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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
07 April 2022 (07.04.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/067436 A1

(51) International Patent Classification:
G06F 21/32 (2013.01)

(21) International Application Number:
PCT/CA2021/051365

(22) International Filing Date:
30 September 2021 (30.09.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/085,598 30 September 2020 (30.09.2020) US

(71) Applicant: **MASTERCARD TECHNOLOGIES CANADA ULC** [CA/CA]; 475 Howe Street, 20th Floor, Vancouver, British Columbia V6C 2B3 (CA).

(72) Inventors: **MCGEE, Perry**; c/o Mastercard Technologies Canada ULC, 475 Howe Street, 20th Floor, Vancouver, British Columbia V6C 2B3 (CA). **CHAN, Sik Suen**; c/o Mastercard Technologies Canada ULC, 475 Howe Street, 40th Floor, Vancouver, British Columbia V6C 2B3 (CA). **LAPTIEV, Anton**; 202-3338 Webber Lane, Vancouver, British Columbia V6S 0J7 (CA). **FRENTIU, Cristian**; c/o Mastercard Technologies Canada ULC, 475 Howe Street, 20th Floor, Vancouver, British Columbia V6C 2B3 (CA).

(74) Agent: **BERESKIN & PARR LLP / S.E.N.C.R.L.**; Scotia Plaza, 40 King Street West, 40th Floor, Toronto, Ontario M5H 3Y2 (CA).

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO,

(54) Title: USER IDENTIFICATION WITH INPUT PROFILE RECORD

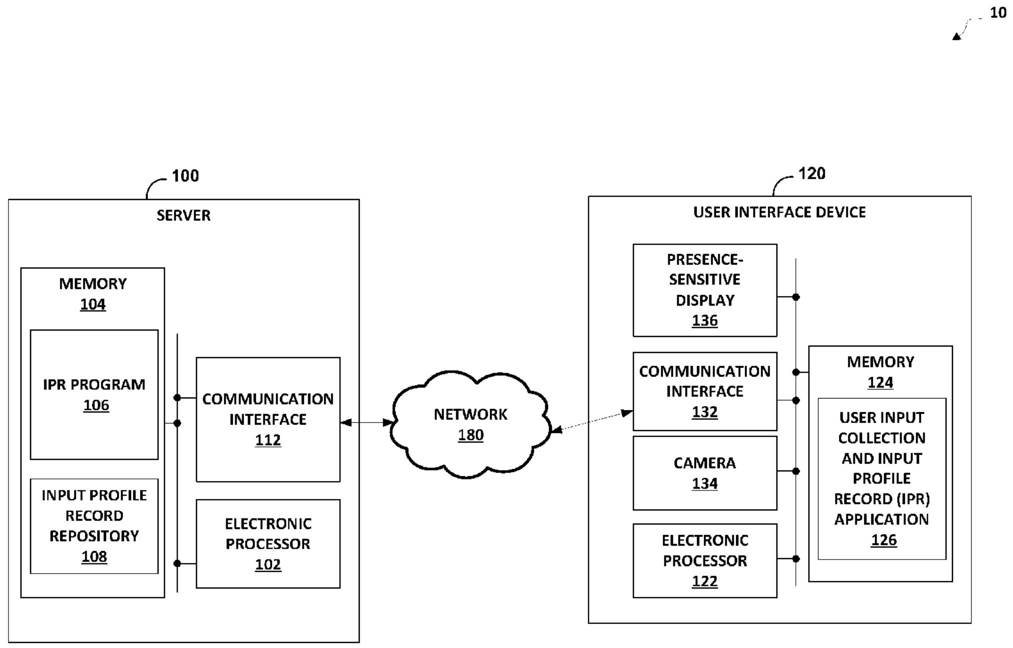


FIG. 1

(57) **Abstract:** User identification with an input profile record (IPR). In one embodiment, a server includes a memory and an electronic processor. The electronic processor is configured to receive a plurality of input profile records (IPRs) associated with a first user, the plurality of IPRs each based on a plurality of user inputs and indicative of identity of the first user, control the memory to store the plurality of IPRs in the input profile record repository, receive a current IPR associated with a second user, determine whether the second user is the first user by comparing a first one or more biometric features based on the plurality of IPRs and a second one or more biometric features based on the current IPR, and responsive to determining that the second user is the first user, output an identity confirmation that the second user is the first user.

WO 2022/067436 A1

[Continued on next page]

NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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))*

— *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*

USER IDENTIFICATION WITH INPUT PROFILE RECORD

FIELD

[0001] The present disclosure relates generally to user identification. More specifically, the present disclosure relates to user identification with an input profile record.

BACKGROUND

[0002] Conventionally, user identification occurs in a variety of different ways. For example, a user may be identified with individual or combinations of distinctive biometrics that are associated with the user. In a different example, a user may be identified after receiving a one-time password to a registered user device associated with the user.

SUMMARY

[0003] However, several problems exist with conventional user identification. One problem is that conventional identification only occurs at certain points in time (e.g., turning on a smartphone). Another problem is that conventional biometric identification is fixed to the initial biometric used to set up the user identification.

[0004] The present disclosure improves upon the conventional user identification and solves the aforementioned problems by performing user identification with an input profile record (IPR). The input profile record is based on a plurality of user inputs of a user and the input profile record changes over time. The input profile record may then be continuously used to identify the user's use of any device over time. Further, the addition of IPR events like key-up, and mobile sensors (i.e. acceleration, orientation and rotation etc.), derivation of biometric features from the generated IPRs, and identifying the "right" balance between IPR size, sampling frequency resolution and effectiveness of data capture are all improvements over the conventional user identification.

[0005] One example of the present disclosure includes a server for user identification. The server includes a memory and an electronic processor in communication with the memory. The memory including an input profile record repository. The electronic processor is configured to receive a plurality of input profile records (IPRs) associated with a first user, the plurality of input profile records each based on a plurality of user inputs and indicative of identity of the first user, control the memory to store the plurality of IPRs in the input profile record repository, receive a current IPR associated with a second user, determine whether the second user is the first user by comparing a first one or more biometric features based on the plurality of IPRs and a second one or more biometric features based on the current IPR, and responsive to determining that the second user is the first user, output an identity confirmation that the second user is the first user.

[0006] Another example of the present disclosure includes a method for user identification. The method includes receiving, with the electronic processor, a plurality of input profile records (IPRs) associated with a first user, the plurality of input profile records each based on a plurality of user inputs and indicative of identity of the first user. The method includes controlling, with the electronic processor, a memory to store the plurality of IPRs in an input profile record repository. The method includes receiving, with the electronic processor, a current IPR associated with a second user. The method includes determining, with the electronic processor, whether the second user is the first user by comparing a first one or more biometric features based on the plurality of IPRs and a second one or more biometric features based on the current IPR. The method also includes responsive to determining that the second user is the first user, outputting, with the electronic processor, an identity confirmation that the second user is the first user.

[0007] Yet another example of the present disclosure includes a system. The system includes a user interface device and a server. The user interface device is configured to output a plurality of input profile records (IPRs) associated with a first user, the plurality of input profile records each based on a plurality of user inputs and indicative of identity of the first user. The server includes a memory including an input profile record repository and an electronic processor in communication with the memory. The electronic processor is configured to receive the plurality of IPRs, control the memory to store the plurality of IPRs in the input profile record repository, receive a current IPR associated with a second user, determine whether the second user is the first user by comparing a first one or more biometric features based on the plurality of IPRs and a second one or more biometric features based on the current IPR, and responsive to determining that the second user is the first user, output an identity confirmation that the second user is the first user.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] FIG. 1 is a block diagram illustrating a system with user identification based on an input profile record, in accordance with various aspects of the present disclosure.

[0009] FIG. 2 is a block diagram illustrating a second system with user identification based on an input profile record, in accordance with various aspects of the present disclosure.

[0010] FIG. 3 is a flowchart illustrating a method for identifying a user, in accordance with various aspects of the present disclosure.

[0011] FIG. 4 is a diagram illustrating an example of an input profile record (IPR), in accordance with various aspects of the present disclosure.

[0012] FIG. 5 is a diagram illustrating a second example of the IPR, in accordance with various aspects of the present disclosure.

[0013] FIG. 6 is a diagram illustrating a first example of a dwell time feature, in accordance with various aspects of the present disclosure.

[0014] FIG. 7 is a diagram illustrating four different latency times, in accordance with various aspects of the present disclosure.

[0015] FIG. 8 is a diagram illustrating different latency times for a portion of an example OTP “356024,” in accordance with various aspects of the present disclosure.

[0016] FIG. 9 is a block diagram illustrating a standard number pad layout, in accordance with various aspects of the present disclosure.

[0017] FIG. 10 is block diagram illustrating a standard number row layout, in accordance with various aspects of the present disclosure.

[0018] FIG. 11 is diagram illustrating different categories of distances between number positions in the standard number pad layout of FIG. 9, in accordance with various aspects of the present disclosure.

DETAILED DESCRIPTION

[0019] Before any embodiments of the present disclosure are explained in detail, it is to be understood that the present disclosure is not limited in its application to the details of construction and the arrangement of components set forth in the following description or illustrated in the following drawings. The present disclosure is capable of other embodiments and of being practiced or of being carried out in various ways.

[0020] FIG. 1 is a block diagram illustrating a system 10 with user identification based on an input profile record, in accordance with various aspects of the present disclosure. It should be understood that, in some embodiments, there are different configurations from the configuration illustrated in FIG. 1. The functionality described herein may be extended to any number of servers providing distributed processing.

[0021] In the example of FIG. 1, the system 10 includes a server 100, a user interface device 120, and a network 180. The server 100 includes an electronic processor 102 (for example, a microprocessor or another suitable processing device), a memory 104 (for example, a non-transitory computer-readable storage medium), and a communication interface 112. It should be understood that, in some embodiments, the server 100 may include fewer or additional components in configurations different from that illustrated in FIG. 1. Also, the server 100 may perform additional functionality than the functionality described herein. In addition, the functionality of the server 100 may be incorporated into other servers. As illustrated in FIG. 1, the electronic processor 102, the memory 104, and the communication interface 112 are electrically coupled by one or more control or data buses enabling communication between the components.

[0022] The electronic processor 102 executes machine-readable instructions stored in the memory 104. For example, the electronic processor 102 may execute instructions stored in the memory 104 to perform the functionality described herein.

[0023] The memory 104 may include a program storage area (for example, read only memory (ROM)) and a data storage area (for example, random access memory (RAM), and other non-transitory, machine-readable medium). In some examples, the program storage area may store machine-executable instructions regarding an input profile record (IPR) program 106. In some examples, the data storage area may store data regarding an input profile record repository 108.

[0024] The IPR program 106 causes the electronic processor 102 to collect and store input profile records in the input profile record repository 108. Specifically, the IPR program 106 causes the electronic processor 102 to parse the IPR content received from a user interface device, determine biometric features based on the current IPR and historical/older IPRs associated with the user, and perform user identification using a biometric identification algorithm that compares current biometrics features based on a current IPR to the historical biometric features based on a set of historical IPRs. In some examples, a successful user identification may require ten historical IPRs associated with the user to establish a "user profile."

[0025] The IPR program 106 also causes the electronic processor 102 to update an input profile record stored in the input profile record repository 108. Additionally, the user identification with the IPRs is a "passive" identification that does not need to query a user for additional information.

[0026] In examples, the input profile record repository 108 is a central repository including a plurality of input profile records. Each input profile record is associated with a specific user (e.g., a user account) and/or a specific user interface device. An input profile record stored in the input profile record repository 108 is updated periodically with the IPR program 106 as described above. The input profile record associated with the user interface device 120 is indicative of an identity of a user over a specific period of time. In other words, the input profile record as described herein solves the aforementioned problems with user identification because the input profile record is a dynamic identification of a user over a specific period of time rather than occurring at certain points in time and fixed to an initial biometric used to set up the user identification.

[0027] For example, the biometric algorithm of the IPR program 106 includes a number of typing and sensor behavioral features as set forth in Tables 4–7 (also referred to as "biometric features") from the user inputs set forth in Tables 1–3 and 8 (i.e., events included in the IPR data construct). The maximum available sample rate (or data delay) is 16 milliseconds (ms), which means sensor data is recorded every 16 ms. However, as with a sample rate of 16 ms from the sensors, a size of the IPR exceeds an upload size threshold set forth in Appendix D (e.g., an upload size threshold of 20,000 bytes). Additionally, as described in Appendix D, the size of the IPR may be reduced below the upload size threshold by increasing the sample rate of some or all of the sensors (e.g., an increase to every 100 ms and/or an increase to every 50 ms), which means a balance between a lower size of recorded data (e.g., the IPR) with lower frequency, less accuracy, and a lower number of samples from some or all of the sensors.

[0028] The communication interface 112 receives data from and provides data to devices external to the server 100, such as an input profile record (IPR) from the user interface device 120 via the network 180. For example, the communication interface 112 may include a port or connection for receiving a wired connection (for example, an Ethernet cable, fiber optic cable, a telephone cable, or the like), a wireless transceiver, or a combination thereof. In some examples, the network 180 is the Internet.

