



(51) International Patent Classification:
G06F 21/31 (2013.01)

(21) International Application Number:
PCT/US2014/038544

(22) International Filing Date:
19 May 2014 (19.05.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/834,635 13 June 2013 (13.06.2013) US
14/048,224 8 October 2013 (08.10.2013) US

(71) Applicant: **MOTOROLA MOBILITY LLC** [US/US];
222 W Merchandise Mart Plaza, Suite 1800, Chicago,
Illinois 60654 (US).

(72) Inventors: **VARADARAJAN, Akila**; 132 Garfield Avenue,
Libertyville, Illinois 60048 (US). **KIMOTO, Yukiko**;
1616 Harrison Avenue, Mundelein, Illinois 60060 (US).
MARCO, Limor, P.; 1136 Brandywyn Court, Buffalo
Grove, Illinois 60089 (US). **GATTUSO, Michelle N.**; 764
West Easton, Palatine, Illinois 60067 (US).

(74) Agents: **WATANABE, Hisashi, David** et al.; 222 W Merchandise
Mart Plaza, Suite 1800, Chicago, Illinois 60654
(US).

(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, LT, 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, 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 ELECTRONIC DEVICE ACCESS

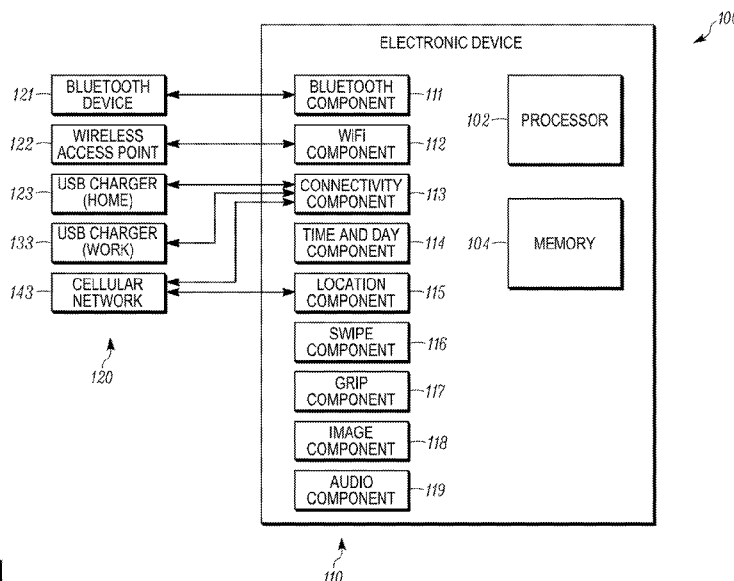


FIG. 1

(57) Abstract: A method on an electronic device (100) for a wireless network is described. Unique IDs, detectable by the electronic device (100), are scanned over a period of time. A unique ID is detected. A plurality of detectable time intervals is determined, within the period of time, for the unique ID. An authentication start time and an authentication end time for the unique ID are determined based on at least three of the plurality of detectable time intervals. Authentication data for the unique ID is stored in a historical database (308). The authentication data includes the authentication start time and the authentication end time. The electronic device (100) is unlocked based on a lookup of authentication data in the historical database (308).

METHOD AND APPARATUS FOR ELECTRONIC DEVICE ACCESS

TECHNICAL FIELD

[0001] The disclosure relates to access security for an electronic device.

BACKGROUND

[0002] Electronic devices, such as smartphones, tablets, and other electronics, are often used to access information that a user wishes to keep secure or private. For example, a home user may have financial information, bank statements, email accounts, or personal files that they access with a tablet. As another example, a business user may access business email or other confidential information with a smartphone. In order to keep this information secured from unauthorized access, the user often sets a security policy on the electronic device to require a PIN entry, biometric reading, or other security procedure. However, many users consider such security procedures to be cumbersome in their setup and use.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] These and/or other embodiments will become apparent and more readily appreciated from the following description of the embodiments, taken in conjunction with the accompanying drawings of which:

[0004] FIG. 1 is a block diagram illustrating an electronic device, according to an embodiment.

[0005] FIG. 2 is a flowchart of a method for authentication that may be performed by the electronic device of FIG. 1, according to an embodiment.

[0006] FIG. 3 is a block diagram illustrating an authentication system that may be implemented by the electronic device of FIG. 1, according to an embodiment.

[0007] FIG. 4 is a flowchart of a method for processing data gathered by the electronic device of FIG. 1 using the authentication system of FIG. 3, according to an embodiment.

[0008] FIG. 5 is a flowchart of a method for storing authentication data that may be performed by the electronic device of FIG. 1, according to an embodiment.

[0009] FIG. 6 is a diagram illustrating a continuous table of the authentication system of FIG. 3, according to an embodiment.

[0010] FIG. 7 is a diagram illustrating a learning table of the authentication system of FIG. 3, according to an embodiment.

[0011] FIG. 8 is a diagram illustrating an authorized table of the authentication system of FIG. 3, according to an embodiment.

[0012] FIG. 9 is a diagram illustrating a match-ready table of the authentication system of FIG. 3, according to an embodiment.

[0013] FIG. 10, a diagram of a table illustrating one example of detectable time intervals for a unique ID, according to an embodiment.

[0014] FIG. 11 is a flowchart of another method for storing authentication data that may be performed by the electronic device of FIG. 1, according to an embodiment.

DETAILED DESCRIPTION

[0015] Current electronic devices have a vast set of data available, related to swipe patterns, location, WiFi networks, Bluetooth devices, facial recognition, voice data, and other data. These data are also often personal to each user and may be collected and analyzed to determine access patterns or profiles for the user. For example, the user may frequently access the electronic device at related times and days during a week. During those times of access, the electronic device may be connected to a Bluetooth headset, a wireless network, a USB charger, or other devices. The user may also have detectable biometric characteristics when accessing the electronic device. For example, the user

may typically use a certain pressure and pattern when “swiping” to access the electronic device. Accordingly, the electronic device may be configured to combine this available data in order to authenticate the user based on which devices are connected, when they are connected, and whether the data fits a previously established history for the user. The electronic device may be configured to bypass a security challenge when the available data suggests that an access attempt is by an authorized user of the electronic device.

[0016] The present disclosure is generally directed to a method and system for providing secure access to an electronic device. In particular, the disclosure is directed to storing authentication data for unique IDs in a historical database and unlocking the electronic device based on a lookup of authentication data in the historical database.

[0017] The present disclosure describes a method on an electronic device for a wireless network. Unique IDs, which are detectable by the electronic device, are scanned over a period of time. A unique ID is detected. A plurality of detectable time intervals is determined, within the period of time, for the unique ID. An authentication start time and an authentication end time for the unique ID are determined based on at least three of the plurality of detectable time intervals. Authentication data for the unique ID is stored in a historical database. The authentication data includes the authentication start time and the authentication end time. The electronic device is unlocked based on a lookup of authentication data in the historical database.

[0018] The present disclosure further describes an electronic device for a wireless network. The electronic device includes a non-transitory memory and a processor configured to retrieve instructions from the memory. The electronic device is configured to scan over a period of time for unique IDs detectable by the electronic device. The electronic device is configured to detect a unique ID. The electronic device is configured to determine, for the unique ID, a plurality of detectable time intervals within the period of time. The electronic device is configured to determine, for the unique ID, an authentication start time and an authentication end time based on at least three of the plurality of detectable time intervals. The electronic device is configured to store authentication data for the unique ID in a historical database. The authentication data

comprises the authentication start time and the authentication end time. The electronic device is configured to unlock the electronic device based on a lookup of authentication data in the historical database.

[0019] Turning to FIG. 1, a block diagram illustrates one example of an electronic device 100 according to an embodiment. Examples of the electronic device 100 include a mobile phone (e.g., smartphone), a tablet computer, a laptop, or other computing device. The electronic device 100 includes a processor 102 and a memory 104, as described herein. The electronic device 100 further includes a plurality of authentication components 110. In the embodiment shown in FIG. 1, the plurality of authentication components 110 includes a Bluetooth component 111, a WiFi component 112, a connectivity component 113, a Time and Day component 114, a location component 115, a swipe component 116, a grip component 117, an image component 118, and an audio component 119. However, alternative embodiments of the electronic device 100 may have additional, or fewer, authentication components 110. While the authentication components 110 are illustrated and described herein as discrete components, they may be combined or divided in alternative embodiments.

[0020] The plurality of authentication components 110 provides various features to the electronic device 100. The authentication components 110 in one example are configured to detect, sense, or receive inputs from external devices (e.g., external devices 120), the user of the electronic device 100, or the environment. In particular, the authentication components 110 may be configured to detect, sense, or receive inputs to identify unique IDs when the user attempts to access or “unlock” the electronic device 100 from a dormant or “locked” state. The electronic device 100 may be configured to unlock the electronic device 100 based on the unique IDs without requiring a security challenge (e.g., PIN entry, swipe pattern, biometric reading) performed by the user. The authentication components 110 may be grouped based on various characteristics, including their relative accuracy, relative importance, or type of data provided (e.g., biometric or non-biometric).

