Methods and Apparatus of Integrating Fingerprint Imagers ...

App. - Filed Apr 29, 2012 - Published Oct 31, 2013 - Yang Lu - Yang Lu
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 ...
Overview · Related · Discuss

www.google.com/patents/US20060120573
Integrated system for detecting and matching fingerprints

App. - Filed Feb 4, 2004 - Published Jun 8, 2006 - Marco Iori - Saibert Co. Ltd.
A system **for** obtaining a quality image by the use of at least one **biometric** ... **info** ... The above described difficulties make it impossible at the present **state** of the art ... **can** obtain the **acquisition** of a **fingerprint** image even **under** critical **conditions** ... and charge input to each image pixel suitable **for keeping** a sufficient contrast ...
Overview · Related · Discuss

www.google.com/patents/US7974446
Personal authentication system using biometrics information

Grant - Filed Jan 23, 2006 - Issued Jul 5, 2011 - Takashi Shinzaki - Fujitsu Limted
A personal authentication system using **biometrics information**, which ... **acquired** through said **biometrics information** inputting section, into a **state** to ... **condition under** which the registered **biometric information** was **acquired**, and a ... **dynamic** ... **can** ... 125 is **for** previously registering and **retaining** the registration **fingerprint** ...
Overview · Related · Discuss

www.google.com/patents/CN203552322U?cl=en
Intelligent lock with image acquisition function
Grant - Filed Sep 29, 2013 - Issued Apr 16, 2014 - 王林祥 - 西安祥泰软件设备系统有限责任公司
The utility model relates to an intelligent lock with an image **acquisition** function. ... image **information** of a current user needing **unlocking** **can** be **acquired** when ... described **fingerprint acquisition** device is used **for** gathering user's **fingerprint**, ... 12 **can** judge whether to detect **unlocking** signal according to the level **state** of ...
Overview · Related · Discuss

www.google.com/patents/US9569655

Digital voting logic for manufacturable finger asperity ...

Grant - Filed Apr 25, 2012 - Issued Feb 14, 2017 - Jack Harper - Jack Harper
Each sensor cell cluster can include a plurality of solid-state sensor cells, where each ... In general, biometric systems do not capture fingerprint information in a ...
Overview · Related · Discuss

www.google.com/patents/CN101493883A?cl=en

Method for unlocking locked operational equipment and ...

App. - Filed Jan 21, 2008 - Published Jul 29, 2009 - 林建良 - 宏达国际电子股份有限公司
The invention discloses a method for unlocking a locked arithmetic device, which ... the biometric characteristic information meets preset conditions; and unlocking ... unlocking device, so the user will not need to be manually unlocked state of ... is acquired user's face contour features 210, and the predetermined condition is ...
Overview · Related · Discuss

www.google.com/patents/US9677894

Vehicle operations based on biometric fingerprint analysis

Grant - Filed Nov 3, 2015 - Issued Jun 13, 2017 - Eli M. Dow - International Business Machines Corporation
Embodiments of the present invention provide a method and system for enacting various ... initially, identifying information is acquired from a user of a vehicle.
Overview · Related · Discuss

IPR2025-01313; Samsung
Ex. 1002 - Page 460

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

All News Images Shopping More Settings Tools

About 45,400 results (0.55 seconds)

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

Biological information acquisition device, method for ...

App. - Filed May 15, 2007 - Published Jan 9, 2008 - 天野和彦 - 精工爱普生株式会社;国立大学法人北海道大学

A biological **information acquisition device** that **acquires information** from a ... to authenticate the regular **user**, the **fingerprint** into line using the regular **user**, iridescent ... **dynamic** range, there quality and accuracy of the biological **information** can ... by irradiating light to **acquire biometric information** of the living **body**; and an ...

Overview · Related · Discuss

www.google.com/patents/WO2016171295A1?cl=en

Authentication in ubiquitous environment

App. - Filed Apr 23, 2015 - Published Oct 27, 2016 - 최운호 - 최운호

In particular, IoT to configure the Network **Device** Currently IoT are generally ... Further, to describe the elements of the present invention, **first**, it is possible to use ... In particular, the **dynamic** signature **sensor** may be coupled to a display ... Bio-**information acquisition** module 311 **acquires** the user's **biometric** ...

Overview · Related · Discuss

www.google.com/patents/US8463003

Biometric information acquisition apparatus, biometric ...



Grant - Filed Dec 2, 2009 - Issued Jun 11, 2013 - Hiroyasu Otsubo - Hitachi Maxell, Ltd.

A **biometric information acquisition** apparatus includes: a light guide that ... a **first** light reflective surface that is opposed to the input surface and is provided at ... A subject image can be **acquired** within a desired range by employing the ... and an image pickup **device** that receives a light beam incident through the ... **dynamic** ...

Overview · Related · Discuss

www.google.com/patents/US9373047

Biometric authentication device, biometric authentication ...

Grant - Filed Mar 9, 2012 - Issued Jun 21, 2016 - Takahiro Aoki - Fujitsu Limited

A **biometric** authentication **device** includes a photographing unit configured to photograph a biological **body** and **acquire** biological **body information**; an authentication unit ... a **user** for which authentication has been frequently unsuccessful to reregister the ... **First**, a description is given of the **sensor** unit 10. ... **Dynamic** ...

Overview · Related · Discuss

www.google.com/patents/CN102110195A?cl=en

Computer system and identification method and device for user

App. - Filed Dec 25, 2009 - Published Jun 29, 2011 - 刘欣房 - 中国长城计算机深圳股份有限公司

The method comprises the following steps of: driving a biological **information** ... of the computer **user**, and comparing the **acquired** biological **information** with the ... and the processing chip the biological **information sensor** bidirectional ... identification command, the **user's biometric information acquisition** computer, ... **First** ...

Overview · Related · Discuss

www.google.com/patents/US20090232362

Biometric information acquisition apparatus and biometric ...



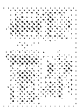
App. - Filed Mar 11, 2009 - Published Sep 17, 2009 - Hiroyasu Otsubo - Hitachi Maxell, Ltd.

A **biometric information acquisition** apparatus includes a light ... and a **first** transfer region to transfer the **biometric information acquired** by ...

Overview · Related · Discuss

www.google.com/patents/EP1791073A1?cl=en

Processing device, helper data generating device, terminal ...



App. - Filed Aug 30, 2006 - Published May 30, 2007 - Kenta Takahashi - Hitachi, Ltd.

When a **user** is authenticated, the authentication terminal (100) generates an ... In general, each time digital data on **biometric information** is **acquired**, its value ...

Overview · Related · Discuss

www.google.com/patents/US8797140

Biometric authentication method and biometric authentication ...



Grant - Filed Mar 3, 2008 - Issued Aug 5, 2014 - Takashi Shinzaki - Fujitsu Limited
... **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 ...
Overview · Related · Discuss

www.google.com/patents/US20160162673

Technologies for learning body part geometry for use in ...



App. - Filed Dec 5, 2014 - Published Jun 9, 2016 - Gershom Kutliroff - Gershom Kutliroff
The **Biometric** authentication processes utilizing the technologies are also described. ... **biometric information** from a **body** part of a **user**, such as the **user's** hand. ... that utilize the **biometric** reference template generated by the **first device**. ... then be **acquired**, e.g., with a depth **sensor** such as a depth camera.
Overview · Related · Discuss

www.google.com/patents/US20080123905

Biometrics device



App. - Filed Jun 26, 2007 - Published May 29, 2008 - Kazutaka Ito - Kazutaka Ito
The present invention relates to a **biometrics device**, and more particularly to a vein ... since it enables image **information** on a living **body** to be **acquired** processed ... 1 of a vein authentication **device**, which is a **first** embodiment of the invention, ... Sweep-type **fingerprint sensor device** capable of guiding a finger in a fixed ...
Overview · Related · Discuss

IPR2025-01313; Samsung
Ex. 1002 - Page 462

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	3	"8667562".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/02/16 23:03
L2	1426	("HIRABAYASHI, MASAYUKI" or "HASHIMOTO, YASUNOBU" or "YOSHIZAWA, KAZUHIKO").inv.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/02/16 23:37
L3	1	l2 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	2020/02/16 23:41
L4	1	l2 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	2020/02/16 23:44
L5	1	l2 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	2020/02/16 23:46
L6	1	l2 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	2020/02/16 23:49
L7	1	l2 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	2020/02/16 23:51
L8	2	l2 and ((receiv$3 with (dynamic with	US-PGPUB;	OR	OFF	2020/02/16

IPR2025-01313; Samsung
Ex. 1002 - Page 463

		biometric with information)) with (transmit$4 with (first with communication with interface)))	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			23:52
L9	1	l2 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	2020/02/16 23:55
L10	1	l2 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	2020/02/17 00:00
L11	1	l2 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	2020/02/17 00:04
L12	1	l2 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	2020/02/17 00:05
L13	1	l2 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	2020/02/17 00:12
L14	1	l2 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	2020/02/17 00:14
S179	2	"10423769".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/02/15 22:49
S180	2	"9373047".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	OFF	2020/02/16 16:27

			IBM_TDB			
S181	0	"20100131414".pn.	USPAT	OR	OFF	2020/02/16 17:40
S182	3	"20100131414".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/02/16 17:40
S183	1	"9314193".pn.	USPAT	OR	OFF	2020/02/16 17:57
S184	2	"8218459".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/02/16 18:55

EAST Search History (Interference)

< This search history is empty>

2/ 17/ 2020 12:18:00 AM
C:\ Users\ ttruong4\ Documents\ EAST\ Workspaces\ Case-16535574-080819.wsp

STIC
Scientific and Technical Information Center

1. 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 466

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 467

3. ## 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 468

HTML Full Text PDF Full Text (2.8MB) USPTO Full Text Options

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 469

5. ## 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 470

6. ## 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 471

7. 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 472

8. ## 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 473

9. 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 474

10. 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 475

11. ## 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 476

12. ## 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 477

13. ## 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 478

14. ## 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 479

15. ## 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*. January 2019 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 important 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 480

16. ## 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 481

17. 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 482

18. ## Continuous and transparent multimodal **authentication**: reviewing the state of the art.

By: Al Abdulwahid, Abdulwahid; Clarke, Nathan; Stengel, Ingo; Furnell, Steven; Reich, Christoph. *Cluster Computing* , Mar2016, Vol. 19 Issue 1, p455-474, 20p. Publisher: Springer Nature.; Abstract Individuals, businesses and governments undertake an ever-growing range of activities online and via various Internet-enabled digital devices. Unfortunately, these activities, services, **information** and devices are the targets of cybercrimes. Verifying the **user** legitimacy to use/access a digital device or service has become of the utmost importance. **Authentication** is the frontline countermeasure of ensuring only the authorized **user** is granted access; however, it has historically suffered from a range of issues related to the security and usability of the approaches. They are also still mostly functioning at the point of entry and those **performing** sort of re-**authentication** executing it in an intrusive manner. Thus, it is apparent that a more innovative, convenient and secure **user authentication** solution is vital. This paper reviews the **authentication** methods along with the current use of **authentication** technologies, aiming at developing a current state-of-the-art and identifying the open problems to be tackled and available solutions to be adopted. It also investigates whether these **authentication** technologies have the capability to fill the gap between high security and **user** satisfaction. This is followed by a literature review of the existing research on continuous and transparent multimodal **authentication**. It concludes that providing **users** with adequate protection and convenience requires innovative robust **authentication** mechanisms to be utilized in a universal level. Ultimately, a potential federated **biometric authentication** solution is presented; however it needs to be developed and extensively evaluated, thus operating in a transparent, continuous and **user**-friendly manner. [ABSTRACT FROM AUTHOR]; (*AN 114014182*), Database: Complementary Index

Subjects: COMPUTER access control; COMPUTER crimes; ELECTRONIC countermeasures; **BIOMETRIC** identification; ELECTRONIC **authentication**

Linked Full Text **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 483

19. **Biometric User Authentication** for IT Security : From Fundamentals to Handwriting

By: Vielhauer, Claus. Series: Advances in **Information** Security, Vol. 18. New York : Springer. 2006. eBook. Description: **Biometric user authentication** techniques evoke an enormous interest by science, industry and society. Scientists and developers constantly pursue technology for automated determination or confirmation of the identity of subjects **based** on measurements of physiological or behavioral traits of humans. **Biometric User Authentication** for IT Security: From Fundamentals to Handwriting conveys general principals of passive (physiological traits such as fingerprint, iris, face) and active (learned and trained ... (*AN 150663*), 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; COMPUTERS / **User** Interfaces; **Biometric** identification

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 484

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 485

21. ## Sensors of Smart Devices in the Internet of Everything (IoE) Era: Big Opportunities and Massive Doubts.

By: Masoud, Mohammad; Jaradat, Yousef; Manasrah, Ahmad; Jannoud, Ismael. *Journal of Sensors*. 5/15/2019, p1-26. 26p. Abstract: Smart device industry allows developers and designers to embed different sensors, processors, and memories in small-size electronic devices. Sensors are added to enhance the usability of these devices and improve the quality of experience through data collection and analysis. However, with the era of big data and machine learning, sensors' data may be processed by different techniques to infer various hidden **information**. The extracted **information** may be beneficial to device **users**, developers, and designers to enhance the management, operation, and development of these devices. However, the extracted **information** may be used to compromise the security and the privacy of humans in the era of Internet of Everything (IoE). In this work, we attempt to review the process of inferring meaningful data from smart devices' sensors, especially, smartphones. In addition, different useful machine learning applications **based** on smartphones' sensors data are shown. Moreover, different side channel attacks utilizing the same sensors and the same machine learning algorithms are overviewed. [ABSTRACT FROM AUTHOR] DOI: 10.1155/2019/6514520. (*AN: 136455227*), Database: Computers & Applied Sciences Complete

Subjects: Intelligent sensors; Electronic apparatus & appliances; Internet; Big data; Machine learning

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

IPR2025-01313; Samsung
Ex. 1002 - Page 486

22. Speaker **Authentication**

By: Li, Qi. Series: Signals and Communication Technology. Heidelberg : Springer. 2012. eBook. Description: This book focuses on use of voice as a **biometric** measure for personal **authentication**. In particular,'Speaker Recognition'covers two approaches in speaker **authentication**: speaker verification (SV) and verbal **information** verification (VIV). The SV approach attempts to verify a speaker's identity **based** on his/her voice characteristics while the VIV approach validates a speaker's identity through verification of the content of his/her utterance(s). SV and VIV can be combined for new applications. This ... (*AN 1245129*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Electronics / General; COMPUTERS / Artificial Intelligence / Computer Vision & Pattern Recognition; TECHNOLOGY & ENGINEERING / Engineering (General); Automatic speech recognition

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 487

23. **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: Computers & Applied Sciences Complete

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

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

IPR2025-01313; Samsung
Ex. 1002 - Page 488

24. ## Insight Into Insiders and IT.

By: Homoliak, Ivan; Toffalini, Flavio; Guarnizo, Juan; Elovici, Yuval; Ochoa, Martín. *ACM Computing Surveys.* Mar2019, Vol. 52 Issue 2, p1-40. 40p.
Abstract: Insider threats are one of today's most challenging cybersecurity issues that are not well addressed by commonly employed security solutions. In this work, we propose structural taxonomy and novel categorization of research that contribute to the organization and disambiguation of insider threat incidents and the defense solutions used against them. The objective of our categorization is to systematize knowledge in insider threat research while using an existing grounded theory method for rigorous literature review. The proposed categorization depicts the workflow among particular categories that include incidents and datasets, analysis of incidents, simulations, and defense solutions. Special attention is paid to the definitions and taxonomies of the insider threat; we present a structural taxonomy of insider threat incidents that is **based** on existing taxonomies and the 5W1H questions of the **information** gathering problem. Our survey will enhance researchers' efforts in the domain of insider threat because it provides (1) a novel structural taxonomy that contributes to orthogonal classification of incidents and defining the scope of defense solutions employed against them, (2) an overview on publicly available datasets that can be used to test new detection solutions against other works, (3) references of existing case studies and frameworks modeling insiders' behaviors for the purpose of reviewing defense solutions or extending their coverage, and (4) a discussion of existing trends and further research directions that can be used for reasoning in the insider threat domain. [ABSTRACT FROM AUTHOR]
DOI: 10.1145/3303771. (*AN: 137310279*), Database: Computers & Applied Sciences Complete

Subjects: Grounded theory; Literature reviews; Definitions; Workflow software; Computer crime prevention

HTML Full Text **USPTO Full Text Options**

25. ## Review of continuous touch **based user authentication**.

