June 2023

IOT DEVICES AS PAYMENT INSTRUMENT FOR ATM TRANSACTIONS

VARADHARAJAN RAGHAVENDRAN
VISA

ABHAY KUDWA
VISA

DEB GHOSH
VISA

“IOT DEVICES AS PAYMENT INSTRUMENT FOR ATM TRANSACTIONS”

VISA

INVENTORS:

VARADHARAJAN RAGHAVENDRAN

ABHAY KUDWA

DEB GHOSH

TECHNICAL FIELD

[0001] The present subject matter is, in general, related to contactless secure transactions, and particularly to a method for performing Automated Teller Machine (ATM) operations without a card, but utilizing mobile phones and other Internet-of-Things (IoT) enabled devices.

BACKGROUND

[0002] In general, many people use Automated Teller Machines (ATMs) to perform various financial transactions, for example, to withdraw cash/money from a checking account or from a savings account that corresponds to a card provided held by the user. ATMs may also be used to deposit money to the user's savings account. Traditional payment instruments utilize a card (for example, the card issued by a bank i.e., a credit card or a debit card) to perform one or more operations in the ATM. For withdrawing money from the user account, the user/cardholder must input the bank-issued card into the ATM machine along with the password/PIN of the card. Based on password authentication, users may withdraw money from the ATM.

[0003] However, in these traditional payment instruments, bank-issued card information may be easily copied, and card passwords may be easily cracked, which leads to safety issues. Therefore, there is a need for contactless secure transactions and secure authentication mechanisms such as Quick Response (QR) code-enabled authentications.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, 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. 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:

[0005] **FIG. 1** discloses a schematic diagram of a system and a payment process flow, in accordance with some embodiments of the present disclosure.

[0006] **FIG. 2** discloses an additional embodiment of the system and the payment process flow, in accordance with some embodiments of the present disclosure.

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

[0008] 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

[0009] 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.

[0010] 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.

[0011] 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.

[0012] 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.

[0013] 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.

[0014] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to" unless expressly specified otherwise.

[0015] 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. For example, a first unit may be in communication with a second unit even though the first unit passively receives information and does not actively transmit information to the second unit. As another example, a first unit may be in communication with a second unit if at least one intermediary unit (e.g., a third unit located between the first unit and the second unit) processes information received from the first unit and communicates the processed information to the second unit. In some non-limiting embodiments, 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.

[0016] 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”.

[0017] As used herein, the term "mobile device" may refer to any electronic device that may be transported and operated by a user, which may also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network (e.g., 3G, 4G or similar networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network. Examples of mobile devices include mobile phones (e.g., cellular phones), PDAs, tablet computers, net books, laptop computers, personal music players, hand-held specialized readers, wearable devices (e.g., watches), vehicles (e.g., cars), etc. A mobile device may comprise any suitable hardware and software for performing such functions and may also include multiple devices or components (e.g., when a device has remote access to a network by tethering to another device - i.e., using the other device as a relay - both devices taken together may be considered a single mobile device).

[0018] As used herein, the term "Authentication data" may refer to any data suitable for authenticating a user or mobile device. Authentication data may be obtained from a user or a device that is operated by the user. Examples of authentication data obtained from a user may include PINs (personal identification numbers), passwords, etc. Examples of authentication data that may be obtained from a device may include device serial numbers, hardware secure element identifiers, device fingerprints, phone numbers, IMEI numbers, etc.

[0019] **FIG. 1** discloses a schematic diagram of a system and a payment process flow, in accordance with some embodiments of the present disclosure.

[0020] As shown in FIG. 1, user 101 may interact with an Automated Teller Machine (ATM) 102 and a user payment instrument 105. The term "user" may include an individual who has a savings, current or any other type of account with a bank and uses a bank-issued card to perform one or more transactions in the ATM 102. In some embodiments, the user 101 may be associated with one or more personal accounts and/or mobile devices. Accordingly, the user 101 may also be referred to alternatively as a cardholder, account holder, customer, or consumer. The ATM 102 may be configured to allow users to perform various financial transactions at any time.