[0021] The Bluetooth component 111 provides a Bluetooth capability to the electronic device 100 and allows connectivity to one or more other Bluetooth-enabled devices, such as a Bluetooth device 121. The Bluetooth device 121 may be a Bluetooth-enabled headset, Bluetooth-enabled automobile, or other Bluetooth-enabled device. The Bluetooth component 111 in one example detects Bluetooth-enabled devices and identifies those devices by a unique ID, such as a Bluetooth hardware address, Bluetooth device name, Bluetooth device class, or any combination thereof. The Bluetooth component 111 may identify unique IDs for Bluetooth-enabled devices that are detected, connected with the Bluetooth component 111, or both. Alternative forms of the unique ID will be apparent to those skilled in the art.

[0022] The WiFi component 112 provides a wireless network capability and allows the electronic device 100 to connect to one or more wireless-enabled communication devices or wireless networks, such as a wireless access point 122. The WiFi component 112 may implement one or more wireless standards, such as one or more of the IEEE 802.11 family of standards. The WiFi component 112 in one example detects wireless-enabled devices and identifies those devices by a unique ID, such as a hardware address (e.g., medium access control (MAC) address), service set identification (SSID), basic service set identification (BSSID), received signal strength indicator (RSSI), internet protocol (IP) address, or any combination thereof. The WiFi component 112 may identify unique IDs for wireless-enabled communication devices or networks that are detected, connected with the WiFi component 112, or both. Alternative forms of the unique ID will be apparent to those skilled in the art.

[0023] The connectivity component 113 provides a communication capability to other electronic devices. The connectivity component 113 may include one or more antennas, wired or wireless interfaces, ports, or other connectivity mechanisms (not shown). The connectivity component 113 may be coupled to another device that provides for additional antennas, interfaces, ports, or connectivity mechanisms, such as a universal serial bus (USB) hub. In the embodiment shown in FIG. 1, the connectivity component 113 is connectable to a first USB charger 123, a second USB charger 133, and a cellular or other wireless network 143. The USB charger 123 may be located at a

home of the user of the electronic device 100 while the USB charger 133 may be located at a work location of the user of the electronic device 100. The cellular network 143 may include a long term evolution (LTE) network, code division multiple access (CDMA) network, Universal Mobile Telecommunications System (UMTS) network, or other wireless network. The connectivity component 113 may be connected to the USB chargers 123 and 133, the cellular network 143, or other devices either separately, concurrently, or in any combination thereof. The connectivity component 113 in one example detects connected devices and identifies those devices by a unique ID. For example, the connectivity component 113 may identify a USB device by a USB hardware address, USB device name, other identifying information, or any combination thereof. The connectivity component 113 may identify a cellular network by a cell ID, service provider name, network address, other identifying information, or any combination thereof. Alternative forms of the unique ID will be apparent to those skilled in the art. Additional examples of other devices for connection to the connectivity component 113 include a High-Definition Multimedia Interface (HDMI) device, radio frequency identification (RFID) device, or infrared (IR) communication device.

[0024] The Time and Day component 114 provides a current time and current day for various actions and events. For example, if the user makes an attempt to unlock the electronic device 100, the Time and Day component 114 may provide the current time and day for that attempt or any unique IDs detected during the unlock attempt.

[0025] The location component 115 provides a location service for the electronic device 100. For example, the location component 115 is configured to determine a current location of the electronic device 100 based on at least one of Global Positioning System (GPS) data, WiFi data (e.g., from the WiFi component 112 and wireless access point 122), Google® location services, cell IDs (e.g., from the connectivity component 113 and cellular network 143), or any combination thereof. The location component 115 in one example determines a unique ID based on the location of the electronic device 100 such that the unique ID indicates the location (e.g., a street address, latitude/longitude coordinates, etc.).

[0026] The swipe component 116 provides a swipe feature for the electronic device 100 and allows the user to interact with a touch screen (not shown) of the electronic device 100. For example, the swipe component 116 may sense a user's input in the form of a touch signal. The swipe component 116 in one example analyzes the sensed touch signal to determine one or more characteristics of the user's input (e.g., duration, pressure, X and Y coordinates, or size). The swipe component 116 in one example determines a unique ID for the user's input based on the characteristics. The unique ID for the swipe component 116 may be implemented as a data structure, user profile, or other format.

[0027] The grip component 117 provides a grip analysis feature for the electronic device 100. The grip component 117 in one example includes one or more sensors (not shown) that sense a user's input in the form of the manner in which the user grips the electronic device 100. Examples of the sensors include gyroscopes, accelerometers, motion sensors, or position sensors. The grip component 117 in one example analyzes the orientation of the electronic device 100 to determine one or more characteristics of the user's grip. The grip component 117 in one example determines a unique ID for the user's grip based on the characteristics. The unique ID for the grip component 117 may be implemented as a data structure, user profile, or other format.

[0028] The image component 118 provides an image-taking feature to the electronic device 100. For example, the image component 118 may include a camera (e.g., charged coupled device (CCD) or complementary metal-oxide-semiconductor (CMOS) device) for capturing still or moving images. The image component 118 may be configured for facial detection of the user. For example, the image component 118 may use facial detection algorithms to identify the user based on full or partially recognized facial features (e.g., eye position, nose position, etc.). The image component 118 in one example determines a unique ID based on the identified facial features. The unique ID for the image component 117 may be implemented as a data structure, user profile, or other format.

[0029] The audio component 119 provides an audio recording feature to the electronic device 100. For example, the audio component 119 may include a microphone or other audio capture device. The audio component 119 may be configured for voice recognition of the user, speech recognition of the user, or other sounds associated with the environment (e.g., background noise). For example, the audio component 119 may use voice recognition algorithms to recognize a keyword spoken by the user and captured as audio by the audio component 119. The audio component 119 determines a unique ID based on the captured audio. The unique ID for the audio component 117 may be implemented as a data structure, user profile, or other format.

[0030] Turning to FIG. 2, a flowchart 200 illustrates one example of a method for authentication that may be performed by the electronic device 100. The electronic device 100 waits (NO at 202) for an unlock attempt by a user. Upon the unlock attempt (YES at 202), the electronic device 100 detects (204) unique IDs from the authentication components 110. The number of unique IDs detected by each authentication component 110 may be a fixed number or variable number. For example, the WiFi component 112 may detect several SSIDs and return each as a separate unique ID during a single instance of the detection step. In contrast, other components (e.g., the swipe component 116, grip component 117, image component 118, or audio component 119) may be configured to provide only a single unique ID for each instance of the detection step.

[0031] The user of the electronic device 100 may attempt to unlock the electronic device 100 many times throughout a day, week, or other period of time. Accordingly, the electronic device 100 may scan over a period of time (e.g., several days, several weeks, or longer) for the unique IDs. The electronic device 100 in an embodiment detects the unique IDs upon the unlock attempt, instead of continuously, which may reduce power consumption and thus increase battery life of the electronic device 100.

[0032] After detection of the unique IDs, the electronic device 100 determines (206) whether the detected unique IDs provide a sufficient match for authentication of the user. The electronic device 100 thus determines whether the unlock attempt is successful or unsuccessful based on the detected unique IDs. The sufficiency of the match may be

based on the number of unique IDs detected, the history related to those unique IDs (including insufficient history for comparison), which authentication component 110 detected the unique ID, or other factors. If the match is insufficient (NO at 206), the electronic device 100 performs a security challenge (208) to authenticate the user. Upon a failure of the security challenge (NO at 208), the electronic device 100 may end (210) the unlock attempt and discard the detected unique IDs. Alternatively, the electronic device 100 may allow multiple security challenges.

[0033] Upon a successful unlock through a sufficient match (YES at 206) or successful security challenge (YES at 208), the electronic device 100 stores (212) the detected unique IDs and unlocks (214) for the user. Because either the unique ID match or the security challenge was successful, the user has been authenticated, and the electronic device 100 stores the detected unique IDs (e.g., as a history) for future authentication matches.

[0034] The electronic device 100 in an embodiment “learns” the unique IDs from the authentication components 110 which correspond to the authorized user. The electronic device 100 stores those corresponding unique IDs for future authentication matching, as opposed to having the user of the electronic device 100 manually enter various unique IDs for matching. In alternative embodiments, the electronic device 100 may be configured to use a combination of learning and manual entry of the unique IDs.

[0035] The electronic device 100 in one example processes the unique IDs to form authentication data. In one example, the processing includes a determination of start times and end times for the unique IDs. In another example, biometric-based or profile-based unique IDs (e.g., those from the swipe component 116, the grip component 117, the image component 118, or audio component 119) may be processed to determine a “match-ready” unique ID or profile for matching purposes. Examples of such processing include neural network processing, heuristics, statistical analysis, or other forms of processing, which will be apparent to those skilled in the art. The electronic device 100 may be configured to perform the processing on the unique IDs when a sufficient number of unique IDs have been detected over time. For example, the electronic device 100 may

wait for at least twenty days of data before processing the unique IDs. The type of processing, sufficient number of unique IDs, or duration of time may be preselected or dynamically determined based on the unique IDs. Additionally, the type of processing, sufficient number of unique IDs, and duration of time may be the same or different for each authentication component 110.

