November 2020

METHOD AND SYSTEM FOR FACILITATING PAYMENT TRANSACTIONS IN OFFLINE MODE

MOHANKUMAR RAMACHANDRAN
VISA

METHOD AND SYSTEM FOR FACILITATING PAYMENT TRANSACTIONS IN OFFLINE MODE

VISA

INVENTOR:

MOHANKUMAR RAMACHANDRAN

TECHNICAL FIELD

[0001] This disclosure relates to a method and a system for facilitating payment transactions in an offline mode.

BACKGROUND

[0002] Card readers such as Point of Sale (POS) terminals are available to process electronic payment transactions between a merchant and a customer. However, both the devices [POS associated with the merchant and mobile device associated with customer] are required to be online to be able to send payment information to remote authorization servers, which then confirms the payment information. However, in some situations, one of the devices may be in a location where the internet connection is either unavailable or inconsistent for establishing connection between the devices. At present offline mobile payments at POS terminal is performed using Near-Field-Communication (NFC) enabled mobile devices, but most of the mobile device which does not have NFC are not able to use offline mobile payments.

[0003] In order to overcome the above-mentioned shortcomings, the present invention facilitates payment transactions in offline mode using WiFi feature by establishing secure WiFi connection between a mobile device and a WiFi enabled POS terminal.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Additional advantages and details are explained in greater detail below with reference to the exemplary embodiments that are illustrated in the accompanying schematic figures, in which:

[0005] Fig.1 illustrates a block diagram of a system for facilitating payment transactions in offline mode in accordance with some embodiments of the present disclosure.

[0006] Fig.2 illustrates a process for registering card holder/user details with a server for generating a unique Identification (ID) in accordance with some embodiments of the present disclosure.

[0007] Fig.3 illustrates a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

DESCRIPTION OF THE DISCLOSURE

[0008] It is to be understood that the present disclosure may assume various alternative variations and step sequences, except where expressly specified to the contrary. It is also to be understood that the specific devices and processes illustrated in the attached drawings and described in the following specification are simply exemplary and non-limiting embodiments or aspects. Hence, specific dimensions and other physical characteristics related to the embodiments or aspects disclosed herein are not to be considered as limiting.

[0009] For purposes of the description hereinafter, the terms “end,” “upper,” “lower,” “right,” “left,” “vertical,” “horizontal,” “top,” “bottom,” “lateral,” “longitudinal,” and derivatives thereof shall relate to the disclosed subject matter as it is oriented in the drawing figures. However, it is to be understood that the disclosed subject matter may assume various alternative variations and step sequences, except where expressly specified to the contrary. It is also to be understood that the specific devices and processes illustrated in the attached drawings, and described in the following specification, are simply exemplary embodiments or aspects of the disclosed subject matter. Hence, specific dimensions and other physical characteristics related to the embodiments or aspects disclosed herein are not to be considered as limiting unless otherwise indicated.

[0010] No aspect, component, element, structure, act, step, function, instruction, and/or the like used herein should be construed as critical or essential unless explicitly described as such. Also, as used herein, the articles “a” and “an” are intended to include one or more items and may be used interchangeably with “one or more” and “at least one.” Furthermore, as used herein, the term “set” is intended to include one or more items (e.g., related items, unrelated items, a combination of related and unrelated items, and/or the like) and may be used interchangeably with “one or more” or “at least one.” Where only one item is intended, the term “one” or similar language is used. Also, as used herein, the terms “has,” “have,” “having,” or the like are intended to be open-ended terms. Further, the phrase “based on” is intended to mean “based at least partially on” unless explicitly stated otherwise.

[0011] As used herein, the terms “communication” and “communicate” may refer to the reception, receipt, transmission, transfer, provision, and/or the like of information (e.g., data, signals, messages, instructions, commands, and/or the like). For one unit (e.g., a device, a system, a component of a device or system, combinations thereof, and/or the like) to be in communication with another unit means that the one unit is able to directly or indirectly receive information from and/or transmit information to the other unit. This may refer to a direct or indirect connection (e.g., a direct communication connection, an indirect communication connection, and/or the like) that is wired and/or wireless in nature. Additionally, two units may be in communication with each other even though the information transmitted may be modified, processed, relayed, and/or routed between the first and second unit. In some non-limiting embodiments or aspects, a message may refer to a network packet (e.g., a data packet and/or the like) that includes data. It will be appreciated that numerous other arrangements are possible.