[0021] The user payment instrument 105 may include Internet-of-Things (IoT) enabled devices, such as, without limiting to, smartphones, tablets and so on, which may be used to perform one or more ATM operations. The user payment instrument 105 may receive instructions from the user 101 to perform financial transactions. Here, the one or more ATM operations may include, without limiting to, cash disbursement from the user account, depositing funds to the user account, and contactless account transfer, that is, transferring funds between two different accounts via an online medium. For example, an account holder may use IoT enabled device to transfer funds from the user's savings account or to complete bill payment from the user's funds to any biller/merchant in the world. Consequently, the present disclosure aims to reduce the transaction time compared to time spent on physical interaction with the ATM and helps the users to securely complete the transaction. The use of IoT-based user payment instrument 105 in ATMs is further explained in the below steps:

[0022] In step 1: Initially, the user 101 requests the ATM 102 to perform a user account action. For example, the user 101 may wish to withdraw funds from his/her account or the user may deposit funds to his/her account.

[0023] In step 2: The ATM 102 initiates a VISA-linked device authentication 103 process to authenticate a device used by the user 101, upon receiving the user request.

[0024] In step 3: Based on the outcome of the authentication, the ATM 102 generates a Quick Response (QR) code along with the payment information 104.

[0025] In step 4: Communication between the ATM 102 and the user payment instrument 105 is initiated to perform financial transactions without a bank-issued card of the user 101. The user payment instrument 105 may have an application running on it and may communicate with a server at a remote location. For example, the server may be VISA authentication gateway or VISA payment gateway. Further, the application may refer to a computer code or other data stored on a computer readable medium (for example, memory element or secure element) of the user payment instrument 105 that may be executable by a processor of the instrument 105 to complete a task. The messages are transmitted among the devices over a wireless or a wired communication network using a secure communications protocol such as, but not limited to, File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP), Secure Hypertext Transfer Protocol (HHTPS), Secure Socket Layer (SSL), ISO and so on. Thereafter, the user payment instrument 105 may be used to scan the generated QR code along with the payment information, which opens a preconfigured authentication application (for example VISA application) and proceeds with the authentication process.

[0026] In step 5: After scanning the QR code, the user payment instrument 105 performs VISA-linked device authentication via VISA authentication gateway redirect to authenticate the user IoT-enabled device without the need to have a physical ATM card as an authentication mechanism. For example, the application installed on the user's device may access camera feature to allow the user to scan a QR code using a built-in camera on the user's device.

[0027] In step 6: Based on the authentication, that is, when the authentication is successful, the user account details are loaded onto the user payment instrument 105 to complete the transaction. The user's consent is obtained for performing the financial transaction over the IoT-enabled devices. Further, the authenticated user device is permitted to create a session for transaction confirmation. If the device authentication was unsuccessful and/or faces an error, then the financial transaction may be stopped/aborted.

[0028] **FIG. 2** discloses an additional embodiment of the system and payment process flow, in accordance with some embodiments of the present disclosure.

[0029] In step 1: A user 101 initiates the interaction with a user payment instrument 105 to create a transaction session. Subsequently, the ATM 102 initiates secure Remote Procedure Calls (RPC) over Bluetooth (BLE) band to a user payment instrument 105. The BLE band is used to broadcast messages from one device to other devices within a small tunable radius

around the beacon. Here, the RPC means that a process in a local system activates a process in a remote system.

[0030] In step 2: The user payment instrument 105 sends an acknowledgment via a channel for successfully creating a secure link between user's device and ATM 102. The secure link provides facilities for securely communicating with the user device and ATM 102 to perform transactions and protect the system from improper access attempts. For example, cardless services allow the user payment instrument 105 to interact with ATM 102 without the need for a physical bank-issued card as an authentication means for the user account. In an embodiment, after the secure channel is created, the ATM 102 initiates appropriate payment flow in an application and verifies the transaction risk score. More specifically, the user device has a mobile application installed thereon and is used for interacting with banks for performing financial transactions on a user account. For example, the first-time fund transactions or high-value fund transactions may be referred to as high-risk score transactions (for example, a risk score of above 30%). Similarly, low-value fund transactions may be referred to as low-risk score transactions (for example, a risk score of below 30%). Based on the risk score, an authentication response may be transmitted to the merchant device to proceed with the authorization of the online payment.