[0036] Turning to FIG. 3, an authentication system 300 that may be implemented by the electronic device of FIG.1, according to an embodiment. The authentication system 300 includes the authentication components 110, a security policy 302 for the electronic device 100, a match component 304, a learning component 306, and a database 308. The security policy 302 in this embodiment is applied to the electronic device 100 for control of the authentication components 110 and match component 304. The security policy 302 may be implemented as a portion or module of an operating system (not shown) of the electronic device 100. The authentication components 110 are configured to provide the detected unique IDs to the database 308 based on the security policy 302. The match component 304 performs the step of matching (206) based on authentication data within the database 308. The match component 304 may be configured to perform a lookup of authentication data and a current set of detected unique IDs in the database 308. In another example, the match component 304 may be configured to receive the current set of detected unique IDs, directly or indirectly, from the authentication components 110. In this example, the match component 304 is configured to perform the lookup of the authentication data within the database 308 to perform the step of matching.

[0037] The learning component 306 performs processing on the database 308 to generate the authentication data based on the unique IDs. As described above, the learning component 306 may perform neural network processing, heuristics, statistical analysis, or other forms of processing.

[0038] The database 308 comprises a historical database for unique IDs. In the embodiment of FIG. 3, the database 308 comprises one instance of a continuous table 310, a learning table 320, an authorized table 330, and a match-ready table 340 for each of the authentication components 110. Accordingly, there are nine instances of each

table 310, 320, 330, and 340 for a total of 36 tables. However, alternative embodiments may use a single instance of each table 310, 320, 330, and 340 for all of the authentication components 110 (thus, a total of four tables). Various tables may be combined or omitted and other embodiments will be apparent to those skilled in the art. For clarity, one instance of the tables 310, 320, 330, and 340 will be discussed herein.

[0039] The continuous table 310 stores detected unique IDs and associated data, for example, as a status indicator or table entry for the unique ID. The associated data in one example includes a date that a unique ID was detected, a start time for an appearance of the unique ID, and an end time for the appearance of the unique ID. Additional data or parameters that may be stored with the unique ID will be apparent to those skilled in the art. The electronic device 100 in one example creates an entry in the continuous table 310 corresponding to the authentication component 110 from which a unique ID is initially detected upon an unlock attempt. Upon a subsequent unlock attempt, the electronic device 100 may determine whether the unique ID is still detected. If detected, the electronic device 100 may update the end time for the corresponding entry. If the unique ID is not detected (e.g., disconnected from the electronic device 100), the electronic device 100 may remove the unique ID's entry from the continuous table 310 and create a new, corresponding entry in the learning table 320.

[0040] The learning table 320 stores unique IDs and associated data. The associated data in one example includes the date, the start time, the end time, and a number of sequential transactions (e.g., unlock attempts) in which the unique ID was detected. Additional parameters or associated data that may be stored, or omitted, will be apparent to those skilled in the art. The learning component 306 in one example processes entries from the learning table 320 to determine and create entries for the authorized table 330, as described herein.

[0041] The authorized table 330 stores authentication data for the unique IDs and associated data that may be used to authenticate the user. The authentication data in one example includes the unique ID and at least one of an authorized start time, an authorized end time, an average number of transactions, authorized days, a last authentication date,

an access frequency, or a number of transactions. Additional parameters or associated data that may be stored, or omitted, will be apparent to those skilled in the art.

[0042] The match-ready table 340 stores match indications of which unique IDs are ready for use by the match component 304. The match indications in one example include the unique ID and an accuracy of the corresponding authentication component 110. The match indications in a further example include a type for the unique ID (e.g., biometric, non-biometric, high priority, low priority, etc.). Additional parameters or associated data that may be stored, or omitted, will be apparent to those skilled in the art.

[0043] Turning to FIG. 4, a flowchart 400 illustrates an embodiment of a method for processing data gathered by the electronic device 100 of FIG. 1 using the authentication system 300. The learning component 306 waits for a trigger from the electronic device 100. The trigger may be a fixed timer (e.g., every 20 days), a dynamic timer (e.g., 20 days for a first trigger, and 5 days for subsequent triggers), or an occurrence of an event. Examples of events include the occurrence of a number of unlock attempts (e.g., one hundred unlock attempts) or upon one or more tables in the database 308 reaching a preselected size. Other examples of triggers will be apparent to those skilled in the art.

[0044] Upon the trigger (YES at 410), the learning component 306 processes (420) the learning table 320 to determine the authentication data. The learning component 306 in one example determines the authentication data based on at least three entries from the learning table 320. The learning component 306 adds (430) the authentication data to the authorized table 330. The learning component 306 adds (440) match indications to the match-ready table. The learning component 306 may add a match indication for unique IDs with sufficient user history for matching. The learning component 306 may add a match indication after a predetermined quantity of authentication data (e.g., a number of transactions, a number of entries, etc.) is stored in the authorized table. The learning component 306 may discard (450) data from the learning table 320 that are not sufficient for creation of authentication data. For example, detectable time intervals that do not match with other detectable time intervals to form a cluster may be discarded after a discard threshold has been reached. Additionally, the learning component 306 may

discard data from the authorized table 330 or the match-ready table 340 where that data has not been used to authenticate the user, based on the last authorization date.

[0045] Turning to FIGS. 5-9, a flowchart 500 illustrates an embodiment of a method for storing authentication data that may be performed by the electronic device 100 of FIG. 1, according to an embodiment. FIGS. 6, 7, and 8 are diagrams illustrating embodiments of a continuous table 610, a learning table 720, and an authorized table 830, respectively, for the Bluetooth component 111. FIG. 9 is a diagram of a match-ready table 940. The electronic device 100 in one embodiment performs the method of flowchart 500 for unique IDs from non-biometric authentication components 110 (e.g., the Bluetooth component 111, WiFi component 112, connectivity component 113, and location component 115).

[0046] Referring to the embodiment of FIG. 6, the Bluetooth component 111 detects a Bluetooth-enabled headset with a unique ID “Headset1” (“Headset1 device”) over a period of time including times T1, T2, T3, ... T11, to T12. Each time T1 to T12 represents a consecutive successful unlock attempt by a user when the Headset1 device was detected. At T1, the Headset1 device is initially detected and the electronic device 100 creates a corresponding entry in the continuous table 610 with the date and time. The electronic device 100 updates the end time for the entry at subsequent unlock attempts (T2, T3, and T4). After an inactivity time for the Headset1 device, or upon an unlock attempt when the Headset1 device is not detected, the electronic device 100 determines (502) a detectable time interval for the Headset1 device as a start time and end time when the Headset1 device was detected (e.g., 1:00 pm to 1:10 pm). In one example, the authentication components 110 determine a plurality of detectable time intervals. In another example, the learning component 306 determines the plurality of detectable time intervals. The electronic device 100 removes the entry from the continuous table 610 and creates a corresponding entry LT1 in the learning table 720. The number of transactions in the entry LT1 corresponds to the number of successful unlock attempts (e.g., the four attempts at 1:00 pm, 1:04 pm, 1:06 pm, and 1:10 pm). Analogous entries in the continuous table 610 at T5, T6, and T7 correspond to an entry LT2 of the learning table 720. Analogous entries in the continuous table 610 at T8, T9,

and T10 correspond to an entry LT3 of the learning table 720. Analogous entries in the continuous table 610 at T11 and T12 correspond to an entry LT4 of the learning table 720.

[0047] The electronic device 100 normalizes (504) the start and end times for the entries in the learning table 720 to create a normalized set of detectable time intervals. The electronic device 100 may normalize the start and end times prior to entry into the learning table 720 (e.g., by the authentication components 110) or after entry (e.g., by the learning component 306). In one example, the electronic device 100 normalizes the start and end times to be at single minute intervals. For example, times of 1:00:20 pm, 1:00:44 pm, and 1:00:03 pm may be normalized to 1:00:00 pm. In another example, the electronic device 100 normalizes the start and end times to be at two minute, five minute, or other intervals. The normalization for the start and end times may use a same or different interval. For example, the start times may be normalized to 15 minute intervals while the end times are normalized to 30 minute intervals. The intervals may be preselected or determined based on the detectable time intervals. For example, a larger number of detectable time intervals may be normalized with a larger interval to provide closer matching of the start and end times.