[0029] In the example of FIG. 1, the user interface device 120 includes an electronic processor 122 (for example, a microprocessor or another suitable processing device), a memory 124 (for example, a non-transitory computer-readable storage medium), a communication interface 132, a camera 134, and a presence-sensitive display 136. In some examples, the user interface device may be a smartphone, tablet, laptop, or other suitable user interface device with a presence-sensitive display. As illustrated in FIG. 1, the electronic processor 122, the memory 124, the communication interface 132, the camera 134, and the presence-sensitive display 136 are electrically coupled by one or more control or data buses enabling communication between the components.

[0030] The electronic processor 122 executes machine-readable instructions stored in the memory 124. For example, the electronic processor 122 may execute instructions stored in the memory 124 to perform the functionality described herein.

[0031] The memory 124 may include a program storage area (for example, read only memory (ROM)) and a data storage area (for example, random access memory (RAM), and other non-transitory, machine-readable medium). The program storage area includes a user input collection and input profile record (IPR) application 126. In some examples, the user input collection and IPR application 126 may be a standalone application. In other examples, the user input collection and IPR application 126 is a feature that is part of a separate application (e.g., the user input collection and IPR application 126 may be included as part of a camera application, a banking application, or other suitable application).

[0032] The user input collection and IPR application 126 causes the electronic processor 122 to collect user inputs, i.e., user interactions, from a user relative to a mobile application (e.g., time to fill data field entries, use of specific autofill, or other suitable user inputs) of the user interface device 120 and generate an input profile record (IPR) based on the user inputs (also referred to as a “a mobile platform”). The user input collection and IPR program 106 may also cause the electronic processor 122 to collect user inputs at a particular website (e.g., time to fill data field entries, use of specific autofill, or other suitable user inputs) and generate (or update) the input profile record based on these user inputs (also referred to as a “web platform”).

[0033] In some examples, the user input collection and IPR application 126 causes the electronic processor 122 to collect user inputs with respect to the presence-sensitive display 136 (e.g., type of keyboard, typing speed, use of patterns, or other suitable user inputs (see Tables 1–3)). In these examples, the user input collection and IPR application 126 may also cause the electronic processor 122 to output the generated IPR to the server 100 via the communication interface 132 and the network 180. Additionally, in some examples, the user input collection and IPR application 126 may cause electronic processor 122 to control the memory 124 to store the user inputs that are collected and/or the IPR that is generated for a period of time or until the generated IPR is output to the server 100.

[0034] In other examples, the user input collection and IPR application 126 causes the electronic processor 122 to collect user inputs with respect to the camera 134 (e.g., facial recognition, user gestures, or other suitable user inputs, which may be part of the mobile platform. In these examples, the user input collection and IPR application 126 may also cause the electronic processor 122 to generate (or update) an IPR based on the aforementioned user inputs and output the IPR to the server 100 via the communication interface 132 and the network 180. Additionally, in some examples, the user input collection and IPR application 126 may cause electronic processor 122 to control the memory 124 to store the user inputs that are collected and/or the IPR that is generated for a period of time or until the generated IPR is output to the server 100.

[0035] The communication interface 132 receives data from and provides data (e.g., generated IPR(s)) to devices external to the user interface device 120, i.e., the server 100. For example, the communication interface 132 may include a port or connection for receiving a wired connection (for example, an Ethernet cable, fiber optic cable, a telephone cable, or the like), a wireless transceiver, or a combination thereof.

[0036] The camera 134 includes an image sensor that generates and outputs image data of a subject. In some examples, the camera 134 includes a semiconductor charge-coupled device (CCD) image sensor, a complementary metal-oxide-semiconductor (CMOS) image sensor, or other suitable image sensor. The electronic processor 122 receives the image data of the subject that is output by the camera 134.

[0037] The presence-sensitive display 136 includes a display screen with an array of pixels that generate and output images. In some examples, the display screen is one of a liquid crystal display (LCD) screen, a light-emitting diode (LED) and liquid crystal display (LCD) screen, a quantum dot light-emitting diode (QLED) display screen, an interferometric modulator display (IMOD) screen, a micro light-emitting diode display screen (mLED), a virtual retinal display screen, or other suitable display screen. The presence-sensitive display 136 also includes circuitry that is configured to detect the presence of the user. In some examples, the circuitry is a resistive or capacitive panel that detects the presence of an object (e.g., a user's finger).

[0038] It should be understood that, in some embodiments, the server 100 may include fewer or additional components in configurations different from that illustrated in FIG. 1. Also, the server 100 may perform additional functionality than the functionality described herein. In addition, some of the functionality of the user interface device 120 (for example, the IPR generation) may be incorporated into other servers (e.g., incorporated into the server 100). Likewise, some of the functionality of the server 100 may be incorporated into the user interface device 120 (for example, the user identification).

[0039] To summarize, the user interface device 120 collects IPR data for each transaction at a mobile application or at a web page. From the raw IPR data, the server 100 may parse out a set of meaningful biometric features that differentiates same users from different users.

[0040] A passive biometric identification algorithm included in the IPR program 106 compares biometric feature values (from current IPR) to biometric feature values seen in the past (from historical IPRs), and when the current biometric feature values fall within a "reasonable" range of what is seen in the past, the server 100 may identify the user to be the same as a previous user. The passive biometric identification algorithm is an anomaly detection type of algorithm.

[0041] For the set of biometric feature values seen in the past IPRs, the set may be considered as a "training profile." In general, a minimum of two to ten and a maximum of ten to fifteen (i.e. rolling window of last X transactions) IPRs may be required to build profiles for comparison with the biometric identification algorithm. Each biometric feature may also contribute a different weight to the overall model prediction, where a biometric feature with higher predictability power would have a higher weight.

[0042] To return the "different user" identification confirmation, the server 100 may determine whether a biometric score is less than a lower threshold. To return the "same user" identification confirmation, the server 100 may determine whether a biometric score is greater than an upper threshold and the lower threshold. To return the "undetermined" identification confirmation, the server 100 may determine whether a biometric score is greater than the lower threshold and less than the upper threshold.

[0043] In some examples, the biometric identification algorithm returns a biometric score between 0 to 1, where closer to 1 means more likely a match. Additionally, in some examples, the upper and lower thresholds are set based on feedback data (i.e. confirmed fraudulent identifications) from clients such that the biometric identification algorithm accurately classifies all different users as no-matches to reduce or eliminate false positives.

[0044] FIG. 2 is a block diagram illustrating a second system 200 with user identification based on an input profile record, in accordance with various aspects of the present disclosure. It should be understood that, in some embodiments, there are different configurations from the configuration illustrated in FIG. 2. The functionality described herein may be extended to any number of servers providing distributed processing.

[0045] In the example of FIG. 2, the system 200 includes the server 100 as described above in FIG. 1 and a user interface device 220. Consequently, the description of the server 100 is not repeated below to avoid redundant descriptions. Additionally, the user interface device 220 is any electronic device that user may use to interface with the server 100. For example, the user interface device 200 may be a mouse, a keyboard, a desktop computer, or other suitable user interface device.

[0046] In the example of FIG. 2, the user interface device 220 includes an electronic processor 222 (for example, a microprocessor or another suitable processing device), a memory 224 (for example, a non-transitory computer-readable storage medium), and a communication interface 232.

[0047] It should be understood that, in some embodiments, the user interface device 220 may include fewer or additional components in configurations different from that illustrated in FIG. 2. Also, the user interface device 220 may perform additional functionality than the functionality described herein. As illustrated in FIG. 2, the electronic processor 222, the memory 224, and the communication interface 232 are electrically coupled by one or more control or data buses enabling communication between the components.

[0048] The electronic processor 222 executes machine-readable instructions stored in the memory 224. For example, the electronic processor 222 may execute instructions stored in the memory 224 to perform the functionality described herein.

[0049] The memory 224 may include a program storage area (for example, read only memory (ROM)) and a data storage area (for example, random access memory (RAM), and other non-transitory, machine-readable medium). For example, when the user interface device 220 is a desktop computer, the program storage area may include a user input collection and input profile record (IPR) application 226 that is similar to the user input collection and IPR application 126 as described above.

[0050] The communication interface 232 receives data from (e.g., IPR generation signal) and provides data (e.g., generated IPR(s)) to devices external to the user interface device 220, i.e., the server 100. For example, the communication interface 232 may include a port or connection for receiving a wired connection (for example, an Ethernet cable, fiber optic cable, a telephone cable, a universal serial bus (USB) cable, or other suitable wired connection), a wireless transceiver, or a combination thereof.

[0051] In the example of FIG. 2, the server 100 may send a command (e.g., the IPR generation signal) to the user interface device 220 to collect user input(s) from a user's interaction with the user interface device 220 for a specific period of time. For example, when the user interface device 220 is a computer mouse, the server 100 may send a command to the computer mouse to collect user input(s) from the user's interaction with the computer mouse for a specific period of time.

[0052] In the example of FIG. 2, the user input collection and IPR application 226 may also cause the electronic processor 222 to generate (or update) an IPR based on the aforementioned user input(s) and output the IPR to the server 100 via the communication interface 232 and the network 180. Additionally, in some examples, the user input collection and IPR application 226 may cause electronic processor 222 to control the memory 224 to store the user input(s) that are collected and/or the IPR that is generated for a period of time or until the generated IPR is output to the server 100.

[0053] FIG. 3 is a flowchart illustrating a method 300 for identifying a user, in accordance with various aspects of the present disclosure. FIG. 3 is described with respect to the server 100 and the user interface device 120 of FIG. 1. However, FIG. 3 is equally applicable to the server 100 and the user interface device 220 of FIG. 2, although the server 100 controls the user interface device 220 to collect user inputs for a specific period of time.

[0054] The method 300 includes receiving, with an electronic processor, a plurality of input profile records (IPRs) associated with a first user, the plurality of IPRs are each based on a plurality of user inputs and are each indicative of an identity of the first user (at block 302). For example, the electronic processor 102 receives a plurality of input profile records associated with a first user, the plurality of input profile records are each based on the plurality of user inputs provided by the first user, and are each indicative of an identity of the first user of the user interface device 120.

[0055] The method 300 includes controlling, with the electronic processor, a memory to store the plurality of input profile records (IPRs) in an input profile record repository (at block 304). For example, the electronic processor 102 controls the memory 104 to store the IPRs that are received in the input profile record repository 108.

[0056] The method 300 includes receiving, with the electronic processor, a current input profile record (IPR) associated with a second user (at block 306). For example, the electronic processor 102 receives a current IPR associated with a current user of the user interface device 120 from the user interface device 120.

[0057] The method 300 includes determining, with the electronic processor and a biometric identification algorithm, whether the second user is the first user by comparing a first one or more biometric features based on the plurality of input profile records and a second one or more biometric features based on the current IPR (at block 308). For example, the electronic processor 102 determines whether the current user of the user interface device 120 is the first user of the user interface device 120 by comparing a first one or more biometric features based on the plurality of input profile records associated with the first user and a second one or more biometric features based on the current IPR associated with the second user.

[0058] The method 300 includes responsive to determining that the second user is the first user, outputting, with the electronic processor, an identity confirmation that the second user is the first user (at block 310). For example, the electronic processor 102 controls the communication interface 112 to output an identity confirmation that the current user of the user interface device 120 is the first user of the user interface device 120 to the user interface device 120 via the network 180 in response to the electronic processor 102 determining that the current user is the first user.

[0059] Alternatively, in some examples, the electronic processor 102 controls the communication interface 112 to output an identity confirmation that the current user of the user interface device 120 is the first user of the user interface device 120 to a second server or other computing device via the network 180 in response to the electronic processor 102 determining that the current user is the first user. In these examples, the second server or other computing device may have initiated the identification of the second user by requesting the server 100 to identify whether the first user is the second user.

[0060] In some examples, the current IPR may be from a second user interface device that is different from the user interface device. In these examples, the identity confirmation confirms the second user of the second user interface is the same as the first user of the user interface device.

[0061] Additionally, in some examples, in determining whether the second user is the first user by comparing the first one or more biometric features based on the plurality of IPRs and the second one or more biometric features based on the current IPR, the method 300 may further include generating, with a biometric identification algorithm, the first one or more biometric features from the plurality of IPRs, generating, with the biometric identification algorithm, the second one or more biometric features from the current IPR, generating, with the biometric identification algorithm, a biometric score based on difference between the second one or more biometric features and the first one or more biometric features, determining whether the biometric score is less than a lower threshold, determining whether the biometric score greater than the lower threshold and less than an upper threshold, and determining whether the biometric score is greater than the lower threshold and the upper threshold. In these examples, the second user is the first user when the biometric score is greater than the lower threshold and the upper threshold, the second user is not the first user when the biometric score is lower than the lower threshold and the upper threshold, and the second user is undetermined relative to the first user when the biometric score is higher than the lower threshold and lower than the upper threshold.

[0062] Additionally, in these examples, in generating, with the biometric identification algorithm, the first one or more biometric features from the plurality of IPRs and generating, with the biometric identification algorithm, the second one or more biometric features from the current IPR, the method 300 may further include determining a first one or more latencies of a first dwell time based on the plurality of IPRs, and determining a second one or more latencies of a second dwell time based on the current IPR.