By: Shaji, Shamily; Das, Smija; Kizhakkethottam, Jubilant J. *2015 IEEE International Conference on **Information** & Automation* , 2015, p1-5, 5p.
Publisher: IEEE. (*AN 111122830*), Database: Complementary Index

Get Full Text at IEEE *Xplore*® **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 489

26. Abstract.

Basic & Clinical Pharmacology & Toxicology. Jan2019 Supplement S, p3-119. 117p. DOI: 10.1111/bcpt.13173. (*AN: 134091944*), Database: Academic Search Complete

Subjects: NON-insulin-dependent diabetes; AIR pollution; DEEP learning; MAGNETIC resonance imaging of the brain; SKIN disease diagnosis; REHABILITATION

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

27. Abstract.

Basic & Clinical Pharmacology & Toxicology. Dec2018 Supplement S2, Vol. 124, p3-119. 117p. DOI: 10.1111/bcpt.13173. (*AN: 133465006*), Database: Academic Search Complete

Subjects: NON-insulin-dependent diabetes; AIR pollution; SKIN injuries; MAGNETIC nanoparticles; MAGNETIC resonance imaging; Diagnostic Imaging Centers

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

IPR2025-01313; Samsung
Ex. 1002 - Page 490

28. ## On Hunting Animals of the **Biometric** Menagerie for Online Signature.

By: Houmani, Nesma; Garcia-Salicetti, Sonia. *PLoS ONE*. 4/7/2016, Vol. 11 Issue 4, p1-26. 26p. Abstract: Individuals behave differently regarding to **biometric authentication** systems. This fact was formalized in the literature by the concept of **Biometric** Menagerie, defining and labeling **user** groups with animal names in order to reflect their characteristics with respect to **biometric** systems. This concept was illustrated for face, fingerprint, iris, and speech modalities. The present study extends the **Biometric** Menagerie to online signatures, by proposing a novel methodology that ties specific quality measures for signatures to categories of the **Biometric** Menagerie. Such measures are combined for retrieving automatically writer categories of the extended version of the **Biometric** Menagerie. Performance analysis with different types of classifiers shows the pertinence of our approach on the well-known MCYT-100 database. [ABSTRACT FROM AUTHOR] DOI: 10.1371/journal.pone.0151691. (*AN: 114319557*), Database: Academic Search Complete

Subjects: MENAGERIES; **BIOMETRIC** identification; HUNTING; ZOOLOGICAL nomenclature; DIGITAL signatures; Hunting and Trapping; Zoos and Botanical Gardens

PDF Full Text (6.6MB) **USPTO Full Text Options**

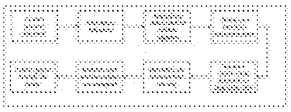
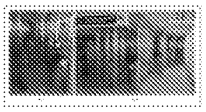
IPR2025-01313; Samsung
Ex. 1002 - Page 491

29. ## **Biometric** Recognition in Automated Border Control: A Survey.

By: LABATI, RUGGERO DONIDA; GENOVESE, ANGELO; MUÑOZ, ENRIQUE; PIURI, VINCENZO; SCOTTI, FABIO; SFORZA, GIANLUCA. *ACM Computing Surveys*. Nov2016, Vol. 49 Issue 2, p24-24:39. 39p. 3 Color Photographs, 5 Diagrams, 3 Charts, 1 Map. Abstract: The increasing demand for traveler clearance at international border crossing points (BCPs) has motivated research for finding more efficient solutions. Automated border control (ABC) is emerging as a solution to enhance the convenience of travelers, the throughput of BCPs, and national security. This is the first comprehensive survey on the **biometric** techniques and systems that enable automatic identity verification in ABC. We survey the **biometric** literature relevant to identity verification and summarize the best practices and **biometric** techniques applicable to ABC, relying on real experience collected in the field. Furthermore, we select some of the major **biometric** issues raised and highlight the open research areas. [ABSTRACT FROM AUTHOR] DOI: 10.1145/2933241. (*AN: 116668794*), Database: Computers & Applied Sciences Complete

Subjects: Biometric identification; Border security; Surveillance detection; Boundaries; Security management

Show all 12 images



PDF Full Text (1.1MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 492

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 493

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 166 Related articles All 4 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 634 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 549 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 520 Related articles All 2 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 »

Dynamic modification of a messaging language

OK Thörn - 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 168 Related articles All 4 versions »

Dynamic card verification values and credit transactions

M Stanfield, G Tsantes, J Vacca - US Patent 8,567,670, 2013 - Google Patents
... Examples of computer-readable media include hard drives, flash memory, other **dynamic** memory, and other ... User's computing **device** 202 may include a user **interface** 213 to **receive** user input 214 ... In step 502, the user's computing **device** 401 **receives** a request from the user to ...
☆ 99 Cited by 123 Related articles All 4 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 237 Related articles All 2 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 494

Biometric input **device with** peripheral **port**

CS Dunn, SJ Borza, G Freedman - US Patent 5,987,155, 1999 - Google Patents

... in the absence of a detected peripheral card and transmitting a signal **received** from the ... the smart card 5 and for providing **information** thereto and **receiving information** therefrom ... are registered and the users are provided access upon presentation of their **biometric information** ...

☆ 99 Cited by 255 Related articles All 2 versions »

Wireless smart card and integrated personal area network, near field **communication** and contactless payment system

M Loh, A Tam - US Patent App. 12/234,499, 2009 - Google Patents

... An NFC Antenna 344 is connected to the transceiver to transmit or **receive** the NFC or ... the wireless smart card 104 can be queried in a secure manner for **dynamic** authentication of ... If yes, the process continues by requesting/**receiving** a **device** PIN from the wireless smart card ...

☆ 99 Cited by 331 Related articles All 2 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 448 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 885 Related articles All 27 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 100 Related articles All 6 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 297 Related articles All 8 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 211 Related articles All 15 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 99 Related articles All 5 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 73 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 838 Related articles All 13 versions

IPR2025-01313; Samsung
Ex. 1002 - Page 496

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 107 Related articles All 6 versions

Biometric signature **authentication** using radon transform-**based** watermarking techniques

E Maiorana, P Campisi, A Neri - 2007 **Biometrics** Symposium, 2007 - ieeexplore.ieee.org

... M(B) connected with the mean value of each Radon projection. **Doing** this for each subband a' C F, four host vectors wa ... cors das os: tures vectors as follows: features which will be used to **perform** the first level of **user authentication** ... bedding **performed** in the ridgelet domain ...

☆ 99 Cited by 48 Related articles All 4 versions

IPR2025-01313; Samsung
Ex. 1002 - Page 497

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 positioning **information**. Download PDF **Info** ... 87995597A US 6148261 A US6148261 A US 6148261A Authority US United States Prior art keywords map processor map **information information** communicator Prior ...

☆ 99 Cited by 634 Related articles All 2 versions »

Secure **dynamic** credential distribution over a network

CR Lehew, HS Pyle, NJ Fang - US Patent 7,546,373, 2009 - Google Patents

... is an example of a time when the second computing device may wish to automatically **receive** a securely ... 4B) in a secure fashion due to the encryption of the client's public key, and **received** by the ... Just after **receiving** and decrypting the credentials as shown in area EE of FIG ...

☆ 99 Cited by 49 Related articles All 4 versions »

Systems and methods for **dynamic** authentication using physical keys

GL Thione, J Trevor, D Hilbert - US Patent 7,562,385, 2009 - Google Patents

... lists to adjust the group of valid user devices from which a confirmation may be **received** ... system 100 authenticates the service bureau's multi-function guest device 307 to **receive information** from the ... to the physical key based on the **first** set of associations; **receiving**, over a ...

☆ 99 Cited by 90 Related articles All 4 versions »

Methods and systems for single sign on with **dynamic** authentication levels

R Wenzel, A Kalinovsky, JM Billinghay... - US Patent ..., 2012 - Google Patents

... ELECTRICITY; H04—ELECTRIC **COMMUNICATION** TECHNIQUE; H04L—**TRANSMISSION** OF DIGITAL **INFORMATION**, eg TELEGRAPHIC ... Method and systems for single sign on with **dynamic** authentication levels is ... The method include **receiving** a data request for access to a ...

☆ 99 Cited by 122 Related articles All 4 versions »

Mobile device with scannable image including **dynamic** data

A Gaddam, G Prakash, S Aissi - US Patent 9,779,345, 2017 - Google Patents

... It may also **receive** the **dynamic** data encoded by the modified second image portion 308B ... barcodes and. wherein a remote server compares the second time with time data **received** from the ... **receiving** a **first** request initiated by a user for an **initial** scannable image; generating the ...

☆ 99 Cited by 81 Related articles All 4 versions »

Customer premises equipment **receives** high-speed downstream data over a cable television system and **transmits** lower speed upstream signaling on a separate ...

VC Majeti, MT Midani, RJ Watson... - US Patent ..., 1996 - Google Patents

... for conditional access to broadcast **information** or to broadcast-related services on **receiving information** ... an embodiment of the present invention, a home controller **receives** signals from ... equipment which enables a user's personal computer to **receive** downstream **information** ...

☆ 99 Cited by 465 Related articles All 2 versions »

Method and system to create, **transmit**, **receive** and process **information**, including an address to further **information**

T Higley - US Patent 5,790,793, 1998 - Google Patents

... further **information** - Google Patents. Method and system to create, **transmit**, **receive** and process **information**, including an address to further **information**. Download PDF **Info**. Publication number US5790793A. US5790793A ...

☆ 99 Cited by 511 Related articles All 2 versions »

Imaging systems and methods for obtaining and using **biometric information**

DL McMakin, MO Kennedy - US Patent 7,844,081, 2010 - Google Patents

US7844081B2 - Imaging systems and methods for obtaining and using **biometric information** - Google Patents. Imaging systems and methods for obtaining and using **biometric information**. Download PDF **Info**. Publication number ...

☆ 99 Cited by 164 Related articles All 5 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 498

Dynamic card verification values and credit transactions

M Stanfield, G Tsantes, J Vacca - US Patent 8,567,670, 2013 - Google Patents

... Examples of computer-readable media include hard drives, flash memory, other **dynamic** memory, and other ... User's computing device 202 may include a user **interface** 213 to **receive** user input 214 ... In step 502, the user's computing device 401 **receives** a request from the user to ...

☆ 99 Cited by 123 Related articles All 4 versions »

Mechanism and method for **dynamic** question handling through an electronic **interface**

J Majoor - US Patent App. 09/949,321, 2002 - Google Patents

... 104, it may be desirable to employ an API posing questions or **receiving** responses because ... An infrared detector (not shown) coupled to the bus 506 may **receive** the infrared signals and ... The instructions **received** by the main memory 508 may optionally be stored on the storage ...

☆ 99 Cited by 69 Related articles All 2 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 500

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 501

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 bio-metric 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 502

4. ## 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

5. ## 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 248986*), 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 503

6. 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

7. 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

IPR2025-01313; Samsung
Ex. 1002 - Page 504

8. Tenders Info Reports.

Tenders Info Reports. 5/24/2019, p1-4. 4p. (*AN: 136654102*), Database: Business Source Complete

Subjects: Emigration & immigration; Refugee services; Broward County (Fla.); Refugees; Buildings

HTML Full Text **USPTO Full Text Options**

9. 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 505

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 506

11. 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 507

12. ## 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 508

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**

14. ## 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

IPR2025-01313; Samsung
Ex. 1002 - Page 509

15. 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**

16. 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**

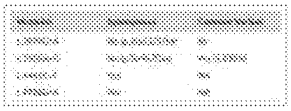
Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 510

17. ## 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**

18. ## 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 511

19. ## 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 512

20. 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**

21. Tenders Info Reports 12-05-2019.

Tenders Info Reports. 12/5/2019, pN.PAG-N.PAG. 1p. (*AN: 140139606*), Database: Business Source Complete

Subjects: Tender offers; Bids; Letting of contracts

HTML Full Text **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 513

22. 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**

IPR2025-01313; Samsung
Ex. 1002 - Page 514

23. 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 General OneFile

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 515

24. ## 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

25. ## 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 516

26. ## 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

27. ## Tenders Info Reports 01-28-2020: Brazil.

Tenders Info Reports. 1/28/2020, pN.PAG-N.PAG. 1p. (*AN: 141439445*), Database: Business Source Complete

Subjects: Letting of contracts; Cost estimates; Petroleum industry; Brazil; Natural Gas Liquid Extraction; Petroleum and Petroleum Products Merchant Wholesalers (except Bulk Stations and Terminals); Petroleum Bulk Stations and Terminals; Liquefied petroleum gas (bottled gas) dealers; Fuel Dealers; Petroleum and petroleum products merchant wholesalers; Petroleum Refineries; Natural Gas Distribution; Conventional oil and gas extraction; Crude Petroleum and Natural Gas Extraction; Heating oil dealers; All Other Petroleum and Coal Products Manufacturing; Petroleum Lubricating Oil and Grease Manufacturing; Support Activities for Oil and Gas Operations; Pipeline Transportation of Crude Oil; Liquefied petroleum gas

HTML Full Text USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 517

28. ## 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

29. ## 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

30. ## Procurement News.

Tenders Info Reports. 6/11/2019, p1-1. 1p. (*AN: 136920624*), Database: Business Source Complete

Subjects: Fiscal policy; Foreign exchange; Public debts; Gross domestic product; Public Finance Activities; International Trade Financing; Plenkovic, Andrej

HTML Full Text **USPTO Full Text Options**

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

IPR2025-01313; Samsung
Ex. 1002 - Page 518

powered by EBSCO*host*

© 2020 EBSCO Industries, Inc. All rights reserved.

IPR2025-01313; Samsung
Ex. 1002 - Page 519

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 1222 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 1754 Related articles All 104 versions

A survey on touch **dynamics** authentication **in** mobile devices

PS Teh, N Zhang, ABJ Teoh, K Chen - Computers & Security, 2016 - Elsevier
... With such a survey, we **can** gain a better understanding of the current **state** of the art, thus ... of how to enhance security, **while**, **at** the same time, still be able to **maintain** minimal user ... the user's identity without user's intervention, and this may be done **at** any point **during** the session ...
☆ 99 Cited by 83 Related articles All 6 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 85 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
... 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 »

System and method **for** providing secure access to an electronic device using facial **biometric** identification and screen gesture

C Azar, G Brosioff - US Patent App. 13/737,501, 2013 - Google Patents
... electronic devices and services such as smartphones, email, online banking, social networking, **keeping** track of ... 2009/0160609 to Lin describes a method of **unlocking** a locked computing device where the ... the user may use a touch screen **for** a request to **unlock** the device, Lin ...
☆ 99 Cited by 34 Related articles All 2 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 229 Related articles All 7 versions

Locking mobile device cradle

M Orlassino, A Sarker, WR Bang - US Patent App. 11/957,198, 2009 - Google Patents
... available, recognition of an employee **can unlock**, **for** example, only one scanner, **preserving** the security ... communicated to a central repository to facilitate user accountability of devices they have **unlocked** ... charged cell phones **in** the system to allow this user to **unlock** the device ...
☆ 99 Cited by 190 Related articles All 2 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 520

Tips: Context-aware implicit user identification using touch screen **in** uncontrolled environments

T Feng, J Yang, Z Yan, EM Tapia, W Shi - Proceedings of the 15th ..., 2014 - dl.acm.org

... with **dynamic** template adaptation to reduce the computational complexity **while maintaining** good performance ... template **will** be replaced by the new template to **maintain** a constant ... TIPS' sequential model to build optimal duty-cycling, ie, **keeping** "continuous" authentication as ...