[0031] In step 3: After performing the first-time transaction via the application, a user authentication process may be initiated for payment using a registered authentication standard. As an example, the user account details may include a username and a password-based login, access key, and other authentication processes. The authentication process may be used to ensure that the user is authorized to access their specific account through the user payment instrument 105. After initiating the payment flow, the risk score may be indicated as low-risk transaction, and loaded token details for payment authentication may be submitted to the server. In this context, a token may be a type of credential, such as a string of numbers, letters, or any other suitable characters or may even include payment tokens. In some embodiments, the format of the token may be configured to allow the entity receiving the token to identify it as a token and recognize the entity that has issued the token.

[0032] In step 4: The authenticated payment information may be submitted to an Automated Clearing System (ACS) 204 system to perform financial transactions. The ACS 204 is

generally used for the electronic transfer of funds between two different bank accounts through an online medium.

[0033] In step 5: The ACS 204 may send a notification about the ‘success’ or ‘unsuccessful’ of the transaction. If the ACS transaction was unsuccessful, the financial transaction process may be stopped. As an example, the authorization response here may include one or more of status indicators. That is, an approved transaction may be indicated as ‘successful’ transaction and a declined transaction may be indicated as an ‘unsuccessful’ transaction.

[0034] In step 6: After the transaction is successfully completed, the ACS 204 may broadcast the payment information to a merchant or an acquiring bank. The acquirer may typically be a business entity (for example, a commercial bank) that has a business relationship with a particular merchant or other entity.

[0035] In step 7: The user payment instrument 105 continues with the settlement flows with the ATM 102 to complete the payment transaction received from the user. The settlement flows may include a cash disbursement from the user account or a money and/or fund deposit to the user account.

General computer system:

[0036] FIG. 3 illustrates a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[0037] In an embodiment, FIG. 3 illustrates a block diagram of an exemplary computer system 300 that may be used to implement the system. In some embodiments, the computer system 300 may include a central processing unit (“CPU” or “processor”) 302. The processor 302 may include at least one user payment instrument 105 to perform ATM operations via a network interface 303 and communication network 309. The processor 302 may include at least one data processor for executing program components for executing user or system-generated business processes. A user may include a person, a person using a device such as those included in this disclosure, or such a device itself. 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.

[0038] 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, Bbayonet 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.

[0039] 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.

[0040] 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 313. 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.

[0041] 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, communication network 309 may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, etc.

[0042] In some embodiments, the processor 302 may be disposed of in communication with a memory 305 (e.g., RAM, ROM, etc. not shown in Fig. 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.

[0043] Memory 305 may store a collection of program or database components, including, without limitation, user interface 306, an operating system 307, a web browser 308 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.

[0044] 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. The User interface 306 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, checkboxes, menus, scrollers, windows, widgets, etc. Graphical User Interfaces (GUIs) may

be employed, including, without limitation, Apple® Macintosh® operating systems' Aqua®, IBM® OS/2®, Microsoft® Windows® (e.g., Aero, Metro, etc.), web interface libraries (e.g., ActiveX®, Java®, Javascript, AJAX, HTML, Adobe® Flash®, etc.), or the like.

[0045] 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. In some embodiments, the computer system 300 may implement a mail server stored program component. The mail server may be an Internet mail server such as Microsoft Exchange, or the like. The mail server may utilize facilities such as ASP, ActiveX, ANSI C++/C#, Microsoft .NET, Common Gateway Interface (CGI) scripts, Java, JavaScript, PERL, PHP, Python, WebObjects, etc. The mail server may utilize communication protocols such as Internet Message Access Protocol (IMAP), Messaging Application Programming Interface (MAPI), Microsoft Exchange, Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), or the like.