[0063] In some examples, the plurality of IPRs and the current IPR may each include an IPR header and a plurality of IPR events. The plurality of IPR events includes a key down event and a key up event. The plurality of user inputs is a one-time-password (OTP) and each user input of the plurality of user inputs includes the key down event and the key up event associated with each key in the OTP.

[0064] FIG. 4 is a diagram illustrating an example of an input profile record 400, in accordance with various aspects of the present disclosure. The input profile record (IPR) 400 is a transport mechanism that collects and verifies an end user's device interactions and behaviors. Interactions related to the users are captured and the use of their keyboard, mouse, motion and other interaction behaviors that can be extracted from the end user's device. In a typical integration, the IPR 400 is sent to the platform for processing, profiling, analysis and verification.

[0065] The device interaction events may be captured, for example, using a JavaScript Widget or Native Mobile SDKs, by hooking into application and/or platform based event callbacks that are available and compiles them into a text based data structure as illustrated in the IPR 400 of FIG. 4. The text based data structure is composed mainly of individual events separated by a token and concatenated into a string. Each event type may have a variable number of parameters to capture the details of that event type. Each parameter within an event is also separated by another token or sentinel value.

[0066] The server-side parsers are built to support any combination of input events as long as the header event, described below, is present. This enables IPR parsing to be forward compatible such that the parser will not cause any errors when the parser sees event types that it does not support. These events will be logged as “Unknown Events” and execute no special parsing rules.

[0067] When split on the event separator token (semi-colon character), the IPR 400 expands into an IPR 500. FIG. 5 is a diagram illustrating a second example of the IPR 500, in accordance with various aspects of the present disclosure.

Table 1 – IPR Header Event Details

The first event in the IPR 500 contains header information in the format of:

Index	Title	Description	Example Value
0	Encoding Type	Set to ncip for all 2.2 IPRs.	ncip
1	Reserved	Reserved field, always zero	0
2	Unix Timestamp (base 16)	The unix time in seconds as recorded at the initialization of the JavaScript. Represented as base 16.	538eb08a
3	Encoding Version (base 16)	Encoding version. Current versions are 1 and 2 and 3 (current)	3
4	Time Resolution (base 16)	The number of milliseconds in each time interval. Default is 10 (or ‘a’ in base 16).	a

Table 2 – IPR Common Event Details

All other events, other than the header event, follow the base/common structure described in this table:

Index	Title	Type	Description
0	Event Type	string	An ID indicating the event type (reference

			the ID column in the next table)
1	Time Since Last Event (base 16)	string	The number of time intervals since the last event. The Time Resolution parameter provided in the header defines the number of milliseconds in each time interval.
2…N	Event_Type Parameter 1... N	Mixed	Numbers are represented as base16, otherwise string. 1 ... N denotes a variable range of possible Event Type Parameters, where N is the total number of Event Type specific parameters.

Table 3 – IPR Events

The following table describes each of the events and the associated data parameters they contain. These event specific parameters start after the "Time Since Last Event," as mentioned above in Table 2.

Identifier	**Event**	**Event Parameters**	**Description**
st	Form State	N pairs of: 1. DOM ID - Element ID/Name of the target field 2. Length - The current length of the input element when the state was logged. These pairs continue for each input field that are bound to and recording IPR data from	Logged each time the IPR widget initializes in the end user's browser.
ff	Form Field Focus	1. ID - *Element ID/Name of the target field*	Sent when a user focuses an input field on the form.
fb	Form Field Blur	1. ID - *Element ID/Name of the target field*	Sent when a user blurs (leaves focus) any type of

			HTML input field on the form.
kd	Key down		Sent whenever a key down occurs.
ku	Key up		Sent whenever a key up occurs.
mm	Mouse Move	1. X - *Horizontal position of the mouse* 2. Y - *Vertical position of the mouse*	Sent at configurable frequency, providing mouse position, in pixels, relative to the top left of the document area. Default sample rate is every 5 seconds.
mc	Mouse Click	1. X - *Horizontal position of the mouse* 2. Y - *Vertical position of the mouse* 3. ID - *Element ID/Name that was clicked*	Sent whenever the mouse is clicked on the page.
te	Touch Event	1. X - *Horizontal coordinate of the touch* 2. Y - *Vertical coordinate of the touch* 3. ID - *Element ID/Name that was touched*	Sent whenever a touch start event occurs on the page. When available, the X and Y coordinate are the touch point relative to the viewport, including any scroll offset. These will be -1 if the touches page X and page Y properties are unavailable.
ac	Accelerometer		For devices with accelerometer data.
fs	Form Submit	1. X - *Horizontal coordinate of the mouse* 2. Y - *Vertical coordinate of the mouse*	A special event that is called before the post back occurs. Called for both 'Enter' pressed and button click. Passes in the mouse position at the time of event.
kk	Total Keys	1. Length - The current length of the value of the element when it was focused. 2. ID - ElementID/Name that was focused	Triggers along with the *FormFieldFocus(ff)* event. This field is not currently used internally, but may be useful in the future so it has been restored in this encoding format document. This event type is still

			currently active in the JavaScript widget IPR.
sp	Scroll Position		Determine if the page was scrolled or not and if so what position it's at on a configurable frequency.
nccl	Control List		
ts	Time Sync	1. *Now - Current time in MS* 2. *Delta - Time since the IPR Init in MS*	Logs a time sync every 15 seconds
mms	Mouse Movement Sample	1. Time Since Last MMS 2. Number of sub samples taken 3. NOP *or* minVelocityX minVelocityY ** *If the event is not a "NOP" event:* 4. maxVelocityX maxVelocityY ** 5. Average Magnitude of Velocity 6. Total Distance Moved 7. Min Acceleration 8. Max Acceleration 9. Average Acceleration	Mouse Movement Data is cached any time the mouse is moved and samples of the movement are taken on configurable frequencies. Samples are made up of a number of sub-samples that collect and aggregate movement data to keep the payload small. The third (and last) parameter will hold the value "NOP" if no mouse activity was detected among the collection of sub-samples when a full sample is recorded. If mouse movement activity is detected for at least one sub-sample the full sample will be populated and provided to the IPR. ** Min and Max velocity are expressed as vectors separated by a space, since the comma is used for parameters. All numbers are represented as base16 with the decimal shifted 4 places to the right to preserve accuracy of values below 0. All numerical units are expressed as Screens / Second. Where a screen is the size of the

			window.screen.(width|height) properties.
dms	Device Motion Sample	Same format as mms, but with 3 dimensions. Uses alpha/beta/gamma instead of x/y. 3. minVelocityAlpha minVelocityBeta minVelocityGamma 4. maxVelocityAlpha maxVelocityBeta maxVelocityGamma	The Device Motion Sample uses the same format and sampling implementation as mms. *Devices return Alpha as 0 to 360* Alpha = DeviceAlpha *Devices return Beta as -180 to 180* Beta = DeviceBeta + 180 *Devices return Gamma as -90 to 90* Gamma = DeviceGamma + 90 Note in iOS pitch, roll, and yaw terminology is used by CoreMotion. They correlate as such: alpha - yaw beta - pitch gamma - roll
dm	Device Motion	1. DeviceAlpha 2. DeviceBeta + 180 3. DeviceGamma + 90	Sent at configurable frequency, providing device motion, in alpha/beta/gamma notation. Default sample rate is every 5 seconds.
so	Stop		Indicates that IPR recording was turned off using the widget "stop" function.
tr	Truncate	1. Length of original IPR before truncation	Indicates that a truncation event has occurred. The truncated IPR is appended with a truncate event and data contains the original length of the IPR before it was truncated.

[0068] The details above show no field identifier on key down events. The lack of a field identifier reduces the size of the IPR payload. When a form field focus event occurs, the following key down events are assumed to belong to that form field focus event. The parsing code however is set up to parse key down event entries that also contain an element name, for example, key down, bf (i.e., number of milliseconds since the last event in base 16), password. The key down events will contain the form identifier and so the behavior described above must be preserved if IPR parsing is changed.

[0069] Since key up event capture and enhanced key down profiling were added for both desktop and mobile IPRs, additional features could generally apply for both physical and touch keyboards, although there would be feature implementation differences based on differences in desktop IPR data and mobile IPR data. For example, FIG. 6 is a diagram illustrating a first example of a dwell time feature 600, in accordance with various aspects of the present disclosure.

[0070] The dwell time feature 600 is an amount of time during which a key (physical or software) remains in contact (down/up for physical and press/release for software) with a user. As illustrated in FIG. 6, the dwell time feature 600 includes a first down press 600, a first dwell time 602, a first up release 604, a second down press 606, a second dwell time 608, and a second up release 610. In the IPRs 400 and 500 described above, time elements are in time deltas (time since last event), rather than timestamps.

Table 4 – Characteristics of Dwell Time Feature

#	**Feature Name**	**Feature Description**	**Feature Type**
1	Each of these are individual features: otp_otp_dwell_1 otp_otp_dwell_2 otp_otp_dwell_3 otp_otp_dwell_4 otp_otp_dwell_5 otp_otp_dwell_6	Dwell time for each position (i.e., 1, 2, 3, 4, 5, 6) in the one-time password (OTP) sequence. A difference in performance is noted when the position of a digit within an OTP sequence is included for key press durations and latencies.	Numeric
2	total_dwell	Total dwell time for the OTP sequence (sum of dwell times for all keys pressed when inputting the OTP) SUM(otp_position1_dwell, otp_position2_dwell, otp_position3_dwell, otp_position4_dwell, otp_position5_dwell, otp_position6_dwell)	Numeric
3	total_dwell_to_dd	Proportion of total dwell time relative to total down-	Numeric

		down latency. (total_dwell - otp_position6_dwell) / total_dd_time Since the last key does not have an associated down-down time, the last key is excluded from the calculation.	
4	total_dwell_to_uu	Proportion of total dwell time relative to total up-up latency. (total_dwell - otp_position1_dwell) / total_uu_time Since the first key does not have an associated up-up time, the first key is excluded from the calculation.	Numeric
5	mean_dwell	Average dwell time (of a single key) for the OTP sequence	Numeric
6	max_dwell	Longest dwell time in the OTP sequence	Numeric
7	min_dwell	Shortest dwell time in the OTP sequence	Numeric
8	std_dwell	Standard deviation of dwell times for the OTP sequence	Numeric
9	Each of these are individual features: dwell_to_dd1 dwell_to_dd2 dwell_to_dd3 dwell_to_dd4 dwell_to_dd5	Proportion of dwell time relative to down-down latency (see "Latency" section below for definition) for each key pressed.* For example: otp_position1_dwell / dd1 *Since the last key pressed does not have an associated down-down latency, there are only 5 down-down latencies in a 6-digit OTP, so the last key pressed would not have this feature.	Numeric
10	mean_dwell_to_dd	Average proportion of dwell time relative to down-down latency across all keys pressed.	Numeric

		AVG(dwell_to_dd1, dwell_to_dd2, dwell_to_dd3, dwell_to_dd4, dwell_to_dd5)	
11	std_dwell_to_dd	Standard deviation of proportion of dwell time relative to down-down latency across all keys pressed. STD(dwell_to_dd1, dwell_to_dd2, dwell_to_dd3, dwell_to_dd4, dwell_to_dd5)	Numeric
12	Each of these are individual features: dwell_to_uu1 dwell_to_uu2 dwell_to_uu3 dwell_to_uu4 dwell_to_uu5	Proportion of dwell time relative to up-up latency (see "Latency" section below for definition) for each key pressed.* For example: otp_position2_dwell / uu1 *Since the first key pressed does not have an associated up-up latency, there are only 5 up-up latencies in a 6-digit OTP, so the first key pressed would not have this feature.	Numeric
13	mean_dwell_to_uu	Average proportion of dwell time relative to up-up latency across all keys pressed. AVG(dwell_to_uu1, dwell_to_uu2, dwell_to_uu3, dwell_to_uu4, dwell_to_uu5)	Numeric
14	std_dwell_to_uu	Standard deviation of proportion of dwell time relative to up-up latency across all keys pressed. STD(dwell_to_uu1, dwell_to_uu2, dwell_to_uu3, dwell_to_uu4, dwell_to_uu5)	Numeric

[0071] Another aspect of the dwell time feature 600 is latency, which is an amount of time between consecutive keystrokes, where keystroke is a pair of key events involving a press and release of a single key. Latency may be broken into four different types: 1) Down-Down, 2) Up-Down, 3) Up-Up, and 4) Down-Up. FIG. 7 is a diagram illustrating four different latency times 700–706, in accordance with various aspects of the present disclosure. The first latency 700 is the down-down latency that is the amount of time between pressing a key and pressing the next key. The second latency 702 is the down-up latency that is the amount of time between pressing a key and releasing the next key. The third latency 704 is the up-down latency (also known as “Flight Time”) that is the amount of time between releasing a key and pressing the next key. The fourth latency 706 is the up-up latency that is the amount of time between releasing a key and releasing the next key.

[0072] Generally, dwell time is positive because keystrokes follow a down-up-down-up pattern. However, in some instances, dwell time may be negative when the sequence of keystrokes does not follow the down-up-down-up pattern (for example, due to fast typing or use of shift keys).