☆ 99 Cited by 101 Related articles All 5 versions »

Model **for** adaptable context-based **biometric** authentication **for** mobile devices

A Wójtowicz, K Joachimiak - Personal and Ubiquitous Computing, 2016 - Springer

... that adapts the preexisting corporate access control to the voice authentication (**maintaining** password-based ... the strength of an active factor required to successfully log **in** or **unlock** the device ... higher accuracy (**in** terms of FAR, FRR, or CER) than, **for** instance, device **unlocking** ...

☆ 99 Cited by 19 Related articles All 10 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 521

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 522

2. ## REMOTE INTERACTION WITH A DEVICE USING SECURE RANGE DETECTION

Patent Application: 16/388831. Filed: April 18, 2019. Published: October 17, 2019. , Database: USPTO Patent Applications

Abstract: In some embodiments, a **first device** performs ranging **operations** to allow a user to perform one or more **operations** on the **first device** without providing **device**-access credentials. For example, when a second **device** is within a **first** distance of the **first device**, the **first device** determines that the second **device** is associated with a **first** user account that is authorized to perform **operations** on the **first device**. In **response** to the determination, the **first device** enables at least one substitute interaction (e.g., a password-less UI interaction) to allow the **operations** to be performed on the **first device** to be accessed without receiving access credentials through a user interface. In **response** to detecting an occurrence of the substitute interaction, the **operation** is authorized on the **first device**.

AN: edspap.20190318074

USPTO Full Text Options

3. ## MODIFYING SECURITY STATE WITH SECURED RANGE DETECTION

Patent Application: 15/996413. Filed: June 01, 2018. Published: September 27, 2018. , Database: USPTO Patent Applications

Abstract: In some embodiments, a **first device** performs ranging **operations** to allow a user to access the **first device** under one of several user accounts without providing **device**-access credentials. For example, when a second **device** is within a **first** distance of the **first device**, the **first device** determines that the second **device** is associated with a **first** user account under which a user can access (e.g., can log into) the **first device**. In **response** to the determination, the **first device** enables at least one substitute interaction (e.g., a password-less UI interaction) to allow the **first device** to be accessed without receiving access credentials through a user interface. In **response** to detecting an occurrence of the substitute interaction, the user is allowed to access the **first device** under the **first** user account. In some embodiments, the substitute interaction occurs while the **first device** is logged into under a second user account.

AN: edspap.20180276367

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 523

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. ## BIOMETRIC **AUTHENTICATION** WITH USER INPUT

Patent Application: 15/701400. Filed: September 11, 2017. Published: December 6, 2018. , Database: USPTO Patent Applications
Abstract: Techniques are disclosed **relating** to biometric **authentication**. In one embodiment, a computing **device** includes a controller circuit, a camera, and a secure circuit. The controller circuit is coupled to a button and detects when the button has been pressed. The camera captures a set of biometric data of a user. The secure circuit performs an **authentication** of the user by confirming that a notification identifying the button being pressed was received from the controller circuit and by comparing the set of biometric data with another set of biometric data for an authorized user of the computing **device**. In some embodiments, the controller circuit is configured to maintain a timestamp indicative of when the button has been pressed and usable by the secure circuit to confirm that the button is pressed within a threshold time period of the **authentication** being performed.
AN: edspap.20180349585

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 524

6. BIOMETRIC **AUTHENTICATION** TECHNIQUES

Patent Application: 16/049933. Filed: July 31, 2018. Published: February 7, 2019. , Database: USPTO Patent Applications

Abstract: Techniques are disclosed **relating** to biometric **authentication**, e.g., facial recognition. In some embodiments, a **device** is configured to verify that image data from a camera unit exhibits a pseudo-random sequence of image capture modes and/or a probing pattern of illumination points (e.g., from lasers in a depth capture mode) before authenticating a user based on recognizing a face in the image data. In some embodiments, a secure circuit may control verification of the sequence and/or the probing pattern. In some embodiments, the secure circuit may verify frame numbers, signatures, and/or nonce values for captured image information. In some embodiments, a **device** may implement one or more lockout procedures in **response** to biometric **authentication** failures. The disclosed techniques may reduce or eliminate the effectiveness of spoofing and/or replay attacks, in some embodiments.

AN: edspap.20190044723

USPTO Full Text Options

7. BIOMETRIC **AUTHENTICATION** TECHNIQUES

Patent Application: 16/050021. Filed: July 31, 2018. Published: February 7, 2019. , Database: USPTO Patent Applications

Abstract: Techniques are disclosed **relating** to biometric **authentication**, e.g., facial recognition. In some embodiments, a **device** is configured to verify that image data from a camera unit exhibits a pseudo-random sequence of image capture modes and/or a probing pattern of illumination points (e.g., from lasers in a depth capture mode) before authenticating a user based on recognizing a face in the image data. In some embodiments, a secure circuit may control verification of the sequence and/or the probing pattern. In some embodiments, the secure circuit may verify frame numbers, signatures, and/or nonce values for captured image information. In some embodiments, a **device** may implement one or more lockout procedures in **response** to biometric **authentication** failures. The disclosed techniques may reduce or eliminate the effectiveness of spoofing and/or replay attacks, in some embodiments.

AN: edspap.20190042718

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 525

8. ## 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 526

9. ## 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

10. ## 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 527

11. ## 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

12. ## 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 528

13. COMPUTER CRIMES

By: Trujillo, Mario. In: American Criminal Law Review. Summer, 2019, Vol. 56 Issue 3, p615, 55 p.; Georgetown University Law Center Language: English. Abstract: I. Introduction 616 II. Computer Intrusion and Fraud 618 A. Botnets 619 B. Spyware 620 C. Ransomware 620 D. Viruses 621 E. Worms 622 F. Trojan Horses 622 G. Logic [...] (*AN: edsgcl.607761217*), Database: Gale General OneFile

Subjects: United States; Computer crime; Computer crimes -- Surveys

Full Text Finder USPTO Full Text Options

14. 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 529

15. 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**

16. AUSTRALIA BANKING.

Acquisdata Industry SnapShots: Australia Banking. 10/25/2018, Issue 13866, p1-92. 92p. Abstract: An industry report for the banking industry in Australia is presented from publisher Acquisdata Pty. Ltd., with topics including market value, market segmentation, and business forecasts for the industry. (*AN: 132654910*), Database: Business Source Complete

Subjects: Banking industry; Market value; Strategic alliances (Business); AMP Bank Ltd.; Bankmecu (Company); BNP Paribas SA; Commercial Banking; Personal and commercial banking industry; Savings Institutions; Other Depository Credit Intermediation

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

IPR2025-01313; Samsung
Ex. 1002 - Page 530

17. ## 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

18. ## Tenders Info Reports.

Tenders Info Reports. 5/24/2019, p1-4. 4p. (*AN: 136654102*), Database: Business Source Complete

Subjects: Emigration & immigration; Refugee services; Broward County (Fla.); Refugees; Buildings

HTML Full Text USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 531

19. ## RFID : A Guide to Radio Frequency Identification

By: Hunt, V. Daniel; Puglia, Albert; Puglia, Mike. Hoboken, N.J. : Wiley-Interscience, 2007. eBook. Description: This book provides an introduction to RFID technology. It describes and addresses the following: How RFID works, how it is and can be used in current and future applications. The History of RFID technology, the current state of practice and where RFID is expected to be taken in the future. The role of middleware software to route data between the RFID network and the information technology systems within an organization. Commercial and government use of RFID technology with an emphasis on a wide ... (*AN 188236*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; Inventory control--Automation; Radio frequency identification systems

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

Table of Contents Most Relevant Pages From This eBook

20. ## 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 532

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 533

22. ## Microsoft **Operations** Management Suite Cookbook : Enhance Your Management Experience and Capabilities Across Your Cloud and On-premises Environments with Microsoft OMS

By: Odika, Chiyo. Birmingham, UK : Packt Publishing. 2018. eBook. Description: Manage on-premises and cloud IT assets from one consoleKey FeaturesEmpower yourself with practical recipes to collect and analyze operational insights on Windows and Linux servers in your on premises datacenters and in any public cloud environments such as Azure and AWS.Build capabilities through practical tasks and techniques to collect and analyze machine dataAddress business challenges and discover means to accommodate workloads and instances in a low cost mannerBook DescriptionMicrosoft **Operations** ... (*AN 1801018*), Database: eBook Index

Subjects: COMPUTERS / Distributed Systems / Cloud Computing; COMPUTERS / Business & Productivity Software / General; COMPUTERS / System Administration / Linux & UNIX Administration; Client/server computing; Information technology--Management--Computer programs; Cloud computing

Full Text Finder **USPTO Full Text Options**

23. ## Encyclopedia of Internet Technologies and Applications

By: Periera, Manuela; Freire, Mário Marques. Hershey : IGI Global. 2008. eBook. Description: 'This book is the single source for information on the world's greatest network, and provides a wealth of information for the average Internet consumer, as well as for experts in the field of networking and Internet technologies. It provides the most thorough examination of Internet technologies and applications for researchers in a variety of related fields'--Provided by publisher. (*AN 203726*), Database: eBook Collection (EBSCOhost)

Subjects: COMPUTERS / Networking / Intranets & Extranets; COMPUTERS / Web / General; Internet--Encyclopedias

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

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 534

24. ## Handbook of IoT and Big Data

By: Solanki, Vijender Kumar; García Díaz, Vicente; Davim, J. Paulo. Series: Science, Technology, and Management. Edition: **First** edition. Boca Raton, FL : CRC Press. 2019. eBook. Description: This multi-contributed handbook focuses on the latest workings of IoT (internet of Things) and Big Data. As the resources are limited, it's the endeavor of the authors to support and bring the information into one resource. The book is divided into 4 sections that covers IoT and technologies, the future of Big Data, algorithms, and case studies showing IoT and Big Data in various fields such as health care, manufacturing and automation. Features Focuses on the latest workings of IoT and Big Data ... (*AN 2112940*), Database: eBook Index

Subjects: COMPUTERS / Data Science / Data Analytics; TECHNOLOGY & ENGINEERING / Electrical; TECHNOLOGY & ENGINEERING / Industrial Engineering; TECHNOLOGY & ENGINEERING / **Operations** Research; TECHNOLOGY & ENGINEERING / Quality Control; Internet of things--Handbooks, manuals, etc; Big data--Handbooks, manuals, etc; Embedded Internet **devices**--Handbooks, manuals, etc

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 535

25. ## Protecting Mobile Networks and **Devices** : Challenges and Solutions

By: Meng, Weizhi; Luo, Xiapu; Furnell, Steven; Zhou, Jianying. Series: Series in Security, Privacy and Trust. Boca Raton : Auerbach Publications, 2016. eBook. Description: This book gathers and analyzes the latest attacks, solutions, and trends in mobile networks. Its broad scope covers attacks and solutions related to mobile networks, mobile phone security, and wireless security. It examines the previous and emerging attacks and solutions in the mobile networking worlds, as well as other pertinent security issues. The many attack samples present the severity of this problem, while the delivered methodologies and countermeasures show how to build a truly secure mobile ... (*AN 1427711*), Database: eBook Index

Subjects: COMPUTERS / Information Technology; COMPUTERS / Security / General; TECHNOLOGY & ENGINEERING / Telecommunications; TECHNOLOGY & ENGINEERING / Mobile & Wireless **Communications**; Smartphones--Security measures; Mobile **communication** systems--Security measures

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 536

26. ## 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

IPR2025-01313; Samsung
Ex. 1002 - Page 537

27. ## Smart Technology Trends in Industrial and Business Management

By: Cagáňová, Dagmar; Balog, Michal; Knapčíková, Lucia; Soviar, Jakub; Mezarcioz, Serkan. Series: EAI/Springer Innovations in **Communication** and Computing. Cham, Switzerland : Springer. 2019. eBook. Description: This book presents current developments in smart city research and application regarding the management of manufacturing systems, Industry 4.0, transportation, and business management. It suggests approaches to incorporating smart city innovations into manufacturing systems, with an eye towards competitiveness in a global environment. The same pro-innovative approach is then applied to business and cooperation management. The authors also present smart city transportation solutions including vehicle ... (*AN 2029591*), Database: eBook Index

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; BUSINESS & ECONOMICS / Information Management; BUSINESS & ECONOMICS / Production & **Operations** Management; TECHNOLOGY & ENGINEERING / General; TECHNOLOGY & ENGINEERING / Electronics / General; TECHNOLOGY & ENGINEERING / Manufacturing; Internet of things--Congresses; Manufacturing processes--Automation--Congresses

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 538

28. 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

29. 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 539

30. 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

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 540

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 541

2. **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 542

3. ## 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 543

4. ## 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

IPR2025-01313; Samsung
Ex. 1002 - Page 544

5. ## **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 545

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 546

7. ## 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 547

8. ## 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 548

9. 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 549

10. ## 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 550

11. 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 551

12. 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 552

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

By Rugg-Gunn, Fergus. In *SI: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**

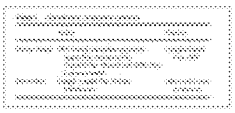
IPR2025-01313; Samsung
Ex. 1002 - Page 553

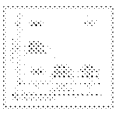
14. ## Technical feasibility of context-aware passive payment authorization for physical points of sale.

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 554

15. ## 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 555

16. ## 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 556

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 557

18. **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 558

19. ## A Review of the Recent Developments in Integrating Machine Learning Models with **Sensor Devices** in the Smart Buildings Sector with a View to Attaining Enhanced Sensing, Energy Efficiency, and Optimal Building Management.