[0012] As used herein, the term “computing device” may refer to one or more electronic devices that are configured to directly or indirectly communicate with or over one or more networks. A computing device may be a mobile or portable computing device, a desktop computer, a server, and/or the like. Furthermore, the term “computer” may refer to any computing device that includes the necessary components to receive, process, and output data, and normally includes a display, a processor, a memory, an input device, and a network interface. A “computing system” may include one or more computing devices or computers. An “application” or “application program interface” (API) refers to computer code or other data sorted on a computer-readable medium that may be executed by a processor to facilitate the interaction between software components, such as a client-side front-end and/or server-side back-end for receiving data from the client. An “interface” refers to a generated display, such as one or more graphical user interfaces (GUIs) with which a user may interact, either directly or indirectly (e.g., through a keyboard, mouse, touchscreen, etc.). Further, multiple computers, e.g., servers, or other computerized devices, such as an autonomous vehicle including a vehicle computing system, directly or indirectly communicating in the network environment may constitute a “system” or a “computing system”.

[0013] It will be apparent that systems and/or methods, described herein, can be implemented in different forms of hardware, software, or a combination of hardware and software. The actual specialized control hardware or software code used to implement these systems and/or methods is not limiting of the implementations. Thus, the operation and behavior of the systems and/or methods are described herein without reference to specific software code, it being understood that software and hardware can be designed to implement the systems and/or methods based on the description herein.

[0014] Some non-limiting embodiments or aspects are described herein in connection with thresholds. As used herein, satisfying a threshold may refer to a value being greater than the threshold, more than the threshold, higher than the threshold, greater than or equal to the threshold, less than the threshold, fewer than the threshold, lower than the threshold, less than or equal to the threshold, equal to the threshold, etc.

[0015] Fig.1 illustrates block diagram of a system for facilitating payment transactions in offline mode in accordance with some embodiments of the present disclosure.

[0016] As shown in Fig.1, the system 100 may include a mobile device 101, a Point of Sale (POS) terminal 103 used at a merchant location, an acquirer 105 associated with the merchant and a server 107 associated with an issuer 109. In order to establish a secure connection between the mobile device 101 and the POS terminal 103, a user [also referred to as a card holder] of the mobile device 101 may first provide mobile number details at the POS terminal 103. Upon receiving the mobile number details, the POS terminal 103 may create a message with mobile number in ISO 8583 standard [Hash value of Mobile number] and transmits the message to the acquirer 105. The acquirer 105 may transmit the message to the server 107. The server 107 may check for details of account holder in its database and upon successful verification, the server 107 may generate a unique ID [also referred as first ID] based on a first technique and transmits the first ID to the acquirer 105. The acquirer 105 may transmit the first ID to the POS terminal 103. The first ID may be a one-time generated unique ID. Upon receiving the first ID, the POS terminal 103 may set the received first ID as password and create a WiFi Hotspot.

[0017] In an embodiment, the process for generating the first ID based on the first technique is illustrated below.

1. At first the server 107 matches the message [Mobile Number Hash Value] received against the data stored in a database associated with the server 107. As an example, the database may include data such as {MobileHash1: [Token1, counter1], MobileHash2: [Token 2, counter 2] and the like. As an example, the Mobile Number Hash Value may match with MobileHash1: [Token1, counter1].
2. Thereafter, the server 107 may calculate the Hash value using SHA3-224 with [Token1, counter1] data and then counter 1 is incremented. As an example, the calculated Hash value may be SHA3-224(string ([Token1, counter1]))). The Hash value using SHA3-224 may equal to 56 hexadecimal digits], and these 56 digits are transmitted to the POS terminal 103 so that they can be used as a WiFi Hotspot password.

[0018] In an embodiment, once the WiFi Hotspot is created at the POS terminal 103, the card holder may provide a password which was set during registration process in the mobile device 101 based on which a unique ID [second ID] is generated on card holder's mobile device 101 using a second technique. The process of generating unique ID based on password set by the user during registration process is explained in Fig.2. The second ID and the first ID are same as they are generated by the first technique and the second technique implemented by the server 107 and hence a secure connection is established between the POS terminal 103 and the mobile device 101 of the user for payment processing.

