(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 July 2016 (14.07.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/111489 A1

(51) International Patent Classification:
*G06F 21/32* (2013.01) *H04W 12/06* (2009.01)
*G06F 21/31* (2013.01)

(21) International Application Number:
PCT/KR2015/014269

(22) International Filing Date:
24 December 2015 (24.12.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/589,741 5 January 2015 (05.01.2015) US

(71) Applicant: **SAMSUNG ELECTRONICS CO., LTD.** [KR/KR]; 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 16677 (KR).

(72) Inventors: **RAVINDRAN, Sourabh**; 7601 Churchill Way, #238, Dallas, Dallas County, Texas 75251 (US). **LOSEU, Vitali**; 330 E. Las Colinas Boulevard, #316, Irving, Dallas County, Texas 75039 (US). **POLLEY, Michael**; 7617 Windmill Lane, Garland, Dallas County, Texas 75044 (US). **GOEL, Manish**; 4417 Helston Drive, Plano, Collin County, Texas 75024 (US). **LEE, Kyong-ho**; 1121 Belvedere Drive, Allen, Texas 75013 (US). **LEE, Seok-jun**; 1752 Vermont Court, Allen, Texas 75013 (US).

(74) Agent: **Y.P.LEE, MOCK & PARTNERS**; 12F Daelim Acrotel, 13 Eonju-ro 30-gil, Gangnam-gu, Seoul 06292 (KR).

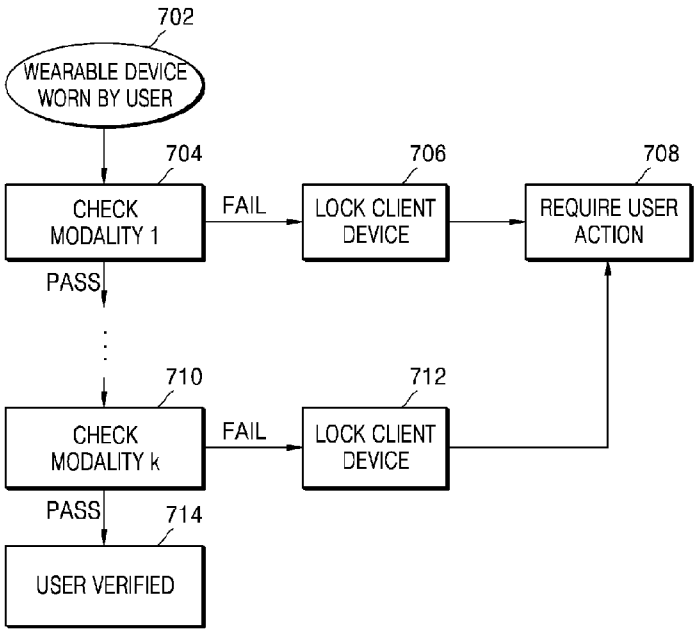
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

**Published**:

— *with international search report (Art. 21(3))*

(54) Title: METHOD AND APPARATUS FOR USER AUTHENTICATION USING BIOMETRICS




(57) Abstract: A wearable device is provided for authentication that includes a memory element and processing circuitry coupled to the memory element. The memory element configured to store a plurality of user profiles. The processing circuitry is configured to identify a pairing between the wearable device and a client device. The processing circuitry is configured to identify a user of the wearable device. The processing circuitry also is configured to determine if the identified user matches a profile of the plurality of user profiles. The processing circuitry is also configured to responsive to the identified user matching the profile, determine if the profile provides authorization to access the client device. The processing circuitry is also configured to responsive to the profile providing authorization to the client device, send a message to the client device authorizing access to the client device.

WO 2016/111489 A1

# Description

# Title of Invention: METHOD AND APPARATUS FOR USER AUTHENTICATION USING BIOMETRICS

## Technical Field

[1] The present application relates generally to user authentication and, more specifically, to a method and apparatus for using wearable devices to authenticate a user and provide improved user experience while interacting with digital devices and data.

## Background Art

[2] When a user is authenticated (either via biometrics, password or other modality) the authentication is valid only on the authenticated device and the authentication is usually invalid after certain period of inactivity. It is a challenge to make the authentication persist for a longer duration without compromising security. Further, making the authentication persist across several devices and applications while maintaining security is not straight forward.

[3] Mobile devices rely on the use of a single modality, such as fingerprint or iris, to perform biometric based user authentication. Such biometric systems suffer from a high false rejection and they require a user response such as swiping a finger.

[4] A high false rejection rate could result from adjusting for low false acceptance rates. A false rejection is when a user who should be authenticated is denied. A false acceptance is when a user who should not be authenticated is accepted. Every biometric has a trade-off between false accepts and false rejects, achieving low equal error rates is difficult especially when errors due to failure-to-capture is taken into account. A high false reject rate corresponds to bad user experience.

[5] The need for user to actively engage in the authentication process upon request leads to comparatively larger delays in user authentication and negatively impacts user experience. Users are less likely to adopt a biometric authentication solution if it requires substantially more effort.

## Disclosure of Invention

## Technical Problem

[6] When a user is authenticated (either via biometrics, password or other modality) the authentication is valid only on the authenticated device and the authentication is usually invalid after certain period of inactivity. It is a challenge to make the authentication persist for a longer duration without compromising security. Further, making the authentication persist across several devices and applications while maintaining security is not straight forward.

## Solution to Problem

[7] A wearable device comprises a memory element configured to store a plurality of user profiles, and processing circuitry coupled to the memory element, the processing circuitry configured to identify a pairing between the wearable device and a device, identify a user of the wearable device, determine if the identified user matches a profile of the plurality of user profiles, responsive to the identified user matching the profile, determine if the profile provides authorization to access the client device, and responsive to the profile providing authorization to the client device, send a message to the client device authorizing access to the client device.

## Advantageous Effects of Invention

[8] One or more embodiments of this disclosure provide a method and apparatus to perform multi-modal user identification, use of wearable device to identify user, use of wearable device in conjunction with other info to identify the user, and temporarily pairing a client device to a user, which enables seamless access to the user-specific sensitive information (as long as the pairing persists).

## Brief Description of Drawings

[9] For a more complete understanding of the present disclosure and its advantages, reference is now made to the following description taken in conjunction with the accompanying drawings, in which like reference numerals represent like parts:

[10] FIGURE 1 illustrates an example wireless network according to this disclosure;

[11] FIGURE 2 illustrates an example UE according to this disclosure;

[12] FIGURE 3 illustrates a receiver operating curve of a biometric authentication modality;

[13] FIGURE 4 illustrates receiver operating curves of combined biometric authentication modality in accordance with an embodiment of this disclosure;

[14] FIGURE 5 illustrates a parallel mode in accordance with an embodiment of this disclosure;

[15] FIGURE 6 illustrates a cascade mode in accordance with an embodiment of this disclosure;

[16] FIGURE 7 illustrates a process for a cascade mode without varying confidence verification in accordance with an embodiment of this disclosure;

[17] FIGURE 8 illustrates a process for a cascade mode in accordance with an embodiment of this disclosure;

[18] FIGURE 9 illustrates a process for varying confidence verification in parallel mode in accordance with an embodiment of this disclosure;

[19] FIGURE 10 illustrates block diagram of system of a wearable device in accordance with an embodiment of this disclosure;

[20] FIGURE 11 illustrates block diagram of system of a wearable device with environmental sensors in accordance with an embodiment of this disclosure;

[21] FIGURE 12 illustrates a process for pairing in accordance with an embodiment of this disclosure;

[22] FIGURE 13 illustrates a process for on demand authentication with on demand sensing in accordance with an embodiment of this disclosure;

[23] FIGURE 14 illustrates a process for on demand authentication with continuous sensing in accordance with an embodiment of this disclosure;

[24] FIGURE 15 illustrates a process for continuous authentication with continuous sensing in accordance with an embodiment of this disclosure; and

[25] FIGURE 16 illustrates a process for a one time authentication, followed by monitoring authentication state in accordance with an embodiment of this disclosure.

## Best Mode for Carrying out the Invention

[26] A first embodiment provides a wearable device is provided for authentication that includes a memory element and processing circuitry coupled to the memory element. The memory element configured to store a plurality of user profiles. The processing circuitry is configured to identify a pairing between the wearable device and a device. The processing circuitry is configured to identify a user of the wearable device. The processing circuitry also is configured to determine if the identified user matches a profile of the plurality of user profiles. The processing circuitry is also configured to responsive to the identified user matching the profile, determine if the profile provides authorization to access the client device. The processing circuitry is also configured to responsive to the profile providing authorization to the client device, send a message to the client device authorizing access to the client device.

[27] A second embodiment provides a method is provided for authentication. The method includes identifying a pairing between the wearable device and a device. The method also includes identifying a user of the wearable device. The method also includes determining if the identified user matches a profile of the plurality of user profiles. The method also includes responsive to the identified user matching the profile, determining if the profile provides authorization to access the client device. The method also includes responsive to the profile providing authorization to the client device, sending a message to the client device authorizing access to the client device.

[28] A third embodiment provides a wearable device in conjunction with another device for authentication that includes a memory element and processing circuitry coupled to the memory element. The memory element on the non-wearable device is configured to store a plurality of user profiles. The processing circuitry on the non-wearable device is configured to identify a pairing between the wearable device and a device.

The processing circuitry is configured to identify a user of the wearable device. The processing circuitry also is configured to determine if the identified user matches a profile of the plurality of user profiles. The processing circuitry is also configured to responsive to the identified user matching the profile, determine if the profile provides authorization to access the client device. The processing circuitry is also configured to receive periodic requests from the client device to verify that the authorization is still valid.