[0046] In some embodiments, the computer system 300 may implement a mail client stored program component. The mail client may be a mail viewing application, such as APPLE® MAIL, MICROSOFT® ENTOURAGE®, MICROSOFT® OUTLOOK®, MOZILLA® THUNDERBIRD®, etc.

[0047] 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., be non-transitory. Examples include Random Access Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, Compact Disc (CD) ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[0048] The described operations may be implemented as a method, system or article of manufacture using standard programming and/or engineering techniques to produce software, firmware, hardware, or any combination thereof. The described operations may be implemented as code maintained in a “non-transitory computer readable medium”, where a processor may read and execute the code from the computer readable medium. The processor is at least one of a microprocessor and a processor capable of processing and executing the queries. A non-transitory computer readable medium may include media such as magnetic storage medium (e.g., hard disk drives, floppy disks, tape, etc.), optical storage (CD-ROMs, DVDs, optical disks, etc.), volatile and non-volatile memory devices (e.g., EEPROMs, ROMs, PROMs, RAMs, DRAMs, SRAMs, Flash Memory, firmware, programmable logic, etc.), etc. Further, non-transitory computer-readable media may include all computer-readable media except for transitory. The code implementing the described operations may further be implemented in hardware logic (e.g., an integrated circuit chip, Programmable Gate Array (PGA), Application Specific Integrated Circuit (ASIC), etc.).

[0049] 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.

[0050] 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, non-volatile memory, hard drives, CD ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[0051] 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.

[0052] With respect to the use of substantially any plural and/or singular terms herein, those having skill in the art can translate from the plural to the singular and/or from the singular to the plural as is appropriate to the context and/or application. The various singular/plural permutations may be expressly set forth herein for the sake of clarity.

"IOT DEVICES AS PAYMENT INSTRUMENT FOR ATM TRANSACTIONS"

ABSTRACT

The present disclosure relates to a method and a system for performing Automated Teller Machine (ATM) transactions using a user payment instrument without a physical bank-issued card. According to the present disclosure, a user requests an ATM to perform a user transaction request such as withdrawal of funds from the user account or depositing funds to the user account. Based on the user transaction request, the ATM generates a Quick Response (QR) code with payment information. Thereafter, a user payment instrument may be used to scan the generated QR code, which opens an authentication application, after the user payment instrument is authenticated. Further, the user account details are loaded onto the user payment instrument to perform the financial transaction on the ATM without the physical bank-issued cards.

