January 2023

A METHOD AND SYSTEM FOR PROVIDING NON-VISUAL INTERACTION BASED AUTHENTICATION

RAKESH RAMAMURTHY
VISA

AMRENDRA NARAYAN JHA
VISA

MADHUSMITA MOHAPATRA
VISA

AVI BOMB
VISA

SANTOSH KUMAR KVS
VISA

TITLE "A METHOD AND SYSTEM FOR PROVIDING NON-VISUAL INTERACTION BASED AUTHENTICATION"

VISA

RAKESH RAMAMURTHY

AMRENDRA NARAYAN JHA

MADHUSMITA MOHAPATRA

AVI BOMB

SANTOSH KUMAR KVS

TECHNICAL FIELD

[001] The present disclosure generally relates to the field of authentication mechanisms of user equipment. More particularly, but not exclusively, the disclosure relates to a method and a system for providing non-visual interaction based authentication.

BACKGROUND

[002] With advent in technology, various personal devices are available which can be utilised to make human life easy. Such devices include laptops, computers, smart watches, mobile phones, phablets, and the like. Often, such devices entail personal payment/banking information when we utilise the same to facilitate payments. Such information is highly sensitive and must be kept confidential.

[003] Generally, such devices are highly visual in nature, thereby facilitating visual authentication mechanisms. This makes these devices susceptible to shoulder-surfing attacks, which can result in misuse of the personal payment/banking information. Moreover, some specially abled users of such devices may be visually impaired. It is then extremely difficult for these users to safeguard themselves from the shoulder-surfing attacks since they utilise accessibility features. Due to which, there exists a need to develop robust and safe non-visual interaction based authentication mechanism.

[004] The information disclosed in this background of the disclosure section is only for enhancement of understanding of the general background of the invention and should not be taken as an acknowledgement or any form of suggestion that this information forms the prior art already known to a person skilled in the art.

BRIEF DESCRIPTION OF THE DRAWINGS

[005] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, serve to explain the disclosed principles. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears.

[006] The same numbers are used throughout the figures to reference like features and components. Some embodiments of device or system and/or methods in accordance with embodiments of the present subject matter are now described, by way of example only, and with reference to the accompanying figures, in which:

[007] **FIGURE 1** shows an exemplary environment for providing non-visual interaction based authentication in accordance with some embodiments of the present disclosure;

[008] **FIGURE 2** shows an exemplary flowchart illustrating a method for providing non-visual interaction based authentication, in accordance with some embodiments of the present disclosure; and

[009] **FIGURE 3** illustrates a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[010] The figures depict embodiments of the disclosure for purposes of illustration only. One skilled in the art will readily recognize from the following description that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles of the disclosure described herein.

DESCRIPTION OF THE DISCLOSURE

[011] In the present document, the word “exemplary” is used herein to mean “serving as an example, instance, or illustration.” Any embodiment or implementation of the present subject matter described herein as “exemplary” is not necessarily to be construed as preferred or advantageous over other embodiments.

[012] While the disclosure is susceptible to various modifications and alternative forms, specific embodiment thereof has been shown by way of example in the drawings and will be described in detail below. It should be understood, however that it is not intended to limit the disclosure to the particular forms disclosed, but on the contrary, the disclosure is to cover all modifications, equivalents, and alternative falling within the spirit and the scope of the disclosure.

[013] The terms “comprises”, “comprising”, or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a setup, device, or method that comprises a list of components or steps does not include only those components or steps but may include other components or steps not expressly listed or inherent to such setup or device or method. In other words, one or more elements in a device or system or apparatus proceeded by “comprises… a” does not, without more constraints, preclude the existence of other elements or additional elements in the device or system or apparatus.

[014] The terms “an embodiment”, “embodiment”, “embodiments”, “the embodiment”, “the embodiments”, “one or more embodiments”, “some embodiments”, and “one embodiment” mean “one or more (but not all) embodiments of the invention(s)” unless expressly specified otherwise.