[0019] Fig.2 illustrates a process for registering card holder details with a server 107 for generating a unique ID in accordance with some embodiments of the present disclosure.

[0020] In an embodiment, during registration process, the user may provide details such as payment account information, mobile number, Permanent Account Number (PAN) details and security code in an application configured in the mobile device 101 of the user. The application may be associated with the server 107. The server 107 may verify details provided by the user with the issuer 109 of a card associated with the user in order to determine whether a token generation is applicable for the card holder. In an embodiment, if the verification is successful, the server 107 may generate a unique ID (second ID), using a second technique, along with a random counter and provide the second ID and the random number to the mobile device 101. The unique ID generated, random counter and hash of mobile number are mapped and stored in the database associated with the server 107.

[0021] In an embodiment, the process for generating the second ID based on the second technique is illustrated below.

1. In an embodiment, N number of SHA3-224 Hash values may be calculated using [Token1, counter1], [Token1, counter1 - i], [Token1, counter1 - i*2]……[Token1,counter1 - i*N-1] data and then counter1 is incremented. As an example, SHA3-224(string([Token1,counter1])),………SHA3-224(string([Token1,counter1-i*N-1]))), where N is number of failures accepted before resync, and I is the step value, both N and I can be tweaked based on security reasons.
2. Each Hash value represents a 56 digit data, which is used to try to connect with the POS terminal 103. One of the passwords out of pool of N passwords will match and a secure connection is established, else the card holder has to resync by connecting to the network.
3. If resync is necessary, then the card holder has to be online, and the server 107 may reset the counter to a random number and same will be stored in mobile for future offline payments.

[0022] Once the secure connection is established between the mobile device 101 and the POS terminal 103, the available payment processing techniques may be implemented for performing payment transactions.

[0023] Some of the advantages of the present disclosure are listed below.

[0024] The present disclosure overcomes the need for NFC feature for performing offline payment transaction at POS terminal.

[0025] The present disclosure establishes secure WiFi connection between the POS terminal and mobile device for payment transaction processing.

[0026] Fig.3 illustrates a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[0027] In an embodiment, the computer system 300 may be used to implement the system. The computer system 300 may include a central processing unit ("CPU" or "processor") 302. The processor 302 may include at least one data processor for passive liveness detection. 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.

[0028] 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 employ communication protocols/methods such as, without limitation, audio, analog, digital, monoaural, radio corporation of America (RCA) connector, stereo, IEEE-1394 high speed serial bus, serial bus, universal serial bus (USB), infrared, personal system/2 (PS/2) port, bayonet neill-concelman (BNC) connector, coaxial, component, composite, digital visual interface (DVI), high-definition multimedia interface (HDMI), radio frequency (RF) antennas, S-Video, video graphics array (VGA), IEEE 802.11b/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), worldwide interoperability for microwave access (WiMax), or the like, etc.

[0029] Using the I/O interface 301, the computer system 300 may communicate with one or more I/O devices such as input devices 312 and output devices 313. For example, the input devices 312 may be an antenna, keyboard, mouse, joystick, (infrared) remote control, camera, card reader, fax machine, dongle, biometric reader, microphone, touch screen, touchpad, trackball, stylus, scanner, storage device, transceiver, video device/source, etc. The output devices 313 may be a printer, fax machine, video display (e.g., cathode ray tube (CRT), liquid crystal display (LCD), light-emitting diode (LED), plasma, plasma display panel (PDP), organic light-emitting diode display (OLED) or the like), audio speaker, etc.

[0030] In some embodiments, the processor 302 may be disposed in communication with a communication network 309 via a network interface 303. The network interface 303 may communicate with the communication network 309. 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. The communication network 309 may include, without limitation, a direct interconnection, local area network (LAN), wide area network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, etc. Using the network interface 303 and the communication network 309, the computer system 300 may communicate with a database 314, which may be the enrolled templates database 113. The network interface 303 may employ connection protocols include, but not limited to, 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.