[0048] The learning component 306 clusters (506) the detectable time intervals for the unique IDs. In one embodiment, the learning component 306 clusters the detectable time intervals with respective start times and end times that are within a preselected threshold (e.g., 30 minutes, 1 hour, 3 hours, etc.). For example, the learning component 306 selects a normalized set of time intervals with adjacent normalized start times and with adjacent normalized end times. Referring to FIG. 7, the learning component 306 clusters the LT1, LT3, LT5, and LT7 entries into a first cluster and clusters the LT2, LT4, LT6, and LT8 entries into a second cluster. In alternative embodiments, the electronic device 100 may cluster the entries before normalizing the start and end times. The learning component 306 determines (508) authentication data, including an authentication start time, based on the start times of the cluster, and an authentication end time, based on the end times of the cluster. In the embodiment of FIG. 7, the learning component 306 selects an earliest start time for each cluster (12:58 pm and 5:18 pm) as the authentication

start times and the latest start time for each cluster (1:10 pm and 5:28 pm) as the authentication end times. An alternative embodiment is described with reference to FIG. 10.

[0049] After determining the authentication start times and authentication end times, the learning component 306 determines (510) whether prior authentication data (e.g., a prior instance of authentication data for the unique ID) exists within the database 308 (e.g., within the authorized table 330 or match-ready table 340). If prior authentication data is not found (NO at 510), the learning component 306 stores (512) the authentication data in the database 308. For example, the learning component 306 stores the current authentication data as a new entry within the authorized table 330. Referring to FIG. 8, the learning component 306 creates an entry AT1 in the authorized table 830 for the LT1, LT3, LT5, and LT7 entries and creates an entry AT2 in the authorized table 830 for the LT2, LT4, LT6, and LT8 entries. The learning component 306 determines an average number of transactions for the entry AT1 by averaging the number of transactions for each entry LT1, LT3, LT5, and LT7 (i.e., 4, 3, 3, and 4, respectively). The learning component 306 determines the authorized days for the entry AT1 based on the corresponding dates for the start times and end times. As shown in FIG. 7, the learning component 306 determines the authorized days to be Mondays and Tuesdays based on the dates 5/27/2013, 5/28/2013, 6/3/2013, and 6/4/2013. The learning component 306 determines a number of transactions for the entry AT1 by the number of entries used (i.e., the four entries: LT1, LT3, LT5, and LT7). The learning component 306 creates the entry AT2 analogously to the entry AT1 (i.e., based on the LT2, LT4, LT6, and LT8 entries).

[0050] The electronic device 100 in one embodiment updates the authentication data (e.g., the last authorization day, the number of transactions, the access frequency) upon a successful unlock attempt using the authentication data. For example, if the Headset1 device is used to authenticate the user at 5:20 pm on 6/10/2013, the electronic device 100 updates the last authentication date to 6/10/2013 and increments the number of transactions to 5 transactions. The electronic device 100 may update authentication data in the authorized table 330, the match-ready table 340, or both.

[0051] If the learning component 306 determines (YES at 510) that prior authentication data exists for a same unique ID, the learning component 306 updates (514) the authentication data in the authorized table 330. The learning component 306 determines (516) whether the current authentication data takes priority over prior authentication data. The learning component 306 in one embodiment determines the priority based on at least one of the last authentication date, the number of transactions, or the access frequency for the current authentication data and the prior authentication data. For example, if the prior authentication data has not been used within a predetermined threshold (e.g., several months), or has not been used as many times as the current authentication data, the learning component 306 may determine that the current authentication data takes priority. Other thresholds or factors for determining priority of the authentication data will be apparent to those skilled in the art.

[0052] If the current authentication data does not take priority, the learning component 306 proceeds to step 512. If the current authentication data takes priority, the learning component 306 combines (518) or normalizes the prior authentication data with the current authentication data. For example, the learning component 306 may normalize an authenticated start time of 5:18 pm for current authentication data to a one hour interval (e.g., 5:00 pm) in order to provide an overlap with prior authentication data with an authenticated start time of 5:28 pm. The learning component 306 may combine the current and prior authentication data to gradually move the authentication start and end times towards a new schedule of the user.

[0053] The learning component 306 in one embodiment discards authentication data as part of the updating step (512). The learning component 306 may discard authentication data based on a lack of use, overlap with other authentication data, or other factors which will be apparent to those skilled in the art. For example, if authentication data exists in the database 308 but has not been used to authenticate the user within a discard threshold (e.g., six months), the learning component 306 may delete that authentication data from the database 308. The discard threshold may be fixed or dynamically determined (e.g., based on available authentication data in the database 308).

[0054] Turning to FIG. 10, a table 1000 illustrates one example of detectable time intervals for a unique ID, according to an embodiment. In this alternative embodiment, the learning component 306 performs additional processing on clusters of detectable time intervals to select the authentication start times and authentication end times. As shown in FIG. 10, the learning component 306 normalizes the start times and end times to one minute intervals and sorts the start times and end times.

[0055] After the normalization and sorting, the learning component 306 selects the authentication start time such that a number of subsequent start times, within a first time threshold of the authentication start time, is maximized. For example, where the first time threshold is thirty minutes, the number of subsequent start times to the first entry of 9:00 AM is two (i.e., 9:10 AM and 9:30 AM). However, the number of subsequent start times to the entry of 9:45 AM is four (i.e., 10:10 AM, 10:11 AM, 10:12 AM, 10:15 AM). Accordingly, the learning component 306 selects the entry of 9:45 AM as the authentication start time. In case of multiple entries with a same number of subsequent start times, the learning component 306 may select an earliest entry. In a case when the maximum number of subsequent start times does not meet a selection threshold, the learning component 306 may exit the processing without storing authentication data. The selection threshold may be based on the number of entries in the table 1000, for example, 25% of the number of entries. Alternatively, the selection threshold may be based on a minimum threshold, for example, at least three entries. The electronic device 100 may avoid storing authentication data with a low likelihood of successful authentication of the user.

[0056] After the normalization and sorting, the learning component 306 also selects the authentication end time such that a number of previous end times, within a second time threshold of the authentication end time, is maximized. The first time threshold and the second time threshold may be the same or different. In the example of FIG. 10, a second time threshold of thirty minutes provides the last entry of 5:40 PM with three previous end times (i.e., 5:10 PM, 5:20 PM, and 5:30 PM). The learning component 306 may select the entry of 5:10 PM as the authentication end time to provide a maximum number of previous end times (i.e., 4:40 PM, 4:45 PM, 4:49 PM, and 5:00 PM). In a case

when the maximum number of previous end times does not meet a threshold, the learning component 306 may exit the processing without storing authentication data.

[0057] FIG. 11 is a flowchart 1100 of another method for storing unique IDs that may be performed by the electronic device of FIG. 1. The method of FIG. 11 in one example is performed by the learning component 306 for unique IDs from biometric-based or profile-based unique IDs (e.g., those from the swipe component 116, the grip component 117, the image component 118, or audio component 119) to perform the step of storing (212, FIG. 2). Biometric-based authentication components 110 may not be capable of 100% accuracy, as will be understood by those skilled in the art. Accordingly, the learning component 306 may store the accuracy of the corresponding authentication component 110 with the authentication data.

[0058] The learning component 306 receives and stores (1102) the unique ID in the learning table 320. The learning component 306 determines (1104) whether sufficient data exists to determine authentication data based on the unique IDs for the corresponding authentication component 110. Processing of the unique IDs for biometric-based or profile-based authentication components 110 may require many unique IDs for processing such as neural network processing. The learning component 306 may wait for a threshold number of unique IDs before processing. The threshold number of unique IDs may be the same or different for each authentication component 110. The learning component 306 may adjust the threshold number over time. For example, to provide a high initial number of unique IDs (e.g., 500 unique IDs) for a first processing and a lower subsequent number of unique IDs (e.g., 100 unique IDs) for subsequent processing.

[0059] If sufficient data exists for processing, the learning component 306 processes (1106) the unique IDs using neural network processing, heuristics, statistical analysis, or other forms of processing to generate authentication data based on the unique IDs (e.g., a profile of the user). In one example, the learning component 306 performs neural network processing on unique IDs from the swipe component 116 to determine a swipe profile for authentication data. The match component 304 may use the authentication

data, as described above. In an embodiment, the learning component 306 processes both unique IDs and previous authentication data to create new authentication data. The learning component 306 stores (1108) the authentication data in the database 308. If sufficient data does not exist for processing, the method ends (1110).

[0060] It can be seen from the foregoing that a method and system for providing secure access to an electronic device have been provided. In view of the many possible embodiments to which the principles of the present discussion may be applied, it should be recognized that the embodiments described herein with respect to the drawing figures are meant to be illustrative only and should not be taken as limiting the scope of the claims. Therefore, the techniques as described herein contemplate all such embodiments as may come within the scope of the following claims and equivalents thereof.