[015] The terms “including”, “comprising”, “having” and variations thereof mean “including but not limited to”, unless expressly specified otherwise.

[016] The present disclosure relates to a method and a system for providing non-visual interaction based authentication. Such non-visual interaction based authentication may be provided in any user equipment of a user. Moreover, such non-visual interaction based authentication may be especially provided for specially abled users which utilise accessibility features. The method includes combining non-visual interaction modalities for entering authentication PIN (personal identification number) discreetly, using at least buttons available on the user equipment. The method allows user equipment to be concealed while entering the authentication PIN. Moreover, even when the user equipment is visible, it makes it difficult for an attacker to guess an exact combination of authentication PIN.

[017] In the following detailed description of the embodiments of the disclosure, reference is made to the accompanying drawings that form a part hereof, and in which are shown by way of illustration specific embodiments in which the disclosure may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the disclosure, and it is to be understood that other embodiments may be utilized and that changes may be made without departing from the scope of the present disclosure. The following description is, therefore, not to be taken in a limiting sense.

[018] **Figure 1** shows an exemplary embodiment for providing non-visual interaction based authentication**,** in accordance with some embodiments of the present disclosure.

[019] As shown in Figure 1, an environment 100 comprises a user equipment 101, a server 102, and a communication network 103. The server 102 is communicably connected to the user equipment 101 via the communication network 103. The communication network 103 is implemented as a wired network, a wireless network, or as a combination of both wired and wireless networks.

[020] The user equipment 101 is associated with a user 104 for providing non-visual interaction based authentication of an authentication PIN (Personal Identification Number) for accessing a personal banking portal. In an embodiment, the user 104 is specially abled. The user equipment 101 may include, but not limited to, a mobile phone, a laptop, a computer, a tablet, a phablet, a smart device. In an embodiment, the method and system for providing non-visual interaction based authentication is provided to the user 104 using an application associated with the user equipment 101. Particularly, the application may be a fintech application. The fintech application may be associated with the server 102. Since the server 102 is communicably connected to the user equipment 101, the application may be accessible on the user equipment 101. Inputs for interacting with the application may be received from the user 104 via the user equipment 101.

[021] The user 104 provides inputs via different modalities available in the user equipment 101 to access the personal banking portal associated with the user 104. Such modalities may include, but not limited to, buttons, fingerprint, voice, face, and the like. For instance, buttons on the user equipment 101 may be pressed to generate the input. When the modality is the fingerprint, a fingerprint scanner may be used to scan a fingerprint of the user 104. When the modality is the voice, a voice of the user 104 may be recorded and matched using a microphone. When the modality is the face, a face of the user 104 may be recorded and matched using a camera. The inputs provided by the user 104 may include the authentication PIN provided via non-visual interaction of the user 104 with the user equipment 101. The non-visual interaction may be implemented via different modalities of the user equipment 101, or a combination of the modalities. The authentication PIN may be inputted as a combination of options on a given modality, or as a combination of the multiple modalities. In an example, the authentication PIN may be entered using a combination of buttons available on the user equipment 101. Herein, the user 104 may press the buttons based on a predefined combination/encoded pattern for inputting the authentication PIN. The authentication PIN is authenticated by mapping with a registered authentication PIN previously stored at the server 102. If the authentication PIN corresponds to the registered authentication PIN, then the authentication PIN

is correct, and then the user 104 is provided access to the personal banking portal. However, if the authentication PIN is incorrect, the user 104 is prompted to re-enter the authentication PIN.

[022] **Figure 2** shows an exemplary flowchart illustrating a method 200 for providing non-visual interaction based authentication, in accordance with some embodiments of the present disclosure.