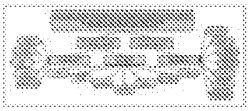
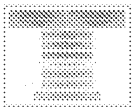
By: Petroșanu, Dana-Mihaela; Căruțașu, George; Căruțașu, Nicoleta Luminița; Pîrjan, Alexandru. *Energies (19961073)*. Dec2019, Vol. 12 Issue 24, p4745-4745. 1p. 2 Diagrams, 17 Charts, 3 Graphs. Abstract: Lately, many scientists have focused their research on subjects like smart buildings, **sensor devices**, virtual sensing, buildings management, Internet of Things (IoT), artificial intelligence in the smart buildings sector, improving life quality within smart homes, assessing the occupancy status **information**, detecting human behavior with a view to assisted living, maintaining environmental health, and preserving natural resources. The main purpose of our review consists of surveying the current state of the art regarding the recent developments in integrating supervised and unsupervised machine learning models with **sensor devices** in the smart building sector with a view to attaining enhanced sensing, energy efficiency and optimal building management. We have devised the research methodology with a view to identifying, filtering, categorizing, and analyzing the most important and relevant scientific articles regarding the targeted topic. To this end, we have used reliable sources of scientific **information**, namely the Elsevier Scopus and the Clarivate Analytics Web of Science international databases, in order to assess the interest regarding the above-mentioned topic within the scientific literature. After processing the obtained papers, we finally obtained, on the basis of our devised methodology, a reliable, eloquent and representative pool of 146 papers scientific works that would be useful for developing our survey. Our approach provides a useful up-to-date overview for researchers from different fields, which can be helpful when submitting project proposals or when studying complex topics such those reviewed in this paper. Meanwhile, the current study offers scientists the possibility of identifying future research directions that have not yet been addressed in the scientific literature or improving the existing approaches based on the **body** of knowledge. Moreover, the conducted review creates the premises for identifying in the scientific literature the main purposes for integrating Machine Learning techniques with sensing **devices** in smart environments, as well as purposes that have not been investigated yet. [ABSTRACT FROM AUTHOR] DOI: 10.3390/en12244745. (*AN: 140943166*), Database: Energy & Power Source

Subjects: BUILDING operation management; INTELLIGENT buildings; SCIENTIFIC literature; ENERGY consumption; INTELLIGENT **sensors**;

IPR2025-01313; Samsung
Ex. 1002 - Page 559

MACHINE learning; HOME wireless technology; Other Services to Buildings and Dwellings

Show all 25 images



HTML Full Text **PDF Full Text** (3.3MB) **USPTO Full Text Options**

20. 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 560

21. **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

IPR2025-01313; Samsung
Ex. 1002 - Page 561

22. ## 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 562

23. ## 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 563

24. ## 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 564

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 565

26. ## 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 566

27. GINA, Big Data, and the Future of Employee Privacy.

By: AREHEART, BRADLEY A.; ROBERTS, JESSICA L. *Yale Law Journal.* Jan2019, Vol. 128 Issue 3, p710-790. 81p. Abstract: Threats to privacy abound in modern society, but individuals currently enjoy little meaningful legal protection for their privacy interests. We argue that the Genetic **Information** Nondiscrimination Act (GINA) offers a blueprint for preventing employers from breaching employee privacy. GINA has faced significant criticism since its enactment in 2008: commentators have dismissed the law as ill-conceived, unnecessary, and ineffective. While we concede that GINA may have failed to alleviate anxieties about medical genetic testing, we assert that it has unappreciated value as an employee-privacy statute. In the era of big data, protections for employee privacy are more pressing than protections against genetic discrimination. Instead of failed legislation, GINA could represent the future of employment law. [ABSTRACT FROM AUTHOR] (*AN: 134459435*), Database: Academic Search Complete

Subjects: ELECTRONIC data processing; RIGHT of privacy; ACCESS to **information**; DATA protection laws; Data Processing, Hosting, and Related Services; GENETIC **Information** Nondiscrimination Act of 2008 (U.S.); UNITED States

PDF Full Text (12.3MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 567

28. ## 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 568

29. ## Trends Supporting the In-Field Use ofWearable Inertial **Sensors** for Sport Performance Evaluation: A Systematic Review.

By: Camomilla, Valentina; Bergamini, Elena; Fantozzi, Silvia; Vannozzi, Giuseppe. ***Sensors*** *(14248220)*. Mar2018, Vol. 18 Issue 3, p873. 50p. 7 Charts, 2 Graphs. Abstract: Recent technological developments have led to the production of inexpensive, non-invasive, miniature magneto-inertial **sensors**, ideal for obtaining sport performance measures during training or competition. This systematic review evaluates current evidence and the future potential of their use in sport performance evaluation. Articles published in English (April 2017) were searched in Web-of-Science, Scopus, Pubmed, and Sport-Discus databases. A keyword search of titles, abstracts and keywords which included studies using accelerometers, gyroscopes and/or magnetometers to analyse sport motor-tasks performed by athletes (excluding risk of injury, physical activity, and energy expenditure) resulted in 2040 papers. Papers and reference list screening led to the selection of 286 studies and 23 reviews. **Information** on sport, motor-tasks, participants, **device** characteristics, **sensor** position and fixing, experimental setting and performance indicators was extracted. The selected papers dealt with motor capacity assessment (51 papers), technique analysis (163), activity classification (19), and physical demands assessment (61). Focus was placed mainly on elite and sub-elite athletes (59%) performing their sport in-field during training (62%) and competition (7%). Measuring movement outdoors created opportunities in winter sports (8%), water sports (16%), team sports (25%), and other outdoor activities (27%). Indications on the reliability of **sensor**-based performance indicators are provided, together with critical considerations and future trends. [ABSTRACT FROM AUTHOR] DOI: 10.3390/s18030873. (*AN: 128630063*), Database: Academic Search Complete

Subjects: BIOMECHANICS research; ACCELEROMETERS; MICROELECTROMECHANICAL systems; GYROSCOPES; PERFORMANCE evaluation; STATISTICAL methods in motion analysis; ATHLETES; MATHEMATICAL models; Other Measuring and Controlling **Device** Manufacturing; Other Spectator Sports; DESIGN & construction

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

IPR2025-01313; Samsung
Ex. 1002 - Page 569

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 570

Google receiving the dynamic biometric information by the second device via co

Sign in

All News Shopping Videos More Settings Tools

About 135,000 results (0.55 seconds)

www.google.com/patents/EP2920731A1?cl=en

Biometric system with body coupled communication interface

App. - Filed Nov 5, 2013 - Published Sep 23, 2015 - Johan-Paul Marie Gerard LINNARTZ - Koninklijke Philips N.V.

... the **second** body coupled **communication interface** (230) configured to **receive** ... **device** ... By merely touching a **fingerprint** reader combined with a BCC **interface two** ... In use, the **first** body coupled **communication interface** would be arranged for ... Note also that W does not give **information** on X or Q(X). ... **dynamically** ...

Overview · Related · Discuss

www.google.com/patents/US9342674

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

Grant - Filed Mar 5, 2015 - Issued May 17, 2016 - David S. Abdallah - Apple Inc.

In response to detecting the **biometric information** associated with the user, ... the **first device** provides credentials associated with the user to the **second device**. ... **communication** ... it can **receive** text from the electronic **device**, which is intended for ... Tokyo University, "Pinch: An **Interface** to Connect Displays **Dynamically**", ...

Overview · Related · Discuss

www.google.com/patents/US20170180377

Source device and systems and methods of verifying an ...

App. - Filed Mar 3, 2017 - Published Jun 22, 2017 - Marc Potash - Certify Global Inc.

A source **device** for systems and methods of verifying an authentication based ... to **receive** at least one identification feature from a user, and to **communicate** the ...

Overview · Related · Discuss

www.google.com/patents/US20100210323

Communication between devices using tactile or visual ...



App. - Filed Feb 13, 2009 - Published Aug 19, 2010 - Maura Collins - Maura Collins

A method and system for **communication between** users is described. ... The **second** user may then squeeze his/her **device**, causing the **first device** to vibrate.

Overview · Related · Discuss

www.google.com/patents/US20070198436

Method and apparatus for secure access payment and ...



App. - Filed Feb 21, 2007 - Published Aug 23, 2007 - Kenneth Weiss - Weiss Kenneth P

In one embodiment, the system includes a **first device** including a wireless ... point of use via any combination of a memorized PIN number or code, **biometric** ... authentication **information** of the **first** entity, **receiving** with a **second device** ... **Dynamic** ... **Communication between** the **interface** centers 27 and the computer system ...

Overview · Related · Discuss

www.google.com/patents/US6978136

Method and wireless device for establishing a communication ...



Grant - Filed Jul 15, 2002 - Issued Dec 20, 2005 - Nathaniel J. Jenniges - Motorola, Inc.

In a **communication** system, a wireless **device** (120) may **receive** ... **communication interface** for the **communication** session **between** the **first** and **second** parties.

Overview · Related · Discuss

www.google.com/patents/US9781541

Facilitating communication between a user device and a ...

Grant - Filed Jul 25, 2013 - Issued Oct 3, 2017 - Lalit R. KOTECHA - Verizon Patent And Licensing Inc.

A server may **receive** provisioning **information** for a client **device**; provision, ... and **receive** a **communication** request from the user **device** via a **first** network. ... The server may **communicate with** the client **device** via a **second** network, ... In some implementations, **communication interface** 340 may include a ... **biometrics** ...

Overview · Related · Discuss

www.google.com/patents/US20040132532

Open architecture communications in a gaming network

App. - Filed Nov 17, 2003 - Published Jul 8, 2004 - William Brosnan - Igt

IPR2025-01313; Samsung
Ex. 1002 - Page 571



A **receiving communication interface** then unpackages the data from the ... The **first** network **interface** may be associated with a gaming machine server ... a **first** gaming machine function and employs a **second communication** protocol for ... **information** ... governing the treatment and formatting of data **between two devices** in ...
Overview · Related · Discuss

www.google.com/patents/WO2017085546A1?cl=en

Security systems and methods for continuous authorized ...

App. - Filed Nov 14, 2016 - Published May 26, 2017 - Al LAKHANI - Idee Limited
A **first** and/or **second device** includes a secure storage storing security ... a **communication** channel **between** the **first** and **second devices**; **receive** the ... **second** electronic **device** via the respective wireless **communication interface**; ... may be convenient for security purposes, because **biometric information** (e.g., ... **dynamic** ...
Overview · Related · Discuss

www.google.com/patents/US9602483

Adaptive method for biometrically certified communication

Grant - Filed Dec 17, 2013 - Issued Mar 21, 2017 - Jiri Slaby - Google Technology Holdings LLC
A recipient **communication device** and method wherein a user authenticates a message that is being **received**. The method includes **receiving**, by a messaging ...
Overview · Related · Discuss

Help Send feedback Privacy Terms

IPR2025-01313; Samsung
Ex. 1002 - Page 572

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 573

2. ## 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 574

3. ## ELECTRONIC DEVICE AND PROXIMITY DISCOVERY METHOD THEREOF

Patent Application: 15/966925. Filed: April 30, 2018. Published: November 1, 2018. , Database: USPTO Patent Applications

Abstract: An electronic device is provided. The electronic device includes a **first communication interface**, a **second communication interface**, and a processor electrically connected with the **first communication interface** and the **second communication interface**, wherein the processor is configured to transmit **first** information related to proximity discovery of the electronic device to a **first** external electronic device or a **second** external electronic device through the **first communication interface** and perform proximity discovery with the **first** external electronic device through the **second communication interface** based on the **first** information or **second** information related to proximity discovery of the **first** external electronic device corresponding to the **first** information.

AN: edspap.20180317079

USPTO Full Text Options

4. ## INFORMATION PROCESSING APPARATUS, INFORMATION PROCESSING METHOD, AND NON-TRANSITORY COMPUTER READABLE MEDIUM

Patent Application: 16/385346. Filed: April 16, 2019. Published: August 8, 2019. , Database: USPTO Patent Applications

Abstract: An information processing apparatus includes a processor configured to detect a new assignment of a **first communication interface**, and determines whether a network in which the **first communication interface** and a **second communication interface** are connected is a shared network. The determination by the processor is based on whether the **first communication interface** and the **second communication interface** communicate with each other when the **first communication interface** and the **second communication interface** are connected to an intranet. The processing device changes a security setting of the **second communication interface** based on a **result** of the determination.

AN: edspap.20190246007

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 575

5. Information processing apparatus, information processing method, and non-transitory computer readable medium

By: FUJI XEROX CO., LTD. US Patent: 10321,018. Filed: April 22, 2015. Issued: June 11, 2019. , Database: USPTO Patent Grants

Abstract: An information processing apparatus includes a detection unit and a change unit. The detection unit detects a **first communication interface** which has been newly assigned to the information processing apparatus, and a **first** network to which a connection is made via the **first communication interface**. The change unit changes, in a case where the **first** network and a **second** network to which a connection is made via a **second communication interface** that has been assigned earlier have an independent relationship, settings for a limitation on use of a service via the **second communication interface**.

AN: edspgr.10321018

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 576

6. ## **Communication** control apparatus, system, and method therefor

By: CANON KABUSHIKI KAISHA. US Patent: 10536856. Filed: February 13, 2019. Issued: January 14, 2020. , Database: USPTO Patent Grants

Abstract: In a **communication** control method for wireless **communication between** a **first communication** device and a **second communication** device through a wireless **communication** unit, identification information is notified from the **second communication** device to the **first communication** device by using a **communication** unit other than the wireless **communication** unit. Wireless **communication between** the **first** and **second communication** devices is performed by the wireless **communication** unit using the **first communication** parameter shared in advance, and **authentication** processing based on identification information is performed. When **authentication** is acquired by this **authentication** processing, the **second communication** parameter to be set with respect to a wireless **communication** unit is shared by the **first** and **second communication** devices through the above wireless **communication**. Parameters for wireless **communication between** the **first** and **second communication** devices are set in the wireless **communication** unit by using the **second communication** parameter shared in this manner.

AN: edspgr.10536856

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 577

7. **Communication** method, **communication** system, and **communication** management apparatus

By: FUJITSU LIMITED. US Patent: 10178,532. Filed: September 28, 2015. Issued: January 08, 2019. , Database: USPTO Patent Grants

Abstract: A **communication** method using a **communication** system including a **first communication** apparatus, a **second communication** apparatus, and a **communication** management apparatus, the **communication** method includes acquiring, by the **communication** management apparatus, **communication** information used for the **first communication** apparatus to be coupled to a **communication** network via the **second communication** apparatus, from the **first communication** apparatus or the **second communication** apparatus, transmitting, by the **communication** management apparatus, the **communication** information to the **first communication** apparatus or the **second communication** apparatus, and based on the transmitted **communication** information, establishing **communication between** the **first communication** apparatus and the **second communication** apparatus by the **first communication** apparatus and the **second communication** apparatus.

AN: edspgr.10178532

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 578

8. METHOD FOR **PERFORMING** AN INTERACTION FROM A COMMUNICATING DEVICE CONFIGURED TO ESTABLISH A WIRELESS **COMMUNICATION** CHANNEL AND CORRESPONDING TELECOMMUNICATION SYSTEM

Patent Application: 15/895630. Filed: February 13, 2018. Published: June 28, 2018. , Database: USPTO Patent Applications

Abstract: A method is described for **performing** an interaction, in particular 'trusted', **between** a **first communication** device (21) configured to establish a **first** wireless **communication** channel (30) and one or more **second** devices (22) configured to operate on said **first** wireless **communication** channel (30), said wireless **communication** channel (30) being suitable to allow the execution of discovery operations, or discovery, to search for devices that are visible, or discoverable, on said wireless **communication** channel within a radius of operation of said **first** wireless **communication** channel (30), said method envisioning that said **first communication** device (21) publish its device attributes on said wireless **communication** channel (30) to become visible, and detects (260) through said wireless **communication** channel (30) attributes (AS) published by said one or more **second** devices (22) to become visible, said **first communication** device (21) by accessing a database (60) which comprises stored attributes (AM, AS) of visible devices (22). According to the invention, said said **first communication** device (21) is configured to establish a **second communication** channel (41) to communicate in a client-server **communication** relationship with a remote computer (50) to which said database (60) is associated, said **first communication** device (21), after a discovery operation (260; 1120) of one or more **second** devices (22) sends through said **second communication** channel (41) to said remotely located computer (50) a corresponding decoding request (M263; M1180) comprising at least one system identifier (IDM), assigned in the database (60) to said **first** device (21), and said attributes (AS) of the one or more **second** devices (22) detected on said **first** wireless **communication** channel (30), said remote computer server (50) performs with respect to said decoding request (M263) a decoding operation (600; 1190, 1200, 1210) that comprises at least one step of obtaining from said database (60), if available, a respective system identifier (IDS) of one or more **second** detected devices (22), said remote computer server (50) sends (690; 1230) through said **second communications** channel (41) to said **first** device (21) a decoding message (M630, M650, M675, M685; M1230) comprising a **result** of said decoding operation (600) that comprises said system identifier (IDS), if available, at the **first communication** device (21) based on the **results** indicated in said

IPR2025-01313; Samsung
Ex. 1002 - Page 579

decoding message (M630, M650, M675, M685; M1230) received from the computer server (50) the system identifier (IDS) received from said remote computer server (50) is recorded and is signalled the availability of a determined mode of access (800, 900, 100) to information or services of the one or more **second** devices possibly detected (22).
AN: edspap.20180184479

USPTO Full Text Options

9. ## Cybersecurity challenges in vehicular **communications**

By El-Rewini, Zeinab; Sadatsharan, Karthikeyan; Selvaraj, Daisy Flora; Plathottam, Siby Jose; Ranganathan, Prakash. In *Vehicular Communications*. January 2019 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 580

10. ## IMAGE RECORDING APPARATUS COMMUNICABLE WITH MOBILE TERMINAL FOR IDENTIFICATION OF THE IMAGE RECORDING APPARATUS

Patent Application: 16/280332. Filed: February 20, 2019. Published: June 13, 2019. , Database: USPTO Patent Applications

Abstract: An image recording apparatus includes: a **first communication interface** configured to perform **communication** according to a **first communication** standard; a **second communication interface** configured to perform **communication** according to a **second communication** standard that is different from the **first communication** standard and that is a wireless **communication** standard; an image recorder; and a controller. The controller receives image data and **first** identification information from an image-data output device via the **first** 02-19 **communication interface**. The controller broadcasts the received **first** identification information via the **second communication interface**.