[0061] The apparatus described herein may include a processor, a memory for storing program data to be executed by the processor, a permanent storage such as a disk drive, a communications port for handling communications with external devices, and user interface devices, including a display, touch panel, keys, buttons, etc. When software modules are involved, these software modules may be stored as program instructions or computer readable code executable by the processor on a non-transitory computer-readable media such as magnetic storage media (e.g., magnetic tapes, hard disks, floppy disks), optical recording media (e.g., CD-ROMs, Digital Versatile Discs (DVDs), etc.), and solid state memory (e.g., random-access memory (RAM), read-only memory (ROM), static random-access memory (SRAM), electrically erasable programmable read-only memory (EEPROM), flash memory, thumb drives, etc.). The computer readable recording media may also be distributed over network coupled computer systems so that the computer readable code is stored and executed in a distributed fashion. This computer readable recording media may be read by the computer, stored in the memory, and executed by the processor.

[0062] The disclosed embodiments may be described in terms of functional block components and various processing steps. Such functional blocks may be realized by any number of hardware and/or software components configured to perform the specified

functions. For example, the disclosed embodiments may employ various integrated circuit components, e.g., memory elements, processing elements, logic elements, look-up tables, and the like, which may carry out a variety of functions under the control of one or more microprocessors or other control devices. Similarly, where the elements of the disclosed embodiments are implemented using software programming or software elements, the disclosed embodiments may be implemented with any programming or scripting language such as C, C++, JAVA®, assembler, or the like, with the various algorithms being implemented with any combination of data structures, objects, processes, routines or other programming elements. Functional aspects may be implemented in algorithms that execute on one or more processors. Furthermore, the disclosed embodiments may employ any number of conventional techniques for electronics configuration, signal processing and/or control, data processing and the like. Finally, the steps of all methods described herein may be performed in any suitable order unless otherwise indicated herein or otherwise clearly contradicted by context.

[0063] For the sake of brevity, conventional electronics, control systems, software development and other functional aspects of the systems (and components of the individual operating components of the systems) may not be described in detail. Furthermore, the connecting lines, or connectors shown in the various figures presented are intended to represent exemplary functional relationships and/or physical or logical couplings between the various elements. It should be noted that many alternative or additional functional relationships, physical connections or logical connections may be present in a practical device. The words “mechanism”, “element”, “unit”, “structure”, “means”, “device”, “controller”, and “construction” are used broadly and are not limited to mechanical or physical embodiments, but may include software routines in conjunction with processors, etc.

[0064] No item or component is essential to the practice of the disclosed embodiments unless the element is specifically described as “essential” or “critical”. It will also be recognized that the terms “comprises,” “comprising,” “includes,” “including,” “has,” and “having,” as used herein, are specifically intended to be read as open-ended terms of art. The use of the terms “a” and “an” and “the” and similar

referents in the context of describing the disclosed embodiments (especially in the context of the following claims) are to be construed to cover both the singular and the plural, unless the context clearly indicates otherwise. In addition, it should be understood that although the terms “first,” “second,” etc. may be used herein to describe various elements, these elements should not be limited by these terms, which are only used to distinguish one element from another. Furthermore, recitation of ranges of values herein are merely intended to serve as a shorthand method of referring individually to each separate value falling within the range, unless otherwise indicated herein, and each separate value is incorporated into the specification as if it were individually recited herein.

[0065] The use of any and all examples, or exemplary language (e.g., “such as”) provided herein, is intended merely to better illuminate the disclosed embodiments and does not pose a limitation on the scope of the disclosed embodiments unless otherwise claimed. Numerous modifications and adaptations will be readily apparent to those of ordinary skill in this art.

CLAIMS

1. A method, on an electronic device for a wireless network, the method comprising:
scanning over a period of time for unique IDs detectable by the electronic device;
detecting a unique ID;
determining, for the unique ID, a plurality of detectable time intervals within the period of time;
determining, for the unique ID, an authentication start time and an authentication end time based on at least three of the plurality of detectable time intervals;
storing authentication data for the unique ID in a historical database, wherein the authentication data comprises the authentication start time and the authentication end time;
unlocking the electronic device based on a lookup of authentication data in the historical database.
2. The method of claim 1, wherein scanning over the period of time comprises:
scanning for unique IDs upon an unlock attempt initiated by a user of the electronic device.
3. The method of claim 2, wherein detecting the unique ID comprises:
upon a successful unlock attempt, storing a status indicator for the unique ID that indicates a detection start time and a detection end time for the unique ID.

4. The method of claim 3, wherein storing the status indicator comprises:
- upon a successful unlock attempt and upon an initial detection of the unique ID, creating and storing the status indicator for the unique ID;
 - upon a successful unlock attempt and upon a subsequent detection of the unique ID, updating the detection end time of the status indicator for the unique ID;
 - if the unique ID is not detected upon a successful unlock attempt, storing a detectable time interval for the unique ID with the detection start time and the detection end time;
 - removing the status indicator after storing the detectable time interval.
5. The method of claim 1, wherein the plurality of detectable time intervals comprises respective detection start times and respective detection end times, wherein determining the authentication start time and the authentication end time comprises:
- normalizing the respective detection start times and the respective detection end times for the plurality of detectable time intervals;
 - selecting a normalized set of detectable time intervals from the plurality of detectable time intervals with adjacent normalized start times and with adjacent normalized end times;
 - selecting the authentication start time based on the adjacent normalized start times;
 - selecting the authentication end time based on the adjacent normalized end times.

6. The method of claim 5, wherein selecting the authentication start time comprises:
selecting the authentication start time, from the start times of the normalized set of detectable time intervals, such that a number of subsequent start times that are within a first time threshold of the authentication start time is maximized;
wherein selecting the authentication end time comprises:
selecting the authentication end time, from the end times of the normalized set of detectable time intervals, such that a number of previous end times, within a second time threshold of the authentication end time, is maximized.
7. The method of claim 1, wherein storing the authentication data comprises:
storing an instance of authentication data for the unique ID in the historical database, the authentication data comprising the authentication start time, the authentication end time, a set of authorized days, a last authorization date, an access frequency, and an average number of transactions per day.

8. The method of claim 7, wherein storing the instance of the authentication data for the unique ID comprises:

before storing a current instance of the authentication data, determining whether a prior instance of authentication data for the unique ID exists in the historical database;

if the prior instance of authentication data for the unique ID exists, normalizing the authentication start time, the authentication end time, and the authentication days for the current instance based on the authentication start time, the authentication end time, and the authentication days for the prior instance;

storing, in the historical database, the current instance of the authentication data with the normalized authentication start time, the normalized authentication end time, the normalized set of authorized days, the last authorization date, the access frequency, and an average number of transactions per day.

9. The method of claim 7, wherein storing the instance of the authentication data comprises:

combining a first instance of authentication data for the unique ID with a second instance of authentication data for the unique ID when an access frequency for the first instance meets a preselected threshold;

storing the combined instance of the authentication data for the unique ID in the historical database.

10. The method of claim 7, further comprising:

discarding an instance of the authentication data for the unique ID from the historical database when the last authorization date of the instance is older than a discard threshold.

11. The method of claim 1, wherein detecting the unique ID comprises:
detecting at least one of a hardware address, a cell id, or a network address for a wireless network.
12. The method of claim 1, wherein detecting the unique ID comprises:
determining a location of the electronic device;
determining the unique ID based on the location of the electronic device, wherein the unique ID indicates the location.
13. The method of claim 1, wherein detecting the unique ID comprises:
detecting a unique ID of a Bluetooth device, Universal Serial Bus device, High-Definition Multimedia Interface device, radio frequency identification device, or infrared communication device.

14. An electronic device for a wireless network, the electronic device comprising:
- a non-transitory memory; and
 - a processor configured to retrieve instructions from the memory;
- wherein:
- the electronic device is configured to scan over a period of time for unique IDs detectable by the electronic device;
 - the electronic device is configured to detect a unique ID;
 - the electronic device is configured to determine, for the unique ID, a plurality of detectable time intervals within the period of time;
 - the electronic device is configured to determine, for the unique ID, an authentication start time and an authentication end time based on at least three of the plurality of detectable time intervals;
 - the electronic device is configured to store authentication data for the unique ID in a historical database, wherein the authentication data comprises the authentication start time and the authentication end time;
 - the electronic device is configured to unlock the electronic device based on a lookup of authentication data in the historical database.
15. The electronic device of claim 14, wherein:
- the electronic device is configured to scan for unique IDs upon an unlock attempt initiated by a user of the electronic device.

16. The electronic device of claim 14, wherein:

the plurality of detectable time intervals comprises respective detection start times and respective detection end times;

the electronic device is configured to normalize the respective detection start times and the respective detection end times for the plurality of detectable time intervals;

the electronic device is configured to select a normalized set of detectable time intervals from the plurality of detectable time intervals with adjacent normalized start times and with adjacent normalized end times;

the electronic device is configured to select the authentication start time based on the adjacent normalized start times;

the electronic device is configured to select the authentication end time based on the adjacent normalized end times.

17. The electronic device of claim 14, wherein:

the electronic device is configured to store an instance of authentication data for the unique ID in the historical database;

the authentication data comprises the authentication start time, the authentication end time, a set of authorized days, a last authorization date, and an access frequency.