[29] Before undertaking the DETAILED DESCRIPTION below, it may be advantageous to set forth definitions of certain words and phrases used throughout this patent document: the terms "include" and "comprise," as well as derivatives thereof, mean inclusion without limitation; the term "or," is inclusive, meaning and/or; the phrases "associated with" and "associated therewith," as well as derivatives thereof, may mean to include, be included within, interconnect with, contain, be contained within, connect to or with, couple to or with, be communicable with, cooperate with, interleave, juxtapose, be proximate to, be bound to or with, have, have a property of, or the like; and the term "controller" means any device, system or part thereof that controls at least one operation, such a device may be implemented in hardware, firmware or software, or some combination of at least two of the same. It should be noted that the functionality associated with any particular controller may be centralized or distributed, whether locally or remotely. Definitions for certain words and phrases are provided throughout this patent document, those of ordinary skill in the art should understand that in many, if not most instances, such definitions apply to prior, as well as future uses of such defined words and phrases.

## Mode for the Invention

[30] FIGURES 1 through 16, discussed below, and the various embodiments used to describe the principles of the present disclosure in this patent document are by way of illustration only and should not be construed in any way to limit the scope of the disclosure. Those skilled in the art will understand that the principles of this disclosure may be implemented in any suitably arranged device or system.

[31] FIGURE 1 illustrates an example wireless network 100 according to this disclosure. The embodiment of the wireless network 100 shown in FIGURE 1 is for illustration only. Other embodiments of the wireless network 100 could be used without departing from the scope of this disclosure.

[32] As shown in FIGURE 1, the wireless network 100 includes an eNodeB (eNB) 101, an eNB 102, and an eNB 103. The eNB 101 communicates with the eNB 102 and the eNB 103. The eNB 101 also communicates with at least one Internet Protocol (IP) network 130, such as the Internet, a proprietary IP network, or other data network.

[33] The eNB 102 provides wireless broadband access to the network 130 for a first plurality of user equipments (UEs) within a coverage area 120 of the eNB 102. The first plurality of UEs includes a UE 111, which may be located in a small business (SB); a UE 112, which may be located in an enterprise (E); a UE 113, which may be located in a WiFi hotspot (HS); a UE 114, which may be located in a first residence (R); a UE 115, which may be located in a second residence (R); and a UE 116, which may be a mobile device (M) like a cell phone, a wireless laptop, a wireless PDA, or the like. The eNB 103 provides wireless broadband access to the network 130 for a second plurality of UEs within a coverage area 125 of the eNB 103. The second plurality of UEs includes the UE 115 and the UE 116. In some embodiments, one or more of the eNBs 101-103 may communicate with each other and with the UEs 111-116 using 5G, LTE, LTE-A, WiMAX, WiFi, Bluetooth, NFC or other wireless communication techniques.

[34] Depending on the network type, other well-known terms may be used instead of "eNodeB" or "eNB," such as "base station" or "access point." For the sake of convenience, the terms "eNodeB" and "eNB" are used in this patent document to refer to network infrastructure components that provide wireless access to remote terminals. Also, depending on the network type, other well-known terms may be used instead of "user equipment" or "UE," such as "mobile station," "subscriber station," "remote terminal," "wireless terminal," or "user device." For the sake of convenience, the terms "user equipment" and "UE" are used in this patent document to refer to remote wireless equipment that wirelessly accesses an eNB, whether the UE is a mobile device (such as a mobile telephone or smartphone) or is normally considered a stationary device (such as a desktop computer or vending machine).

[35] Dotted lines show the approximate extents of the coverage areas 120 and 125, which are shown as approximately circular for the purposes of illustration and explanation only. It should be clearly understood that the coverage areas associated with eNBs, such as the coverage areas 120 and 125, may have other shapes, including irregular shapes, depending upon the configuration of the eNBs and variations in the radio environment associated with natural and man-made obstructions.

[36] Although FIGURE 1 illustrates one example of a wireless network 100, various changes may be made to FIGURE 1. For example, the wireless network 100 could include any number of eNBs and any number of UEs in any suitable arrangement. Also, the eNB 101 could communicate directly with any number of UEs and provide those UEs with wireless broadband access to the network 130. Similarly, each eNB 102-103 could communicate directly with the network 130 and provide UEs with direct wireless broadband access to the network 130. Further, the eNB 101, 102, and/or 103 could provide access to other or additional external networks, such as external

telephone networks or other types of data networks.

[37] FIGURE 2 illustrates an example UE 116 according to this disclosure. The embodiment of the UE 116 illustrated in FIGURE 2 is for illustration only, and the UEs 111-115 of FIGURE 1 could have the same or similar configuration. However, UEs come in a wide variety of configurations, and FIGURE 2 does not limit the scope of this disclosure to any particular implementation of a UE.

[38] As shown in FIGURE 2, the UE 116 includes an antenna 205, a radio frequency (RF) transceiver 210, transmit (TX) processing circuitry 215, a microphone 220, and receive (RX) processing circuitry 225. The UE 116 also includes a speaker 230, a main processor 240, an input/output (I/O) interface (IF) 245, a keypad 250, a display 255, and a memory 260. The memory 260 includes a basic operating system (OS) program 261 and one or more applications 262.

[39] The RF transceiver 210 receives, from the antenna 205, an incoming RF signal transmitted by an eNB of the network 100. The RF transceiver 210 down-converts the incoming RF signal to generate an intermediate frequency (IF) or baseband signal. The IF or baseband signal is sent to the RX processing circuitry 225, which generates a processed baseband signal by filtering, decoding, and/or digitizing the baseband or IF signal. The RX processing circuitry 225 transmits the processed baseband signal to the speaker 230 (such as for voice data) or to the main processor 240 for further processing (such as for web browsing data).

[40] The TX processing circuitry 215 receives analog or digital voice data from the microphone 220 or other outgoing baseband data (such as web data, e-mail, or interactive video game data) from the main processor 240. The TX processing circuitry 215 encodes, multiplexes, and/or digitizes the outgoing baseband data to generate a processed baseband or IF signal. The RF transceiver 210 receives the outgoing processed baseband or IF signal from the TX processing circuitry 215 and up-converts the baseband or IF signal to an RF signal that is transmitted via the antenna 205.

[41] The main processor 240 can include one or more processors or other processing devices and execute the basic OS program 261 stored in the memory 260 in order to control the overall operation of the UE 116. For example, the main processor 240 could control the reception of forward channel signals and the transmission of reverse channel signals by the RF transceiver 210, the RX processing circuitry 225, and the TX processing circuitry 215 in accordance with well-known principles. In some embodiments, the main processor 240 includes at least one microprocessor or microcontroller.

[42] The main processor 240 is also capable of executing other processes and programs resident in the memory 260. The main processor 240 can move data into or out of the memory 260 as required by an executing process. In some embodiments, the main

processor 240 is configured to execute the applications 262 based on the OS program 261 or in response to signals received from eNBs or an operator. The main processor 240 is also coupled to the I/O interface 245, which provides the UE 116 with the ability to connect to other devices such as laptop computers and handheld computers. The I/O interface 245 is the communication path between these accessories and the main processor 240.

[43] The main processor 240 is also coupled to the keypad 250 and the display unit 255. The operator of the UE 116 can use the keypad 250 to enter data into the UE 116. The display 255 may be a liquid crystal display or other display capable of rendering text and/or at least limited graphics, such as from web sites.

[44] The memory 260 is coupled to the main processor 240. Part of the memory 260 could include a random access memory (RAM), and another part of the memory 260 could include a Flash memory or other read-only memory (ROM).

[45] The sensors 270 are also coupled to the main processor 240. The sensors 270 can detect events or changes in quantities and provide a corresponding output. For example, sensors 270 can include gyroscope, accelerometer, proximity sensor, ambient light sensor, magnetometer, location sensors, and the like. In some embodiments, the sensors 270 are configured with calibrations 271. The calibrations 271 allow for a baseline to measure changes against and can be adjusted. The sensors 270 can also obtain readings 272. The readings can be changes between a measurement and the baseline calibration. The readings 272 can be stored in memory 260 as well as other storage devices.

[46] Although FIGURE 2 illustrates one example of UE 116, various changes may be made to FIGURE 2. For example, various components in FIGURE 2 could be combined, further subdivided, or omitted and additional components could be added according to particular needs. As a particular example, the main processor 240 could be divided into multiple processors, such as one or more central processing units (CPUs) and one or more graphics processing units (GPUs). Also, while FIGURE 2 illustrates the UE 116 configured as a mobile telephone or smartphone, UEs could be configured to operate as other types of mobile or stationary devices.

[47] Various embodiments of this disclosure recognize and take into account that current biometric modalities are not in a wearable form factor. For example, fingerprint based authentication either uses a separate fingerprint scanning device or a mobile device with integrated fingerprint scanner.

[48] Various embodiments of this disclosure recognize and take into account that there are wearable biometrics such as wristbands that are EKG based authentication devices and iris recognition watches, but both of these devices need user action. Also these devices suffer from “failure to capture,” which refers to a capture of low-fidelity data from a

sensor front-end that makes it difficult to authenticate.

[49] Various embodiments of this disclosure recognize and take into account that there have been cameras used to detect a person's gait but these systems are not in the wearable form-factor and are not always in the user's immediate vicinity. There are also user behavior based methods such as keystroke dynamics that cannot be used with devices that do not have keyboards or touchscreens. Neither are these in a wearable form factor.

[50] One or more embodiments of this disclosure provide using multiple biometric modalities to solve high false rejections; each of which is tuned for very low false rejects. The multiple modalities could then be combined to provide both low false rejects and low false accepts. The multiple modalities could be behavioral, bio-dynamics, and other biometric methods. Some examples for these modalities are accelerometer based motion signature, skin type, variation of heart-rate with activity, social and device interaction patterns, body composition, metabolism based markers, and the like. In an example embodiment, the biometric modalities do not need active user input/action. A one-time authentication requiring active user input can be used.