[0031] The communication network 309 includes, but is not limited to, a direct interconnection, a peer to peer (P2P) network, local area network (LAN), wide area network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, Wi-Fi and such. The communication network 309 may either be a dedicated network or a shared network, which represents an association of the different 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.

[0032] In some embodiments, the processor 302 may be disposed in communication with a memory 305 (e.g., RAM, ROM, etc. not shown in FIGURE 3) 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.

[0033] The memory 305 may store a collection of program or database components, including, without limitation, user interface 306, an operating system 307, etc. In some embodiments, computer system 300 may store user/application data, such as, the data, variables, records, etc., as described in this disclosure. Such databases may be implemented as fault-tolerant, relational, scalable, secure databases such as Oracle or Sybase.

[0034] The operating system 307 may facilitate resource management and operation of the computer system 300. Examples of operating systems include, without limitation, Apple™ Macintosh ™ OS X™, UNIX™, Unix-like system distributions (e.g., Berkeley Software Distribution (BSD), FreeBSD™, Net BSD™, Open BSD™, etc.), Linux distributions (e.g., Red Hat™, Ubuntu™, K-Ubuntu™, etc.), International Business Machines (IBM™) OS/2™, Microsoft Windows™ (XP™, Vista/7/8, etc.), Apple iOS™, Google Android™, Blackberry™ operating system (OS), or the like. In some embodiments, the computer system 300 may implement web browser 308 stored program components. Web browser 308 may be a hypertext viewing application, such as Microsoft™ Internet Explorer™, Google Chrome™, Mozilla Firefox™, Apple™ Safari™, etc. Secure web browsing may be provided using secure hypertext transport protocol (HTTPS), secure sockets layer (SSL), transport layer security (TLS), etc. Web browsers 308 may utilize facilities such as AJAX, DHTML, Adobe™ Flash, Javascript, Application Programming Interfaces (APIs), etc.

[0035] According to some non-limiting embodiments or aspects, a computer program product including at least one non-transitory computer-readable medium including one or more instructions.

[0036] 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. It must also be noted that as used herein, the singular forms “a,” “an,” and “the” include plural references unless the context clearly dictates otherwise.

[0037] 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. Examples include random access memory (RAM), read-only memory (ROM), volatile memory, nonvolatile memory, hard drives, CD ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[0038] 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. Accordingly, the disclosure of the embodiments of the disclosure is intended to be illustrative, but not limiting, of the scope of the disclosure.

METHOD AND SYSTEM FOR FACILITATING PAYMENT TRANSACTIONS IN OFFLINE MODE

ABSTRACT

The present disclosure relates to a method and a system for facilitating payment transactions in offline mode. The system comprises a mobile device associated with user, a POS terminal, and a server. At first, the user provides details of mobile number at the POS terminal which is forwarded to the server as a message. The server creates a unique ID based on the mobile number and provides the unique ID to the POS terminal. At the POS terminal, the user provides password which is set during registration of user with the server using which another unique ID is generated by an application in the mobile device. Once both unique ID's match, a secure connection is set up between the POS terminal and the mobile device for facilitating the payment transactions. The present disclosure overcomes need for NFC feature for performing offline payment transaction at a POS terminal and establishes secure WiFi connection between the POS terminal and the mobile device for the payment transaction processing.