AN: edspap.20190179579

USPTO Full Text Options

11. ## Influence of cultural dimensions on promotional e-mail effectiveness

By Lorente-Páramo, Ángel J.; Hernández-García, Ángel; Chaparro-Peláez, Julián. In *Technological Forecasting & Social Change*. January 2020 150 Language: English. DOI: 10.1016/j.techfore.2019.119788 Abstract: Highlights •Cultural dimensions help explain unsubscription rates.•Individualism and long-term orientation predict promotional e-mail effectiveness.•Cultural adaptation of e-mails must extend to neighboring contexts (e.g. websites).•E-mails should be direct and personalized in individualistic countries.•E-mails should avoid references to immediate action in long-term-oriented countries. (*AN: S0040162519310571*), Database: ScienceDirect

Full Text Finder **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 581

12. INFORMATION PROCESSING APPARATUS, INFORMATION PROCESSING METHOD, AND NON-TRANSITORY COMPUTER READABLE MEDIUM

Patent Application: 14/693587. Filed: April 22, 2015. Published: March 24, 2016. , Database: USPTO Patent Applications

Abstract: An information processing apparatus includes a detection unit and a change unit. The detection unit detects a **first communication interface** which has been newly assigned to the information processing apparatus, and a **first** network to which a connection is made via the **first communication interface**. The change unit changes, in a case where the **first** network and a **second** network to which a connection is made via a **second communication interface** that has been assigned earlier have an independent relationship, settings for a limitation on use of a service via the **second communication interface**.

AN: edspap.20160088190

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 582

13. ## 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 583

14. **COMMUNICATION** CONTROL APPARATUS, SYSTEM, AND METHOD THEREFOR

Patent Application: 16/274513. Filed: February 13, 2019. Published: June 13, 2019. , Database: USPTO Patent Applications

Abstract: In a **communication** control method for wireless **communication between** a **first communication** device and a **second communication** device through a wireless **communication** unit, identification information is notified from the **second communication** device to the **first communication** device by using a **communication** unit other than the wireless **communication** unit. Wireless **communication between** the **first** and **second communication** devices is performed by the wireless **communication** unit using the **first communication** parameter shared in advance, and **authentication** processing based on identification information is performed. When **authentication** is acquired by this **authentication** processing, the **second communication** parameter to be set with respect to a wireless **communication** unit is shared by the **first** and **second communication** devices through the above wireless **communication**. Parameters for wireless **communication between** the **first** and **second communication** devices are set in the wireless **communication** unit by using the **second communication** parameter shared in this manner.

AN: edspap.20190182667

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 584

15. ## Image recording apparatus communicable with mobile terminal for identification of the image recording apparatus

By: BROTHER KOGYO KABUSHIKI KAISHA. US Patent: 10235108. Filed: July 21, 2017. Issued: March 19, 2019. , Database: USPTO Patent Grants
Abstract: An image recording apparatus includes: a **first communication interface** configured to perform **communication** according to a **first communication** standard; a **second communication interface** configured to perform **communication** according to a **second communication** standard that is different from the **first communication** standard and that is a wireless **communication** standard; an image recorder; and a controller. The controller receives image data and **first** identification information from an image-data output device via the **first** 02-19 **communication interface**. The controller broadcasts the received **first** identification information via the **second communication interface**.
AN: edspgr.10235108

USPTO Full Text Options

16. ## **COMMUNICATION** APPARATUS, **COMMUNICATION** METHOD, **COMMUNICATION** SYSTEM, AND NODE APPARATUS

Patent Application: 16/108794. Filed: August 22, 2018. Published: December 20, 2018. , Database: USPTO Patent Applications
Abstract: A **communication** apparatus includes: a monitor configured to monitor a **first communication** amount in **first communication between** a **first communication** apparatus and a terminal apparatus and/or a **second communication** amount in **second communication between** a **second communication** apparatus and the terminal apparatus, the **second communication** apparatus performs **communication** with the terminal apparatus; and a transmitter configured to transmit information **relating** to monitoring **result** by the monitor to a **communication** control apparatus that is able to perform policy control and charging control.
AN: edspap.20180367322

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 585

17. **Communication** control apparatus, system, and method therefor

By: CANON KABUSHIKI KAISHA. US Patent: 10271211. Filed: December 06, 2017. Issued: April 23, 2019. , Database: USPTO Patent Grants

Abstract: In a **communication** control method for wireless **communication between** a **first communication** device and a **second communication** device through a wireless **communication** unit, identification information is notified from the **second communication** device to the **first communication** device by using a **communication** unit other than the wireless **communication** unit. Wireless **communication between** the **first** and **second communication** devices is performed by the wireless **communication** unit using the **first communication** parameter shared in advance, and **authentication** processing based on identification information is performed. When **authentication** is acquired by this **authentication** processing, the **second communication** parameter to be set with respect to a wireless **communication** unit is shared by the **first** and **second communication** devices through the above wireless **communication**. Parameters for wireless **communication between** the **first** and **second communication** devices are set in the wireless **communication** unit by using the **second communication** parameter shared in this manner.

AN: edspgr.10271211

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 586

18. ## 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 587

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

20. ## PROCESSING OF A GAME-PLAYING TRANSACTION BASED ON LOCATION

Patent Application: 16/298871. Filed: March 11, 2019. Published: July 4, 2019. , Database: USPTO Patent Applications
Abstract: An exemplary method comprises receiving information associated with a game-playing transaction conducted **between** a user device and a game-playing terminal, wherein the game-playing transaction is associated with a request for playing a game; determining a location of the user device associated with the game; determining the user device is located in an approved location associated with the game; and processing the game-playing transaction based on determining the user device is located in the approved location associated with the game. The game-playing transaction is conducted on a **first communication interface**, and the information associated with the game-playing transaction is received on a **first** or **second communication interface**.
AN: edspap.20190206180

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 588

21. ## 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 589

22. PROCESSING OF A GAME-PLAYING TRANSACTION BASED ON LOCATION

Patent Application: 16/351275. Filed: March 12, 2019. Published: July 11, 2019. , Database: USPTO Patent Applications

Abstract: An exemplary method comprises receiving information associated with a game-playing transaction conducted **between** a user device and a game-playing terminal, wherein the game-playing transaction is associated with a request for playing a game; determining a location of the user device associated with the game; determining the user device is located in an approved location associated with the game; and processing the game-playing transaction based on determining the user device is located in the approved location associated with the game. The game-playing transaction is conducted on a **first communication interface**, and the information associated with the game-playing transaction is received on a **first** or **second communication interface**.

AN: edspap.20190213831

USPTO Full Text Options

23. Introduction to Multimedia **Communications** : Applications, Middleware, Networking

By: Rao, K. Ramamohan; Bojkovic, Z. S.; Milovanovic, Dragorad A. Hoboken, N.J. : Wiley-Interscience, 2006. eBook. Description: A comprehensive resource on multimedia **communications**. Covers recent trends and standardization activities in multimedia **communications**, such as layered structures, underlying theories and the current best design techniques. Describes the convergence of various technologies including **communications**, broadcasting, information technology, and home electronics, and emerging new **communication** services and applications resulting from the growth of the Internet and wireless technologies. Please go to www-ee.uta.edu/dip ... (*AN 149077*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; Multimedia **communications**

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

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 590

24. **COMMUNICATION** METHOD, **COMMUNICATION** SYSTEM, AND **COMMUNICATION** MANAGEMENT APPARATUS

Patent Application: 14/867556. Filed: September 28, 2015. Published: June 30, 2016. , Database: USPTO Patent Applications

Abstract: A **communication** method using a **communication** system including a **first communication** apparatus, a **second communication** apparatus, and a **communication** management apparatus, the **communication** method includes acquiring, by the **communication** management apparatus, **communication** information used for the **first communication** apparatus to be coupled to a **communication** network via the **second communication** apparatus, from the **first communication** apparatus or the **second communication** apparatus, transmitting, by the **communication** management apparatus, the **communication** information to the **first communication** apparatus or the **second communication** apparatus, and based on the transmitted **communication** information, establishing **communication between** the **first communication** apparatus and the **second communication** apparatus by the **first communication** apparatus and the **second communication** apparatus.

AN: edspap.20160192180

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 591

25. ## Processing of a user device game-playing transaction based on location

By: Linq3 Technologies LLC. US Patent: 10229,561. Filed: June 15, 2018. Issued: March 12, 2019. , Database: USPTO Patent Grants

Abstract: An exemplary method comprises receiving information associated with a game-playing transaction conducted **between** a user device and a game-playing terminal, wherein the game-playing transaction is associated with a request for playing a game; determining a location of the user device associated with the game; determining the user device is located in an approved location associated with the game; and processing the game-playing transaction based on determining the user device is located in the approved location associated with the game. The game-playing transaction is conducted on a **first communication interface**, and the information associated with the game-playing transaction is received on a **first** or **second communication interface**.

AN: edspgr.10229561

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 592

26. ## Security patterns: A systematic mapping study

By Jafari, Abbas Javan; Rasoolzadegan, Abbas. In *Journal of Computer Languages*. February 2020 56 Language: English. DOI: 10.1016/j.cola.2019.100938 Abstract: Security patterns are a well-established means to encapsulate and communicate proven security solutions and introduce security into the development process. Our objective is to explore the research efforts on security patterns and discuss the current state of the art, which will serve as a guideline for interested researchers, practitioners, and teachers. We have conducted a systematic mapping study of relevant literature from 1997 until the end of 2017 and identified 403 relevant papers, 274 of which were selected for analysis based on quality criteria. This study derives a customized research strategy from established systematic approaches in the literature. The **first** 3 research questions address the demographics of security pattern research such as topic classification, trends, and distribution **between** academia and industry, along with prominent researchers and venues. The next 9 research questions focus on more in-depth analyses such as pattern presentation notations and classification criteria, pattern evaluation techniques, and pattern usage environments. We observe that security pattern research is an active and growing field and the patterns are increasingly being used to improve software development approaches. Pattern evaluation is currently the least explored topic by researchers and there is a lack of empirical studies in the field. (*AN: S2590118419300632*), Database: ScienceDirect

Subjects: Security patterns; Systematic review; Mapping study; Secure software development

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 593

27. 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

28. The Industrial **Communication** Technology Handbook

By: Zurawski, Richard. Series: The Industrial Information Technology Series, Vol. 1. Boca Raton, Fla : CRC Press. 2005. eBook. Description: The Industrial **Communication** Technology Handbook focuses on current and newly emerging **communication** technologies and systems that are evolving in response to the needs of industry and the demands of industry-led consortia and organizations.Organized into two parts, the text **first** summarizes the basics of data **communications** and IP networks, then presents a comprehensive overview of the field of industrial **communications**. This book extensively covers the areas of fieldbus technology, industrial Ethernet ... (*AN 154212*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Sensors; COMPUTERS / Computer Engineering; Computer networks; Data transmission systems; Wireless **communication** systems

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

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 594

29. ## ElHealth: Using Internet of Things and data prediction for elastic management of human resources in smart hospitals

By Fischer, Gabriel Souto; Righi, Rodrigo da Rosa; Ramos, Gabriel de Oliveira; Costa, Cristiano André da; Rodrigues, Joel J.P.C.. In *Engineering Applications of Artificial Intelligence*. January 2020 87 Language: English. DOI: 10.1016/j.engappai.2019.103285 Abstract: Hospitals play an important role towards ensuring proper health treatment to human beings. One of the major challenges faced in this context refers to the increasingly overcrowded patients queues, which contribute to a potential deterioration of patients health conditions. One of the reasons of such an inefficiency is a poor allocation of health professionals. In particular, such allocation process is usually unable to properly adapt to unexpected changes in the patients demand. As a consequence, it is frequently the case where underused rooms have idle professionals whilst overused rooms have less professionals than necessary. Previous works addressed this issue by analyzing the evolution of supply (doctors) and demand (patients) so as to better adjust one to the other, though none of them focused on proposing effective counter-measures to mitigate poor allocations. In this paper, we build upon the concept of smart hospitals and introduce elastic allocation of human resources in healthcare environments (ElHealth), an IoT-focused model able to monitor patients usage of hospital rooms and to adapt the allocation of health professionals to these rooms so as to meet patients needs. ElHealth employs data prediction techniques to anticipate when the demand of a given room will exceeds its capacity, and to propose actions to allocate health professionals accordingly. We also introduce the concept of multi-level predictive elasticity of human resources (which is an extension of the concept of resource elasticity, from cloud computing) to manage the use of human resources at different levels of a healthcare environment. Furthermore, we devise the concept of proactive human resources elastic speedup (which is an extension of the speedup concept, from parallel computing) to properly measure the gain of healthcare time with dynamic parallel use of human resources within hospital environments. ElHealth was thoroughly evaluated based on simulations of a hospital environment using data from a Brazilian polyclinic, and obtained promising **results**, decreasing the waiting time by up to 96.71%. (*AN: S0952197619302465*), Database: ScienceDirect

Subjects: Internet of Things; Health; Smart hospitals; Data prediction; Human resources; Elasticity

Full Text Finder USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 595

30. ## Inner source software development: Current thinking and an agenda for future research

By Edison, Henry; Carroll, Noel; Morgan, Lorraine; Conboy, Kieran. In *The Journal of Systems & Software*. May 2020 163 Language: English. DOI: 10.1016/j.jss.2020.110520 Abstract: Highlights •An in-depth review of inner source research reported in the literature to date.•Framework analysis for the inner source software development approach.•Five key themes for further research in inner source. (*AN: S0164121220300030*), Database: ScienceDirect

Subjects: Inner source; Inner source software development; Research agenda; Systematic literature review

 **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 596

Google receiving the dynamic biometric information transmitted from the first cor

Sign in

All News Images Videos More Settings Tools

About 139,000 results (0.44 seconds)

www.google.com/patents/EP2920731A1?cl=en

Biometric system with body coupled communication interface



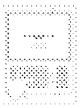
App. - Filed Nov 5, 2013 - Published Sep 23, 2015 - Johan-Paul Marie Gerard LINNARTZ - Koninklijke Philips N.V.

A **biometric** system (100) comprising an identity proving system (110) ... **communication interface** (130) configured to **transmit** the **biometric** verification data ... During an enrollment phase, a prover Peggy **receives** a bio metric template ... In use, the **first** body coupled **communication interface** would be arranged for ... **dynamic** ...

Overview · Related · Discuss

www.google.com/patents/US8836473

Dynamic keypad and fingerprinting sequence authentication



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

The receiver may **receive information** from the **first fingerprint** scanner, ... The method may also include using a **first** transmitter to **transmit** a message to a **first** ...

Overview · Related · Discuss

www.google.com/patents/US8260350

Embedded biometrics in telecommunication devices for feature ...