18. The electronic device of claim 17, wherein:

the electronic device is configured to determine whether a prior instance of authentication data for the unique ID exists in the historical database before storage of a current instance of the authentication data;

the electronic device is configured to normalize the authentication start time, the authentication end time, and the authentication days for the current instance based on the authentication start time, the authentication end time, and the authentication days for the prior instance if the prior instance of authentication data for the unique ID exists;

the electronic device is configured to store, in the historical database, the current instance of the authentication data with the normalized authentication start time, the normalized authentication end time, the normalized set of authorized days, the last authorization date, and the access frequency.

19. The electronic device of claim 17, wherein:

the electronic device is configured to combine a first instance of authentication data for the unique ID with a second instance of authentication data for the unique ID when an access frequency for the first instance meets a preselected threshold;

the electronic device is configured to store the combined instance of the authentication data for the unique ID in the historical database.

20. The electronic device of claim 17, wherein:

the electronic device is configured to discard an instance of the authentication data for the unique ID from the historical database when the last authorization date of the instance is older than a discard threshold.

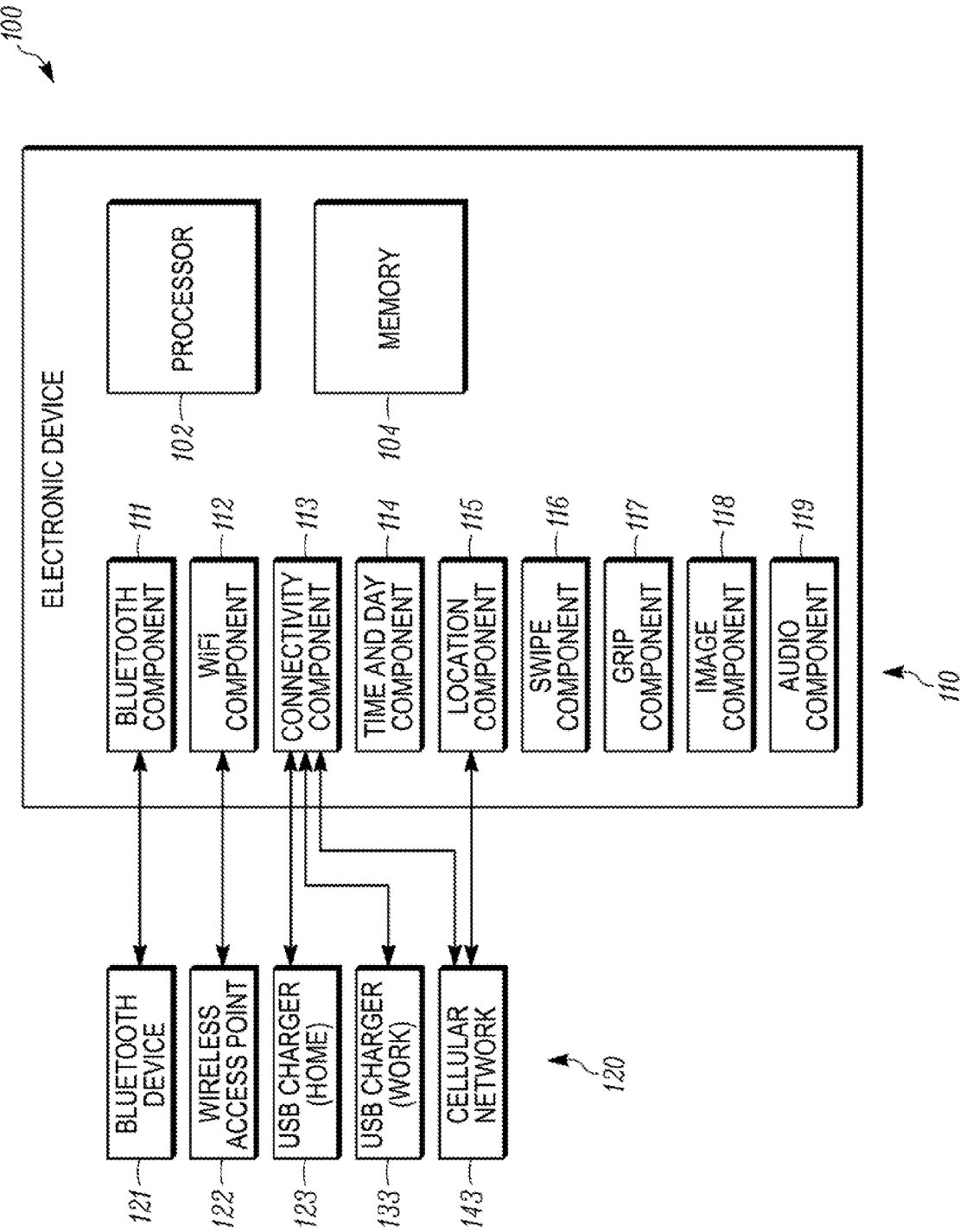


FIG. 1

2/8

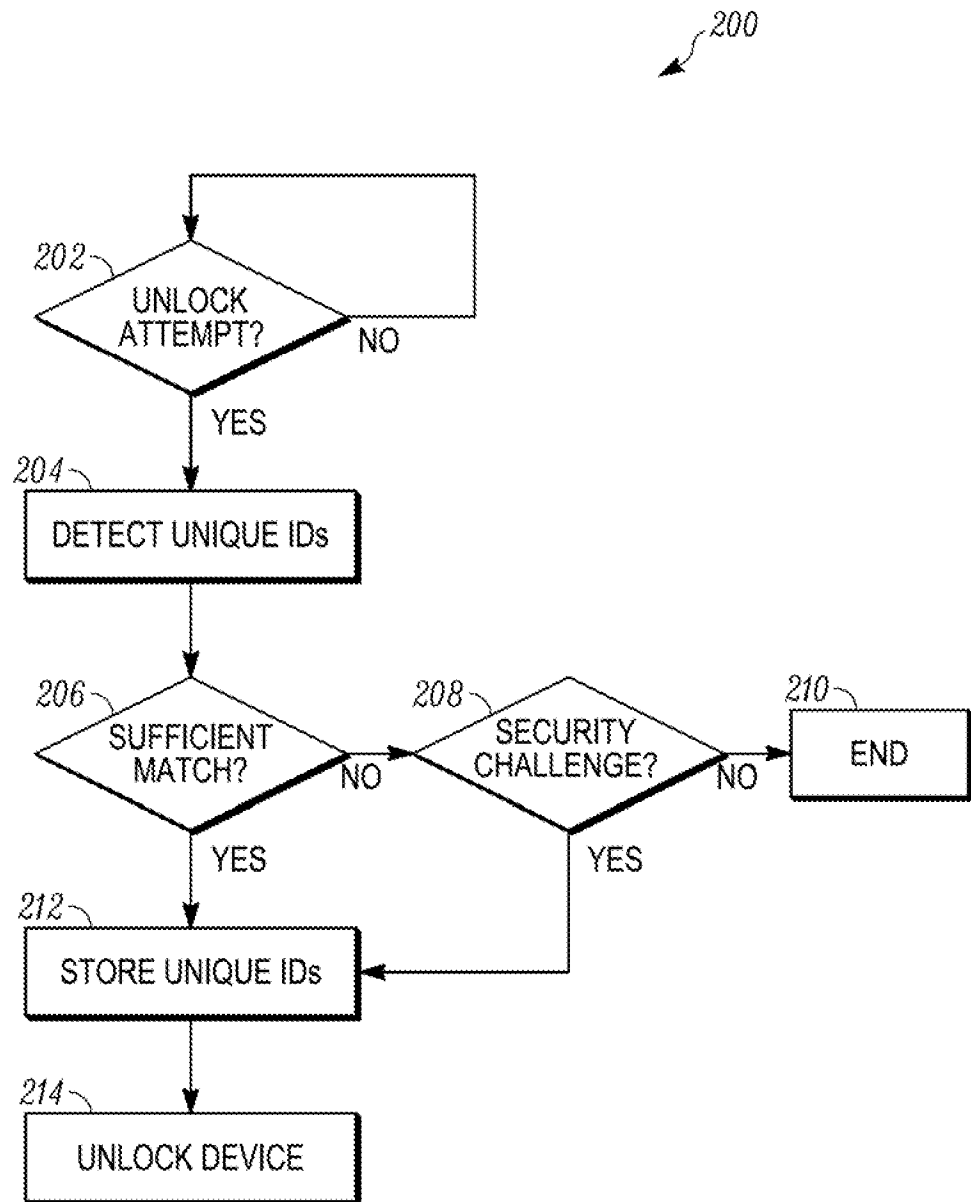


FIG. 2

3/8

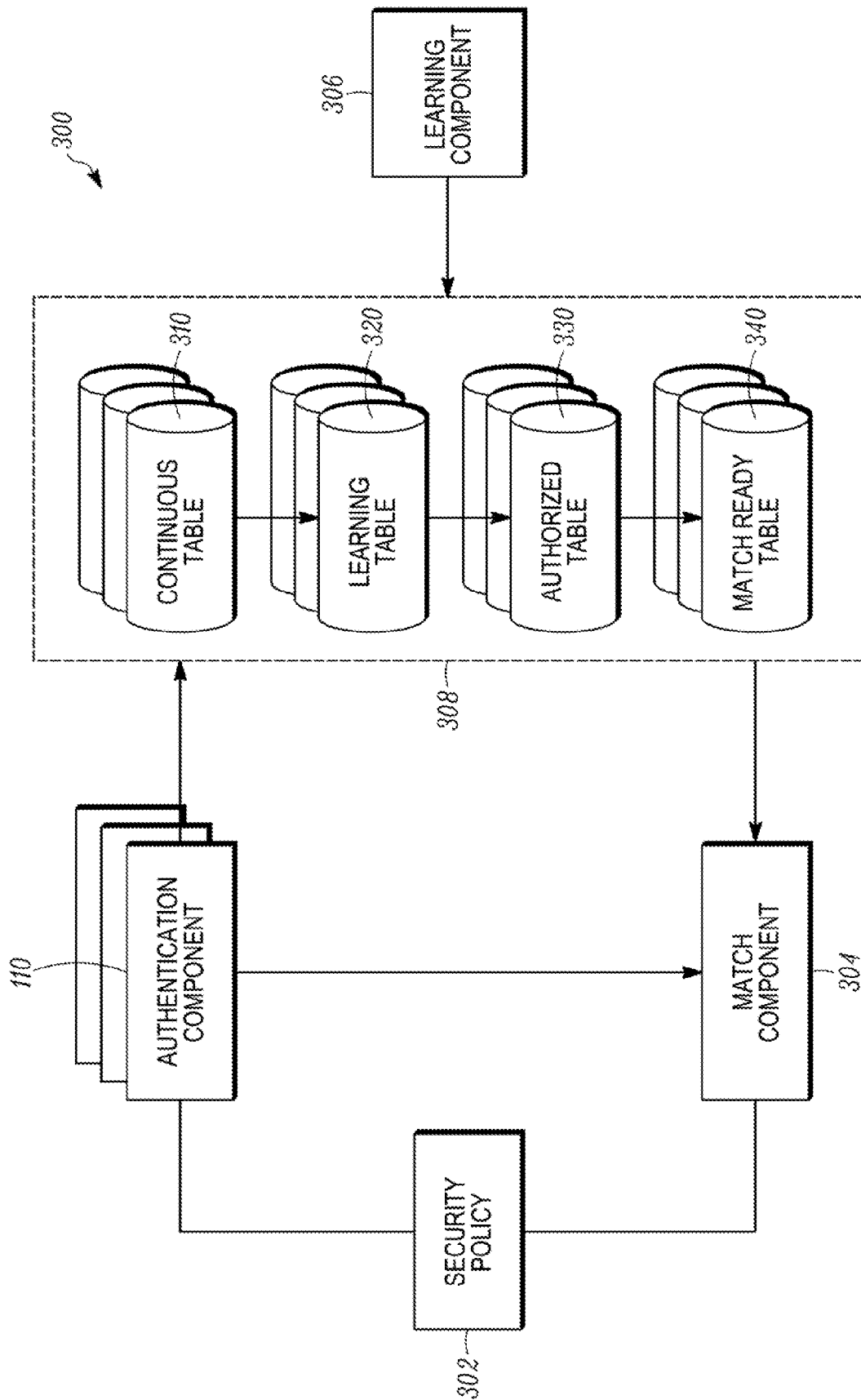


FIG. 3

4/8

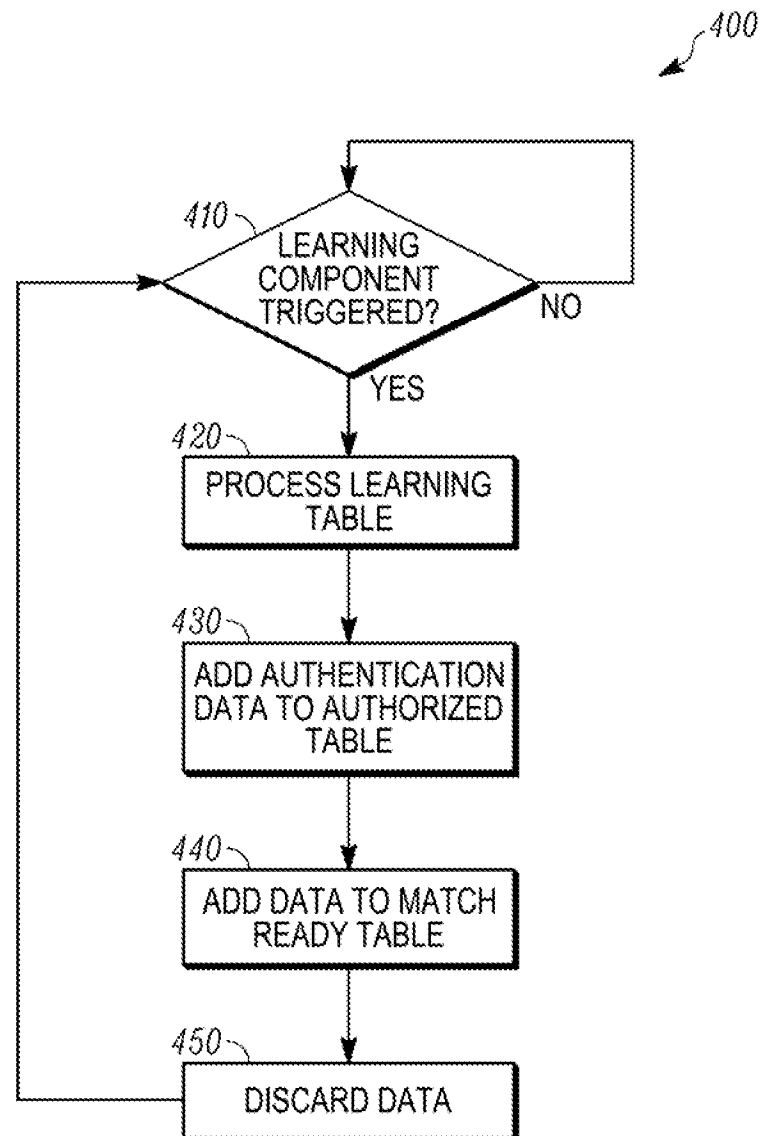


FIG. 4

5/8

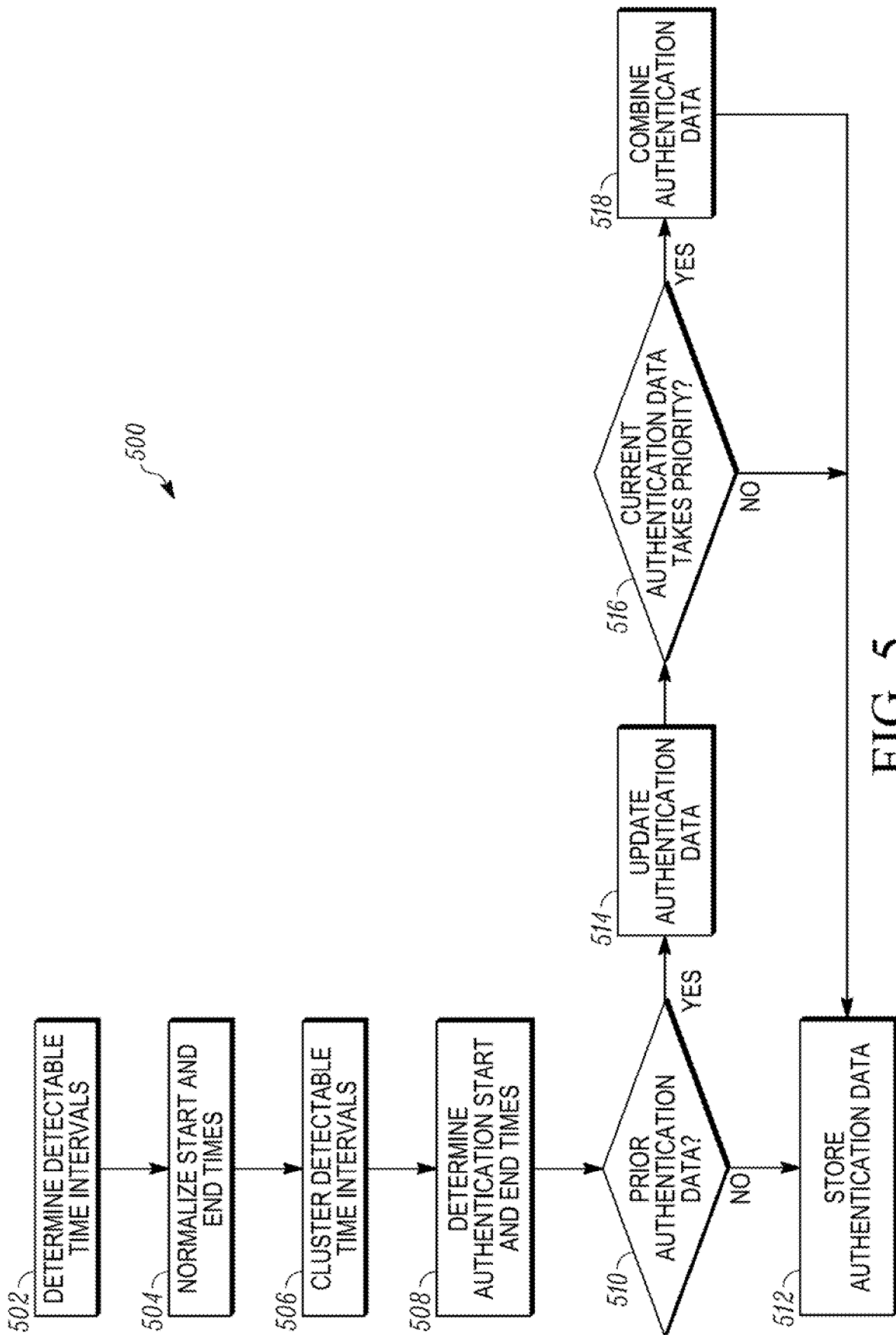


FIG. 5

6/8

610

BLUETOOTH CONTINUOUS TABLE

