January 2024

SYSTEM AND METHOD FOR PERFORMING TRANSACTIONS USING UNIFIED TRANSACTION IDENTIFIER (ID)

NEERAJ SURANA
VISA

HARDIK JAIN
VISA

PRAJNA SHETTY
VISA

PRETHWISH BANERJEE
VISA

SYSTEM AND METHOD FOR PERFORMING TRANSACTIONS USING UNIFIED TRANSACTION IDENTIFIER (ID)

VISA

INVENTOR:

- **NEERAJ SURANA**
- **HARDIK JAIN**
- **PRAJNA SHETTY**
- **PRETHWISH BANERJEE**

TECHNICAL FIELD

[0001] The present subject matter in general relates to payment systems, and particularly, to a method and a system for performing transactions using unified transaction identifier (ID).

BACKGROUND

[0002] Currently, there are different payment methods for performing transactions such as business-to-business transactions, and the like. Few common payment modes payment card (e.g., credit card, debit card, and/or the like), and online payment services (e.g., PayPal™ and/or the like). Online payment services (e.g., PayPal™ and/or the like) may require at least one of a user or a recipient account details (e.g., transaction amount, identities of parties, payment account information, and/or the like), and/or the like, to be manually entered each time when a transaction is initialized to be performed.

[0003] Conventionally online payments are performed by using transaction identification (ID) number. Herein, instead of entering all the account details of the user every time, to transfer amount to the recipient, the user can enter the ID number and perform transaction. However, such a method does not consider security and safety of the transaction. Also, the ID number may be different for each payment method i.e., credit card may have one ID number, debit card may have other ID number, online payment applications may have another ID number, and the like, which may be difficult for the user to remember. Hence, there is a requirement for a single ID, that can be used for all types of payments.

[0004] The information disclosed in the background section of the disclosure 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

[0005] 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:

[0006] Figure 1 illustrates an exemplary environment for performing transactions using unified transaction identifier (ID), in accordance with some embodiments of the present disclosure;

[0007] Figure 2 shows a flowchart illustrating a method for performing transactions using unified transaction identifier (ID), in accordance with some embodiments of the present disclosure;

[0008] Figures 3A-3B show exemplary illustrations of performing transactions using unified transaction identifier (ID), in accordance with some embodiments of the present disclosure; and

[0009] Figure 4 illustrates a block diagram of an exemplary computer system for performing transactions using unified transaction identifier (ID), in accordance with some embodiments of the present disclosure.

[0010] 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

[0011] 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.

[0012] 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.

[0013] 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.

[0014] 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.

[0015] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to", unless expressly specified otherwise.

[0016] The present disclosure provides a method and a system for performing transactions using a unified transaction identifier (ID). In the present disclosure, the transactions are performed using a unified ID. Firstly, a unified ID is generated by a unified ID system. A user may register the unified ID system for generating the unified ID. During registration, the unified ID system may receive credentials of a user, requiring a unified ID, such as, an account number, a Personal Identification Number (PIN), and the like. Further, the unified ID system generates the unified ID, based on the credentials received from the user. Herein, the unified ID is linked with one or more accounts of the user, such that payment can be initiated via any of payment cards such as, a debit card and a credit card, and online payments associated with the one or more accounts of the user. Hence, the user can perform transactions from any modes such as the payment cards, the online payments, and the like, to which the unified ID is linked. Post registering, the user such as, a sender having a unified ID can initiate a transaction with a recipient having a unified ID. Herein, while initiating the transaction from the sender to the recipient, the sender provides the unified ID of the recipient. Upon entering the unified ID of the recipient, the unified ID system determines a risk rate and a payment limit associated with the initiated transaction based on the recipient transaction history, recipient category, and the

like. Then, the determined risk rate associated with the transaction is notified to the sender. Thus, the present disclosure facilitates a user to be able to make a choice whether to perform a transaction or not, based on the risk rate and the payment limit associated with the recipient's transaction. Hence, the present disclosure provides a safe and secure transaction to the user.

[0017] Figure 1 shows an exemplary environment 100 for performing transactions using a unified transaction identifier (ID). The exemplary environment 100 comprises a unified ID system 101, a sender 102 and a recipient 103. In the present disclosure, the unified ID system 101 is used to generate a unified ID for a user and perform transactions using the unified ID. The unified ID may include a series of alphanumeric string, numeric string, and the like. The unified ID system 101 may be implemented as data processors, cloud data servers, data receiver, server, data center/ database, monitor, storage system, collaborator, application stacks, and the like. t. The unified ID system 101 may communicate over a network with an application implemented in the sender 102 and the recipient 103. The network may include, without limitation, a Local Area Network (LAN), a Wide Area Network (WAN), a wireless network (e.g., using Wireless Application Protocol), the Internet, and the like.