[0073] For the example OTP “356024,” the server 100 may determine each type of latency time for all diagraphs (a diagraph being two consecutive keystrokes). FIG. 8 is a diagram illustrating different latency times 800–806 for a portion of an example OTP “356024,” in accordance with various aspects of the present disclosure. As illustrated in FIG. 8, the portion of the example OTP “356024” is “3560” and includes down-down latencies 800A–800D, down-up latencies 802A–802C, up-down latencies 804A–804C, and up-up latencies 806A–806C.

Table 5 – Dwell Time Latency Features

#	**Feature Name**	**Feature Description**	**Feature Type**	**Consideration**
1	Down-Down (dd) latency. Each of these are individual features: dd1 dd2 dd3 dd4 dd5	Amount of time between pressing a key and pressing the next key for each digraph in the OTP sequence. With the example OTP 356024, there are 5 total digraphs where each digraph corresponds to a transition between the following pairs of keys: Digraph 1: (3, 5) Digraph 2: (5, 6)	Numeric	

		Digraph 3: (6, 0) Digraph 4: (0, 2) Digraph 5: (2, 4)		
2	Up-Up (uu) latency. Each of these are individual features: uu1 uu2 uu3 uu4 uu5	Amount of time between releasing a key and releasing the next key for each digraph in the OTP sequence	Numeric	
3	Up-Down (ud) latency. Each of these are individual features: ud1 ud2 ud3 ud4 ud5	Amount of time between releasing a key and pressing the next key for each digraph in the OTP sequence	Numeric	
4	Down-Up (du) latency. Each of these are individual features: du1 du2 du3 du4 du5	Amount of time between pressing a key and releasing the next key for each digraph in the OTP sequence	Numeric	
5	total_x_time where x in [dd, uu, ud, du]	Total dd, uu, ud, or du time in the OTP sequence	Numeric	Error corrections will make this a larger number - for all features, it would be simpler to only use samples where OTP was inputted without any error
6	mean_x_time where x in [dd, uu, ud, du]	Average dd, uu, ud or du time in the OTP sequence	Numeric	
7	min_x_time where x in [dd, uu, ud, du]	Shortest dd, uu, ud or du time in the OTP sequence	Numeric	
8	max_x_time where x in [dd, uu, ud, du]	Longest dd, uu, ud or du time in the OTP sequence	Numeric	
9	std_x_time	Standard deviation of dd, uu, ud or du times in the OTP sequence	Numeric	

	where x in [dd, uu, ud, du]			
10	otp_position_max_ud_time	The position in the OTP sequence of the key which precedes the longest up-down (flight) time (e.g. longest pause comes after the 2nd digit is typed) and may be further extended to max 1, max 2, max 3... i.e. position of key preceding longest flight time, position of key preceding second longest flight time, etc. ← This may help characterize how users have different rhythms when inputting an OTP (e.g. 3+3 = type first 3 digits, small pause, then types next 3 digits - other patterns like 2+2+2 are also possible)	Numeric - discrete (range 1-6)	Error corrections (if made) might make it trickier to determine the position

[0074] In some examples, the actual OTP assigned may be known in advance and whether the OTP typed was correct/accepted. In these examples, the location/layout structure of the keyboard gives rise to three additional latency features: 1) latency for specific pairs of keys, 2) latencies for distance categories based on a standard number pad layout, and 3) latencies for distance categories based on a standard number row layout. FIG. 9 is a block diagram illustrating a standard number pad layout 900, in accordance with various aspects of the present disclosure. FIG. 10 is block diagram illustrating a standard number row layout 1000, in accordance with various aspects of the present disclosure. FIG. 11 is diagram illustrating different categories 1100–1114 of distances between number positions in the standard number pad layout 900 of FIG. 9, in accordance with various aspects of the present disclosure.

Table 6 – Latency Time Features

#	**Feature Name**	**Feature Description**
1	Latencies for specific pairs of keys	Each of these are individual features: pair_00_x pair_01_x pair_02_x ... pair_99_x (100 total) where x in [dd, uu, ud, du]

		Given 10 possible digits, there are 10 x 10 = 100 possible combinations that exist in an OTP: (0, 0) (0, 1) (0, 2) ... (9, 9) For the example OTP 356024, the 5 pairs would be: (3, 5), (5, 6), (6, 0), (0, 2), (2, 4) The server may then determine, for example, the up-down time for each of these pairs and fill those 100, leaving the pairs which are not applicable in this OTP entry.
2	Latencies for distance categories based on a standard number pad layout.	Each of these are individual features: numpad_pair_cat1_x numpad_pair_cat2_x ... numpad_pair_cat_8_x (8 total) where x in [dd, uu, ud, du] Assuming, for example, that the latency between 7 and 9 is comparable to the latency between 7 and 1 since they are equally as far apart on the number pad. Each of the 100 pairs of digits categorized into 8 different categories of distances (see FIG. 11), and latencies are calculated only within multiple latencies between pairs exist within the same category for an OTP. Assuming for, example, that the latency between 7 and 9 is comparable to the latency between 4 and 6 or between 7 and 1 since they are equally as far apart on the number pad. Each of the 100 pairs of digits above are therefore categorized into 8 different categories of distances, and latencies are calculated only within these 8 categories. Where multiple latencies between pairs exist within the same category for an OTP, the latencies are averaged to produce one latency value for the category.
3	Latencies for distance categories based on a standard number row layout.	Each of these are individual features: numrow_pair_cat1_x numrow_pair_cat2_x ... numrow_pair_cat_10_x (10 total) where x in [dd, uu, ud, du] Assuming, for example, that the latency between 1 and 3 is comparable to the latency be and 7 since they are equally as far apart on the number pad. Each of the 100 pairs of digits categorized into 10 different categories of distances, and latencies are calculated only with where multiple latencies

		between pairs exist within the same category for an OTP. Assuming for, example, that the latency between 1 and 3 is comparable to the latency between 2 and 4 or between 5 and 7 since they are equally as far apart on the number pad. Each of the 100 pairs of digits above are therefore categorized into 10 different categories of distances, and latencies are calculated only within these 10 categories. Where multiple latencies between pairs exist within the same category for an OTP, the latencies are averaged to produce one latency value for the category.

Table 7 – Miscellaneous Keystroke Dynamics

#	**Feature Name**	**Feature Description**	**Feature Type**	**Considerations**
1	total_kd	Total number of key presses (key down events) in the OTP sequence	Numeric - discrete	Considering our expected OTP codes are 6 digits in length, this should be at least 6. More kd's may indicate errors or error correction, and fewer kd's may indicate use of keyboard shortcuts (e.g. copy and paste, which should be flagged/disqualified). Error corrections will make this a larger number - for all features, it would be simpler to only use samples where OTP was inputted without any error.
2	numeric_kd_to_total_kd	Proportion of total number of key down events where a numeric key was pressed	Numeric	If error correction cases are excluded and there is no shift use, this ratio should be 1 most of the time for desktop keyboards. For mobile touch keyboards however, there could be a lot more touch events not for inputting numeric values (e.g.

				scrolling/flicking up and down).
3	total_edit_kd	Total number of times an editing key was used in the OTP sequence (i.e. number of kd's on backspace, delete, insert regardless of keyboard location)	Numeric	Uses new keyboard location profiling of kd events in IPR
4	edit_kd_to_total_kd	Proportion of total number of key down events where an editing key was pressed	Numeric	This would be 0 most of the time if excluded in error correction cases
5	numpad_ind	Indicates whether a full keyboard containing a numpad was used (at least one key was pressed where numpad location was indicated)	Binary	

[0075] The mobile sensor data may be collected, for example, using a JavaScript widget or Native Mobile SDKs from four sensors that capture orientation, rotation, and acceleration data (both with and without the effect of gravity) in three dimensions. In some examples, the sensor events are not aggregated and may be driven at a sixteen millisecond (ms) rate.

Table 7 – Mobile Sensor Features

#	**Feature Name**	**Feature Description**	**Feature Type**
1	*avg_sensor_value_x* *avg_sensor_value_y* *avg_sensor_value_z*	Average sensor value for each axis	Numeric
2	*med_sensor_value_x* *med_sensor_value_y* *med_sensor_value_z*	median sensor value for each axis	Numeric
3	*mean_med_ratio_sensor_value_x* *mean_med_ratio_sensor_value_y* *mean_med_ratio_sensor_value_z*	mean to median sensor value ratio for each axis	Numeric
4	*std_sensor_value_x* *std_sensor_value_y* *std_sensor_value_z*	Std deviation of sensor values for each axis	Numeric
5	*coefvar_sensor_value_x* *coefvar_sensor_value_y* *coefvar_sensor_value_z*	coef. of variation of sensor values for each axis	Numeric

6	*avg_abs_diff_x* *avg_abs_diff_y* *avg_abs_diff_z*	Average absolute difference between each of the sensor readings and their mean for each axis	Numeric
7	*iqr_sensor_value_x* *iqr_sensor_value_y* *iqr_sensor_value_z*	Interquartile range sensor value for each axis	Numeric
8	*avg_result_acceleration*	the average of the square root of the sum of the square of the x, y, z axis values	Numeric
9	*binned_distrib_x_i* *binned_distrib_y_i* *binned_distrib_z_i*	for i from 1 to *n* determine the range of values for each axis (max – min), divide this range into n equal sized bins, and then record what fraction of the sensor values fell within each of the bins. **Note:** here *n* is a parameter. Usually *n*=10	Numeric
10	*n_peaks_norm_x* *n_peaks_norm_y* *n_peaks_norm_z*	Number of the peaks for each axis normalized by the total session time (usually the sensor time series, similarly to other signal data, looks like repetitive ways on the graph, e.g. sinusoid. In this case, the server computes the number of those waves for each axis). The server may also define a threshold value that defines a peak, e.g. discard small peaks.	Numeric - discrete
11	*range_peak_x* *range_peak_y* *range_peak_z*	The difference between max and min peak values for each axis. **Note:** The server may also use ratio.	Numeric
12	*avg_peak_x* *avg_peak_y* *avg_peak_z*	Average peak value for each axis	Numeric
13	*avg_time_bw_peaks_x* *avg_time_bw_peaks_y* *avg_time_bw_peaks_z*	Average time between peaks for each axis. **Note:** this feature assumes that there's more than one peak. If there's no distinguishable peaks based on the threshold in 9, then the server may lower the threshold or compute the average time between first *n* maximum values for each axis, where *n* is a parameter	Numeric

Table 8 – Mobile Sensor Events

ID	Event	Custom Data Parameters	Description
ac	devicemotion.acceleration IncludingGravity	1. Represents the acceleration upon the x axis which is the west to east axis 2. Represents the acceleration upon the y axis which is the south to north axis	Acceleration of the device on the three axis X, Y and

		3. Represents the acceleration upon the z axis which is the down to up axis NOP is device is stationary	Z with the effect of gravity. Acceleration is expressed in m/s2
gy	devicemotion.rotationRate	1. The rate at which the device is rotating about its Z axis; that is, being twisted about a line perpendicular to the screen. 2. The rate at which the device is rotating about its X axis; that is, front to back. 3. The rate at which the device is rotating about its Y axis; that is, side to side. NOP is device is stationary	Rate of change of the device's orientation on the three orientation axis alpha, beta and gamma. Rotation rate is expressed in degrees per seconds.
lac	devicemotion.acceleration	1. Represents the acceleration upon the x axis which is the west to east axis 2. Represents the acceleration upon the y axis which is the south to north axis 3. Represents the acceleration upon the z axis which is the down to up axis NOP is device is stationary	Acceleration of the device on the three axis X, Y and Z. Acceleration is expressed in m/s2
or	deviceorientationevent	1. a number representing the motion of the device around the z axis, express in degrees with values ranging from 0 to 360. 2. a number representing the motion of the device around the x axis, express in degrees with values ranging from -180 to 180. This represents a front to back motion of the device 3. a number representing the motion of the device around the y axis, express in degrees with values ranging from -90 to 90. This represents a left to right motion of the device 4. a boolean that indicates whether or not the device is providing orientation data absolutely - this value is optional, true if provided. NOP is device is stationary	Information from the physical orientation of the device running the web page or mobile application

[0076] One example sampling frequency used for the data collection described above is 62.5 hertz (Hz) (i.e., sensor events driven every sixteen milliseconds). However, the sensor events are stored in the IPR (e.g., the IPR 400 or the IPR 500) and the resulting size of the IPR may exceed a desired threshold (e.g., 20,000 bytes maximum, more preferably, 5 kB).

[0077] After collecting data every 16 ms, the mobile sample resulted in 167,017 observations and a mean of 29,000 bytes. In order the meet the recommended production IPR size of approximately 5 kB, then the IPR must be approximately six times smaller. With the sensor data consuming more than 90% of the IPR size, then the sensor sampling rate must be at least six times slower than the current 16 ms or roughly 100 ms (10 events per second). With the sensor sampling rate set to 100 ms, more than 99% of IPRs will not require truncation and the average IPR would be approximately 5,000 bytes.

[0078] Alternatively, in some examples, instead of setting the sensor sampling rate to 100 ms, the number of sensors collecting data may be reduced (e.g., remove gravity accelerator) and the sensor sampling rate may be set at a more accurate 50 ms sampling rate. In these examples, the data collection is most accurate when using higher sampling rates for sensors that do not have much short time variation (e.g., gyroscope and orientation).