[51] FIGURE 3 illustrates a receiver operating curve of a biometric authentication modality. Every biometric verification modality has a trade-off between false accepts (imposter being wrongly authenticated) versus false rejects (user being wrongly rejected). In FIGURE 3, an example of this trade-off is captured in the ROC curve.

[52] FIGURE 4 illustrates receiver operating curves of combined biometric authentication modality in accordance with an embodiment of this disclosure. The embodiment of the receiver operating curves illustrated in FIGURE 4 is for illustration only. However, receiver operating curves come in a wide variety of configurations, and FIGURE 4 does not limit the scope of this disclosure to any particular implementation of receiver operating curves.

[53] FIGURE 5 illustrates a parallel mode in accordance with an embodiment of this disclosure. The embodiment of the receiver operating curves illustrated in FIGURE 5 is for illustration only. However, a parallel mode come in a wide variety of configurations, and FIGURE 5 does not limit the scope of this disclosure to any particular implementation of a parallel mode.

[54] In FIGURE 5, different modalities are processed simultaneously. The individual decisions and confidence in those results are combined to provide an overall decision (i.e. accept or reject) along with overall confidence in that decision. Further, individual decisions can be selectively combined to provide results with differing confidence scores. In one example of the embodiment, instead of combining individual decisions, data from different modalities can be used to make a single decision.

[55] FIGURE 6 illustrates a cascade mode in accordance with an embodiment of this

disclosure. The embodiment of the receiver operating curves illustrated in FIGURE 6 is for illustration only. However, a cascade mode come in a wide variety of configurations, and FIGURE 6 does not limit the scope of this disclosure to any particular implementation of a cascade mode.

[56] In FIGURE 6, different modalities are evaluated in a cascade structure. Intermediate results with confidence scores are made available at various stages of the cascade. In one example implementation of the cascade structure, the current modality is trained specifically on examples (i.e. subjects) that get through the preceding modality in addition to new examples to better tune the current modality. Current modality does not have to deal with examples that fail the preceding modality thereby making the space of possibilities slightly smaller.

[57] In yet another example implementation of the cascade structure the particular order of the cascade is customized to the data of the user. For example, for user A, biometric 1 can be gait and biometric 2 can be voice, and for user B, biometric 1 can be skin type and biometric 2 can be gait.

[58] One or more embodiments can include non-biometric modalities for user authentication such as passwords, other user specific information, and the like.

[59] An embodiment of this disclosure is based on the on-demand data collection and on-demand data processing. When user makes a request that requires authentication, data is collected from a wearable device, and processed to identify the user.

[60] Another embodiment of this disclosure is based on the continuous data collection and on-demand data processing. Data is collected from the wearable or other sensors continuously and either processed into an intermediate format or stored raw in a data buffer. When user makes a request that requires authentication, the collected data is processed to identify the user.

[61] Yet another embodiment of this disclosure is based on the continuous data collection and continuous data processing. Data is collected from the wearable or other sensors continuously, and processed as soon as enough data is available. When user makes a request that requires authentication, the system verifies whether the last authentication attempt has been successful or not.

[62] Yet another embodiment of this disclosure is based on the initial authentication when user wears the wearable device and after initial authentication tracking the change in authentication state using sensor, mechanical design, or external inputs. One time authentication confirms user identity, and switches the wearable device into an authenticated state and from that point, the system tracks whether the authentication still holds. In the example of a watch form factor, the verification can be done by checking if the person has taken the watch off after the initial authentication. Among other solutions, this can be done via skin conductance or optical sensors, or a mechanical

method of detecting the wearable device is off.

[63] FIGURE 7 illustrates a process for a cascade mode without varying confidence verification in accordance with an embodiment of this disclosure. The controller here may represent the main processor 240 and the memory element may be the memory 260 in FIGURE 2. The embodiment of the process shown in FIGURE 7 is for illustration only. Other embodiments of the process could be used without departing from the scope of this disclosure.

[64] At operation 702, the controller determines that a user wears the wearable device. The wearable device could be any type of wearable device and may be worn by the user in many different methods.

[65] At operation 704, the controller checks a first modality. If the first modality fails, at operation 706, the client device is locked. The client device can be another mobile device. The controller may transmit a message to the client device to lock. Once the client device is locked, at operation 708, the controller requests user action to verify the user and unlock the client device.

[66] At operation 710, another modality is checked. If the other modality fails, at operation 712, the client device is locked and user action is requested at operation 708. If at operations 704 and 710, the modalities pass, at operation 714, the user is verified.

[67] In FIGURE 7, operations 704 and 710 are performed in sequence. In other example embodiments, operations 704 and 710 can be performed in parallel. As used herein, checking a modality can be defined as monitoring a biometric.

[68] FIGURE 8 illustrates a process for a cascade mode in accordance with an embodiment of this disclosure. The controller here may represent the main processor 240 and the memory element may be the memory 260 in FIGURE 2. The embodiment of the process shown in FIGURE 8 is for illustration only. Other embodiments of the process could be used without departing from the scope of this disclosure.

[69] At operation 802, the controller determines that a user wears the wearable device. The wearable device could be any type of wearable device and may be worn by the user in many different methods.

[70] At operation 804, the controller checks a first modality. If the first modality fails, at operation 806, the client device is locked. The client device can be another mobile device. The controller may transmit a message to the client device to lock. Once the client device is locked, at operation 808, the controller requests user action to verify the user and unlock the client device.

[71] At operation 804, if the first modality passes, then at operation 809, the user is verified with a low confidence. A low confidence can be defined as a low confidence that the user has permission to access the client device. A high confidence can be defined as a higher confidence than the lower confidence that the user has permission

to access the client device.

[72] At operation 810, the next modality is checked. If the next modality fails, at operation 812, the client device is locked and user action is requested at operation 808. If at operation 810, the next modality passes, at operation 814, the user is verified with high confidence.

[73] FIGURE 9 illustrates a process for varying confidence verification in parallel mode in accordance with an embodiment of this disclosure. A controller here may represent the main processor 240 and a memory element may be the memory 260 in FIGURE 2. The embodiment of the process shown in FIGURE 9 is for illustration only. Other embodiments of the process could be used without departing from the scope of this disclosure.

[74] At operation 902, the controller determines that a user wears the wearable device. The wearable device could be any type of wearable device and may be worn by the user in many different methods.

[75] At operation 904 and 910, the controller checks the modalities. The operations 904 and 910 can be performed at different or the same times. At operation 920, a decision logic controlled by the processor receives pass or fails (yes or no) from operations 904 and 910. Operations 904 and 910 can also provide confidence scores. As used herein, confidence or confidence scores may be defined as the determined by how close the values of the modalities are to an ideal or registered modality and also the inherent false positive of that modality. Also, as used herein, modality can be referred to as a biometric.

[76] At operation 921, the controller determines whether the decision logic passed or failed the user using the combined confidence score. In response to passing, the controller verifies the user. In response to failing, at operation 906, the controller transmits a signal to the client device to lock the client device. At operation 908, the controller requires and/or requests a user action to unlock the client device. Herein, the user action can be entering a password, a fingerprint scan, and the like.

[77] Various embodiments of this disclosure recognize and take into account that with electronic devices, for example tablets or computers, being shared between multiple people there is none or very little (i) separation of user preferences, and (ii) protection of user-specific sensitive information.

[78] In one or more embodiments, as used herein, a client device can be any electronic device that runs secure applications and may require authentication, for example a mobile device or a personal computer. User-specific sensitive information may include documents, installed applications/programs, settings, preferences, history for applications and programs, and the like.

[79] One or more embodiments of this disclosure provide using multi-modal biometrics

and other sensor info as proxy for user authentication credentials. A wearable device (in conjunction with other info) uniquely identifies the user based on the user, the client device (for example, tablet) is configured to fit the user profile, which enables access to the user specific sensitive information.

[80] One or more embodiments of this disclosure provide a method and apparatus to perform multi-modal user identification, use of wearable device to identify user, use of wearable device in conjunction with other info to identify the user, and temporarily pairing a client device to a user, which enables seamless access to the user-specific sensitive information (as long as the pairing persists).

[81] FIGURE 10 illustrates block diagram of system of a wearable device in accordance with an embodiment of this disclosure. The embodiment of the system of a wearable device illustrated in FIGURE 10 is for illustration only. However, systems come in a wide variety of configurations, and FIGURE 10 does not limit the scope of this disclosure to any particular implementation of the system. The devices in FIGURE 10 can be controlled by a controller and/or processor such as main processor 240 as shown in FIGURE 2.

[82] In an embodiment of this disclosure, the system includes user 1002. The user can be someone who has access to client device 1008. Wearable device 1004 monitors the biometrics for user 1002. Wearable device 1004 can identify a user and send the identity of the user to profile manager 1006. Profile manager 1006 can pair the identity of the user to a user profile. The profile can include user-specific sensitive information. The profile manager 1006 can reside on the wearable device 1006 or client device 1008. The client device (or primary device) 1008 can receive the profile and allow user specific access.

[83] FIGURE 11 illustrates block diagram of system of a wearable device with environmental sensors in accordance with an embodiment of this disclosure. The embodiment of the system of a wearable device illustrated in FIGURE 11 is for illustration only. However, systems come in a wide variety of configurations, and FIGURE 11 does not limit the scope of this disclosure to any particular implementation of the system. The devices in FIGURE 11 can be controlled by a controller and/or processor such as main processor 240 as shown in FIGURE 2.

[84] In an embodiment of this disclosure, the system is similar to the system of FIGURE 10. This system also includes environmental sensors 1102 and a cloud 1104. Wearable device 1004 can use information received about the environment from the environmental sensors 1102 and/or received from the cloud from cloud 1104 along with the biometrics in determining a user identity.