[0018] In an embodiment, the unified ID system 101 may include a processor, an Input/Output (I/O) interface, and the memory. The memory is communicatively coupled to the processor. The memory stores instructions executable by the processor. The processor may comprise at least one data processor for executing program components for executing user or system-generated requests. The memory may be communicatively coupled to the processor. The memory stores instructions, executable by the processor, which, on execution, may cause the processor to perform transaction using the unified ID generated by the unified ID system 101.

[0019] The unified ID system 101 may include an application such as a mobile application. During registration process, based on a request of a user, the unified IS system 101 may generate the unified ID for the user, using credentials of the user. In an embodiment, the user may enter the credentials such as, an account number, Indian Financial System Code (IFSC) code, credit card details, debit card details, and the like, to generate the unified ID. The user may use provides the credentials by entering in the application associated with the unified ID system 101. Upon verifying the credentials, the unified ID system 101 may generate the unified ID for the user and provide it to the user via the application. In an embodiment the unified ID

system 101 may generate a Quick Response (QR) code associated with the generated unified ID.

[0020] The generated unified ID may be linked with one or more accounts of the user, such that payment can be initiated via any one-off, payment cards such as debit cards and credit cards, online payments associated with the one or more accounts of the user. That is, upon linking the unified ID with the one or more accounts, the debit cards, the credit cards, and the like, the user can perform transactions directly without entering any card or account details.

[0021] Once both the sender 102 and the recipient 103 are registered with the unified ID system 101 for generating the unified ID and linking the unified ID with the respective accounts, the sender 102 may initiate the transaction. While initiating the transaction, the sender 102 may have to provide a unified ID of the recipient 103 via the application in a device associated with the sender. Upon receiving the unified ID of the recipient 103, the unified ID system 101 may verify the recipient 103 based on the provided unified ID. Further, the unified ID system 101 may determine a risk rate and payment limit associated with the transaction.

[0022] In an embodiment, the risk rate associated with the transaction may be referred to as an adverse effect of timely payment of the recipient 103. The pay limit associated with the transaction may be referred to as a maximum amount that the recipient 103 is capable of returning to the sender 102. The risk rate and the payment limit associated with the transaction may be determined based on transaction history of the recipient, a category of the recipient 103, profile parameters of the recipient, and the like.

[0023] Further, the unified ID system 101 may notify the sender 102 about the risk rate and the payment limit associated with the transaction. The sender 102 may proceed with the transaction or terminate the transaction based on the risk rate and the payment limit notified by the unified ID system 101. Hence, the unified ID provides a secure and safe transaction between the sender 102 and the recipient.

[0024] Figure 2 shows a flowchart illustrating a method 200 for performing transactions using a unified transaction identifier (ID), in accordance with some embodiments of the present disclosure.

[0025] The method 200 may be described in the general context of computer executable instructions. Generally, computer executable instructions can include routines, programs, objects, components, data structures, procedures, modules, and functions, which perform functions or implement abstract data types.

[0026] The order in which the method 200 is described is not intended to be construed as a limitation, and any number of the described method blocks can be combined in any order to implement the method 200. Additionally, individual blocks may be deleted from the methods without departing from the spirit and scope of the subject matter described herein. Furthermore, the method 200 can be implemented in any suitable hardware, software, firmware, or combination thereof.

[0027] At block 201, during registration, the unified ID system 101 may generate the unified ID for the user. Firstly, to generate the unified ID, the user may have to provide the credentials associated with the account. The credentials may include account details, debit card details, credit card details, and the like of the user. The user may use the application in the device for entering the credentials. The device may be a mobile phone, laptop, tablet, and the like. The application in the device may be associated with the unified ID system 101.Upon the user entering the credentials, the unified ID system 101 may validate credentials and generate the unified ID for the user. In an embodiment, the unified ID may be a human rememberable ID, and the generation of unified ID may be a one-time process. In an embodiment, the unified ID system 101 may generate a Quick Response (QR) code associated with the generated unified ID. Hence, the user may perform the transaction using the unified ID or the associated QR code. In an embodiment, the unified ID may be generated based on user choice.

[0028] In an embodiment, referring to **Figure 3C,** during registration process, a user 313 may enter personal details 315 into a unified ID service 302. Then, the unified ID server 302 may store the personal details 315 of the user 313 in a unified ID database 303. For example, the personal details 315 may be such as, mobile number of the user, email address of the user, and the like. Upon entering the personal details 315, the unified ID service 302 may generate unified ID based on the personal details 315 entered by the user 313. Further, the user 313 may also have an option to choose the unified ID.