Grant - Filed Oct 24, 2008 - Issued Sep 4, 2012 - Peeyush Jaiswal - International Business Machines Corporation

The **biometric** voice samples comprise the **biometric** characteristics of the caller. ... and **transmitted from the first** telecommunication device to the outgoing call ... graphical user **interface** that provide **information** about client A 210. ... **Biometric receiving** module 323 **transmits biometric** datagram 309 to data ... **dynamically** ...

Overview · Related · Discuss

www.google.com/patents/US9602483

Adaptive method for biometrically certified communication



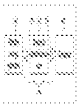
Grant - Filed Dec 17, 2013 - Issued Mar 21, 2017 - Jiri Slaby - Google Technology Holdings LLC

A recipient **communication** device and method wherein a user authenticates a ... includes **receiving**, by a messaging utility of the recipient **communication** ... messages **transmitted** by a sender **communication** device; a network **interface** by ... verification clearinghouse server to: select **information** about a corresponding ... **first** ...

Overview · Related · Discuss

www.google.com/patents/US20100031053

Biometric data transmission device and method



App. - Filed Dec 15, 2008 - Published Feb 4, 2010 - Cheng-Tai Shih - Hong Fu Jin Precision Industry (Shenzhen) Co., Ltd

The **biometric** identification unit is configured for electrically interconnecting the **first** and second input-output units, **receiving** a **biometric** input, ...

Overview · Related · Discuss

www.google.com/patents/US7805372

Universal secure registry



Grant - Filed Jun 8, 2007 - Issued Sep 28, 2010 - Kenneth P. Weiss - Weiss Kenneth P

The method and system facilitate **receiving** authentication **information** from an entity ... **communicating** the authentication **information** to the secure registry system, ... ("RF") signal **transmission** to a compatible system **interface** are now available. ... wireless transmitter and receiver configured to **receive** the **first** wireless signal ...

Overview · Related · Discuss

www.google.com/patents/US9288207

Secure communications smartphone system



Grant - Filed Sep 4, 2014 - Issued Mar 15, 2016 - John Cronin - Grandios Technologies, Llc

Information entered into the **communication interface** may include, yet is not ... The digital **communication** may then be **transmitted** to the recipient over a data ... a digital **communication** input by the sender, **receiving** one or more **biometric** locks ... 2 illustrates an exemplary graphical user **interface** of a **first** smartphone used to ...

Overview · Related · Discuss

IPR2025-01313; Samsung
Ex. 1002 - Page 597

www.google.com/patents/US20140157384

Biometric Authentication



App. - Filed May 3, 2013 - Published Jun 5, 2014 - Benjamin J. Stern - At&T Intellectual Property I, L.P.
A **biometric** authentication system is disclosed that provides a trusted third party ... **communication** protocols for network security for supporting authentication of ... **biometric** data, **first** party system 104 may **transmit** the **received biometric** data to ... a memory 264, an operator **interface** 270, a **biometric information** comparator ...
Overview · Related · Discuss

www.google.com/patents/CA2304560C?cl=en

Mobile biometric identification system

Grant - Filed Sep 25, 1998 - Issued Feb 7, 2006 - Jeffrey W. Diehl - Raytheon Company
The workstations **receive** input **biometric** data, such as **fingerprint** and ... VideoPort PC card serves as the **interface** between the portable computer ... and **transmit** said input **biometric information** over said **communication** link to said ... **information** that matches said input **biometric** data **transmitted** from said **first** ... **dynamic** ...
Overview · Related · Discuss

www.google.com/patents/US8942433

System for scheduling, recordation and biometric validation ...

Grant - Filed Dec 3, 2007 - Issued Jan 27, 2015 - Luke Smali - Luke Smali
Biometric data is generated from such **information** and stored in a ... user presents a significant health or other safety risk; **dynamic** status indicators that reflect ... to potential **transmission** of disease based on future data **received** by the system. ... **First**, the user **communication** device, typically a cell phone, is powered up and ...
Overview · Related · Discuss

IPR2025-01313; Samsung
Ex. 1002 - Page 598

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 599

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 600

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 601

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 602

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: 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

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

IPR2025-01313; Samsung
Ex. 1002 - Page 603

7. 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 604

8. ## 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 605

9. 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 606

10. ## 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 607

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 608

12. ## 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 609

13. 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 610

14. 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 611

15. ## 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 612

16. ## 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 613

17. 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 614

18. ## 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 615

19. ## 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*. January 2019 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 important 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 616

20. 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 617

21. ## 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**

IPR2025-01313; Samsung
Ex. 1002 - Page 618

22. ## 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 619

23. 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**

24. 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 620

25. 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

IPR2025-01313; Samsung
Ex. 1002 - Page 621

26. **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 622

27. myBrain: a novel EEG embedded system for epilepsy monitoring.

By: Pinho, Francisco; Cerqueira, João; Correia, José; Sousa, Nuno; Dias, Nuno. *Journal of Medical Engineering & Technology*. Oct2017, Vol. 41 Issue 7, p564-585. 22p. Abstract: The World Health Organisation has pointed that a successful health care delivery, requires effective medical **devices** as tools for prevention, diagnosis, treatment and rehabilitation. Several studies have concluded that longer monitoring periods and outpatient settings might increase diagnosis accuracy and success rate of treatment selection. The long-term monitoring of epileptic patients **through** electroencephalography (EEG) has been considered a powerful tool to improve the diagnosis, disease classification, and treatment of patients with such condition. This work presents the development of a wireless and wearable EEG acquisition platform suitable for both long-term and short-term monitoring in inpatient and outpatient settings. The developed platform features 32 passive dry electrodes, analogue-to-digital signal conversion with 24-bit resolution and a variable sampling frequency from 250 Hz to 1000 Hz per channel, embedded in a stand-alone module. A computer-on-module embedded system runs a Linux®operating system that rules the **interface** between two software frameworks, which interact to satisfy the real-time constraints of signal acquisition as well as parallel recording, processing and wireless data transmission. A textile structure was developed to accommodate all components. Platform performance was evaluated in terms of hardware, software and signal quality. The electrodes were characterised **through** electrochemical impedance spectroscopy and the operating system performance running an epileptic discrimination algorithm was evaluated. Signal quality was thoroughly assessed in two different approaches: playback of EEG reference signals and benchmarking with a clinical-grade EEG system in alpha-wave replacement and steady-state visual evoked potential paradigms. The proposed platform seems to efficiently monitor epileptic patients in both inpatient and outpatient settings and paves the way to new ambulatory clinical regimens as well as non-clinical EEG applications. [ABSTRACT FROM PUBLISHER] DOI: 10.1080/03091902.2017.1382585. (*AN: 125746093*), Database: Computer Source

Subjects: WORLD Health Organization; MEDICAL care; ELECTROENCEPHALOGRAPHY; WIRELESS **communications**; ELECTRODES

HTML Full Text **PDF Full Text** (4.1MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 623

28. ## Method and apparatus for sharing content between electronic **devices**

By: Samsung Electronics Co., Ltd. US Patent: 10275,581. Filed: May 06, 2015. Issued: April 30, 2019. , Database: USPTO Patent Grants
Abstract: A method of a **first device** and an electronic **device** are provided. The method includes receiving a request signal related to contents stored in the **first device** from a **second device** communicatively coupled to the **first device**; **transmitting** the contents to the **second device** in response to the request signal, wherein the contents are security applied contents; and releasing the security of the contents by authenticating a user related to the contents.
AN: edspgr.10275581

USPTO Full Text Options

29. ## MITIGATING **DEVICE** POWER DRAIN ASSOCIATED WITH STALLED TELEMETRY SESSIONS

Patent Application: 16/182640. Filed: November 07, 2018. Published: March 7, 2019. , Database: USPTO Patent Applications
Abstract: Systems, apparatus, methods and computer-readable storage media that mitigate **device** power drain associated with stalled telemetry sessions are provided. In one embodiment, a **first device** includes a memory and a processor that executes executable components stored in the memory. The executable components include a **communication** component configured to receive a **communication** request from a **second device** via a telemetry **communication** link established between the **first** and **second devices**. The **communication** request can comprise a request for data. The executable components can also comprise a throughput monitoring component configured to monitor uplink throughput measuring successful transmission of the data by the **first device** to the **second device** via the telemetry **communication** link based on reception of the **communication** request. The **communication** component is configured to terminate the telemetry **communication** link based on the uplink throughput being below a threshold value.
AN: edspap.20190070423

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 624

30. METHOD AND APPARATUS FOR SHARING CONTENT BETWEEN ELECTRONIC **DEVICES**

Patent Application: 14/705322. Filed: May 06, 2015. Published: November 12, 2015. , Database: USPTO Patent Applications

Abstract: A method of a **first device** and an electronic **device** are provided. The method includes receiving a request signal related to contents stored in the **first device** from a **second device** communicatively coupled to the **first device**; **transmitting** the contents to the **second device** in response to the request signal, wherein the contents are security applied contents; and releasing the security of the contents by authenticating a user related to the contents.

AN: edspap.20150324605

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 625

Google executing an unlock operation to unlock the first device in response to th

Sign in

All News Videos Images More Settings Tools

About 40,800 results (0.49 seconds)

www.google.com/patents/US8667562
Input to locked computing device

Grant - Filed Sep 30, 2011 - Issued Mar 4, 2014 - Michael J LeBeau - Google Inc.
The at least one command executes so that results of executing ... in response to the user inputs to unlock the device an unlocking operation to convert the ...
Overview · Related · Discuss

www.google.com/patents/US20140376181
Unlocking Method And Electronic Apparatus

App. - Filed Feb 12, 2014 - Published Dec 25, 2014 - Qiang Zhang - Beijing Lenovo Software Ltd.
An unlocking method and an electronic apparatus are described. ... the unlocking operation is detected; and executing the unlocking instruction ... Further, after the obtaining a first matching result, the method further includes: ... authenticated in response to a first touch control unlocking operation carried out ...
Overview · Related · Discuss

www.google.com/patents/EP1964022B1?cl=en
Unlocking a device by performing gestures on an unlock image

Grant - Filed Nov 30, 2006 - Issued Mar 10, 2010 - Imran Chaudhri - Apple Inc.
An unlocked device 100 detects and responds to user input for navigating ... with respect ... The unlock image 402 is dragged along the channel 404 as a result of the ... more or fewer operations, which can be executed serially or in parallel (e.g., ... In some embodiments, the first user-interface state is a lock state and the ...
Overview · Related · Discuss

www.google.com/patents/US20110225426
Trusted group of a plurality of devices with single sign on, ...

App. - Filed Mar 7, 2011 - Published Sep 15, 2011 - Amit Agarwal - Avaya Inc.
Information about the locking or unlocking of the computer can be exchanged with the ... For example, a desktop computer may execute a screen saver that requires a ... and other device information; 4) the ability to unlock and authenticate via a ... Control of less intelligent devices linked to the smart communications devices ...
Overview · Related · Discuss

www.google.com/patents/CN102520857A?cl=en
Mobile phone screen unlocking device and unlocking method ...
App. - Filed Dec 7, 2011 - Published Jun 27, 2012 - 曾元清 - 广东欧珀移动通信有限公司
The mobile phone screen unlocking device provided by the invention has low ... [0001] The present invention relates to an Android platform-based intelligent mobile ... recording user, and sends the result to mode determination unlocking event ... the unlocking event execution module for executing in response to unlocking ...
Overview · Related · Discuss

www.google.com/patents/EP3101868A1?cl=en
Device, method, and graphical user interface for ...
App. - Filed Sep 9, 2014 - Published Dec 7, 2016 - Byron Han - Apple Inc.
While a device is in a locked mode of operation in which access to a ... a request to initiate unlocking the device; and in response to detecting the first input with ...
Overview · Related · Discuss

www.google.com/patents/EP2811724A1?cl=en
Mobile wireless communications device providing near field ...

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

www.google.com/patents/US20160316367
Method and system for secure peer-to-peer mobile communications
App. - Filed Apr 22, 2016 - Published Oct 27, 2016 - Kenneth Hugh Rose - Kenneth Hugh Rose

IPR2025-01313; Samsung
Ex. 1002 - Page 626

The present invention relates to tokens for unlocking secure systems or data. ... the decrypted verification reply and displaying on the first display a result ... and the first mobile communications device, unlocking first authentication data of the first user in the secure token in response to successful execution ...
Overview · Related · Discuss

www.google.com/patents/US20090184801

Method for Unlocking a Lock by a Lock Device Enabled for ...



App. - Filed Mar 17, 2006 - Published Jul 23, 2009 - Olle Bliding - Olle Bliding
A method is presented for unlocking a lock by a lock device enabled for ... communication addresses stored therein; d) generating an evaluation result from said ...
Overview · Related · Discuss

www.google.com/patents/US9367672

Method of locking an application on a computing device

Grant - Filed Mar 13, 2013 - Issued Jun 14, 2016 - Gary James EGGERTON · Blackberry Limited
This is the first application filed for the present technology. ... Alternatively, different gestures may be required to lock and unlock the device. Optionally, the ...
Overview · Related · Discuss

IPR2025-01313; Samsung
Ex. 1002 - Page 627

Office Action Summary	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 --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 12/16/19.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ 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.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-29 is/are pending in the application.

5a) Of the above claim(s) 12-18 is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-11 and 19-29 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, 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.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 8/8/19 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ 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)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

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	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	TBT
TEXT Searched; EAST Searched; NPL Searched - Google/Patents and Scholar	02/17/2020	TBT

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

IPR2025-01313; Samsung
Ex. 1002 - Page 629

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

IPR2025-01313; Samsung
Ex. 1002 - Page 630

Notice of References Cited	Application/Control No. 16/535,574	Applicant(s)/Patent Under Reexamination HIRABAYASHI et al.	
	Examiner THANHNGA B TRUONG	Art Unit 2498	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-9373047-B2	06-2016	Aoki; Takahiro	G06K9/00926	1/1
*	B	US-20100131414-A1	05-2010	Tame; Gavin Randall	G06F21/32	705/67
*	C	US-9314193-B2	04-2016	Haddad; Waleed Sami	G06F3/011	1/1
*	D	US-8218459-B1	07-2012	Stucker; Brian	H04L63/0407	370/261
*	E	US-8667562-B2	03-2014	LeBeau; Michael J	G06F3/048	726/2
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

DETAILED ACTION

1. This action is responsive to the communication filed on December 16, 2019. Claims 1-29 are pending. At this time, claims 1-11 and 19-29 are rejected.

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.

Election/Restrictions

3. Applicant's election of Invention I, claims 1-11 and 19-29, in the reply filed on December 16, 2019 is acknowledged.

Claims 12-18 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to nonelected Invention II, there being no allowable generic or linking claim. Election was made **with traverse** in the reply filed on December 16, 2019. However, Examiner has noticed that there are no arguments included in the Response to Election that filed on December 16, 2019. Therefore, the election will be treated as **without traverse.**

Double Patenting

4. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a

nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-11 and 19-29 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-15 of U.S. Patent No. 10, 423, 769 B2. Although the conflicting claims are not identical, they are not patentably distinct from each other because the two inventions have similar subject matter, especially 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 (see Abstract).