[85] FIGURE 12 illustrates a process for pairing in accordance with an embodiment of this disclosure. A controller here may represent the main processor 240 and a memory

element may be the memory 260 in FIGURE 2. The embodiment of the process shown in FIGURE 12 is for illustration only. Other embodiments of the process could be used without departing from the scope of this disclosure.

[86] At operation 1202, a controller of the wearable device identifies a user. The user can be identified using any of the techniques herein. At operation 1204, the wearable device pairs to the client device(or primary device). At operation 1206, a user profile is loaded or transmitted to the client device. At operation 1208, the controller monitors the pairing to determine whether it persists. Once the pairing has been terminated or lost, at operation 1210, a generic profile is loaded onto the client device or the client device could be locked. A generic profile can lose access to user-specific sensitive information. During operating 1208, the wearable device, the client device, or a combination of both may monitor the pairing status.

[87] Various embodiments take into account and recognize that due to the client device and user mobility, current methods of authentication may not verify the authentication validity past the actual authentication time. This results in very short time outs and frequent requests for re-authentication. Truly seamless authentication requires a method for continuous re-authentication or verification of the authentication validity without an active user input.

[88] FIGURE 13 illustrates a process for on demand authentication with on demand sensing in accordance with an embodiment of this disclosure. A controller here may represent the main processor 240 and a memory element may be the memory 260 in FIGURE 2. The embodiment of the process shown in FIGURE 13 is for illustration only. Other embodiments of the process could be used without departing from the scope of this disclosure.

[89] One or more embodiments of this disclosure provide on demand authentication with on demand sensing. In this embodiment, only a short window of data is required. In other words, the data for an effective authentication can be collected quickly. The authentication process is short and can be performed quickly without user input.

[90] At operation 1302, when user makes an authentication request, at operation 1304, sensor data is collected on demand. At operation 1306, the collected data is then processed to make an authentication decision. At operation 1308, the controller determines whether there is a user match. If there is a user match, at operation 1310, the controller confirms the user. If there is not a match, at operation 1312, the controller denies the user.

[91] Data collected on demand can be, but not limited, to biometric, wearable sensors, and other sensors. Processing may include, but not limited to, processing data from a single data modality and processing data from multiple modalities.

[92] FIGURE 14 illustrates a process for on demand authentication with continuous

sensing in accordance with an embodiment of this disclosure. A controller here may represent the main processor 240 and a memory element may be the memory 260 in FIGURE 2. The embodiment of the process shown in FIGURE 14 is for illustration only. Other embodiments of the process could be used without departing from the scope of this disclosure.

[93] An embodiment of this disclosure provides a process during long window of data or when data collection is takes a while, meaning that data may not be collected on demand and the data is to be collected (or continuously since it is unknown when an authentication request will be made). The authentication process is short and can be performed quickly without user input.

[94] At operation 1406, when user makes an authentication request, at operation 1408, sensor data is collected on demand. At operation 1410, the controller determines whether there is a user match. If there is a user match, at operation 1412, the controller confirms the user. If there is not a match, at operation 1414, the controller denies the user.

[95] At operation 1402, sensor data is collected continuously. The sensor data is either stored raw in a data buffer, or is processed into intermediate data, at operation 1404, and stored into a data buffer. When user makes an authentication request, the stored data is processed to make an authentication decision.

[96] An embodiment of this disclosure provides that some data may be collected on demand, while other data may be collected continuously. Data collected can be, but not limited to, biometric, wearable sensors, and other sensors. The continuously collected data can be stored raw, or stored as a result of intermediate processing that is done continuously. Processing may include processing data from a single data modality and processing data from multiple modalities.

[97] FIGURE 15 illustrates a process for continuous authentication with continuous sensing in accordance with an embodiment of this disclosure. A controller here may represent the main processor 240 and a memory element may be the memory 260 in FIGURE 2. The embodiment of the process shown in FIGURE 15 is for illustration only. Other embodiments of the process could be used without departing from the scope of this disclosure.

[98] An embodiment provides for data to be collected on a continuous basis. The authentication process is executed continuously as enough data becomes available.

[99] At operation 1508, when user makes an authentication request, at operation 1510, the controller updates the authentication state. At operation 1512, the controller determines whether there is a user match. If there is a user match, at operation 1514, the controller confirms the user. If there is not a match, at operation 1516, the controller denies the user.

[100] At operation 1502, sensor data is collected continuously. The sensor data is either stored raw in a data buffer, or is processed into intermediate data, at operation 1504, and stored into a data buffer. When enough data is available, at operation 1506, the stored data is processed to make an authentication decision. When user makes an authentication request, the system verifies whether it is still authenticated (based on the continuous processing).

[101] An embodiment of this disclosure provides that some data may be collected on demand, while other data may be collected continuously. Data collected can be, but not limited to, biometric, wearable sensors, and other sensors. The continuously collected data can be stored raw, or stored as a result of intermediate processing that is done continuously. Processing may include processing data from a single data modality and processing data from multiple modalities.

[102] FIGURE 16 illustrates a process for a one time authentication, followed by monitoring authentication state in accordance with an embodiment of this disclosure. A controller here may represent the main processor 240 and a memory element may be the memory 260 in FIGURE 2. The embodiment of the process shown in FIGURE 16 is for illustration only. Other embodiments of the process could be used without departing from the scope of this disclosure.

[103] An embodiment provides that if there are clear conditions that indicate change from authenticated state to non-authenticated state, and these conditions can be observed by wearable or other sensors, or by other means.

[104] At operation 1602, a user is pre-authenticated and one time data is collected from the wearable device. At operation 1604, the system enters authenticated state using the one time data. At operation 1608, the controller collects data from wearable or other sensors or user other information to, at operation 1610, verify if the conditions invalidating authenticated state have been met.

[105] At operation 1618, when user makes an authentication request, at operation 1606, the controller updates the authentication state. At operation 1606, the authentication state is updated. At operation 1612, the controller determines whether there is a state match. When user makes an authentication request, the system verifies whether it is still in the authenticated state.

[106] If there is a state match, at operation 1614, the controller confirms the user. If there is not a match, at operation 1616, the controller denies the user.

[107] In this embodiment, the initial authentication is performed on demand including but not limited to biometrics, password verification, wearables, and the like. Sensors used for the initial authentication may or may not be the same as sensors used for the verification of the state. The data used for the verification of the state may include, but is not limited to, optical sensors to see if skin is continuously detected and the wearable

has not been taken off, skin conductance sensor to see if skin is continuously detected and the wearable has not been taken off, and to monitor changes in the mechanical setup of the wearable to verify if the conditions invalidating authenticated state have been met. Monitoring changes in mechanical setup may be but is not limited to, in case of a watch form factor wearable, a circuit in a watch strap to see if the watch strap is opened at any point, and the watch is removed.

[108] One or more embodiments of this disclosure provide a user of a wearable device for continuous user authentication, a user of biometrics data for continuous user authentication, a method for continuous user authentication with on demand data collection and on demand processing, a method for continuous user authentication with continuous data collection and on demand processing, a method for continuous user authentication with continuous data collection and continuous processing, use of wearable device to verify a previously confirmed authentication, use of wearable device to continuously verify a previously confirmed authentication, use of biometrics to verify a previously confirmed authentication, use of biometrics to continuously verify a previously confirmed authentication, a method for maintaining a coupling between a wearable device and a previously confirmed user authentication, use of skin conductance for maintain coupling between the wearable device and a previously confirmed user authentication, use of optical sensors for maintain coupling between the wearable device and a previously confirmed user authentication, and use of mechanical or electrical means to ascertain that the wearable device is still coupled to the user in the same manner as when the user identity was confirmed.

[109] An embodiment of this disclosure uses a wearable device to allow the user to log into all of her devices without the need to individually log into them provided the wearable device is first authorized. The requirement that the wearable device be authorized improves the security of the system over other methods that simply use a "designated" device (such as a smart watch) to unlock the primary device when in close proximity. The security is improved by ensuring that the access is tied to the user and not a designated device (which can be stolen).

[110] The wearable device can be authorized in multiple ways:

[111] The user wears the wearable and enters a password (either directly on the wearable or on a device paired to the wearable, as such as a smart phone).

[112] The user wears the wearable device and uses biometric (one or more) to authorize the wearable.

[113] An added security feature is the ability to provide "intent confirmation". This is a method for the user to acknowledge that the action being enabled is indeed with the user's consent. For example, when a secure banking app on a mobile device is clicked, before providing access to the bank account, the user gets a notification on the

wearable to confirm that she is the one performing the action.

[114] Intent confirmation is configurable, providing a trade-off between control and convenience for the user. If the user desires convenience then the intent confirmation can be set to "implicit" meaning as long the authenticated wearable is within a pre-defined wireless range, access is granted without any action from the user wearing the wearable. If the user desires more control then the confirmation can be set to "explicit" meaning the user has to acknowledge by pushing a button, doing a pre-defined gesture etc. before access can be granted or requested action can be completed. Other "in-between" modes can also be set that trades-off convenience and control based on user's preference.

[115] An example embodiment provides a wearable device providing authorization for specific functions of the mobile device. Such as, for example, a banking application, a password, any other application set by the user, and the like.

[116] An example embodiment also provides a way to generate strong passwords for the user. By using this feature the user (while registering a new account or device) can use a very strong password for improved security without the headache or need to remember it.

[117] In an embodiment, once the wearable device is authorized, the validity of the authorization persists (meaning no re-authorization is required) as long as the wearable has not been taken off the user's body. This can be accomplished is multiple ways.