[023] As shown in **Figure 2**, the method 200 for providing non-visual interaction based authentication is performed for the user 104. In an embodiment, the user 104 is specially abled and utilises accessibility features. It will be appreciated that the present disclosure provides a simple and effective solution for safe and robust authentication. The method for providing non-visual interaction based authentication is described herein with respect to the exemplary flowchart provided in Figure 2.

[024] At step 202, the user 104 accesses the fintech application. The fintech application may be associated with one or more issuers and allow the user 104 to access the personal banking portal. It will be appreciated that the user 104 may access the fintech application via user equipment 101 associated with the user 104. The user 104 provides inputs to the user equipment 101 to access the personal banking portal, perform a transaction, check an amount, and the like.

[025] At step 204, the user 104 logs into the personal banking portal using regular authentication. Herein, the regular authentication pertains to currently existing authentication mechanism of entering a PIN, a fingerprint lock, a face lock, a retina lock, and the like. Any such existing authentication mechanism which are supported by the fintech application and the user equipment 101 may be utilised.

[026] At step 206, the user 104 is prompted to enter the authentication PIN. It will be appreciated that the authentication PIN may entered by at least one of: using buttons available on the user equipment 101, combining non-visual interaction modalities available on the user equipment 101.

[027] When the authentication PIN is entered using buttons available on the user equipment 101, it may be entered without the user 104 even looking at the user equipment 101. In such manner, the user equipment 101may be concealed while entering the authentication PIN. Such buttons being utilised may include volume up button, volume down button, screen lock button, power off button, and the like. Based on pressed buttons, digits from 0 to 9 may be encoded to enter the authentication PIN.

[028] In an exemplary embodiment, the digits from 0 to 9 are encoded with respect to the buttons such that each digit/action corresponds to one or more buttons. Herein, digit 0 may be attained by pressing the screen lock button twice consecutively. Digit 1 may be attained by pressing the screen lock button once. Digit 2 may be attained by pressing the volume down button once. Digit 3 may be attained by pressing the volume down button and the screen lock button. Digit 4 may be attained by pressing the volume up button once. Digit 5 may be attained by pressing the volume up button and the screen lock button. Digit 6 may be attained by pressing the volume down button and the volume up button. Digit 7 may be attained by pressing the volume down button, the volume up button, and the screen lock button. Digit 8 may be attained by pressing the volume up button twice consecutively. Digit 9 may be attained by pressing the volume down button twice consecutively. A selection may be confirmed by pressing the power off button once. A recent digit may be removed by a two-finger tap.

[029] Herein, in an example, if the user 104 wishes to enter the authentication PIN ‘4567’, then the user 104 may press the buttons in the following series: the volume up button once for digit 4, the power off button for confirming digit 4, the volume up button and the screen lock button for digit 5, the power off button for confirming digit 5, the volume down button and the volume up button for digit 6, the power off button for confirming digit 6, the volume down button, the volume up button, and the screen lock button for digit 7, and the power off button for confirming digit 7. Moreover, in case the user 104 makes any mistake while inputting the above series, they may utilise the two-finger tap to remove the most recent digit.

[030] When the authentication PIN is entered using multiple non-visual interaction modalities available on the user equipment 101, two or more biometric modalities may be utilised. A combination of such modalities may be unique for users 104, increasing the reliability and accuracy of the present disclosure since it is difficult for an attacker to simultaneously spoof multiple biometric traits.

[031] In an exemplary embodiment, following combination of modalities may be utilised for entering the authentication PIN: keystroke and voice modalities; voice, location, multitouch, locomotion, accelerometer, GPS (global positioning system) and touch screen modalities; face, voice, and keystroke modalities; touch, accelerometer, and gyroscope modalities, gait and location tracking modalities, keystroke, handwriting, swipe and pinch and slide modalities.

[032] At step 208, whether the authentication PIN entry is completed and captured is checked. If the same is completed, then the method advances to step 210. In such cases, the authentication PIN is encoded and stored at the server 102 as the registered authentication PIN using standard mapping approaches. Herein, the authentication PIN is authenticated only when it corresponds to the registered authentication PIN. However, if the same is not completed, then the method retreats to step 206, wherein capturing of the authentication PIN is completed until it is confirmed by the user 104.