Allowable Subject Matter

5. Claims 1-11 and 19-29 would be allowable if a terminal disclaimer will be filed with the next amendment to overcome the Double Patenting rejection above.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

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 at 571-272-8593. The fax and phone numbers 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

February 17, 2020

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 20 Related articles All 8 versions »

A survey of **biometric** recognition methods

K Delac, M Grgic - Proceedings. Elmar-2004. 46th international ..., 2004 - ieeexplore.ieee.org
... **Fingerprint** recognition for identification **acquires** the initial image through live scan of the ... Due to different positioning on the **acquiring sensor**, imperfect imaging conditions, environmental changes ... every user is expected to possess the **biometric** trait being **acquired**, in reality it is ...
☆ 99 Cited by 535 Related articles All 12 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 93 Related articles All 4 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 228 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
... When replayed this image will be seen by this invention to be **static**, with the ... input of control **information** for an electronic **device**, said method comprising: **acquiring** through a ... image correlations between a multiplicity of small regions of the **acquired fingerprint** images; extracting ...
☆ 99 Cited by 143 Related articles All 2 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 72 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 469 Related articles All 22 versions

Person recognition method and **device**

JF Mainguet - US Patent App. 10/541,395, 2006 - Google Patents
... of using an area of silicon at least equal to the size of the print being **acquired** ... person recognition **device**, comprising: a scanning **fingerprint** image **sensor** on one base which **acquires** an image ... **acquiring** using the image **sensor** g an image line or a small number of image lines ...
☆ 99 Cited by 53 Related articles All 2 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 635

Biometrics identification module and personal wearable electronics network based authentication and transaction processing

E Kursun, G Fernandez, A Berson... - US Patent ..., 2018 - Google Patents

... In one embodiment, **static biometrics** and personal identification **information** may be hardcoded/hardwired into the ... Electrical signals (such as brain waves, EKG signals, etc.) may be **acquired** through a ... module/**device** 180 may be a standalone **device**, and may **acquire** data ...

☆ 99 Cited by 81 Related articles All 4 versions »

Biometric sensing device for three dimensional imaging of subcutaneous structures embedded within finger tissue

RM Schmitt, RA Craig - US Patent 9,607,206, 2017 - Google Patents

... or written characters or for recognising patterns, eg fingerprints; G06K9/00006—**Acquiring** or recognising ... 74 is also configured to be operable in a **second** mode for **obtaining** a **second** set ... tissue, a **static** representation of less dynamic, and relatively **static biometric** markers within ...

☆ 99 Cited by 50 Related articles All 4 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 636

Google acquiring the dynamic biometric information from the dynamic biometric Sign in

All News Images Videos More Settings Tools

About 10,600 results (0.57 seconds)

www.google.com/patents/US7020306
Personal authentication system using biometrics information
Grant - Filed Aug 15, 2000 - Issued Mar 28, 2006 - Takashi Shinzaki - Fujitsu Limited
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.
Overview · Related · Discuss

www.google.com/patents/US20160217310
System and method for partial fingerprint enrollment and ...
App. - Filed Jan 27, 2016 - Published Jul 28, 2016 - Jidnya Samir SHAH - Samsung Electronics Co., Ltd.
The mobile **device** includes a **fingerprint** registration unit configured to ... of a user are **acquired** and system registers the user by storing **biometric information** ... a finger coverage **dynamically** by stitching at least one **first** image with at least one ... **Upon** receiving the **information** from the mobile **device**, the orientation **sensor** ...
Overview · Related · Discuss

www.google.com/patents/CN102110195A?cl=en
Computer system and identification method and device for user
App. - Filed Dec 25, 2009 - Published Jun 29, 2011 - 刘欣房 - 中国长城计算机深圳股份有限公司
The method comprises the following steps of: driving a biological **information** ... and the processing chip the biological **information sensor** bidirectional ... 4 is a block diagram of a computer user identity **device** according to an ... in advance **when** the **acquired biometric information** previously stored biological template ... **First** ...
Overview · Related · Discuss

www.google.com/patents/US9418277
Electronic device and method for unlocking the electronic ...
Grant - Filed Oct 21, 2014 - Issued Aug 16, 2016 - Hsin-Wei Wang - Chiun Mai Communication Systems, Inc.
A method for **unlocking** an electronic **device** stores a user **fingerprint** in a storage **device** and presets account **information** corresponding to ... **When** the received **fingerprint** data matches one of the user fingerprints, the ... In this embodiment, the **unlocking** system 11 can include a presetting module 110, an **acquisition** ... **first** ...
Overview · Related · Discuss

www.google.com/patents/EP3035243A1?cl=en
Method of updating biometric feature pattern and electronic ...
App. - Filed Dec 14, 2015 - Published Jun 22, 2016 - Young-Eun Han - Samsung Electronics Co., Ltd
The method includes **acquiring** a plurality of **biometric** images. ... Among the various pieces of **biometric information**, a security method using the ... also includes a **sensor device** configured to receive an input of a **biometric** image. ... **When** it is mentioned that one element (e.g., a **first** element) is "(operatively or ... **Dynamic** ...
Overview · Related · Discuss

www.google.com/patents/EP3101868A1?cl=en
Device, method, and graphical user interface for ...
App. - Filed Sep 9, 2014 - Published Dec 7, 2016 - Byron Han - Apple Inc.
While a **device** is in a locked mode of operation in which access to a ... input with the **fingerprint sensor**: determining whether the **first** input meets one of **unlock** ... **Acquiring** ... **After** collecting the **fingerprint information**, the processing unit is also ... method for user authentication and **dynamic** usability of touch-screen **devices**.
Overview · Related · Discuss

www.google.com/patents/WO2016168982A1?cl=en
Method, apparatus and terminal device for setting interrupt ...
App. - Filed Apr 21, 2015 - Published Oct 27, 2016 - 李丹洪 - 华为技术有限公司
... for a **fingerprint** identification **device**, and the provided **dynamic** interrupt ... a **first acquiring** unit, configured to **acquire** a bottom noise of a ...
Overview · Related · Discuss

www.google.com/patents/US6518560

Automatic gain amplifier for biometric sensor device



Grant - Filed Apr 27, 2000 - Issued Feb 11, 2003 - Hsueh-Li J. Yeh - Veridicom, Inc.
To this end, an automatic gain amplifier is disclosed that separates the **first** peak 20 and ... In step 72, the **biometric sensor device** scans **biometric information** from, ... for specific **biometric** pattern **information when** said separation pixel-value is within ... **acquired** ... **Dynamic** finger detection mechanism for a **fingerprint sensor**.
Overview · Related · Discuss

www.google.com/patents/US9373047

Biometric authentication device, biometric authentication ...

Grant - Filed Mar 9, 2012 - Issued Jun 21, 2016 - Takahiro Aoki - Fujitsu Limited
A **biometric** authentication **device** includes a photographing unit configured to photograph a biological body and **acquire** biological body **information**; an authentication ... biological body **information when** the posture determination unit determines ... **First**, a description is given of the **sensor** unit 10. ... **unlocking** ... **Dynamic** ...
Overview · Related · Discuss

www.google.com/patents/US9471765

Fingerprint authentication with template updating

Grant - Filed Mar 10, 2016 - Issued Oct 18, 2016 - Eric Setterberg - Fingerprint Cards Ab
When it is determined that a **first** match between a present **fingerprint** ... and a representation of at least a **first** previous **fingerprint** image **acquired** in ... the swiping motion sufficient **fingerprint information** can be collected. ... of the electronic **device** in which the **fingerprint** authentication system ... **Unlocking** ...
Overview · Related · Discuss

Help Send feedback Privacy Terms

Remote device **authentication**

S Svensson - US Patent App. 10/028,583, 2003 - Google Patents

... [0018]. Where **authentication** is always **performed** via a ... The network 14 **performs** the same calculation, using RAND and the SSD associated with the ... claim 1 wherein calculating an **authentication** response based on said **authentication** key comprises **performing** a mathematical ...

☆ 99 Cited by 51 Related articles All 2 versions »

Authentication mechanism for wireless **communication** devices

K Ma - US Patent App. 10/460,969, 2005 - Google Patents

... To **perform** this, he must acquire another SIM card from his carrier ... The method of claim 11 wherein said receiving is **performed** by a user inputting on a ... Abandoned US20050021940A1 (en), 2003-06-13, 2003-06-13, **Authentication** mechanism for wireless **communication** devices ...

☆ 99 Cited by 34 Related articles All 2 versions »

Method of mutual **authentication between** a **communication interface** and a host processor of an NFC chipset

B Charrat, P Martineau - US Patent 8,762,720, 2014 - Google Patents

... in contactless data receipt mode and cyclically asks the **interface** CLINT to **perform** a scan ... key, the **authentication** of the host processor being successful if the check was successfully **performed** ... en) *, 2010-07-08, 2012-08-17, Inside Contactless, A method of **performing** a secure ...

☆ 99 Cited by 28 Related articles All 4 versions »

... 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 109 Related articles All 2 versions »

Method and arrangement **relating** to mobile telephone **communications** network

B Granstam, T Gabinus - US Patent 6,587,691, 2003 - Google Patents

Method and arrangement **relating** to mobile telephone **communications** network. Download PDF Info ... Google has not **performed** a legal analysis and makes no representation as to the accuracy of the date listed.) 1999-02-25 Filing date ... 238000004891 **communication** Methods 0 ...

☆ 99 Cited by 234 Related articles All 2 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 46 Related articles All 4 versions »

Authentication relay apparatus, **authentication** relay system, integrated circuit, and **authentication** relay method

Y Yokomitsu, Y Zhang, H Akamine - US Patent App. 11/690,463, 2007 - Google Patents

... terminals is referred to as a master apparatus, and a terminal **performing communication** under the ... 220 is started, so that cipher **communications** can be mutually **performed** therebetween ... acquire from the master apparatus 210 a network key to **perform** cipher **communications** ...

☆ 99 Cited by 179 Related articles All 2 versions »

... using geographical position and universal time determination means to provide **authenticated**, secure, on-line **communication between** remote gaming locations

AE Alcorn, RL Hale - US Patent 6,104,815, 2000 - Google Patents

... Google has not **performed** a legal analysis and makes no representation as to the accuracy of ... of a user terminal adapted to enable a player in one location to remotely **communicate** via a ... 1 of the drawing, a basic remote **communication** terminal assembly in accordance with the ...

☆ 99 Cited by 939 Related articles All 2 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 639

Use of **communication** equipment and method for **authenticating** an item, unit and system for **authenticating** items, and **authenticating** device

MA Amon, A Bleikolm, O Rozumek, E Müller... - US Patent ..., 2010 - Google Patents

... of the invention, the **authenticating** device is a micro-spectrometer for **performing** spectral analysis ... protect the sensor from dirt and mechanical damage, without degrading its optical resolution **performance** ... Said remote server may also **perform authenticating** operations centrally ...

☆ 99 Cited by 137 Related articles All 4 versions »

Electric vehicle **communication interface**

K Kelty, M Tarpenning, S Kohn - US Patent 7,698,078, 2010 - Google Patents

... Google has not **performed** a legal analysis and makes no representation as to ... of the driveline, eg determining the required power. B—**PERFORMING** OPERATIONS; TRANSPORTING; ... potential problems throughout the vehicle environment that will hinder the **performance** of the ...

☆ 99 Cited by 175 Related articles All 4 versions »

IPR2025-01313; Samsung
Ex. 1002 - Page 640

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 641

2. ## A Comprehensive Survey on VANET Security Services in Traffic Management System.

By: Sheikh, Muhammad Sameer; Liang, Jun. *Wireless **Communications** & Mobile Computing* , 9/15/2019, p1-23, 23p Abstract: Recently, vehicular ad hoc networks (VANETs) embark a great deal of attention in the area of wireless and **communication** technology and are becoming one of the prominent research areas in the intelligent transportation system (ITS) because they provide safety and precautionary measures to the drivers and passengers, respectively. VANETs are quite different from the mobile ad hoc networks (MANETs) in terms of characteristics, challenges, system architecture, and their application. In this paper, we summarize the recent state-of-the-art methods of VANETs by discussing their architecture, security, and challenges. Secondly, we discuss the detailed analysis of security schemes and the possible measures to provide secure **communication** in VANETs. Then, we comprehensively cover the **authentication** schemes, which is able to protect the vehicular network from malicious nodes and fake messages. Thus, it provides security in VANETs. Thirdly, we cover the mobility and network simulators, as well as other simulation tools, followed by the performance of **authentication** schemes. Finally, we discuss the comfort and safety applications of VANETs. In sum, this paper comprehensively covers the entire VANET system and its applications by filling the gaps of existing surveys and incorporating the latest trends in VANETs. [ABSTRACT FROM AUTHOR]; DOI: 10.1155/2019/2423915; (*AN 138630898*), Database: Applied Science & Technology Source

Subjects: Intelligent transportation systems; Ad hoc computer networks; Telecommunication; Vehicular ad hoc networks; Wireless **communications**; Other telecommunications; **Communication** Equipment Repair and Maintenance; Telecommunications Resellers; All Other Telecommunications; Radio and Television Broadcasting and Wireless **Communications** Equipment Manufacturing; Wireless Telecommunications Carriers (except Satellite); Investment analysis

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

IPR2025-01313; Samsung
Ex. 1002 - Page 642

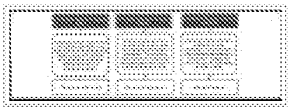
3. ## SOCIAL PRESENCE IN VIRTUAL WORLD COLLABORATION: AN UNCERTAINTY REDUCTION PERSPECTIVE USING A MIXED METHODS APPROACH.

By: Srivastava, Shirish C.; Chandra, Shalini. *MIS Quarterly*. Sep2018, Vol. 42 Issue 3, p779-803. 41p. 2 Diagrams, 11 Charts, 2 Graphs. Abstract: The life-like collaborative potential offered by virtual worlds (VWs) has sparked significant interest for companies to experiment with VWs in order to organize convenient, cost-effective virtual global workplaces. Despite the initial hype, recent years have witnessed a rather stagnant use of VWs for collaboration in organizations. Previous research recognizes that the inherent uncertainties within the VW environment are factors limiting their utilization by businesses. Hence, grounding this research in uncertainty reduction theory (URT), we aim to understand the modalities and mechanisms for mitigating the uncertainties and fostering user trust within VWs so that they can be effectively utilized as a workplace collaboration tool. With this end in view, we propose contextualizing and extending McKnight et al.'s (2002) institutional trust framework to the context of VWs by examining the significant role that social presence has in influencing the efficacy of the institution-based trust-building factors of situational normality and structural assurance in VWs. Using a sequential mixed methods approach (Venkatesh et al. 2013; Venkatesh, Brown, and Sullivan 2016), this research integrates **results** from a quantitative study with findings from a qualitative study to arrive at rich and robust inferences and meta-inferences, with the qualitative method **first** corroborating the inferences obtained from the quantitative research and then complementing them by identifying boundary conditions that may limit the use of VWs in organizations for workplace collaboration. The **results** together suggest not only the direct but also the interactional (complementary and substitutive) influences of social presence on the relationships of the two institutional trust-building factors to user trust in VWs. [ABSTRACT FROM AUTHOR] DOI: 10.25300/MISQ/2018/11914. (*AN: 131141605*), Database: Business Source Complete

Subjects: Virtual work teams; Work environment; Interprofessional relations; Uncertainty reduction theory (**Communication**); Virtual reality; Trust; Mixed methods research; Sequential analysis

Show all 19 images

IPR2025-01313; Samsung
Ex. 1002 - Page 643






PDF Full Text (2.6MB) USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 644

4. ## 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 645

5. ## 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 646

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

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

IPR2025-01313; Samsung
Ex. 1002 - Page 647

7. ## Cybersecurity challenges in vehicular **communications**

By El-Rewini, Zeinab; Sadatsharan, Karthikeyan; Selvaraj, Daisy Flora; Plathottam, Siby Jose; Ranganathan, Prakash. In *Vehicular Communications*. January 2019 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 648

8. IMAGE RECORDING APPARATUS COMMUNICABLE WITH MOBILE TERMINAL FOR IDENTIFICATION OF THE IMAGE RECORDING APPARATUS

Patent Application: 16/280332. Filed: February 20, 2019. Published: June 13, 2019. , Database: USPTO Patent Applications

Abstract: An image recording apparatus includes: a **first communication interface** configured to perform **communication** according to a **first communication** standard; a **second communication interface** configured to perform **communication** according to a **second communication** standard that is different from the **first communication** standard and that is a wireless **communication** standard; an image recorder; and a controller. The controller receives image data and **first** identification information from an image-data output device via the **first** 02-19 **communication interface**. The controller broadcasts the received **first** identification information via the **second communication interface**.