[0079] Thus, the present disclosure provides, among other things, user identification based on an input profile record. Various features and advantages of the invention are set forth in the following claims.

CLAIMS

What is claimed is:

1. A server comprising:

a memory including an input profile record repository; and

an electronic processor in communication with the memory, the electronic processor configured to

receive a plurality of input profile records (IPRs) associated with a first user, the plurality of input profile records each based on a plurality of user inputs and indicative of identity of the first user,

control the memory to store the plurality of IPRs in the input profile record repository,

receive a current IPR associated with a second user,

determine whether the second user is the first user by comparing a first one or more biometric features based on the plurality of IPRs and a second one or more biometric features based on the current IPR, and

responsive to determining that the second user is the first user, output an identity confirmation that the second user is the first user.

2. The server of claim 1, wherein, to determine whether the second user is the first user by comparing the first one or more biometric features based on the plurality of IPRs and the second one or more biometric features based on the current IPR, the electronic processor is further configured to

generate, with a biometric identification algorithm, the first one or more biometric features from the plurality of IPRs,

generate, with the biometric identification algorithm, the second one or more biometric features from the current IPR,

generate, with the biometric identification algorithm, a biometric score based on difference between the second one or more biometric features and the first one or more biometric features,

determine whether the biometric score is less than a lower threshold,

determine whether the biometric score greater than the lower threshold and less than an upper threshold, and determine whether the biometric score is greater than the lower threshold and the upper threshold, and

wherein the second user is the first user when the biometric score is greater than the lower threshold and the upper threshold.

3. The server of claim 2, wherein, to generate, with a biometric identification algorithm, the first one or more biometric features from the plurality of IPRs and generate, with the biometric identification algorithm, the second one or more biometric features from the current IPR, the electronic processor is further configured to

determine a first one or more latencies of a first dwell time based on the plurality of IPRs, and

determine a second one or more latencies of a second dwell time based on the current IPR.

4. The server of claim 2, wherein the second user is not the first user when the biometric score is lower than the lower threshold and the upper threshold, and wherein the second user is undetermined relative to the first user when the biometric score is higher than the lower threshold and lower than the upper threshold.

5. The server claim 1, wherein the plurality of IPRs and the current IPR each include an IPR header and a plurality of IPR events, wherein the plurality of IPR events includes a key down event and a key up event, wherein the plurality of user inputs is a one-time-password (OTP), and wherein each user input of the plurality of user inputs includes the key down event and the key up event associated with each key in the OTP.

6. The server of claim 1, wherein the plurality of IPRs and the current IPR each include an IPR header and a plurality of IPR events, and wherein the plurality of IPR events includes two or more of:

a form state event,

a form field focus event,

a form field blur event,

a key down event,

a key up event,

a mouse move event,

a mouse click event,
a touch event,
an accelerometer event,
a form submit event,
a total keys event,
a scroll position event,
a control list event,
a time sync event,
a mouse movement sample event,
a device motion sample event,
a device motion event,
a stop event, and
a truncate event.

7. The server of claim 1, wherein the first one or more biometric features and the second one or more biometric features each include a plurality of sensor features including two or more of:

average sensor value for each axis,
median sensor value for the each axis,
mean to median sensor value ratio for the each axis,
standard deviation of sensor values for the each axis,
coefficient of variation of sensor values for the each axis,
average absolute difference between sensor readings and the mean for the each axis,
interquartile range sensor value for the each axis,
an average of a square root of a sum of a square of x, y, z axis values,
binned distribution for the each axis,
number of peaks for the each axis normalized by total session time,
difference between maximum and minimum peak values for the each axis,
average peak value for the each axis, and
average time between the peaks for the each axis.

8. A method for user identification, the method comprising:

receiving, with the electronic processor, a plurality of input profile records (IPRs) associated with a first user, the plurality of input profile records each based on a plurality of user inputs and indicative of identity of the first user;

controlling, with the electronic processor, a memory to store the plurality of IPRs in an input profile record repository;

receiving, with the electronic processor, a current IPR associated with a second user;

determining, with the electronic processor, whether the second user is the first user by comparing a first one or more biometric features based on the plurality of IPRs and a second one or more biometric features based on the current IPR; and

responsive to determining that the second user is the first user, outputting, with the electronic processor, an identity confirmation that the second user is the first user.

9. The method of claim 8, wherein determining whether the second user is the first user by comparing the first one or more biometric features based on the plurality of IPRs and the second one or more biometric features based on the current IPR further includes

generating, with a biometric identification algorithm, the first one or more biometric features from the plurality of IPRs,

generating, with the biometric identification algorithm, the second one or more biometric features from the current IPR,

generating, with the biometric identification algorithm, a biometric score based on difference between the second one or more biometric features and the first one or more biometric features,

determining whether the biometric score is less than a lower threshold,

determining whether the biometric score greater than the lower threshold and less than an upper threshold, and

determining whether the biometric score is greater than the lower threshold and the upper threshold, and

wherein the second user is the first user when the biometric score is greater than the lower threshold and the upper threshold.

10. The method of claim 9, wherein, generating, with the biometric identification algorithm, the first one or more biometric features from the plurality of IPRs and generating, with the biometric identification algorithm, the second one or more biometric features from the current IPR further includes

determining a first one or more latencies of a first dwell time based on the plurality of IPRs, and

determining a second one or more latencies of a second dwell time based on the current IPR.

11. The method of claim 9, wherein the second user is not the first user when the biometric score is lower than the lower threshold and the upper threshold, and wherein the second user is undetermined relative to the first user when the biometric score is higher than the lower threshold and lower than the upper threshold.

12. The method claim 8, wherein the plurality of IPRs and the current IPR each include an IPR header and a plurality of IPR events, wherein the plurality of IPR events includes a key down event and a key up event, wherein the plurality of user inputs is a one-time-password (OTP), and wherein each user input of the plurality of user inputs includes the key down event and the key up event associated with each key in the OTP.

13. The method of claim 8, wherein the plurality of IPRs and the current IPR each include an IPR header and a plurality of IPR events, and wherein the plurality of IPR events includes two or more of:

a form state event,

a form field focus event,

a form field blur event,

a key down event,

a key up event,

a mouse move event,

a mouse click event,

a touch event,

an accelerometer event,

a form submit event,

a total keys event,

a scroll position event,

a control list event,

a time sync event,

a mouse movement sample event,

a device motion sample event,

a device motion event,

a stop event, and

a truncate event.

14. The method of 8, wherein the first one or more biometric features and the second one or more biometric features each include a plurality of sensor features including two or more of:

average sensor value for each axis,

median sensor value for the each axis,

mean to median sensor value ratio for the each axis,

standard deviation of sensor values for the each axis,

coefficient of variation of sensor values for the each axis,

average absolute difference between sensor readings and the mean for the each axis,

interquartile range sensor value for the each axis,

an average of a square root of a sum of a square of x, y, z axis values,

binned distribution for the each axis,

number of peaks for the each axis normalized by total session time,

difference between maximum and minimum peak values for the each axis,

average peak value for the each axis, and

average time between the peaks for the each axis.

15. A system comprising:

a user interface device configured to output a plurality of input profile records (IPRs) associated with a first user, the plurality of input profile records each based on a plurality of user inputs and indicative of identity of the first user; and

a server including

a memory including an input profile record repository; and

an electronic processor in communication with the memory, the electronic processor configured to

receive the plurality of IPRs,

control the memory to store the plurality of IPRs in the input profile record repository,

receive a current IPR associated with a second user, determine whether the second user is the first user by comparing a first one or more biometric features based on the plurality of IPRs and a second one or more biometric features based on the current IPR, and

responsive to determining that the second user is the first user, output an identity confirmation that the second user is the first user.

16. The system of claim 15, wherein, to determine whether the second user is the first user by comparing the first one or more biometric features based on the plurality of IPRs and the second one or more biometric features based on the current IPR, the electronic processor is further configured to

generate, with a biometric identification algorithm, the first one or more biometric features from the plurality of IPRs,

generate, with the biometric identification algorithm, the second one or more biometric features from the current IPR,

generate, with the biometric identification algorithm, a biometric score based on difference between the second one or more biometric features and the first one or more biometric features,

determine whether the biometric score is less than a lower threshold,

determine whether the biometric score greater than the lower threshold and less than an upper threshold, and

determine whether the biometric score is greater than the lower threshold and the upper threshold, and

wherein the second user is the first user when the biometric score is greater than the lower threshold and the upper threshold.

17. The system claim 16, wherein, to generate, with a biometric identification algorithm, the first one or more biometric features from the plurality of IPRs and generate, with the biometric identification algorithm, the second one or more biometric features from the current IPR, the electronic processor is further configured to

determine a first one or more latencies of a first dwell time based on the plurality of IPRs, and

determine a second one or more latencies of a second dwell time based on the current IPR.

18. The system of claim 16, wherein the second user is not the first user when the biometric score is lower than the lower threshold and the upper threshold, and wherein the second user is undetermined relative to the first user when the biometric score is higher than the lower threshold and lower than the upper threshold.

19. The system of claim 15, wherein the plurality of IPRs and the current IPR each include an IPR header and a plurality of IPR events, wherein the plurality of IPR events includes a key down event and a key up event, wherein the plurality of user inputs is a one-time-password (OTP), and wherein each user input of the plurality of user inputs includes the key down event and the key up event associated with each key in the OTP.

20. The system of claim 15, wherein the plurality of IPRs and the current IPR each include an IPR header and a plurality of IPR events, and wherein the plurality of IPR events includes two or more of:

a form state event,
a form field focus event,
a form field blur event,
a key down event,
a key up event,
a mouse move event,
a mouse click event,
a touch event,
an accelerometer event,
a form submit event,
a total keys event,
a scroll position event,
a control list event,
a time sync event,
a mouse movement sample event,
a device motion sample event,
a device motion event,
a stop event, and
a truncate event.

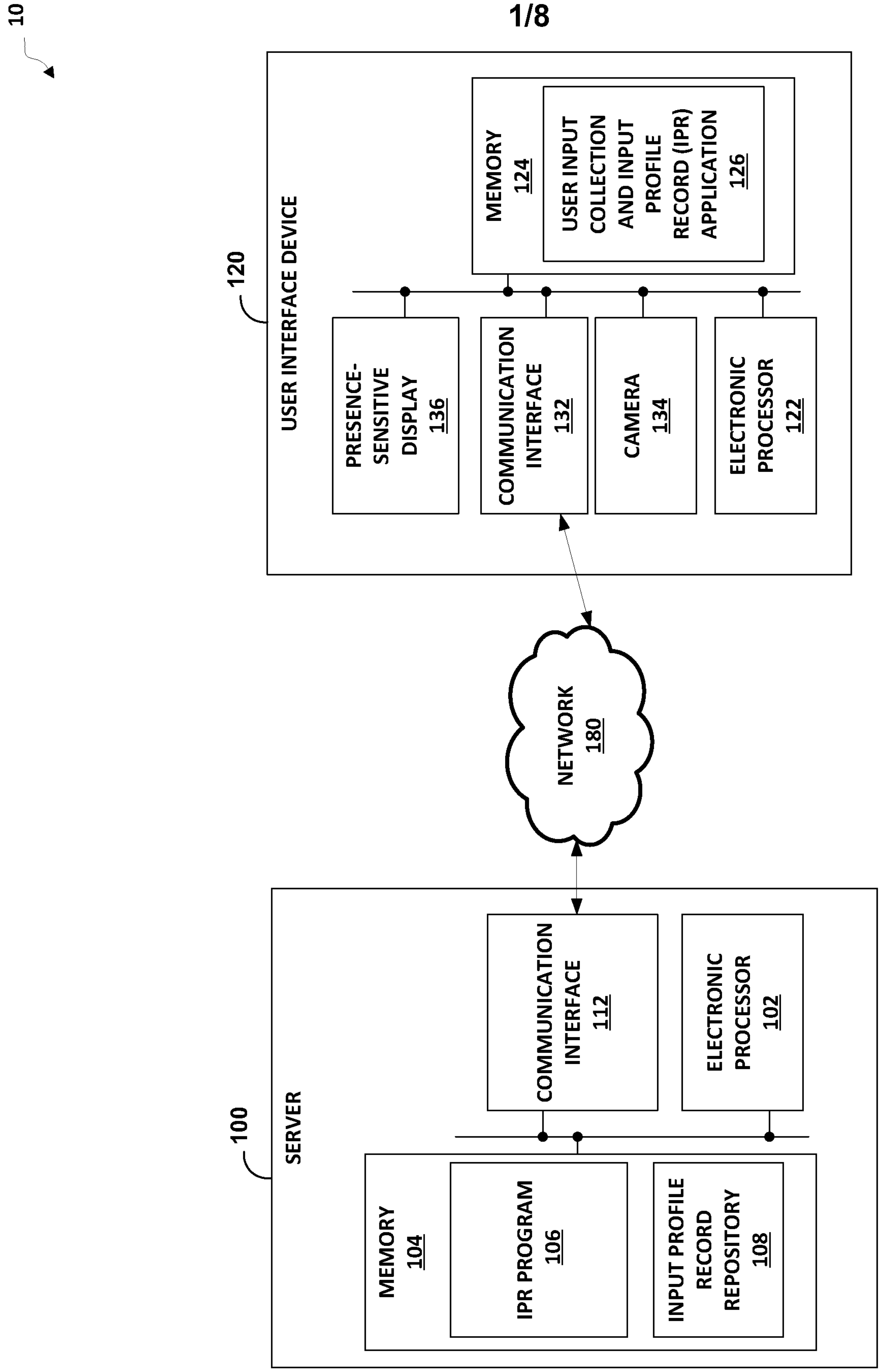

10
120
USER INTERFACE DEVICE
MEMORY 124
USER INPUT COLLECTION AND INPUT PROFILE RECORD (IPR) APPLICATION 126
PRESENCE-SENSITIVE DISPLAY 136
COMMUNICATION INTERFACE 132
CAMERA 134
ELECTRONIC PROCESSOR 122
NETWORK 180
100
SERVER
COMMUNICATION INTERFACE 112
ELECTRONIC PROCESSOR 102
MEMORY 104
IPR PROGRAM 106
INPUT PROFILE RECORD REPOSITORY 108