Fig.1

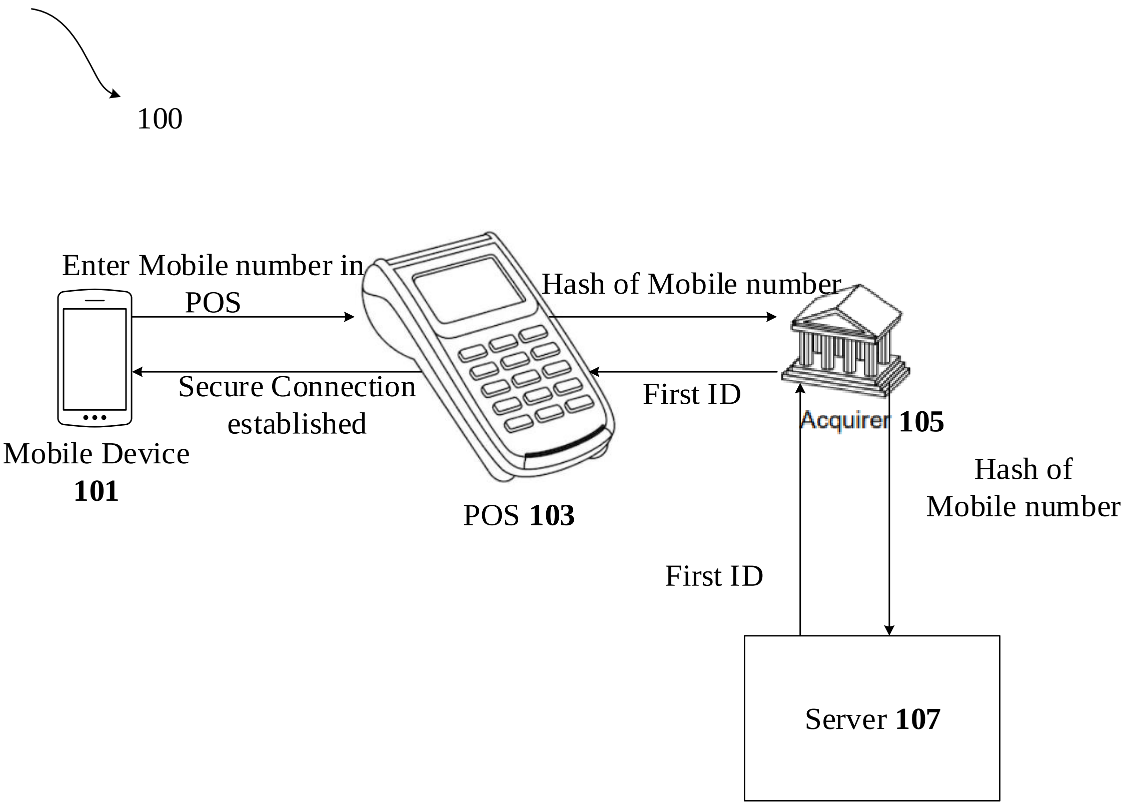
100
Enter Mobile number in POS
Hash of Mobile number
Secure Connection established
First ID
Acquirer 105
Mobile Device 101
POS 103
Hash of Mobile number
First ID
Server 107

Fig.1

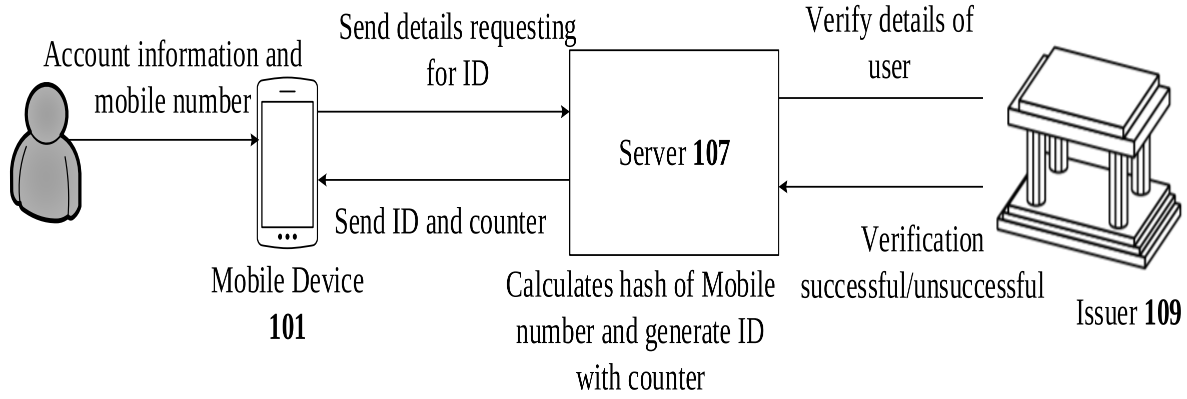
Account information and mobile number
Send details requesting for ID
Verify details of user
Server 107
Send ID and counter
Verification successful/unsuccessful
Mobile Device 101
Calculates hash of Mobile number and generate ID with counter
Issuer 109