[033] At step 210, data pertaining to the authentication PIN is stored in the server 102, when the authentication PIN is correct. The authentication PIN is mapped to the registered authentication PIN previously stored at the server 102 for authenticating the same. If the authentication PIN is correct, then the user 104 is provided access to the personal banking portal. The authentication PIN as entered by the user 104 is validated using the authentication PIN stored in the server 102, using the mapped value and the standard mapping approaches. If the authentication PIN is incorrect, the method retreats to step 206, wherein the user 104 is prompted to re-enter the authentication PIN. If the user 104 incorrectly enters the authentication number of PIN for a pre-defined number of times, then an account associated with the personal banking portal of the user 104 is locked. In an example, the pre-defined number of times may be three times.

[034] Once the authentication PIN is stored in the server 102, it may be utilised for access to the personal banking portal by the user 104 at any given time. The user 104 may directly enter the authentication PIN to access the personal banking portal. Moreover, the user 104 may utilise the authentication PIN in addition with or instead of the regular authentication to access the personal banking portal.

[035] **Figure 3** illustrates a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[036] In an embodiment, the computer system 300 for providing non-visual interaction based authentication. The computer system 300 may include a central processing unit (“CPU” or “processor”) 302. The processor 302 may comprise at least one data processor for executing program components for executing user or system-generated business processes. The processor 302 may include specialized processing units such as integrated system (bus) controllers, memory management control units, floating point units, graphics processing units, digital signal processing units, etc.

[037] The processor 302 may be disposed in communication with one or more input/output (I/O) devices (312 and 313) via I/O interface 301. The I/O interface 301 may employ communication protocols/methods such as, without limitation, audio, analog, digital, stereo, IEEE-1394, serial bus, Universal Serial Bus (USB), infrared, PS/2, BNC, coaxial, component, composite, Digital Visual Interface (DVI), high-definition multimedia interface (HDMI), Radio Frequency (RF) antennas, S-Video, Video Graphics Array (VGA), IEEE 802.n /b/g/n/x, Bluetooth, cellular (e.g., Code-Division Multiple Access (CDMA), High-Speed Packet Access (HSPA+), Global System For Mobile Communications (GSM), Long-Term Evolution (LTE) or the like), etc.

[038] Using the I/O interface 301, the computer system 300 may communicate with one or more I/O devices (312 and 313). In some implementations, the processor 302 may be disposed in communication with a communication network 309 via a network interface 303. The network interface 303 may employ connection protocols including, without limitation, direct connect, Ethernet (e.g., twisted pair 10/100/1000 Base T), Transmission Control Protocol/Internet Protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc. Using the network interface 303 and the communication network 309, the computer system 300 may be connected to the server 102. The communication network 309 can be implemented as one of the several types of networks, such as intranet or any such wireless network interfaces. The communication network 309 may either be a dedicated network or a shared network, which represents an association of several types of networks that use a variety of protocols, for example, Hypertext Transfer Protocol (HTTP), Transmission Control Protocol/Internet Protocol (TCP/IP), Wireless Application Protocol (WAP), etc., to communicate with each other. Further, the communication network 309 may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, etc.

[039] In some embodiments, the processor 302 may be disposed in communication with a memory 305 e.g., RAM, and ROM, etc., via a storage interface 304. The storage interface 304 may connect to memory 305 including, without limitation, memory drives, removable disc drives, etc., employing connection protocols such as Serial Advanced Technology Attachment (SATA), Integrated Drive Electronics (IDE), IEEE-1394, Universal Serial Bus (USB), fiber channel, Small Computer Systems Interface (SCSI), etc. The memory drives may further include a drum, magnetic disc drive, magneto-

optical drive, optical drive, Redundant Array of Independent Discs (RAID), solid-state memory devices, solid-state drives, etc.