FIG. 1

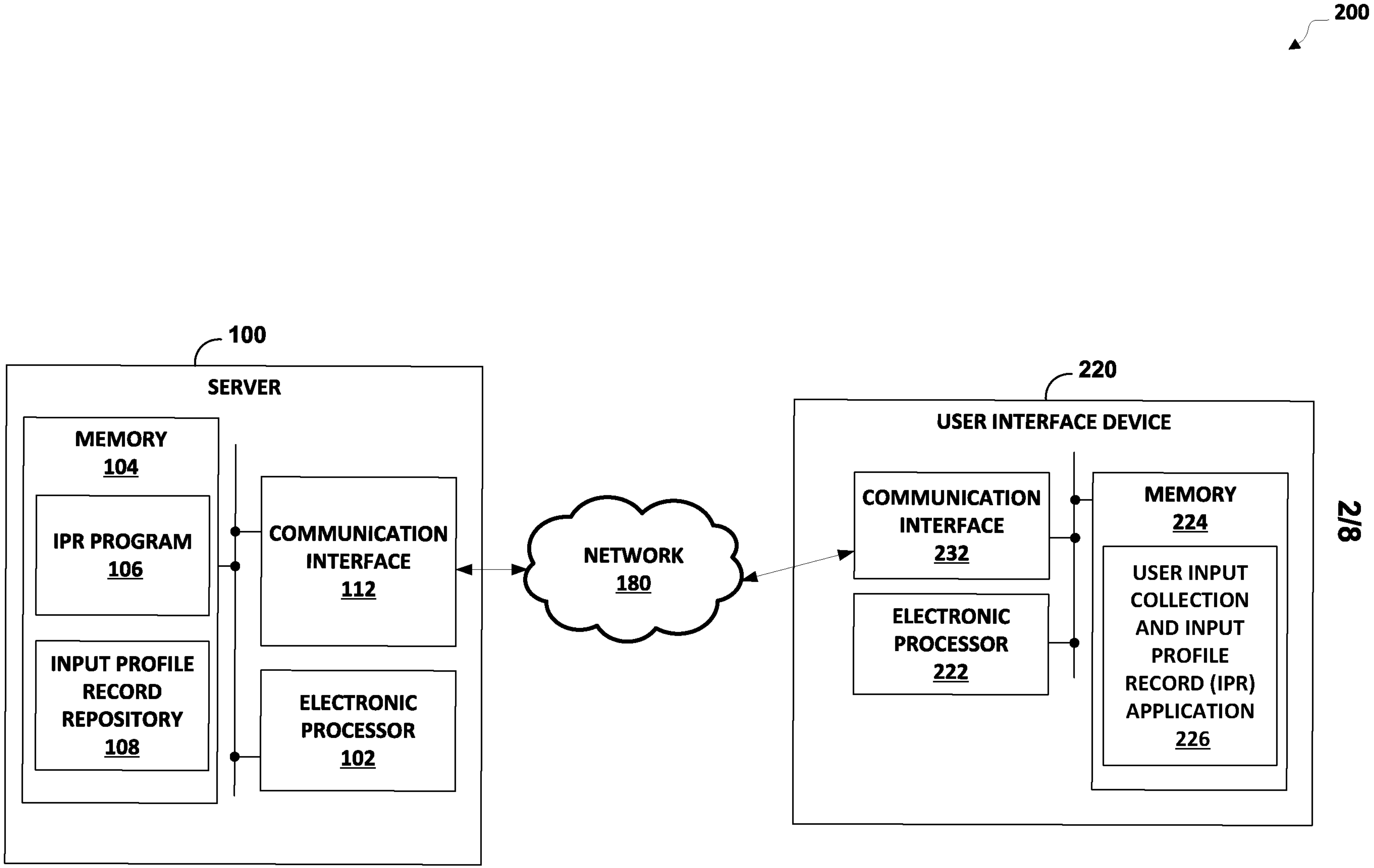

200
100
SERVER
MEMORY 104
IPR PROGRAM 106
INPUT PROFILE RECORD REPOSITORY 108
COMMUNICATION INTERFACE 112
ELECTRONIC PROCESSOR 102
NETWORK 180
220
USER INTERFACE DEVICE
COMMUNICATION INTERFACE 232
ELECTRONIC PROCESSOR 222
MEMORY 224
USER INPUT COLLECTION AND INPUT PROFILE RECORD (IPR) APPLICATION 226

FIG. 2

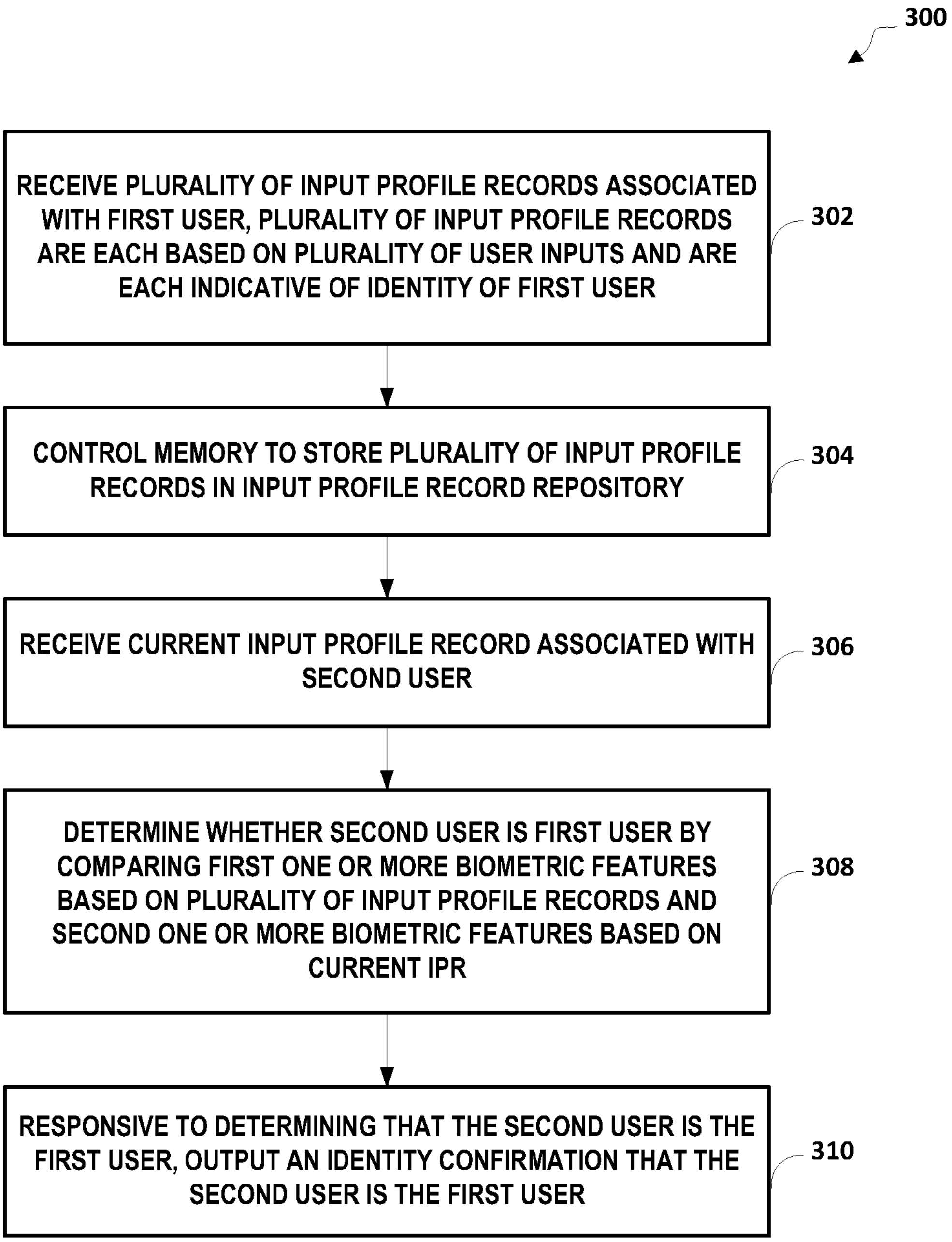
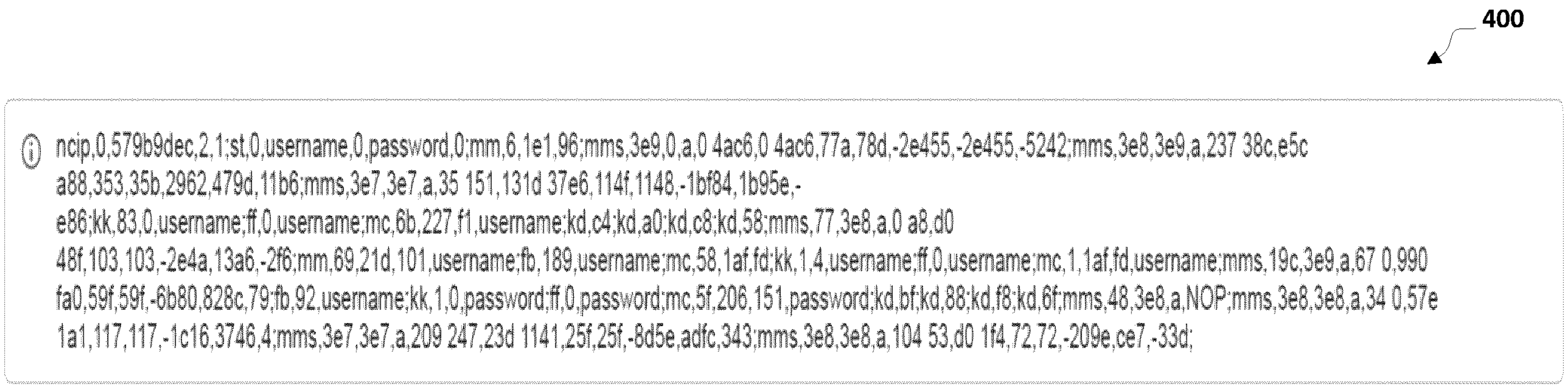
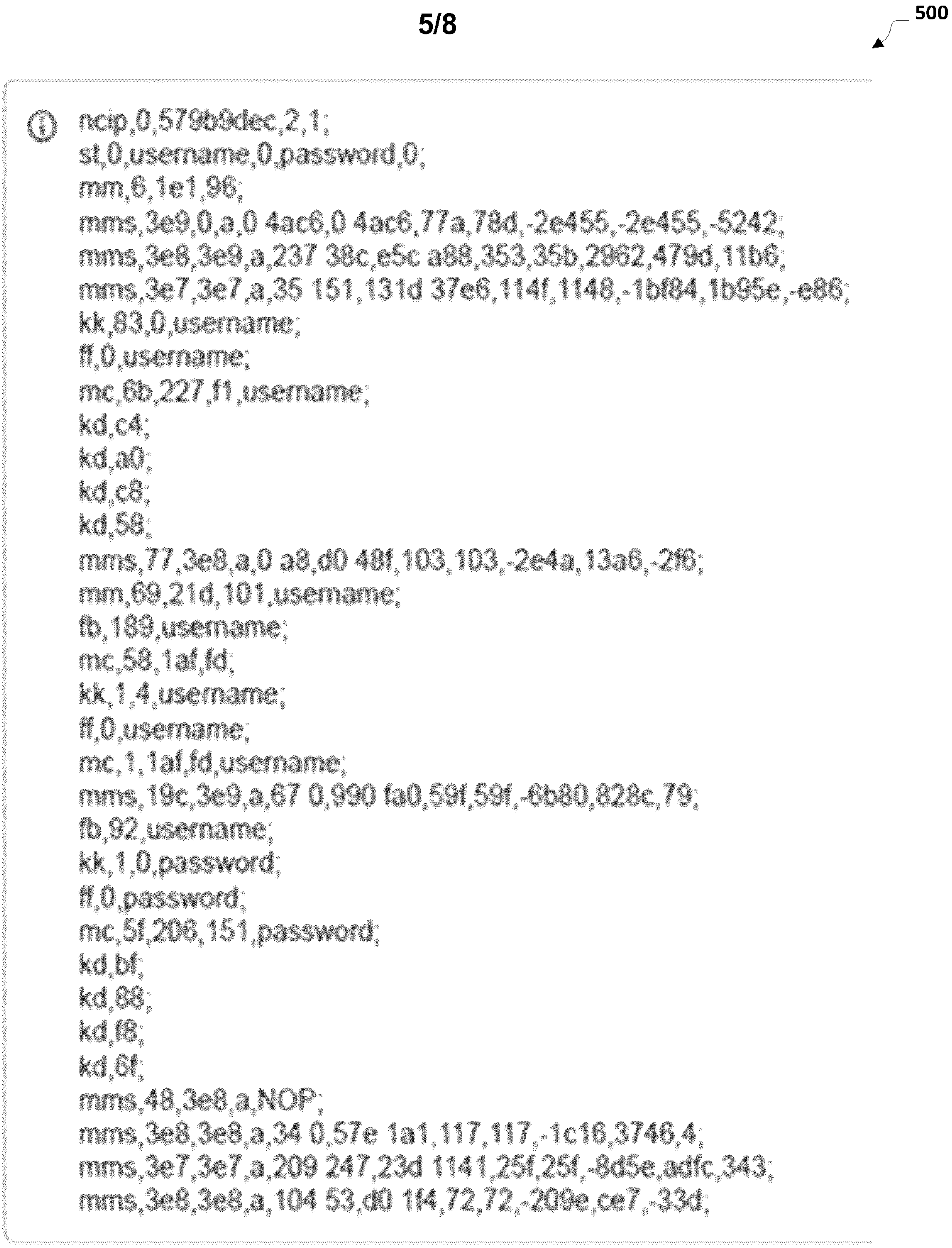