	UNIQUE ID	DATE	START-TIME	END-TIME
T1	HEADSET1	5/27/2013	1:00 PM	1:00 PM
T2	HEADSET1	5/27/2013	1:00 PM	1:04 PM
T3	HEADSET1	5/27/2013	1:00 PM	1:06 PM
T4	HEADSET1	5/27/2013	1:00 PM	1:10 PM
T5	HEADSET1	5/27/2013	5:20 PM	5:20 PM
T6	HEADSET1	5/27/2013	5:20 PM	5:25 PM
T7	HEADSET1	5/27/2013	5:20 PM	5:28 PM
T8	HEADSET1	5/28/2013	12:58 PM	12:58 PM
T9	HEADSET1	5/28/2013	12:58 PM	1:00 PM
T10	HEADSET1	5/28/2013	12:58 PM	1:06 PM
T11	HEADSET1	5/28/2013	5:18 PM	5:18 PM
T12	HEADSET1	5/28/2013	5:18 PM	5:20 PM

FIG. 6

720

BLUETOOTH LEARNING TABLE

	UNIQUE ID	DATE	START TIME	END TIME	NO. OF TRANSACTIONS
LT1	HEADSET1	5/27/2013	1:00 PM	1:10 PM	4
LT2	HEADSET1	5/27/2013	5:20 PM	5:28 PM	3
LT3	HEADSET1	5/28/2013	12:58 PM	1:06 PM	3
LT4	HEADSET1	5/28/2013	5:18 PM	5:20 PM	2
LT5	HEADSET1	6/3/2013	1:04 PM	1:08 PM	3
LT6	HEADSET1	6/3/2013	5:22 PM	5:28 PM	3
LT7	HEADSET1	6/4/2013	12:59 PM	1:10 PM	4
LT8	HEADSET1	6/4/2013	5:19 PM	5:26 PM	2

FIG. 7

830

BLUETOOTH AUTHORIZED TABLE

	UNIQUE ID	AUTH. START TIME	AUTH. END TIME	AVG PER TRANSACTION	AUTH. DAYS	LAST AUTH. DATE	NO. OF TRANSACTIONS
AT1	HEADSET1	12:58 PM	1:10 PM	3.5	MONTUE	6/4/2013	4 TRANSACTIONS
AT2	HEADSET1	5:18 PM	5:28 PM	2.5	MONTUE	6/4/2013	4 TRANSACTIONS

FIG. 8

940

MATCH-READY TABLE

	UNIQUE ID	TYPE	ACCURACY
MR1	SWIPE1	BIOMETRIC	75
MR2	BLUETOOTH1	NON-BIOMETRIC	100
MR3	WIFI1	NON-BIOMETRIC	100

FIG. 9

8/8

START TIME	END TIME
9:00 AM	3:00 PM
9:10 AM	3:10 PM
9:30 AM	3:15 PM
9:45 AM	3:32 PM
10:10 AM	3:45 PM
10:11 AM	3:48 PM
10:12 AM	4:40 PM
10:15 AM	4:45 PM
10:42 AM	4:49 PM
10:43 AM	5:00 PM
10:45 AM	5:10 PM
11:00 AM	5:20 PM
11:10 AM	5:30 PM
11:45 AM	5:40 PM

FIG. 10

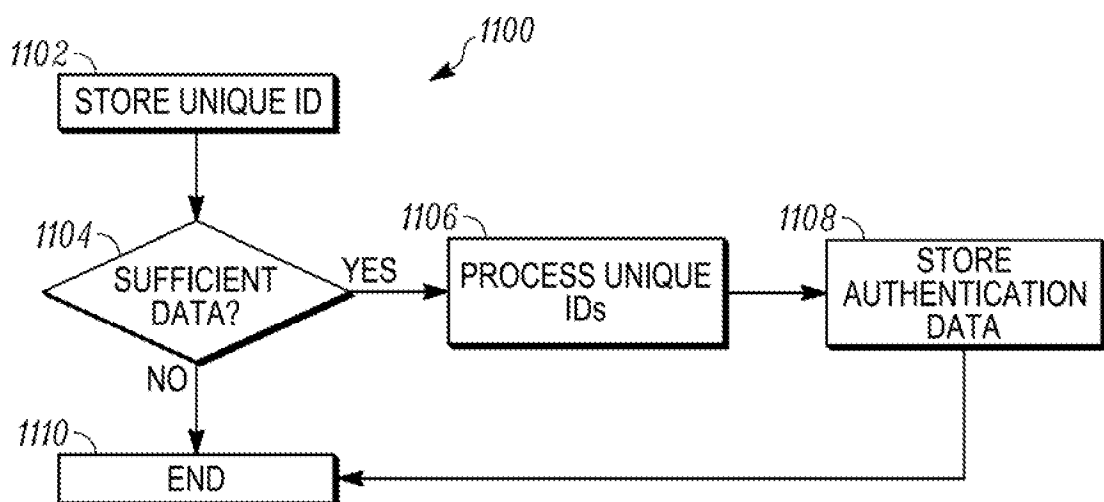


FIG. 11

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2014/038544

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/31

ADD.

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

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/060214 A1 (NAHARI HADI [US]) 8 March 2012 (2012-03-08)	1,11-14