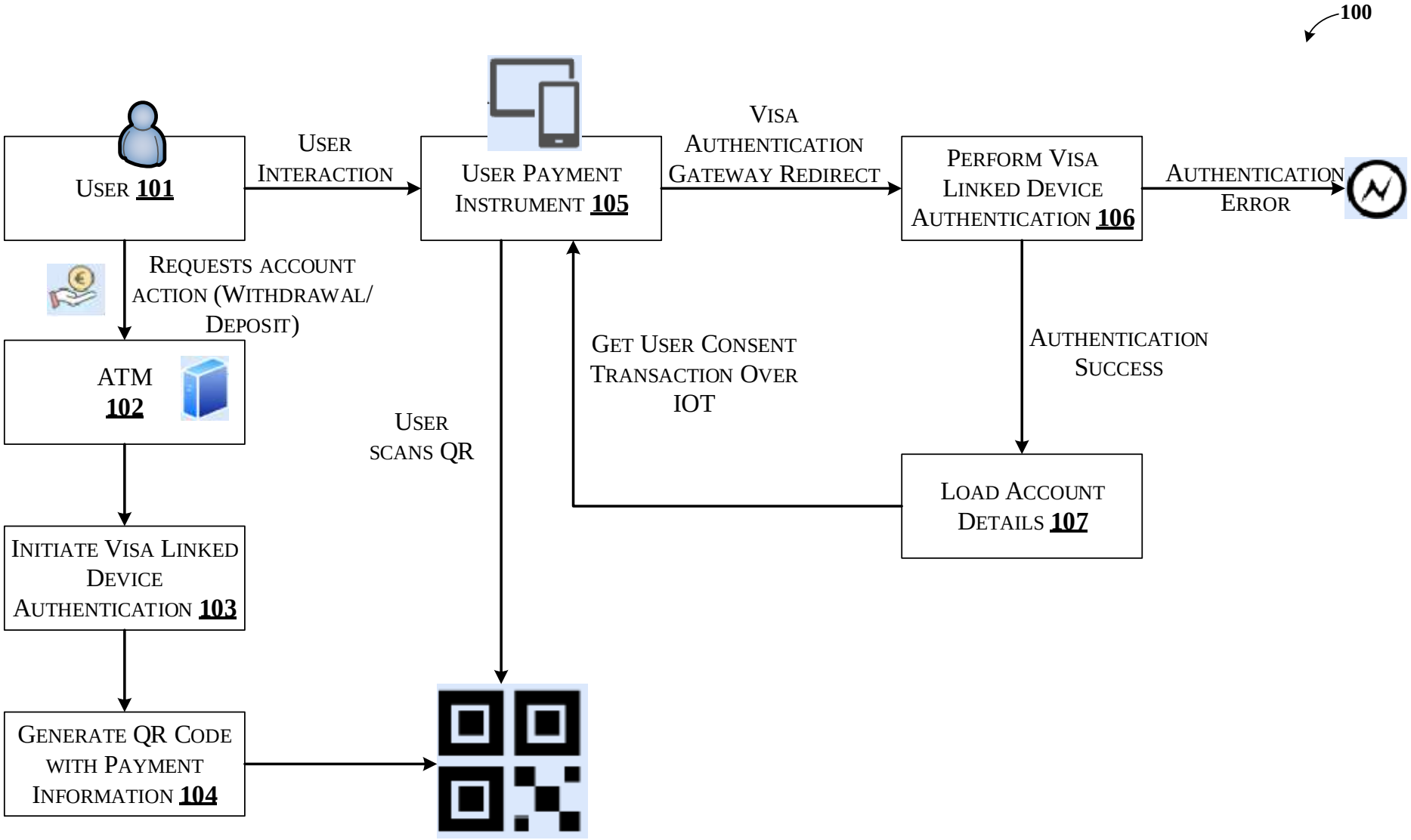
100
USER 101
USER INTERACTION
USER PAYMENT INSTRUMENT 105
VISA AUTHENTICATION GATEWAY REDIRECT
PERFORM VISA LINKED DEVICE AUTHENTICATION 106
AUTHENTICATION ERROR
REQUESTS ACCOUNT ACTION (WITHDRAWAL/ DEPOSIT)
ATM 102
GET USER CONSENT TRANSACTION OVER IOT
AUTHENTICATION SUCCESS
USER SCANS QR
LOAD ACCOUNT DETAILS 107
INITIATE VISA LINKED DEVICE AUTHENTICATION 103
GENERATE QR CODE WITH PAYMENT INFORMATION 104