[0029] At block 202, the generated unified ID may be linked with one or more accounts of the user. As the unified ID of the user may be linked with the one or more accounts, the transaction can be initiated via any of the credit card, the debit card, and the like associated with the one or more accounts of the user. The map of the unified ID with any of the cards or account of the user can be initiated at any time. In an embodiment, the transaction may be initiated via a primary account and a primary payment card selected by the user from a plurality of accounts and a plurality of payment cards, respectively of the user. In an embodiment, the unified ID may be linked with any type of payment cards such as the cards used with Point of Sale (POS), the cards with tap and pay option, the cards with swipe option. Once the user (both the sender 102 and the recipient 103) are registered for the unified ID, the sender 102 may initiate the transaction.

[0030] In an embodiment, referring to **Figure 3C,** upon generating the unified ID for the user 313, the user may use the unified ID to login 314 to the unified ID service 302. The user links the one or more cards and one or more account details 316 with the unified ID. In an embodiment, the user may select one card or one account as primary account to perform usual transactions and the other cards and accounts as secondary accounts to perform transactions when the user intends to perform transactions via other accounts or cards.

[0031] At block 203, the sender 102 may initiate the transaction by providing the unified ID of the recipient 103. In an embodiment, the unified ID of the recipient 103 may be shared by the recipient 103 with the sender 102. The unified ID of the recipient 103 is verified based on stored IDs with the unified ID system 101.

[0032] At block 204, the unified ID system 101 may determine the risk rate and the payment limit associated with the transaction with the recipient 103, based on the transaction history and category of the recipient 103, profile parameters of the recipient, and the like. In an embodiment, the unified ID system 101 may evaluate details of the recipient 103 and verify a reliability score of the recipient 103 before performing the transaction. In case the reliability score is less than a threshold score, or the payment limit associated with the recipient 103 is breached, additional authentication such as, One Time Password (OTP), may be performed.

[0033] In an embodiment, the reliability score may be determined based on spam reporting details of the user. The unified ID service 302 may contain the user details along with spam reporting information. Then, the unified ID service 302 may report the reliability score based

on the unified ID value and a reporting flag allotted with that transaction. The reporting flag refers to the total number of transactions. In an embodiment, the reliability score may be calculated as the reporting flag and stored into a variable as total score. Firstly, mean, and standard deviation of the total users in the transaction may be calculated. Further, mean + 1.5*standard deviation is calculated. Finally, the reliability score for the user is calculated by diving the total score by the number of transactions. Refer to below exemplary table to determine risk rate based on the reliability score.

Reliability score >= Risk Threshold score	Very High Risk Rating
Reliability score < Risk Threshold score and Reliability score >= Risk Threshold/Number of transactions	Medium Risk Rating
Reliability score < Risk Threshold/Number of transactions and Reliability score>=0	Low Risk Rating (Will not be displayed to payee)

Table 1

[0034] In an embodiment, referring to **Figure 3A,** upon entering the unified ID of the recipient 103 by the sender 102 via the application, the unified ID may be forwarded to a unified ID service 302 for determining the risk rate and the payment limit associated with the transaction using the unified ID. The unified ID service 302 may transmit the received unified ID to a unified ID database 303 for obtaining the transaction history, the category, the profile parameters of the recipient 103, and the like, based on which the unified ID service 302 may determine the risk rate and the payment limit associated with the transaction initiated with the recipient 103.

[0035] Referring to **Figure 3B,** the unified ID service 302 may be connected to two databases for obtaining the transaction history, the category of the recipient 103, and the like. First database may be risk rate database 306 for determining the risk rate associated with the transaction. A second database may be a payment limit database 308 for determining the payment limit associated with the transaction. Further, the risk rate database 306 may be in contact with a risk evaluation service 307 and the payment limit database 308 may be in contact with a payment limit calculation service 309. The risk evaluation service 307 may determine the risk rate associated with the transaction and the payment limit calculation service 309 may determine the payment limit associated with the transaction. Upon determining the risk rate

and the payment limit by the risk evaluation service 307 and the payment limit calculation service 309, the risk evaluation service 307 and the payment limit calculation service 309 may store the determined risk rate and the payment limit in the risk rate database 306 and payment limit database 308, respectively. Further, the unified ID service 302 may receive the determined risk rate and the payment limit associated with the transaction.

[0036] Referring back to Figure 3A, upon the unified ID service 302 receiving the determined risk rate and the payment limit associated with the transaction with the recipient 103, the unified ID service 302 may notify the sender 102 about the determined risk rate and the payment limit. In an embodiment, the determined risk rate and the payment limit may be notified in a rating format to the sender 102. The sender 102 may proceed to complete the transaction with the recipient based on the determined risk rate and the payment limit.