[118] - Upon request, perform sensing and authentication of the user wearing the wearable device

[119] - Continuous sensing, and upon request perform authentication of the user wearing the wearable device

[120] - Continuous sensing and continuous authentication of the user wearing the wearable device

[121] Monitoring the state of the wearable device via sensors, mechanical design, user input or other methods to determine that the wearable device was taken off-body. Such as, for example ? a current circuit that is broken when the strap of a watch is unhooked.

[122] In an embodiment of this disclosure, the process of user authentication with biometrics can be done using a wearable device based multi-modal biometric approach. The differentiating factor here is the ability to do "unobtrusive" biometrics that minimizes the need for user input while doing biometrics.

[123] In an embodiment of this disclosure, a client device requests user data from a wearable device. The user attributes can be biometric data, passwords, or other user data used in identifying a user. As used herein, identifying a user can be identifying attributes about a user, and not necessarily identify an identity of the user. Identifying a user is used to compare values from the user attributes to stored profiles.

[124] A client device is provided for authentication that includes a memory element and processing circuitry coupled to the memory element. The memory element configured to store a plurality of user profiles. The processing circuitry is configured to identify a pairing between the wearable device and a client device. The processing circuitry is configured to request an identity of a user of a wearable device. The wearable device retrieves the biometric, password, or other user data and sends this data to the mobile device. The processing circuitry also is configured to determine if the identified user matches a profile of the plurality of user profiles. The processing circuitry is also configured to responsive to the identified user matching the profile; determine if the profile provides authorization to access the client device. The processing circuitry is also configured to responsive to the profile providing authorization to the client device, send a message to the client device authorizing access to the client device.

[125] In another embodiment, a wearable device is provided to detect whether the wearable device is connected to a user or not. The term connected could mean worn by a user, or on a body of a user. In this embodiment, a client device can request the wearable device to confirm whether the wearable device is connected to the user. The connection can identify whether to continue to grant access to the client device.

[126] Although the present disclosure has been described with an exemplary embodiment, various changes and modifications may be suggested to one skilled in the art. It is intended that the present disclosure encompass such changes and modifications as fall within the scope of the appended claims.

# Claims

[Claim 1] A wearable device, comprising:
a memory element configured to store a plurality of user profiles; and
processing circuitry coupled to the memory element, the processing circuitry configured to:
identify a pairing between the wearable device and a client device;
identify a user of the wearable device;
determine if the identified user matches a profile of the plurality of user profiles;
responsive to the identified user matching the profile, determine if the profile provides authorization to access the client device; and
responsive to the profile providing authorization to the client device, send a message to the client device authorizing access to the client device.

[Claim 2] The wearable device of Claim 1, wherein identifying the user of the wearable device comprises the processing circuitry configured to:
monitor at least one biometric of the user.

[Claim 3] The wearable device of Claim 2, wherein determining if the identified user matches the profile of the plurality of user profiles comprises the processing circuitry configured to:
compare the at least one biometric of the user to biometrics associated with the plurality of user profiles.

[Claim 4] The wearable device of Claim 1, wherein identifying the user of the wearable device comprises the processing circuitry configured to:
receive an input of a password.

[Claim 5] The wearable device of Claim 4, wherein determining if the identified user matches the profile of the plurality of user profiles comprises the processing circuitry configured to:
compare the password to passwords associated with the plurality of user profiles.

[Claim 6] The wearable device of Claim 1, wherein a user configurable setting indicates whether a confirmation is required for access to specific functions of the client device.

[Claim 7] The wearable device of Claim 6, wherein, when the confirmation is required, the confirmation is at least one of pre-determined user action, a gesture, a password, and a push of a button.

[Claim 8] The wearable device of Claim 1, further comprising the processing

circuitry configured to:
receive a request from the client device for a password;
generate the password; and
associate the password with the profile.

[Claim 9] The wearable device of Claim 1, further comprising the processing circuitry configured to:
receive a request from the client device to re-authorize the identified user;
responsive to the request, re-identify the user of the wearable device;
determine if the re-identified user matches the profile of the plurality of user profiles;
responsive to the re-identified user matching the profile, determine if the profile provides authorization to access the client device; and
responsive to the profile providing access to the client device, send a message to the client device authorizing the user.

[Claim 10] The wearable device of Claim 1, further comprising the processing circuitry configured to:
continually monitor at least one biometric of the identified user;
receive a request from the client device to verify the identified user; and
responsive to the request, verify the user of the wearable device.

[Claim 11] The wearable device of Claim 1, further comprising the processing circuitry configured to:
continually monitor at least one biometric of the identified user; and
continually authorize the identified user based on the continual monitoring.

[Claim 12] The wearable device of Claim 1, further comprising the processing circuitry configured to:
determine whether the wearable device is removed from the user; and
responsive to the wearable device being removed from the user, de-authorize the user.

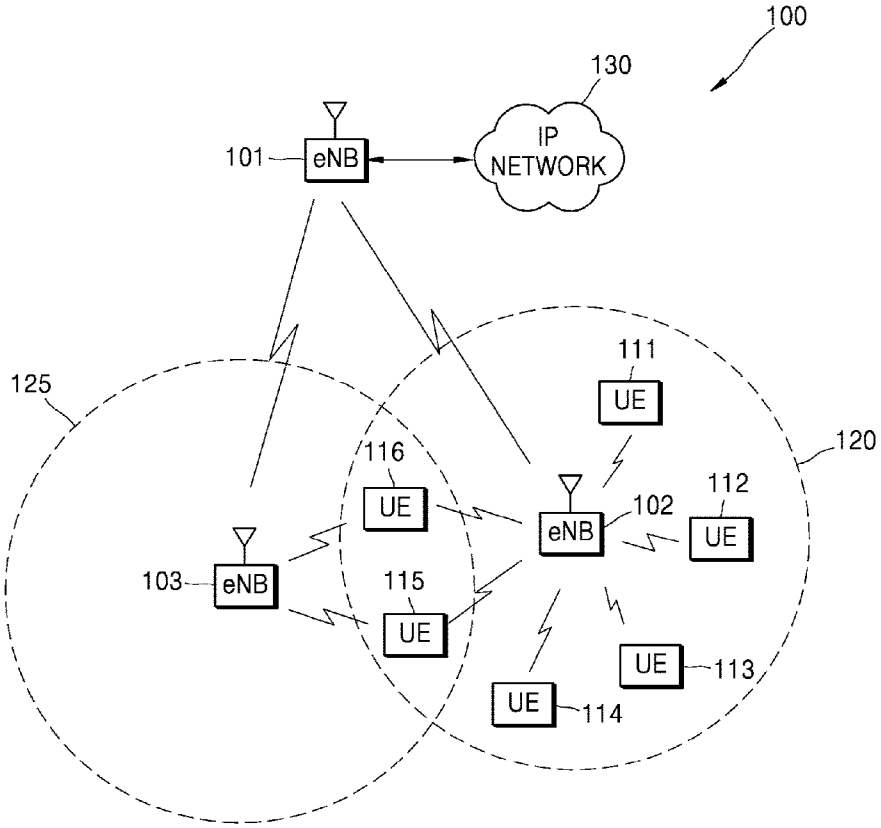
[Claim 13] The wearable device of Claim 1, further comprising the processing circuitry configured to:
receive a request from the client device to authorize the identified user for a function;
responsive to the request, re-identify the user of the wearable device;
determine if the re-identified user matches the profile of the plurality of user profiles;

responsive to the re-identified user matching the profile, determine if the profile provides authorization for the function; and
responsive to the profile providing access to the client device, send a message to the client device authorizing the function.

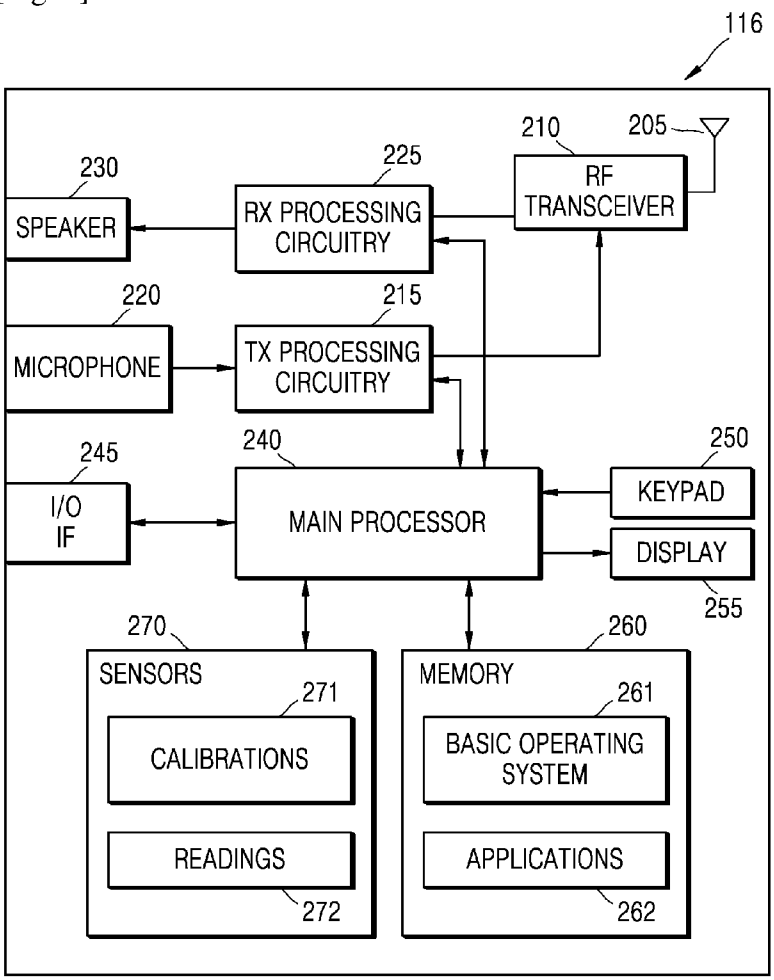
[Claim 14] A method for authenticating a user, the method comprising:
identifying a pairing between a wearable device and a client device;
identifying a user of the wearable device;
determining if the identified user matches a profile of a plurality of user profiles;
responsive to the identified user matching the profile, determining if the profile provides authorization to access the client device; and
responsive to the profile providing authorization to the client device, sending a message to the client device authorizing access to the client device.