[040] The memory 305 may store a collection of program or database components, including, without limitation, user/application, an operating system 307, a web browser 308, a user interface 306, and the like. In some embodiments, computer system 300 may store user/application data, such as the data, variables, records, etc. as described in this invention. Such databases may be implemented as fault-tolerant, relational, scalable, secure databases such as Oracle or Sybase.

[041] The operating system 307 may facilitate resource management and operation of the computer system 300. Examples of operating systems include, without limitation, Apple Macintosh TM OS X TM, UNIX TM, Unix-like system distributions (e.g., Berkeley Software Distribution (BSD), FreeBSD TM, Net BSD TM, Open BSD TM, etc.), Linux distributions (e.g., Red Hat TM, Ubuntu TM, K-Ubuntu TM, etc.).

[042] International Business Machines (IBM TM) OS/2 TM, Microsoft Windows TM (XP TM, Vista/7/8, etc.), Apple iOS TM, Google Android TM, Blackberry TM Operating System (OS), or the like. A user interface may facilitate display, execution, interaction, manipulation, or operation of program components through textual or graphical facilities. For example, user interfaces may provide computer interaction interface elements on a display system operatively connected to the computer system 300, such as cursors, icons, check boxes, menus, windows, widgets, etc. Graphical User Interfaces (GUIs) may be employed, including, without limitation, Apple TM Macintosh TM operating systems' Aqua TM, IBM TM OS/2 TM, Microsoft TM Windows TM (e.g., Aero, Metro, etc.), Unix X-Windows TM, web interface libraries (e.g., ActiveX, Java, JavaScript, AJAX, HTML, Adobe Flash, etc.), or the like.

[043] The illustrated steps are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to

persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments. Also, the words "comprising," "having," "containing," and "including," and other similar forms are intended to be equivalent in meaning and be open ended in that an item or items following any one of these words is not meant to be an exhaustive listing of such item or items or meant to be limited to only the listed item or items.

[044] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term “computer readable medium” should be understood to include tangible items and exclude carrier waves and transient signals, i.e., are non-transitory.

[045] Examples include random access memory (RAM), read-only memory (ROM), volatile memory, non-volatile memory, hard drives, CD ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[046] The terms "an embodiment", "embodiment", "embodiments", "the embodiment", "the embodiments", "one or more embodiments", "some embodiments", and "one embodiment" mean "one or more (but not all) embodiments of the invention(s)" unless expressly specified otherwise.

[047] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to", unless expressly specified otherwise.

[048] The enumerated listing of items does not imply that any or all the items are mutually exclusive, unless expressly specified otherwise. The terms "a", "an" and "the" mean "one or more", unless expressly specified otherwise.

[049] A description of an embodiment with several components in communication with each other does not imply that all such components are required. On the contrary, a variety of optional components are described to illustrate the wide variety of possible embodiments of the invention.

[050] When a single device or article is described herein, it may be readily apparent that more than one device/article (whether they cooperate) may be used in place of a single device/article. Similarly, where more than one device or article is described herein (whether or not they cooperate), it may be readily apparent that a single device/article may be used in place of the more than one device or article, or a different number of devices/articles may be used instead of the shown number of devices or programs. The functionality and/or the features of a device may be alternatively embodied by one or more other devices which are not explicitly described as having such functionality/features. Thus, other embodiments of the invention need not include the device itself.

[051] The illustrated operations of **Figure 2** show certain events occurring in a certain order. In alternative embodiments, certain operations may be performed in a different order, modified, or removed. Moreover, steps may be added to the above-described logic and still conform to the described embodiments. Further, operations described herein may occur sequentially or certain operations may be processed in parallel. Yet further, operations may be performed by a single processing unit or by distributed processing units.

[052] Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter.