Fig.2

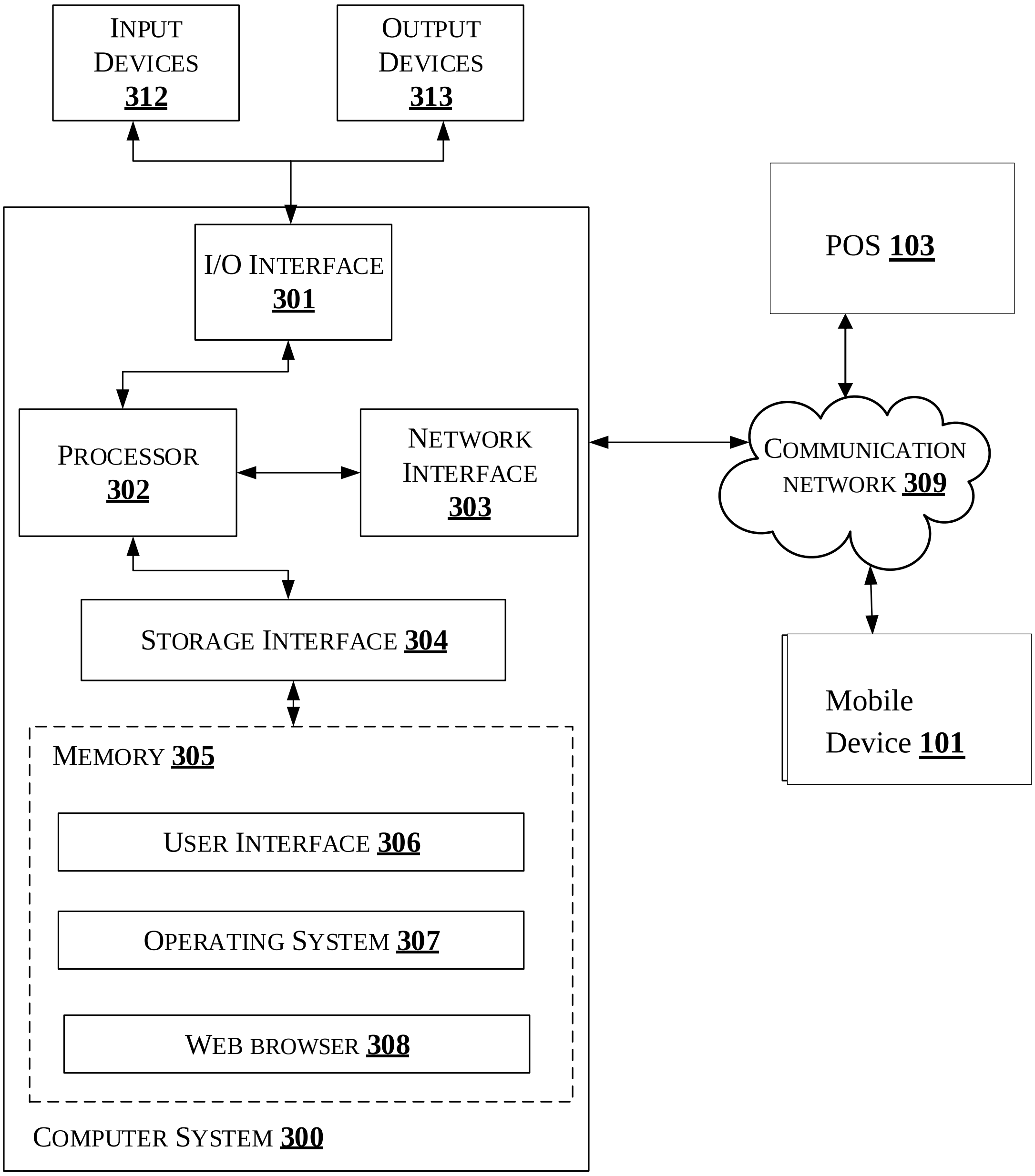
INPUT DEVICES 312
OUTPUT DEVICES 313
I/O INTERFACE 301
POS 103
PROCESSOR 302
NETWORK INTERFACE 303
COMMUNICATION NETWORK 309
STORAGE INTERFACE 304
Mobile Device 101
MEMORY 305
USER INTERFACE 306
OPERATING SYSTEM 307
WEB BROWSER 308
COMPUTER SYSTEM 300

Fig. 3