AN: edspap.20190179579

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 649

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

10. ## Image recording apparatus communicable with mobile terminal for identification of the image recording apparatus

By: BROTHER KOGYO KABUSHIKI KAISHA. US Patent: 10235,108. Filed: July 21, 2017. Issued: March 19, 2019. , Database: USPTO Patent Grants Abstract: An image recording apparatus includes: a **first communication interface** configured to perform **communication** according to a **first communication** standard; a **second communication interface** configured to perform **communication** according to a **second communication** standard that is different from the **first communication** standard and that is a wireless **communication** standard; an image recorder; and a controller. The controller receives image data and **first** identification information from an image-data output device via the **first** 02-19 **communication interface**. The controller broadcasts the received **first** identification information via the **second communication interface**.
AN: edspgr.10235108

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 650

11. Engineering with Logic.

By: Bishop, Steve; Fairbairn, Matthew; Mehnert, Hannes; Norrish, Michael; Ridge, Tom; Sewell, Peter; Smith, Michael; Wansbrough, Keith. *Journal of the ACM*. Jan2019, Vol. 66 Issue 1, p1-77. 77p. Abstract: Conventional computer engineering relies on test-and-debug development processes, with the behavior of common **interfaces** described (at best) with prose specification documents. But prose specifications cannot be used in test-and-debug development in any automated way, and prose is a poor medium for expressing complex (and loose) specifications. The TCP/IP protocols and Sockets API are a good example of this: they play a vital role in modern **communication** and computation, and interoperability between implementations is essential. But what exactly they are is surprisingly obscure: their original development focused on "rough consensus and running code," augmented by prose RFC specifications that do not precisely define what it means for an implementation to be correct. Ultimately, the actual standard is the de facto one of the common implementations, including, for example, the 15 000 to 20 000 lines of the BSD implementation—optimized and multithreaded C code, time dependent, with asynchronous event handlers, intertwined with the operating system, and security critical. This article reports on work done in the Netsem project to develop lightweight mathematically rigorous techniques that can be applied to such systems: to specify their behavior precisely (but loosely enough to permit the required implementation variation) and to test whether these specifications and the implementations correspond with specifications that are executable as test oracles. We developed post hoc specifications of TCP, UDP, and the Sockets API, both of the service that they provide to applications (in terms of TCP bidirectional stream connections) and of the internal operation of the protocol (in terms of TCP segments and UDP datagrams), together with a testable abstraction function **relating** the two. These specifications are rigorous, detailed, readable, with broad coverage, and rather accurate. Working within a general-purpose proof assistant (HOL4), we developed language idioms (within higher-order logic) in which to write the specifications: operational semantics with nondeterminism, time, system calls, monadic relational programming, and so forth. We followed an experimental semantics approach, validating the specifications against several thousand traces captured from three implementations (FreeBSD, Linux, and WinXP). Many differences between these were identified, as were a number of bugs. Validation was done using a special-purpose symbolic model checker programmed above HOL4. Having demonstrated that our logic-based engineering techniques suffice for handling real-world protocols, we argue that similar techniques could be applied to future critical software infrastructure at design time, leading to cleaner designs and (via specification-based testing) more robust and predictable implementations. In

IPR2025-01313; Samsung
Ex. 1002 - Page 651

cases where specification looseness can be controlled, this should be possible with lightweight techniques, without the need for a general-purpose proof assistant, at relatively little cost. [ABSTRACT FROM AUTHOR] DOI: 10.1145/3243650. (*AN: 135307512*), Database: Computers & Applied Sciences Complete

Subjects: Computer engineering; Debugging in computer science; TCP/IP; Automation; Software engineering

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

12. Influence of cultural dimensions on promotional e-mail effectiveness

By Lorente-Páramo, Ángel J.; Hernández-García, Ángel; Chaparro-Peláez, Julián. In *Technological Forecasting & Social Change*. January 2020 150 Language: English. DOI: 10.1016/j.techfore.2019.119788 Abstract: Highlights •Cultural dimensions help explain unsubscription rates.•Individualism and long-term orientation predict promotional e-mail effectiveness.•Cultural adaptation of e-mails must extend to neighboring contexts (e.g. websites).•E-mails should be direct and personalized in individualistic countries.•E-mails should avoid references to immediate action in long-term-oriented countries. (*AN: S0040162519310571*), Database: ScienceDirect

Full Text Finder **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 652

13. ## Design and implementation of Negative **Authentication** System.

By: Dasgupta, Dipankar; Ferebee, Denise; Saha, Sanjib Kumar; Subedi, Kul Prasad; Roy, Arunava; Nag, Abhijit Kumar; Madero, Alvaro; Sanchez, Abel; Williams, John R. *International Journal of Information Security*. Feb2019, Vol. 18 Issue 1, p23-48. 26p. Abstract: Modern society is mostly dependent on online activities like official or social **communications**, fund transfers and so on. Unauthorized system access is one of the utmost concerns than ever before in cyber systems. For any cyber system, robust **authentication** is an absolute necessity for ensuring security and reliable access to all type of transactions. However, more than 80% of the current **authentication** systems are password based, and surprisingly, they are prone to direct and indirect cracking via guessing or side channel attacks. The inspiration of Negative **Authentication** System (NAS) is based on the negative selection algorithm. In NAS, the password-based **authentication** data for valid users are termed as password profile or self-region (positive profile); any element other than the self-region is defined as non-self-region in the same representative space. The anti-password detectors are generated which covers most of the non-self-region. There are also some uncovered regions left in the non-self-region for inducing uncertainty to the attackers. In this work, we describe the design and implementation of three approaches of NAS and its efficacy over the other **authentication** methods. These three approaches represent three different ways to achieve obfuscation of password points with non-password space. The experiments are conducted with both real and simulated password profiles to justify the efficiency of different implementations of NAS. [ABSTRACT FROM AUTHOR] DOI: 10.1007/s10207-017-0395-8. (*AN: 134195910*), Database: Computer Source

Subjects: INTERNET security; PASSWORDS (Computers); CYBERTERRORISM; HASHING; COMPUTER access control; ALGORITHMS

PDF Full Text (3MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 653

14. ## 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 654

15. ## 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 655

16. Introduction to Multimedia **Communications** : Applications, Middleware, Networking

By: Rao, K. Ramamohan; Bojkovic, Z. S.; Milovanovic, Dragorad A. Hoboken, N.J. : Wiley-Interscience. 2006. eBook. Description: A comprehensive resource on multimedia **communications**. Covers recent trends and standardization activities in multimedia **communications**, such as layered structures, underlying theories and the current best design techniques. Describes the convergence of various technologies including **communications**, broadcasting, information technology, and home electronics, and emerging new **communication** services and applications resulting from the growth of the Internet and wireless technologies. Please go to www-ee.uta.edu/dip ... (*AN 149077*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Telecommunications; Multimedia **communications**

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

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 656

17. ## Detection and Prevention of Man-in-the-Middle Spoofing Attacks in MANETs Using Predictive Techniques in Artificial Neural Networks (ANN).

By: Sowah, Robert A.; Ofori-Amanfo, Kwadwo B.; Mills, Godfrey A.; Koumadi, Koudjo M.. *Journal of Computer Networks & **Communications***, 1/20/2019, p1-14, 14p Abstract: A Mobile Ad-Hoc Network (MANET) is a convenient wireless infrastructure which presents many advantages in network settings. With Mobile Ad-Hoc Network, there are many challenges. These networks are more susceptible to attacks such as black hole and man-in-the-middle (MITM) than their corresponding wired networks. This is due to the decentralized nature of their overall architecture. In this paper, ANN classification methods in intrusion detection for MANETs were developed and used with NS2 simulation platform for attack detection, identification, blacklisting, and node reconfiguration for control of nodes attacked. The ANN classification algorithm for intrusion detection was evaluated using several metrics. The performance of the ANN as a predictive technique for attack detection, isolation, and reconfiguration was measured on a dataset with network-varied traffic conditions and mobility patterns for multiple attacks. With a final detection rate of 88.235%, this work not only offered a productive and less expensive way to perform MITM attacks on simulation platforms but also identified time as a crucial factor in determining such attacks as well as isolating nodes and reconfiguring the network under attack. This work is intended to be an opening for future malicious software time signature creation, identification, isolation, and reconfiguration to supplement existing Intrusion Detection Systems (IDSs). [ABSTRACT FROM AUTHOR]; DOI: 10.1155/2019/4683982; (*AN 134209292*), Database: Applied Science & Technology Source

Subjects: Ad hoc computer networks; Intrusion detection systems (Computer security); Computer network security; Wireless **communications**; Wireless Telecommunications Carriers (except Satellite); Radio and Television Broadcasting and Wireless **Communications** Equipment Manufacturing; Host-based intrusion detection systems (Computer security)

HTML Full Text **PDF Full Text** (2.3MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 657

18. ## Policy-Based Security Management System for 5G Heterogeneous Networks.

By: Alquhayz, Hani; Alalwan, Nasser; Alzahrani, Ahmed Ibrahim; Al-Bayatti, Ali H.; Sharif, Mhd Saeed. *Wireless* ***Communications*** *& Mobile Computing.* 11/14/2019, p1-14. 14p. Abstract: Advances in mobile phone technology and the growth of associated networks have been phenomenal over the last decade. Therefore, they have been the focus of much academic research, driven by commercial and end-user demands for increasingly faster technology. The most recent generation of mobile network technology is the fifth generation (5G). 5G networks are expected to launch across the world by 2020 and to work with existing 3G and 4G technologies to provide extreme speed despite being limited to wireless technologies. An alternative network, Y-**Communication** (Y-Comm), proposes to integrate the current wired and wireless networks, attempting to achieve the main service requirements of 5G by converging the existing networks and providing an improved service anywhere at any time. Quality of service (QoS), vertical handover, and security are some of the technical concerns resulting from this heterogeneity. In addition, it is believed that the Y-Comm convergence will have a greater influence on security than was the case with the previous long-term evolution (LTE) 4G networks and with future 5G networks. The purpose of this research is to satisfy the security recommendations for 5G mobile networks. This research provides a policy-based security management system, ensuring that end-user devices cannot be used as weapons or tools of attack, for example, IP spoofing and man-in-the-middle (MITM) attacks. The **results** are promising, with a low disconnection rate of less than 4% and 7%. This shows the system to be robust and reliable. [ABSTRACT FROM AUTHOR] DOI: 10.1155/2019/4582391. (*AN: 139703327*), Database: Computers & Applied Sciences Complete

Subjects: Security management; Security systems; 4G networks; Cell phones; Quality of service; 5G networks; Long-Term Evolution (Telecommunications)

HTML Full Text **PDF Full Text** (4.4MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 658

19. The Industrial **Communication** Technology Handbook

By: Zurawski, Richard. Series: The Industrial Information Technology Series, Vol. 1. Boca Raton, Fla : CRC Press. 2005. eBook. Description: The Industrial **Communication** Technology Handbook focuses on current and newly emerging **communication** technologies and systems that are evolving in response to the needs of industry and the demands of industry-led consortia and organizations.Organized into two parts, the text **first** summarizes the basics of data **communications** and IP networks, then presents a comprehensive overview of the field of industrial **communications**. This book extensively covers the areas of fieldbus technology, industrial Ethernet ... (*AN 154212*), Database: eBook Collection (EBSCOhost)

Subjects: TECHNOLOGY & ENGINEERING / Sensors; COMPUTERS / Computer Engineering; Computer networks; Data transmission systems; Wireless **communication** systems

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

Table of Contents Most Relevant Pages From This eBook

IPR2025-01313; Samsung
Ex. 1002 - Page 659

20. ## Internet of Things for enabling smart environments: A technology-centric perspective.

By: Gomez, Carles; Chessa, Stefano; Fleury, Anthony; Roussos, George; Preuveneers, Davy. *Journal of Ambient Intelligence & Smart Environments* , 2019, Vol. 11 Issue 1, p23-43, 21p Abstract: The Internet of Things (IoT) is a computing paradigm whereby everyday life objects are augmented with computational and wireless **communication** capabilities, typically through the incorporation of resource-constrained devices including sensors and actuators, which enable their connection to the Internet. The IoT is seen as the key ingredient for the development of smart environments. Nevertheless, the current IoT ecosystem offers many alternative **communication** solutions with diverse performance characteristics. This situation presents a major challenge to identifying the most suitable IoT **communication** solution(s) for a particular smart environment. In this paper we consider the distinct requirements of key smart environments, namely the smart home, smart health, smart cities and smart factories, and relate them to current IoT **communication** solutions. Specifically, we describe the core characteristics of these smart environments and then proceed to provide a comprehensive survey of relevant IoT **communication** technologies and architectures. We conclude with our reflections on the crucial features of IoT solutions in this setting and a discussion of challenges that remain open for research. [ABSTRACT FROM AUTHOR]; DOI: 10.3233/AIS-180509; (*AN 134294075*), Database: Applied Science & Technology Source

Subjects: Internet of things; Cloud computing; Wireless **communications**; Augmented reality; Wireless Telecommunications Carriers (except Satellite); Radio and Television Broadcasting and Wireless **Communications** Equipment Manufacturing; Data Processing, Hosting, and Related Services; Smart cities

HTML Full Text **PDF Full Text** (579KB)

USPTO Full Text Options

IPR2025-01313; Samsung
Ex. 1002 - Page 660

21. ## Patent Application Titled 'Data Guard System' Published Online (USPTO 20190207943)

In: Information Technology Newsweekly. July 23, 2019, 1981; NewsRX LLC Language: English. Abstract: 2019 JUL 23 (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.594019663*), Database: Gale General OneFile

Subjects: TCP/IP; Transmission Control Protocol/Internet Protocol (Computer network protocol)

Full Text Finder USPTO Full Text Options

22. ## 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

IPR2025-01313; Samsung
Ex. 1002 - Page 661

23. ## Social-Aware Device-to-Device Offloading Based on Experimental Mobility and Content Similarity Models.

By: Aoude, Lynn; Dawy, Zaher; Sharafeddine, Sanaa; Frenn, Karim; Jahed, Karim. *Wireless **Communications** & Mobile Computing* , 5/16/2018, p1-16, 16p Abstract: Device-to-device (D2D) offloading has been shown to be a highly effective technique to enhance the performance of wireless networks. Yet, for any two mobile users to share data efficiently and reliably via D2D links, they should be in close proximity for long enough period of time, share similar content interests, and have some level of incentive and trust to cooperate. In this work, we focus on the practical implementation aspects of D2D data sharing taking into account realistic operational conditions. To this end, we design and conduct an experimental study to collect location and neighbor discovery data from 38 mobile users in a university campus over several weeks using our own customized crowdsourcing Android mobile application. The collected data is then processed and utilized to empirically model mobility-related parameters that include contact frequency, contact duration, and inter-contact duration. The participating users did also fill a user interest survey in order to correlate mobility and connectivity patterns with content interests and social network relations. The obtained insights are then used to develop a practical implementation framework for designing effective D2D data sharing strategies. To test the proposed ideas under realistic operational constraints, we design and implement a social-aware D2D data sharing Android mobile application and demonstrate its functionality and effectiveness using an example case study scenario. [ABSTRACT FROM AUTHOR]; DOI: 10.1155/2018/5606829; (*AN 129637095*), Database: Applied Science & Technology Source

Subjects: Wireless **communications**; Mobile apps; Empirical research; Wireless Telecommunications Carriers (except Satellite); Radio and Television Broadcasting and Wireless **Communications** Equipment Manufacturing; Network analysis (**Communication**); Android (Operating system)

HTML Full Text **PDF Full Text** (3MB) **USPTO Full Text Options**

IPR2025-01313; Samsung
Ex. 1002 - Page 662