A METHOD AND SYSTEM FOR
PROVIDING NON-VISUAL INTERACTION BASED AUTHENTICATION

ABSTRACT

The present disclosure relates to a method and system for providing non-visual interaction based authentication. Such non-visual interaction based authentication may be provided in any user equipment of a user. Moreover, such non-visual interaction based authentication may be especially provided for specially abled users which utilise accessibility features. The method includes combining non-visual interaction modalities for entering authentication pin discreetly, using buttons or other modalities available on the user equipment.

1/3

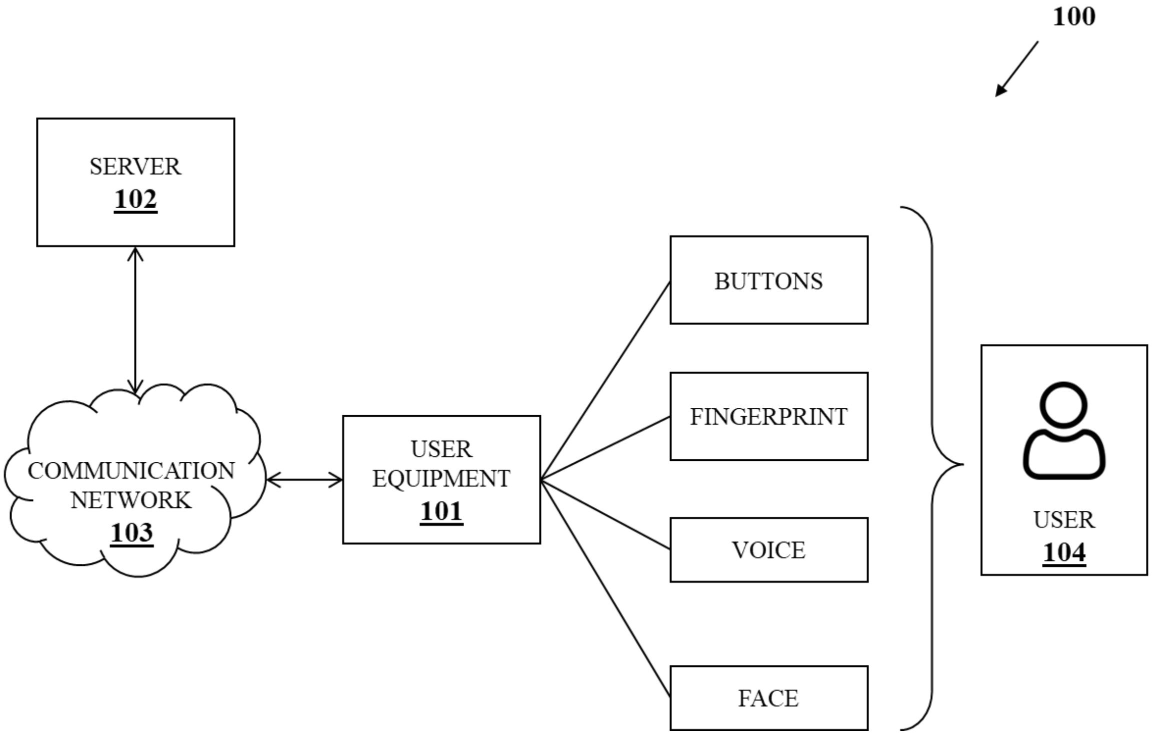
100
SERVER
102
COMMUNICATION
NETWORK
103
USER
EQUIPMENT
101
BUTTONS
FINGERPRINT
VOICE
FACE
USER
104