FIG. 1

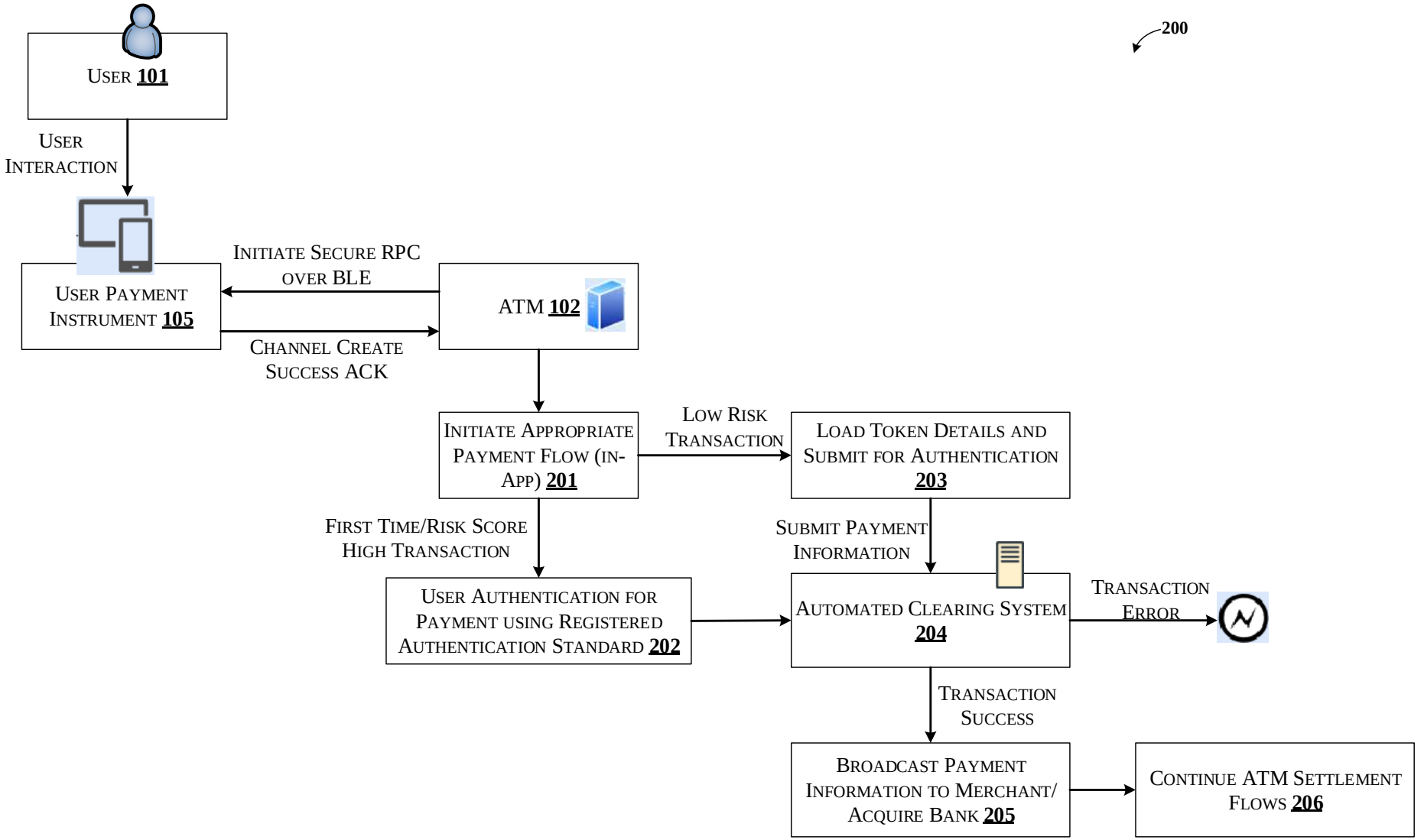
200
USER 101
USER INTERACTION
USER PAYMENT INSTRUMENT 105
INITIATE SECURE RPC OVER BLE
CHANNEL CREATE SUCCESS ACK
ATM 102
INITIATE APPROPRIATE PAYMENT FLOW (IN-APP) 201
LOW RISK TRANSACTION
LOAD TOKEN DETAILS AND SUBMIT FOR AUTHENTICATION 203
FIRST TIME/RISK SCORE HIGH TRANSACTION
SUBMIT PAYMENT INFORMATION
USER AUTHENTICATION FOR PAYMENT USING REGISTERED AUTHENTICATION STANDARD 202
AUTOMATED CLEARING SYSTEM 204
TRANSACTION ERROR
TRANSACTION SUCCESS
BROADCAST PAYMENT INFORMATION TO MERCHANT/ ACQUIRE BANK 205
CONTINUE ATM SETTLEMENT FLOWS 206