[Claim 15] The method of Claim 14, wherein the identifying the user of the wearable device comprises:
monitoring at least one biometric of the user.

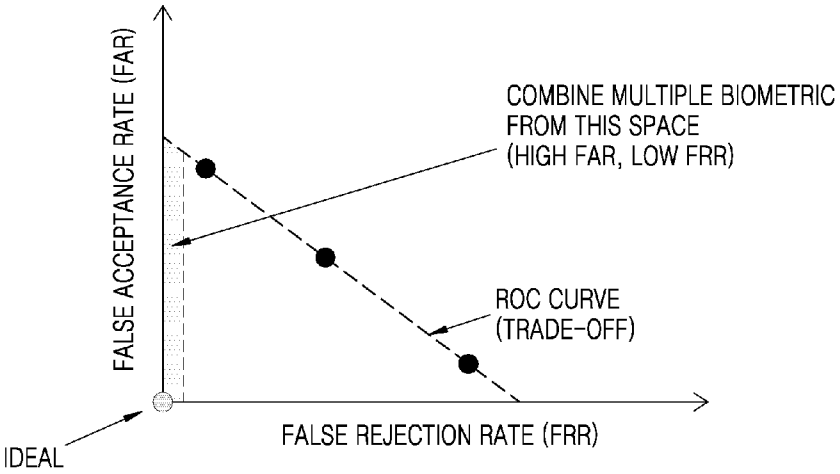
[Fig. 1]


100
130
IP NETWORK
101
eNB
125
111
UE
120
116
UE
112
102
eNB
UE
103
eNB
115
UE
UE
113
UE
114

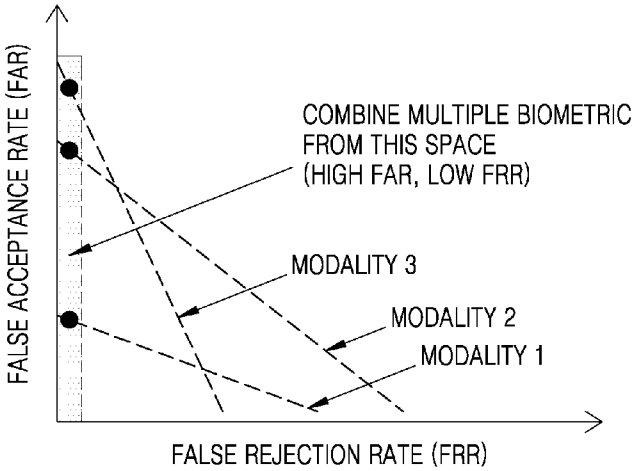
[Fig. 2]


116
210
205
RF TRANSCEIVER
225
230
SPEAKER
RX PROCESSING CIRCUITRY
220
215
MICROPHONE
TX PROCESSING CIRCUITRY
245
240
250
I/O IF
MAIN PROCESSOR
KEYPAD
DISPLAY
255
270
260
SENSORS
271
CALIBRATIONS
READINGS
272
MEMORY
261
BASIC OPERATING SYSTEM
APPLICATIONS
262

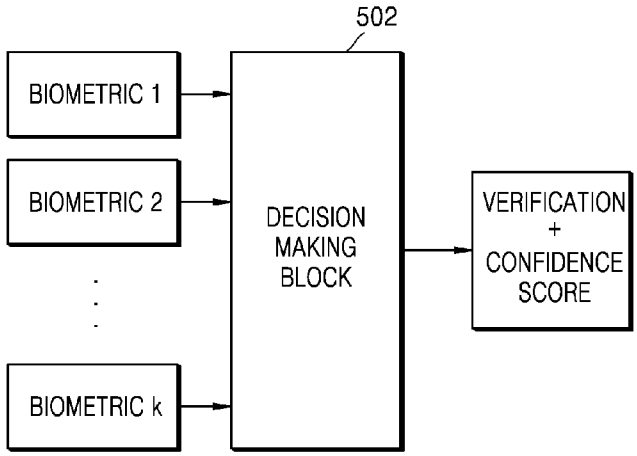
[Fig. 3]



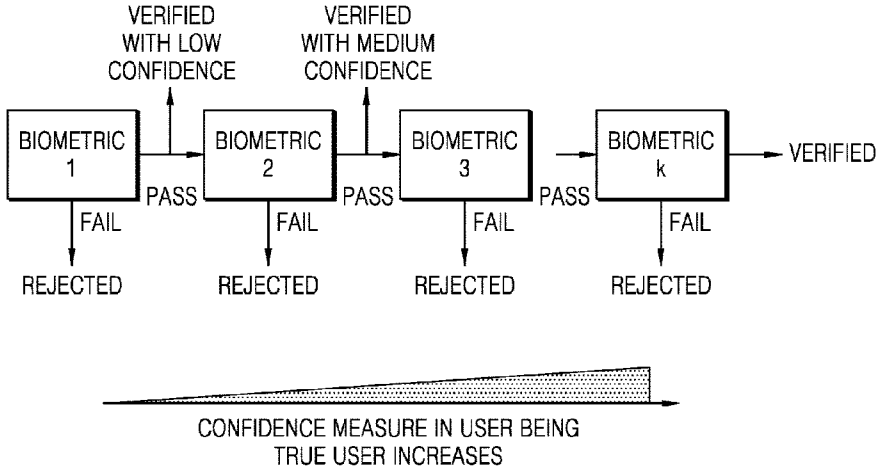

[Fig. 4]



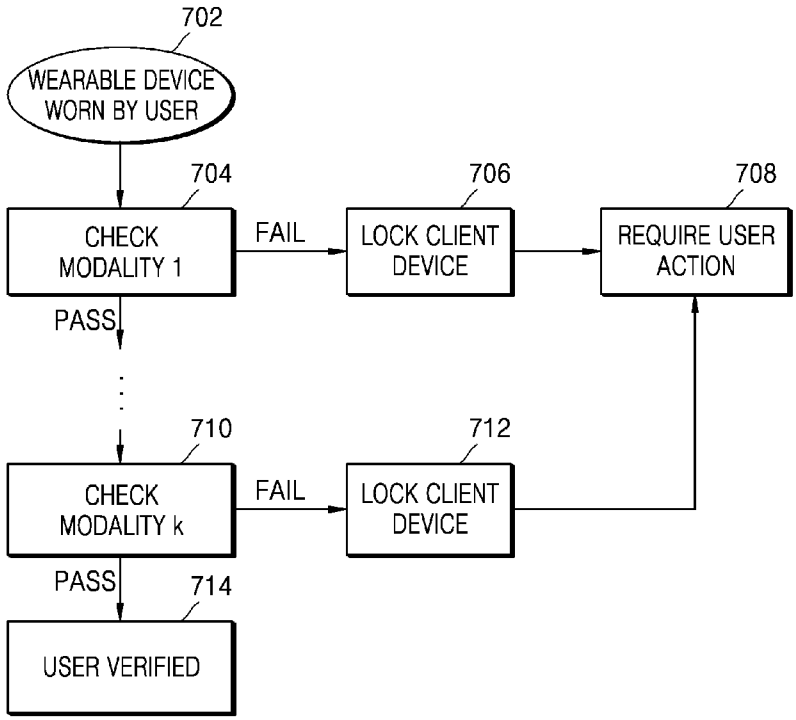

[Fig. 5]



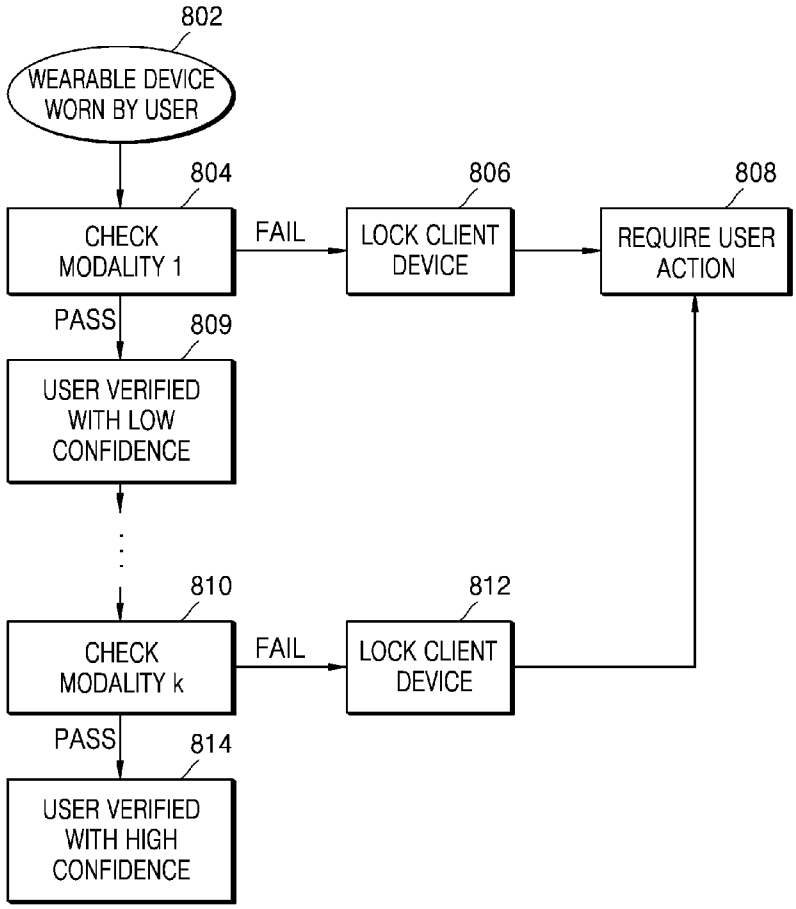
[Fig. 6]