FIGURE 1

2/3

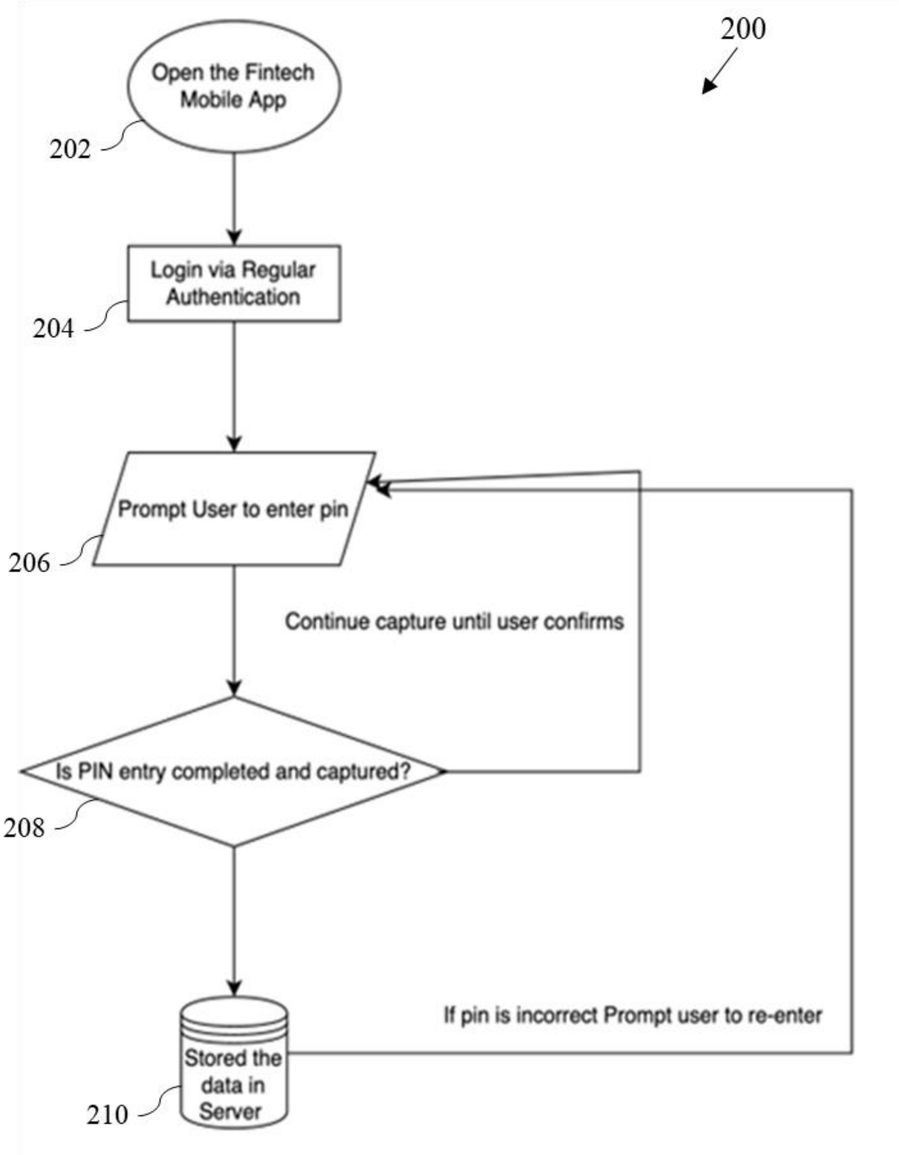
200
Open the Fintech Mobile App
202
Login via Regular Authentication
204
Prompt User to enter pin
206
Continue capture until user confirms
Is PIN entry completed and captured?
208
If pin is incorrect Prompt user to re-enter
Stored the data in Server
210