300
RECEIVE PLURALITY OF INPUT PROFILE RECORDS ASSOCIATED WITH FIRST USER, PLURALITY OF INPUT PROFILE RECORDS ARE EACH BASED ON PLURALITY OF USER INPUTS AND ARE EACH INDICATIVE OF IDENTITY OF FIRST USER
302
CONTROL MEMORY TO STORE PLURALITY OF INPUT PROFILE RECORDS IN INPUT PROFILE RECORD REPOSITORY
304
RECEIVE CURRENT INPUT PROFILE RECORD ASSOCIATED WITH SECOND USER
306
DETERMINE WHETHER SECOND USER IS FIRST USER BY COMPARING FIRST ONE OR MORE BIOMETRIC FEATURES BASED ON PLURALITY OF INPUT PROFILE RECORDS AND SECOND ONE OR MORE BIOMETRIC FEATURES BASED ON CURRENT IPR
308
RESPONSIVE TO DETERMINING THAT THE SECOND USER IS THE FIRST USER, OUTPUT AN IDENTITY CONFIRMATION THAT THE SECOND USER IS THE FIRST USER
310

FIG. 3



```
ncip,0,579b9dec,2,1;st,0,username,0,password,0;mm,6,1e1,96;mms,3e9,0,a,0 4ac6,0 4ac6,77a,78d,-2e455,-2e455,-5242;mms,3e8,3e9,a,237 38c,e5c
a88,353,35b,2962,479d,11b6;mms,3e7,3e7,a,35 151,131d 37e6,114f,1148,-1bf84,1b95e,-
e86;kk,83,0,username;ff,0,username;mc,6b,227,f1,username;kd,c4;kd,a0;kd,c8;kd,58;mms,77,3e8,a,0 a8,d0
48f,103,103,-2e4a,13a6,-2f6;mm,69,21d,101,username;fb,189,username;mc,58,1af,fd;kk,1,4,username;ff,0,username;mc,1,1af,fd,username;mms,19c,3e9,a,67 0,990
fa0,59f,59f,-6b80,828c,79;fb,92,username;kk,1,0,password;ff,0,password;mc,5f,206,151,password;kd,bf;kd,88;kd,f8;kd,6f;mms,48,3e8,a,NOP;mms,3e8,3e8,a,34 0,57e
1a1,117,117,-1c16,3746,4;mms,3e7,3e7,a,209 247,23d 1141,25f,25f,-8d5e,adfc,343;mms,3e8,3e8,a,104 53,d0 1f4,72,72,-209e,ce7,-33d;
```

FIG. 4



```
ncip,0,579b9dec,2,1;
st,0,username,0,password,0;
mm,6,1e1,96;
mms,3e9,0,a,0 4ac6,0 4ac6,77a,78d,-2e455,-2e455,-5242;
mms,3e8,3e9,a,237 38c,e5c a88,353,35b,2962,479d,11b6;
mms,3e7,3e7,a,35 151,131d 37e6,114f,1148,-1bf84,1b95e,-e86;
kk,83,0,username;
ff,0,username;
mc,6b,227,f1,username;
kd,c4;
kd,a0;
kd,c8;
kd,58;
mms,77,3e8,a,0 a8,d0 48f,103,103,-2e4a,13a6,-2f6;
mm,69,21d,101,username;
fb,189,username;
mc,58,1af,fd;
kk,1,4,username;
ff,0,username;
mc,1,1af,fd,username;
mms,19c,3e9,a,67 0,990 fa0,59f,59f,-6b80,828c,79;
fb,92,username;
kk,1,0,password;
ff,0,password;
mc,5f,206,151,password;
kd,bf;
kd,88;
kd,f8;
kd,6f;
mms,48,3e8,a,NOP;
mms,3e8,3e8,a,34 0,57e 1a1,117,117,-1c16,3746,4;
mms,3e7,3e7,a,209 247,23d 1141,25f,25f,-8d5e,adfc,343;
mms,3e8,3e8,a,104 53,d0 1f4,72,72,-209e,ce7,-33d;
```

FIG. 5

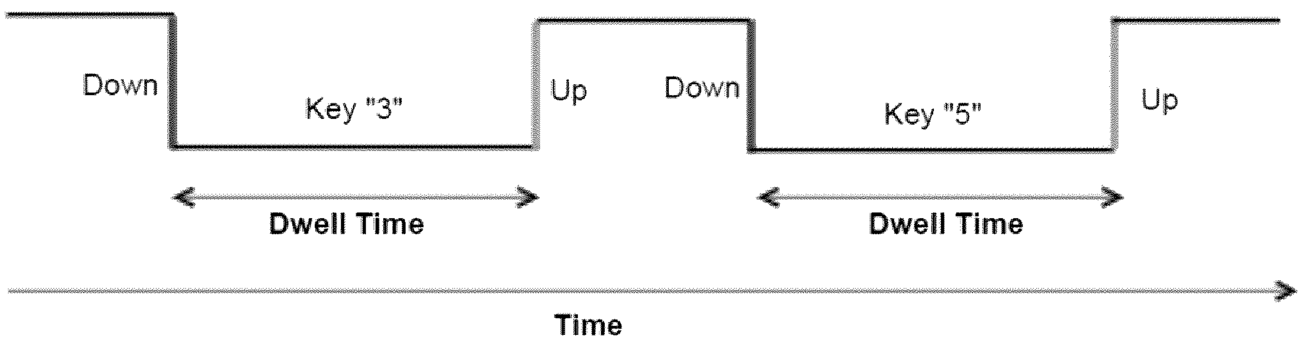

Down
Key "3"
Up
Down
Key "5"
Up
Dwell Time
Dwell Time
Time

FIG. 6

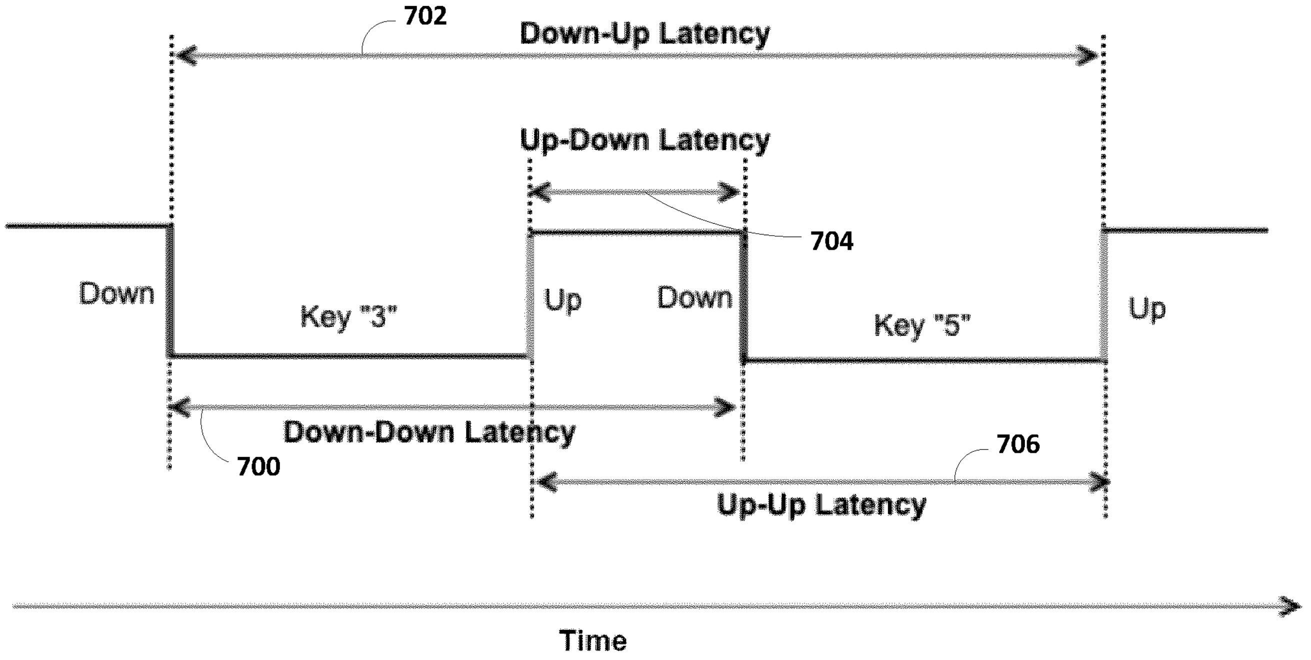

702
Down-Up Latency
Up-Down Latency
704
Down
Key "3"
Up
Down
Key "5"
Up
Down-Down Latency
700
706
Up-Up Latency
Time

FIG. 7

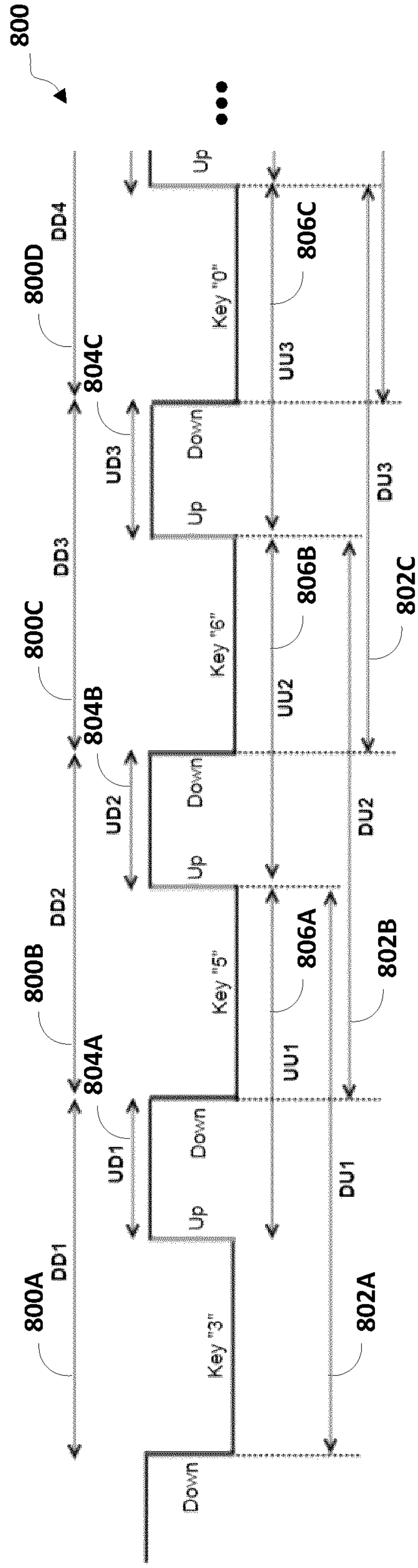

800
800A
DD1
800B
DD2
800C
DD3
800D
DD4
804A
804B
804C
UD1
UD2
UD3
Down
Key "3"
Up
Down
Key "5"
Up
Down
Key "6"
Up
Down
Key "0"
Up
UU1
UU2
UU3
806A
806B
806C
DU1
DU2
DU3
802A
802B
802C