VERIFIED WITH LOW CONFIDENCE
VERIFIED WITH MEDIUM CONFIDENCE
BIOMETRIC 1
BIOMETRIC 2
BIOMETRIC 3
BIOMETRIC k
VERIFIED
PASS
PASS
PASS
FAIL
FAIL
FAIL
FAIL
REJECTED
REJECTED
REJECTED
REJECTED
CONFIDENCE MEASURE IN USER BEING TRUE USER INCREASES

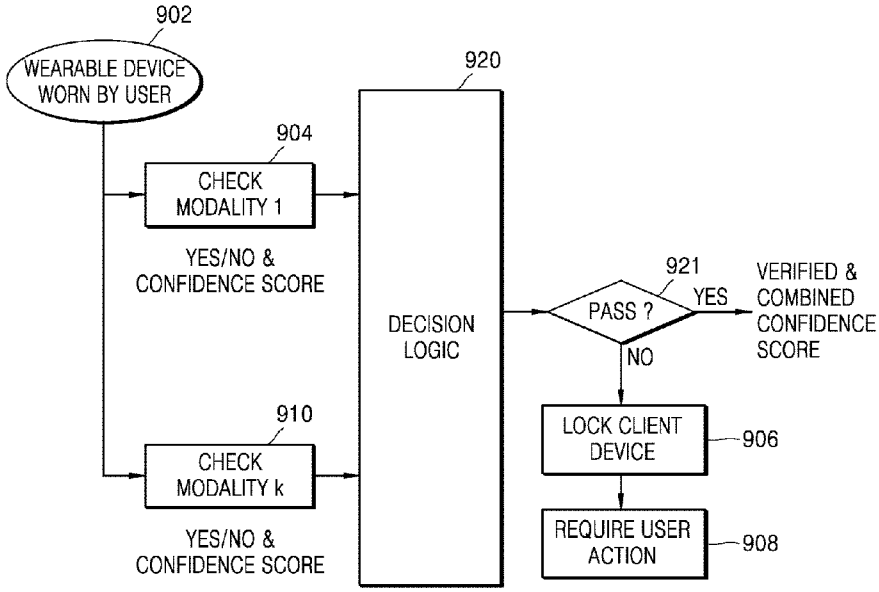
[Fig. 7]


702
WEARABLE DEVICE WORN BY USER
704
CHECK MODALITY 1
FAIL
706
LOCK CLIENT DEVICE
708
REQUIRE USER ACTION
PASS
710
CHECK MODALITY k
FAIL
712
LOCK CLIENT DEVICE
PASS
714
USER VERIFIED

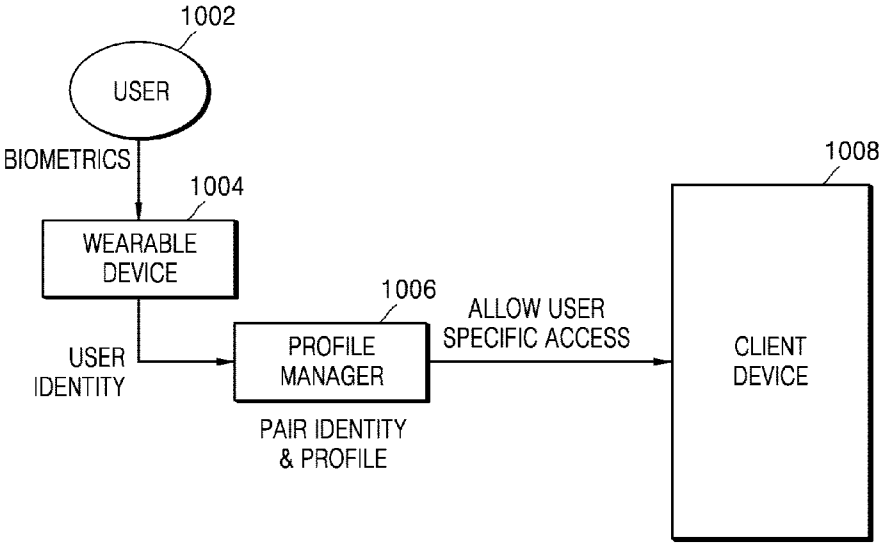
[Fig. 8]


802
WEARABLE DEVICE WORN BY USER
804
CHECK MODALITY 1
FAIL
806
LOCK CLIENT DEVICE
808
REQUIRE USER ACTION
PASS
809
USER VERIFIED WITH LOW CONFIDENCE
810
CHECK MODALITY k
FAIL
812
LOCK CLIENT DEVICE
PASS
814
USER VERIFIED WITH HIGH CONFIDENCE

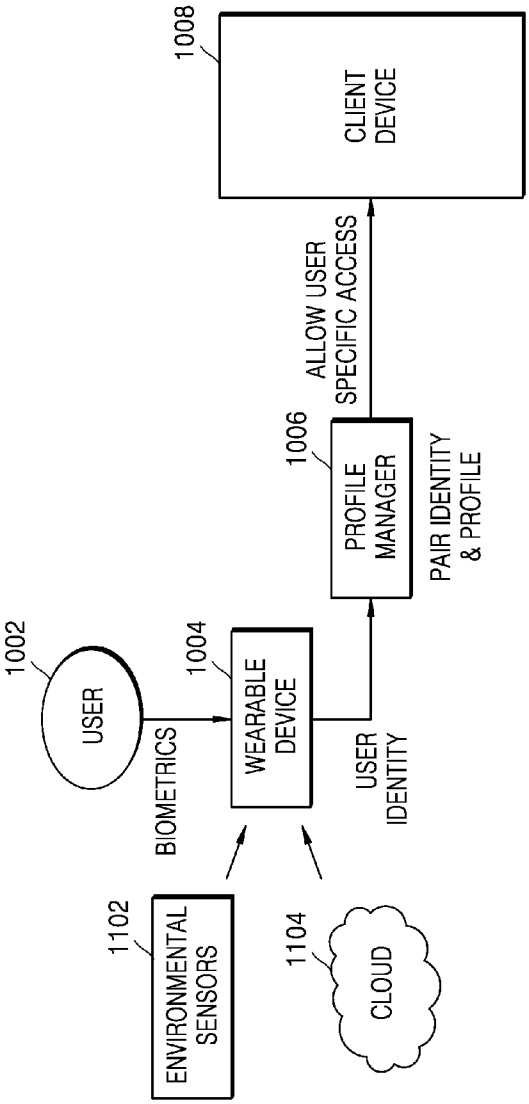
[Fig. 9]


902
WEARABLE DEVICE WORN BY USER
904
CHECK MODALITY 1
YES/NO & CONFIDENCE SCORE
910
CHECK MODALITY k
YES/NO & CONFIDENCE SCORE
920
DECISION LOGIC
921
PASS ?
YES
VERIFIED & COMBINED CONFIDENCE SCORE
NO
LOCK CLIENT DEVICE
906
REQUIRE USER ACTION
908

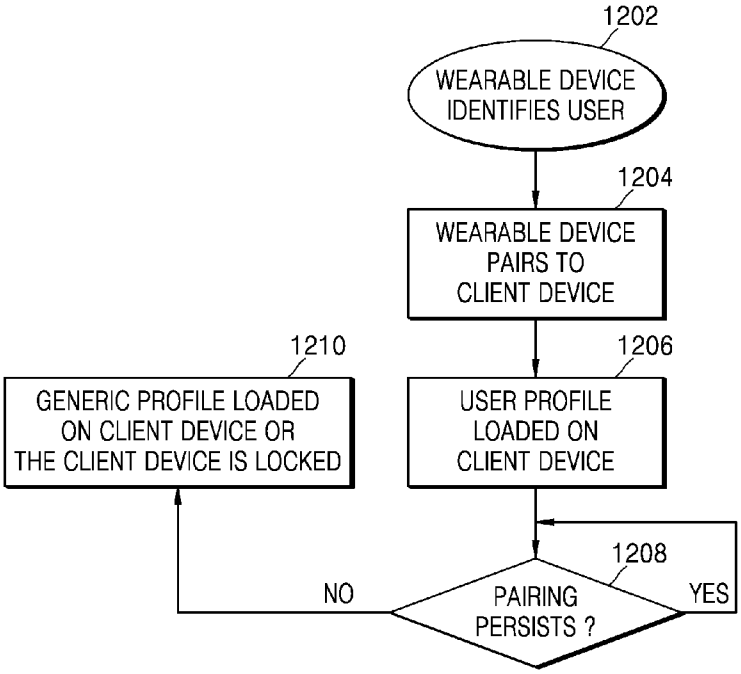
[Fig. 10]


1002
USER
BIOMETRICS
1004
WEARABLE DEVICE
USER IDENTITY
1006
PROFILE MANAGER
PAIR IDENTITY & PROFILE
ALLOW USER SPECIFIC ACCESS
1008
CLIENT DEVICE