FIGURE 2

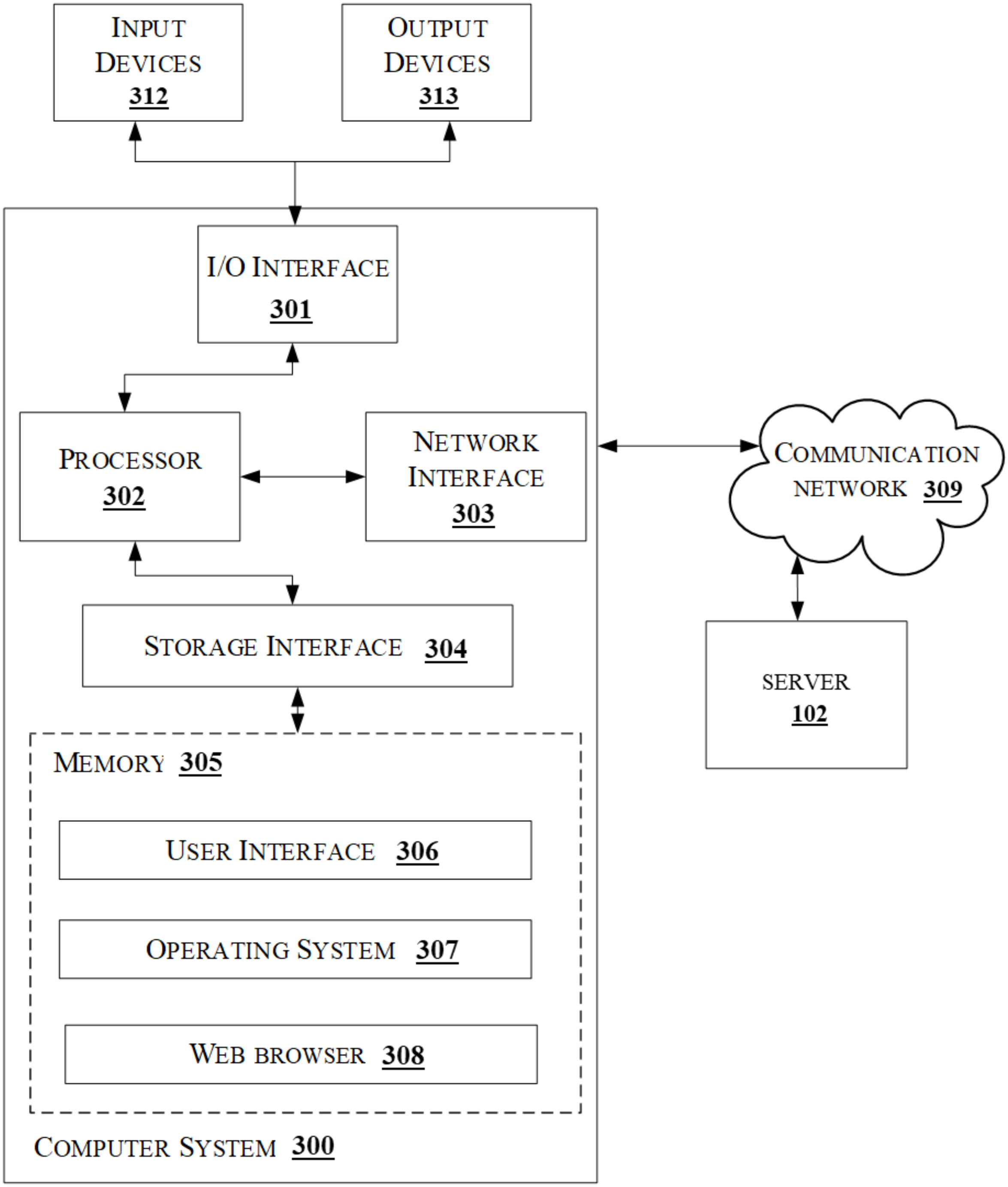
INPUT DEVICES 312
OUTPUT DEVICES 313
I/O INTERFACE 301
PROCESSOR 302
NETWORK INTERFACE 303
COMMUNICATION NETWORK 309
STORAGE INTERFACE 304
SERVER 102
MEMORY 305
USER INTERFACE 306
OPERATING SYSTEM 307
WEB BROWSER 308
COMPUTER SYSTEM 300

FIGURE 3