FIG. 8

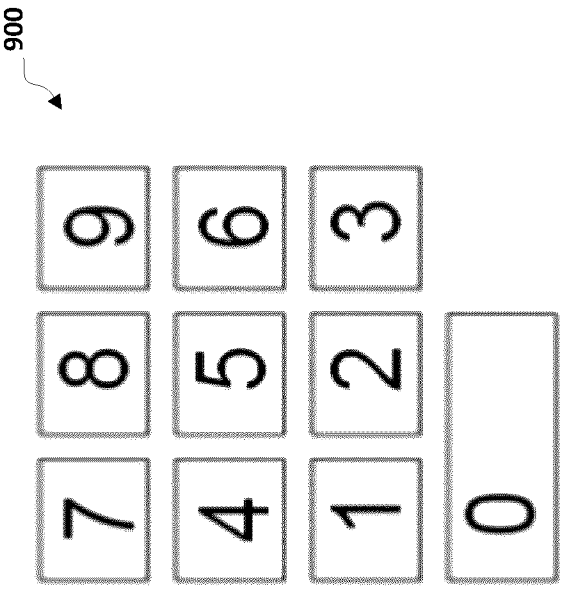

900
7
8
9
4
5
6
1
2
3
0

FIG. 9

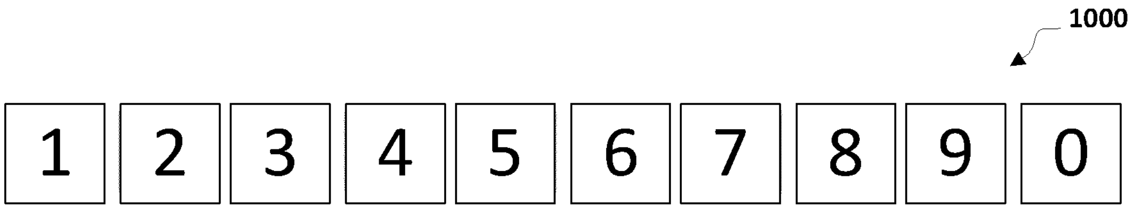

1000
1
2
3
4
5
6
7
8
9
0

FIG. 10

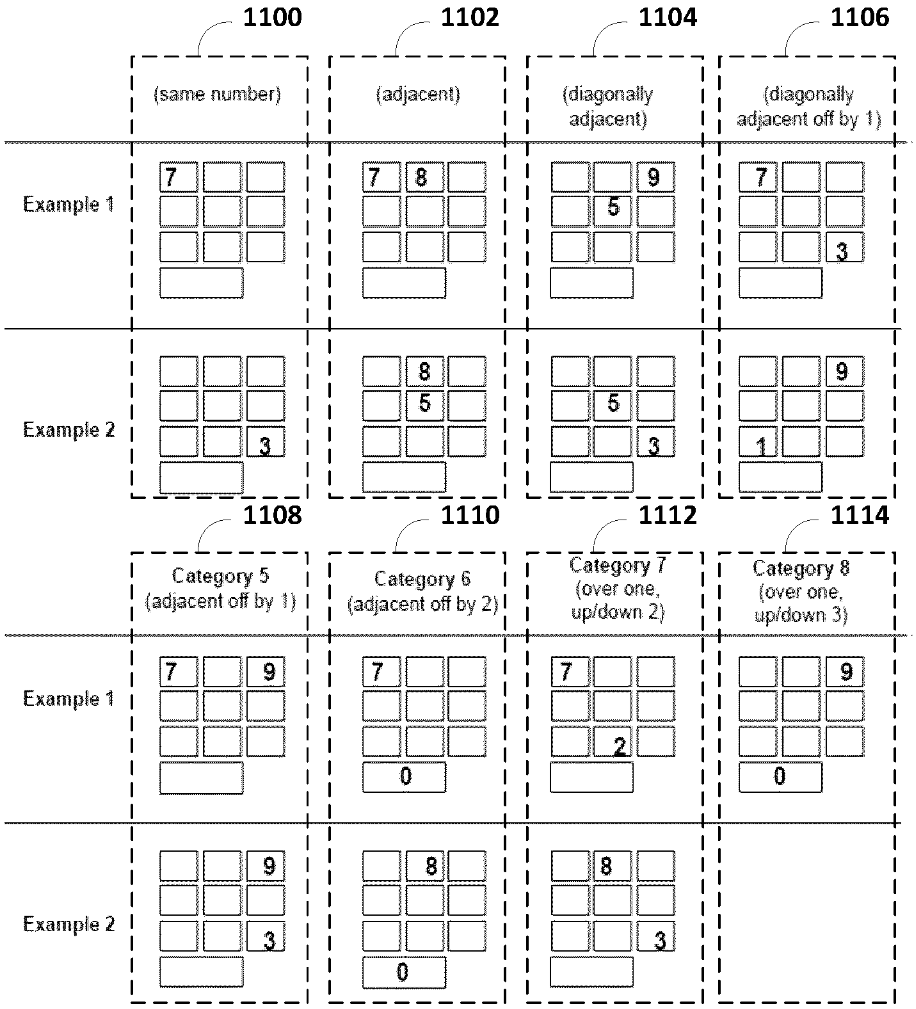

1100
1102
1104
1106
(same number)
(adjacent)
(diagonally adjacent)
(diagonally adjacent off by 1)
Example 1
7
7
8
9
5
7
3
Example 2
3
8
5
5
3
9
1
1108
1110
1112
1114
Category 5 (adjacent off by 1)
Category 6 (adjacent off by 2)
Category 7 (over one, up/down 2)
Category 8 (over one, up/down 3)
Example 1
7
9
7
0
7
2
9
0
Example 2
9
3
8
0
8
3

FIG. 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2021/051365

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***G06F 21/32*** (2013.01)

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)
IPC: ***G06F 21/32*** (2013.01)

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

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Databases: Google patent; Questel/Orbit; Canadian patent database
Search Terms: user identification, keystroke latency, one time password, compare, historical biometric behaviour, current biometric behaviour, user biometric feature, a plurality of historical records, update input profile record periodically, dynamic identification, dwell time, threshold, identity confirm, upper threshold, lower threshold, profile recorder header, Mastercard, Perry McGee, Sik Suen Chan, Anton Laptiev, Cristian Frentiu

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X ----- Y	US 2015/0363785 A1 (PEREZ, K. et al.) 17 December 2015 (17-12-2015) *paragraphs [0001], [0040], [0047], [0055], [0056], [0058], [0059]-[0071], [0075], [0077], [0079], [0080]; Figures 2, 5, 7*	1, 7, 8, 14, 15 ----- 2-6, 9-13, 16-20
Y	US 2015/0095028 A1 (KARPEY, D. et al.) 2 April 2015 (02-04-2015) *paragraph [0055]*	2-4, 9-11, 16-18
Y	US 2008/0306872 A1 (FELSHER, D.) 11 December 2008 (11-12-2008) *paragraphs [0043], [0044], [0055], [0266]*	5, 6, 12, 13, 19, 20

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

*	Special categories of cited documents:	"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
"A"	document defining the general state of the art which is not considered to be of particular relevance	"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
"D"	document cited by the applicant in the international application	"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
"E"	earlier application or patent but published on or after the international filing date	"&"	document member of the same patent family
"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		

Date of the actual completion of the international search
01 November 2021 (01-11-2021)

Date of mailing of the international search report
10 December 2021 (10-12-2021)

Name and mailing address of the ISA/CA
Canadian Intellectual Property Office
Place du Portage I, C114 - 1st Floor, Box PCT
50 Victoria Street
Gatineau, Quebec K1A 0C9
Facsimile No.: 819-953-2476

Authorized officer

Albert Lau (819) 639-8191

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2018/0096354 Al (KOHLI, M.) 5 April 2018 (05-04-2018) *entire document*	
A	WO 2013/006071 Al (SOARES DA SILVA FERREIRA, J.) 10 January 2013 (10-01-2013) *entire document*	
A	US 4,805,222 (YOUNG, J. et al.) 14 February 1989 (14-02-1989) *entire document*	
A	US 7,706,574 B1 (ROSS, G.) 27 April 2010 (27-04-2010) *entire document*	
A	US 2004/0015714 A1 (ABRAHAM, M. et al.) 22 January 2004 (22-01-2004) *entire document*	
A	US 2006/0271790 A1 (CHEN, W.) 30 November 2006 (30-11-2006) *entire document*	
A	US 2013/0055381 A1 (HAO, C. et al.) 28 February 2013 (28-02-2013) *entire document*	
A	WO 97/23816 (WHELAN, M. et al.) 3 July 1997 (03-07-1997) *entire document*	
A	US 2007/0067853 A1 (RAMSEY, M.) 22 March 2007 (22-03-2007) *entire document*	
A	US 2006/0224898 A1 (AHMED, A.) 5 October 2006 (05-10-2006) *entire document*	
A	US 2004/0187037 A1 (CHECCO, J.) 23 September 2004 (23-09-2004) *entire document*	

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US2015363785A1	17 December 2015 (17-12-2015)	None	
US2015095028A1	02 April 2015 (02-04-2015)	US9396730B2	19 July 2016 (19-07-2016)
		US2016300576A1	13 October 2016 (13-10-2016)
		US9607621B2	28 March 2017 (28-03-2017)
US2008306872A1	11 December 2008 (11-12-2008)	US7805377B2	28 September 2010 (28-09-2010)
		AU7182701A	21 January 2002 (21-01-2002)
		US2002010679A1	24 January 2002 (24-01-2002)
		US7587368B2	08 September 2009 (08-09-2009)
		US2010241595A1	23 September 2010 (23-09-2010)
		US8380630B2	19 February 2013 (19-02-2013)
		US2009287837A1	19 November 2009 (19-11-2009)
		US8498941B2	30 July 2013 (30-07-2013)
		US2013159021A1	20 June 2013 (20-06-2013)
		US8600895B2	03 December 2013 (03-12-2013)
		US2014222684A1	07 August 2014 (07-08-2014)
		WO0205061A2	17 January 2002 (17-01-2002)
		WO0205061A3	04 July 2002 (04-07-2002)
US2018096354A1	05 April 2018 (05-04-2018)	US10891617B2	12 January 2021 (12-01-2021)
		CN109716342A	03 May 2019 (03-05-2019)
		EP3520009B1	31 March 2021 (31-03-2021)
		WO2018063509A1	05 April 2018 (05-04-2018)
WO2013006071A1	10 January 2013 (10-01-2013)	None	
US4805222A	14 February 1989 (14-02-1989)	AU6690986A	25 June 1987 (25-06-1987)
		BE905962A	16 April 1987 (16-04-1987)
		CH668844A5	31 January 1989 (31-01-1989)
		CN86108645A	19 August 1987 (19-08-1987)
		DE3642614A1	25 June 1987 (25-06-1987)
		DK624386A	24 June 1987 (24-06-1987)
		ES2003996A6	01 December 1988 (01-12-1988)
		FI865153A	24 June 1987 (24-06-1987)
		FR2592195A1	26 June 1987 (26-06-1987)
		GB2184576A	24 June 1987 (24-06-1987)
		IL81070D0	31 March 1987 (31-03-1987)
		IT8622842D0	23 December 1986 (23-12-1986)
		IT1235762B	28 September 1992 (28-09-1992)
		JPS62157966A	13 July 1987 (13-07-1987)
		KR870006488A	11 July 1987 (11-07-1987)
		NL8603272A	16 July 1987 (16-07-1987)
		NO865224L	24 June 1987 (24-06-1987)
		SE8605446L	24 June 1987 (24-06-1987)
US7706574B1	27 April 2010 (27-04-2010)	None	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2021/051365

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US2004015714A1	22 January 2004 (22-01-2004)	US7260837B2	21 August 2007 (21-08-2007)
		AU4927001A	03 October 2001 (03-10-2001)
		AU2003210825A8	02 September 2003 (02-09-2003)
		CA2403879A1	27 September 2001 (27-09-2001)
		CA2474815C	02 October 2012 (02-10-2012)
		EP1277146A4	21 December 2005 (21-12-2005)
		EP1485776A4	10 December 2008 (10-12-2008)
		MXPA02009205A	10 September 2004 (10-09-2004)
		US7181412B1	20 February 2007 (20-02-2007)
		US7493655B2	17 February 2009 (17-02-2009)
		US7930285B2	19 April 2011 (19-04-2011)
		US8751461B2	10 June 2014 (10-06-2014)
		US10447564B2	15 October 2019 (15-10-2019)
		US2007174295A1	26 July 2007 (26-07-2007)
		US2007276940A1	29 November 2007 (29-11-2007)
		US2009112703A1	30 April 2009 (30-04-2009)
		WO0171620A1	27 September 2001 (27-09-2001)
		WO03067376A3	24 December 2003 (24-12-2003)
US2006271790A1	30 November 2006 (30-11-2006)	US7571326B2	04 August 2009 (04-08-2009)
US2013055381A1	28 February 2013 (28-02-2013)	US9454655B2	27 September 2016 (27-09-2016)
		CN102955908B	12 August 2015 (12-08-2015)
		DE112012003640T5	15 May 2014 (15-05-2014)
		GB2509264B	19 February 2020 (19-02-2020)
		WO2013029412A1	07 March 2013 (07-03-2013)
WO9723816A1	03 July 1997 (03-07-1997)	None	
US2007067853A1	22 March 2007 (22-03-2007)	US7631362B2	08 December 2009 (08-12-2009)
US2006224898A1	05 October 2006 (05-10-2006)	US8230232B2	24 July 2012 (24-07-2012)
		CA2535542C	19 April 2016 (19-04-2016)
		US2004221171A1	04 November 2004 (04-11-2004)
		WO2004097601A1	11 November 2004 (11-11-2004)
US2004187037A1	23 September 2004 (23-09-2004)	US7509686B2	24 March 2009 (24-03-2009)