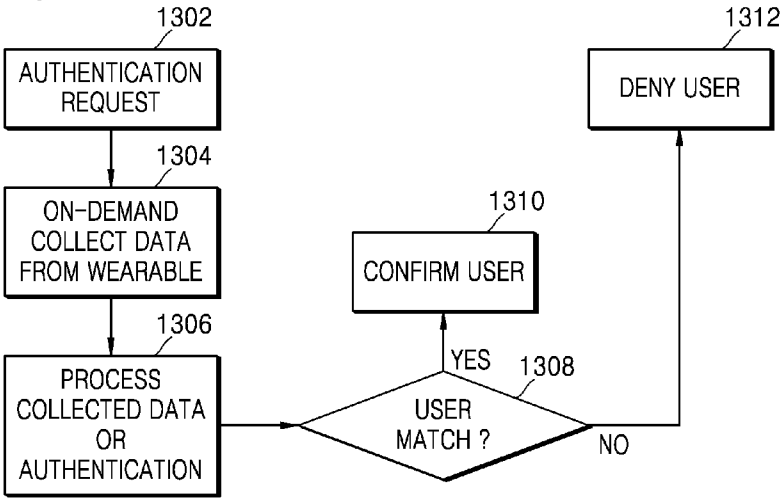
[Fig. 11]


1008
CLIENT DEVICE
ALLOW USER SPECIFIC ACCESS
1006
PROFILE MANAGER
PAIR IDENTITY & PROFILE
1002
USER
1004
WEARABLE DEVICE
BIOMETRICS
USER IDENTITY
1102
ENVIRONMENTAL SENSORS
1104
CLOUD

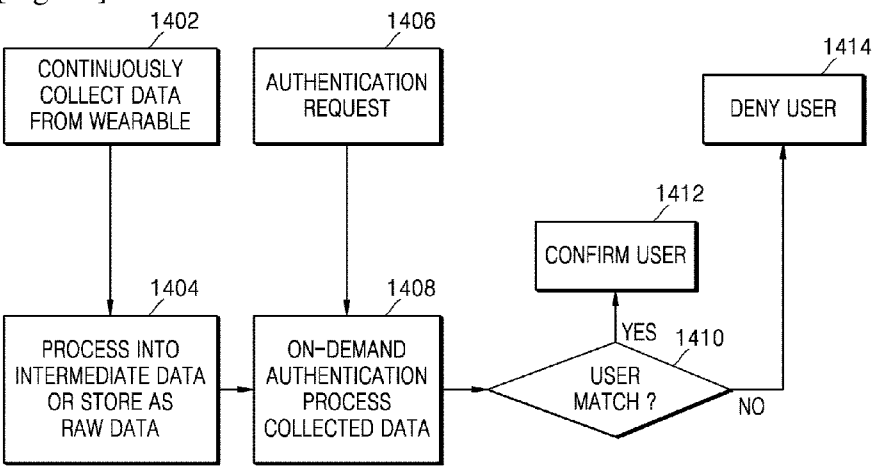
[Fig. 12]



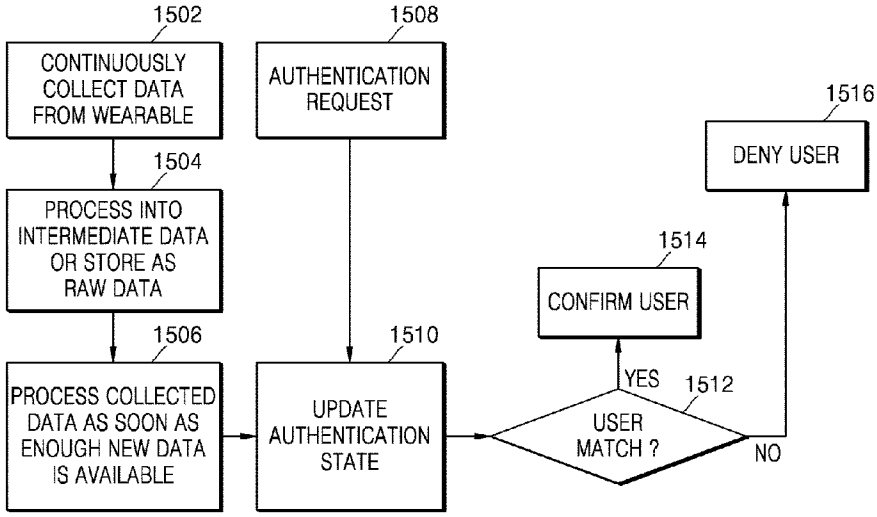

[Fig. 13]



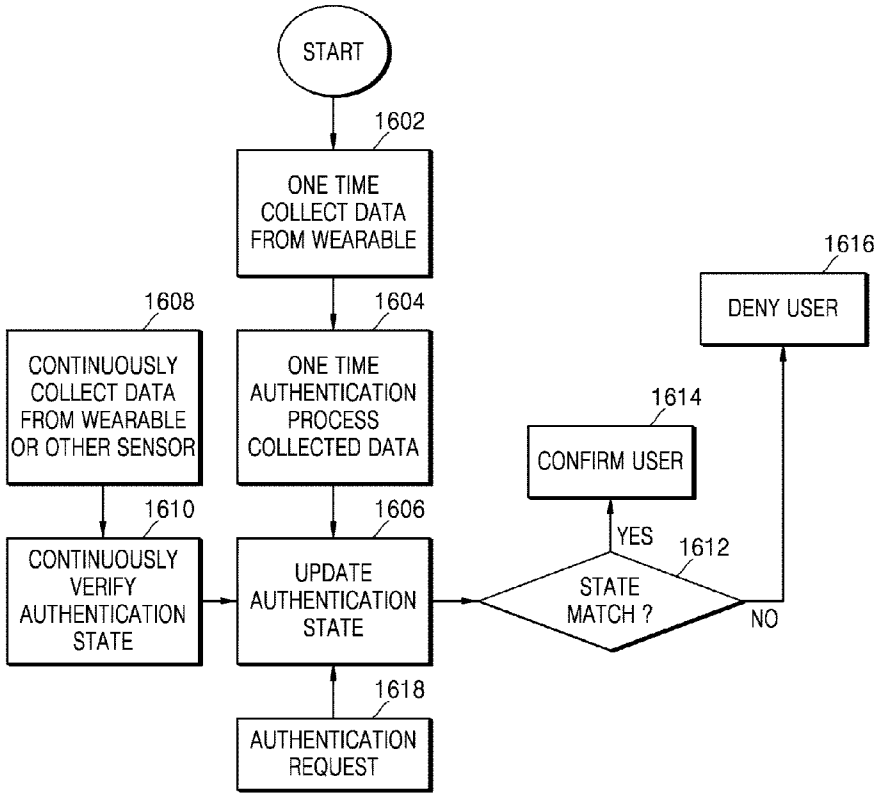

[Fig. 14]



[Fig. 15]


1502
CONTINUOUSLY COLLECT DATA FROM WEARABLE
1504
PROCESS INTO INTERMEDIATE DATA OR STORE AS RAW DATA
1506
PROCESS COLLECTED DATA AS SOON AS ENOUGH NEW DATA IS AVAILABLE
1508
AUTHENTICATION REQUEST
1510
UPDATE AUTHENTICATION STATE
1512
USER MATCH ?
YES
NO
1514
CONFIRM USER
1516
DENY USER

[Fig. 16]


START
1602
ONE TIME COLLECT DATA FROM WEARABLE
1604
ONE TIME AUTHENTICATION PROCESS COLLECTED DATA
1606
UPDATE AUTHENTICATION STATE
1608
CONTINUOUSLY COLLECT DATA FROM WEARABLE OR OTHER SENSOR
1610
CONTINUOUSLY VERIFY AUTHENTICATION STATE
1612
STATE MATCH ?
YES
NO
1614
CONFIRM USER
1616
DENY USER
1618
AUTHENTICATION REQUEST

**INTERNATIONAL SEARCH REPORT**

International application No.
**PCT/KR2015/014269**

**A. CLASSIFICATION OF SUBJECT MATTER**

**G06F 21/32(2013.01)i, G06F 21/31(2013.01)i, H04W 12/06(2009.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)
G06F 21/32; G07C 9/00; G06K 5/00; G06F 17/60; H04L 9/32; G06F 21/00; G06F 21/31; H04W 12/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & keywords: wearable device, pairing, identified user, match, user profile, authorizing, biometrics

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | US 2014-0337634 A1 (GOOGLE INC.) 13 November 2014<br>See paragraphs [0030]-[0044], [0067]-[0106]; claims 1-2, 21; and figures 1A, 3A-3B. | 1-15 |
| Y | US 2003-0046228 A1 (JEAN-MARC BERNEY) 06 March 2003<br>See paragraph [0041]; and figure 7. | 1-15 |
| A | US 2014-0085050 A1 (MICHAEL EDWARD SMITH LUNA) 27 March 2014<br>See paragraphs [0018]-[0037]; and figures 1A-1B. | 1-15 |
| A | US 2013-0268766 A1 (SVEN SCHRECKER) 10 October 2013<br>See paragraphs [0048]-[0050], [0061]-[0066]; and figures 3B, 4. | 1-15 |
| A | US 8371501 B1 (JOHN C. HOPKINS) 12 February 2013<br>See column 9, line 36 - column 12, line 5; and figures 5a-5c. | 1-15 |

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 02 April 2016 (02.04.2016) | **05 April 2016 (05.04.2016)** |


Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
CHIN, Sang Bum
Telephone No. +82-42-481-8398

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No.

**PCT/KR2015/014269**

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2014-0337634 A1 | 13/11/2014 | WO 2014-182360 A1 | 13/11/2014 |
| US 2003-0046228 A1 | 06/03/2003 | CN 100610920 A | 27/04/2005 |
| | | EP 1421543 A1 | 26/05/2004 |
| | | JP 2005-528662 A | 22/09/2005 |
| | | KR 10-2004-0034677 A | 28/04/2004 |
| | | WO 03-021523 A1 | 13/03/2003 |
| US 2014-0085050 A1 | 27/03/2014 | WO 2014-052509 A2 | 03/04/2014 |
| | | WO 2014-052509 A3 | 30/05/2014 |
| US 2013-0268766 A1 | 10/10/2013 | None | |
| US 8371501 B1 | 12/02/2013 | None | |