Y	paragraph [0006] - paragraphs [0011], [0015], [0016], [0017] paragraph [0024] - paragraph [0027] paragraph [0033] - paragraph [0038] -----	2-10, 15-20
Y	WO 2013/006071 A1 (CRITICAL SOFTWARE S A [PT]; UNIV DO MINHO [PT]; SOARES DA SILVA FERREI) 10 January 2013 (2013-01-10) page 7 - page 8 page 12 - page 13 -----	7-10, 17-20
Y	WO 2012/152995 A1 (NOKIA CORP [FI]; JOSHI DHAVAL JITENDRA [IN]; NARAYANAN-SAROJA VIJAY [I]) 15 November 2012 (2012-11-15) page 1 - page 2 page 4 - pages 6, 23 -----	2,3,7, 15,17
	-/-	



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

19 August 2014

Date of mailing of the international search report

27/08/2014

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Ghani, Hamza

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2014/038544

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2010/115610 A1 (TREDoux GAVAN LEONARD [US] ET AL) 6 May 2010 (2010-05-06) paragraph [0010] - paragraph [0012] paragraph [0020] - paragraph [0023] -----	4-6,16
Y	US 7 472 282 B1 (FUJII YUSAKU [JP] ET AL) 30 December 2008 (2008-12-30) column 1 - column 2 column 8 - column 10 -----	7,17
A	US 2007/061590 A1 (BOYE DAG E [US] ET AL) 15 March 2007 (2007-03-15) the whole document -----	1,14
A	US 2005/008148 A1 (JACOBSON DOV [US]) 13 January 2005 (2005-01-13) the whole document -----	1,14

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2014/038544

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012060214	A1	08-03-2012	NONE
WO 2013006071	A1	10-01-2013	NONE
WO 2012152995	A1	15-11-2012	NONE
US 2010115610	A1	06-05-2010	NONE
US 7472282	B1	30-12-2008	JP 4120997 B2 16-07-2008 JP 2000132515 A 12-05-2000 US 7472282 B1 30-12-2008
US 2007061590	A1	15-03-2007	NONE
US 2005008148	A1	13-01-2005	CA 2561812 A1 20-10-2005 CN 1957355 A 02-05-2007 EP 1735942 A2 27-12-2006 JP 2007531942 A 08-11-2007 US 2005008148 A1 13-01-2005 WO 2005099166 A2 20-10-2005