FIG. 2

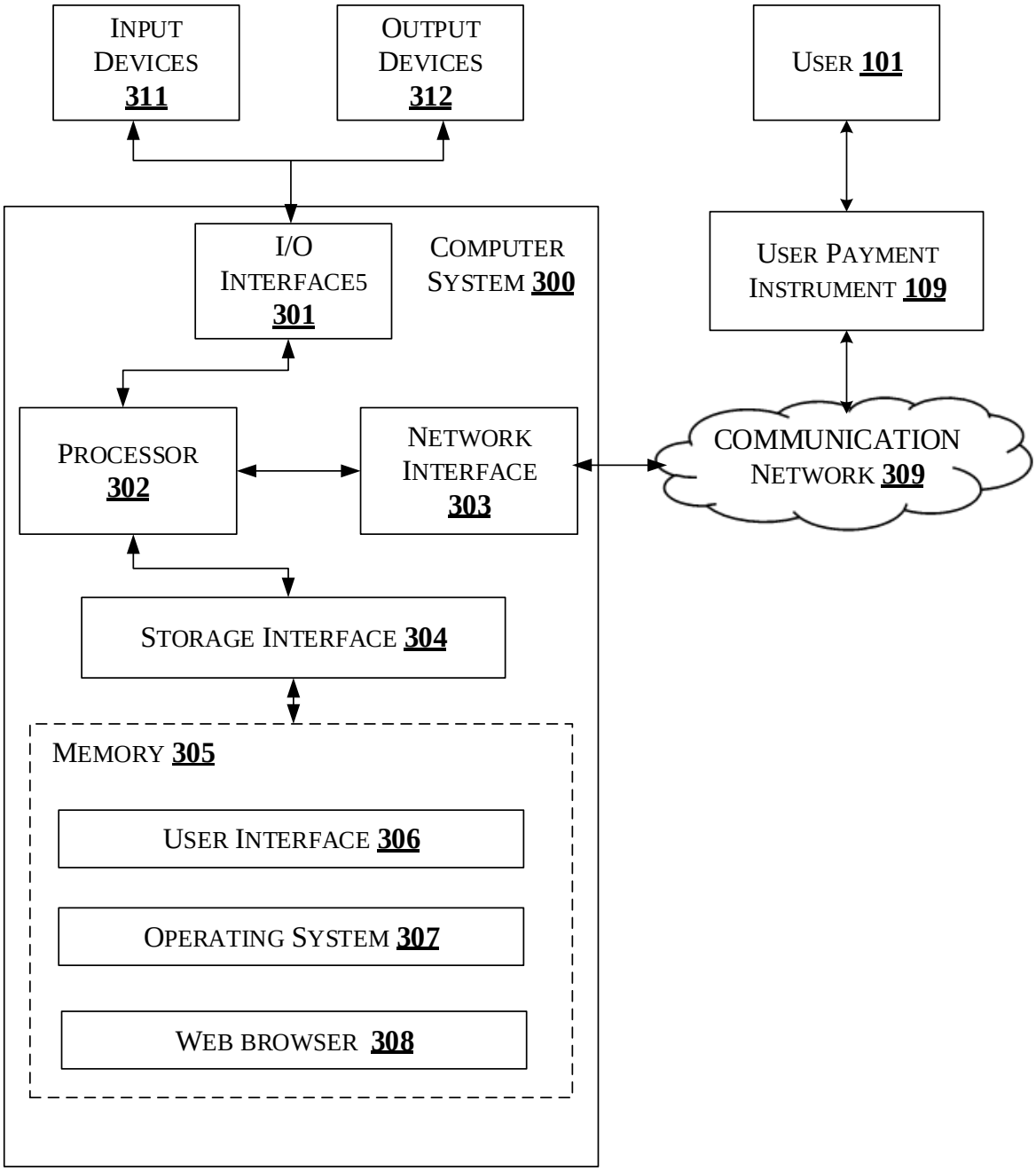
INPUT DEVICES 311
OUTPUT DEVICES 312
USER 101
I/O INTERFACE5 301
COMPUTER SYSTEM 300
USER PAYMENT INSTRUMENT 109
PROCESSOR 302
NETWORK INTERFACE 303
COMMUNICATION NETWORK 309
STORAGE INTERFACE 304
MEMORY 305
USER INTERFACE 306
OPERATING SYSTEM 307
WEB BROWSER 308

FIG. 3