[0037] In an embodiment, payment limit is calculated for the user using the unified ID service 302. The risk rate may be determined by considering time series information on daily scale along with average amount per transaction. For example, a statsmodels.tsa.seasonal.Standard Triangle Language or Standard Tessellation Language (STL) algorithm may be used to remove a seasonality factor of the time series information and then K-Nearest Neighbour (KNN) algorithm with a contamination value may be used with the time series information while inputting the information to the unified ID service 302. In case output from the unified ID service 302 provides an output with outlier, then a risk warning may be promoted to the user.

[0038] Referring back to Figure 2, at block 205, the sender 102 may proceed to complete the initiated transaction based on the determined risk rate and the payment limit. In the case of sender 102 performing the transaction, the sender 102 may provide an amount and confirm payment to complete the transaction successfully. While performing the transaction, upon entering the amount, the unified ID system 101 may display a processing fee amount to be detected from the entered amount. In the case of the sender 102 confirming the amount, the sender 102 may have to enter a Personal Identification Number (PIN) to confirm and transfer the rest of the amount to the recipient 103. In an embodiment, the application in the device may display details of all the transactions performed by the sender 102. In case of performing a fraudulent transaction using the unified ID, the sender 102 may report or provide feedback for the processed transaction as the fraudulent transaction. The risk rate determined for the

recipient 103 may be impacted when any transaction associated with the recipient 103 are indicated as a fraudulent transaction.

General computer system:

[0039] Figure 4 illustrates a block diagram of an exemplary computer system 400 for implementing embodiments consistent with the present disclosure.

[0040] In an embodiment, the computer system 400 may be used to implement the unified ID system 101 of the present disclosure. The computer system 400 may include a Central Processing Unit ("CPU" or "processor") 402. In an embodiment, the processor 402 may be a part of a data processor from the plurality of data processors. In such case, the processor 402 may communicate with other data processors over a communication network 409. The processor 402 may communicate with the sender 102 and the recipient 103 over the communication network 409. The processor 402 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.

[0041] The processor 402 may be disposed in communication with one or more Input/Output (I/O) devices 410 and 411 via I/O interface 401. The I/O interface 401 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.

[0042] Using the I/O interface 401, the computer system 400 may communicate with one or more I/O devices such as input devices 410 and output devices 411. For example, the input devices 410 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 411 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.

[0043] In some embodiments, the processor 402 may be disposed in communication with the communication network 409 via a network interface 403. The network interface 403 may communicate with the communication network 409. The network interface 403 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 409 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 403 and the communication network 409, the computer system 400 may communicate with inputs and provides output. The network interface 403 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.

[0044] The communication network 409 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 409 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 409 may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, etc.

[0045] In some embodiments, the processor 402 may be disposed in communication with a memory 405 (e.g., RAM, ROM, etc. not shown in Figure 4) via a storage interface 404. The storage interface 404 may connect to memory 405 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.

[0046] The memory 405 may store a collection of program or database components, including, without limitation, user interface 406, an operating system 407, etc. In some embodiments, computer system 400 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.

[0047] The operating system 407 may facilitate resource management and operation of the computer system 400. 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.

[0048] In some embodiments, the computer system 400 may implement web browser 408 stored program components. Web browser 408 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 408 may utilize facilities such as AJAX, DHTML, Adobe™ Flash, Javascript, Application Programming Interfaces (APIs), etc. In some embodiments, the computer system 400 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.

[0049] In some embodiments, the computer system 400 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.

[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., 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.

[0051] Advantages of the present disclosure

The present disclosure discloses a method and a system for performing transactions using unified transaction identifier (ID). The present disclosure provides a unified ID of user choice, and the unified ID may be human rememberable. Hence, providing a user convenient unified ID for performing transactions. The present disclosure evaluates a risk rate and a payment limit associated with the transaction based on transaction history of a recipient, recipient category, and the like, hence providing a safe and secure method for reducing fraudulent transactions.

[0052] 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 a 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.).

[0053] 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. 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.

[0054] 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.

[0055] 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.

[0056] 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 sake of clarity.

“SYSTEM AND METHOD FOR PERFORMING TRANSACTIONS USING UNIFIED TRANSACTION IDENTIFIER (ID)”

ABSTRACT

The present disclosure discloses a method and a system for performing transactions using unified transaction identifier (ID). In the present disclosure, the method includes generating a unified ID using credentials of a user during registration process. Herein, the unified ID is linked with one or more accounts of the user, one or more debit cards, credit cards, and the like, of the user. Post registering, the user such as, a sender having a unified ID can initiate a transaction with a recipient having a unified ID. Herein, while initiating the transaction from the sender to the recipient, the sender provides unified ID of the recipient. Upon entering the unified ID of the recipient, the unified ID system determines a risk rate and a payment limit associated with the initiated transaction. Then, the determined risk rate associated with the transaction is notified to the sender to complete or terminate the transaction.

Figure 1

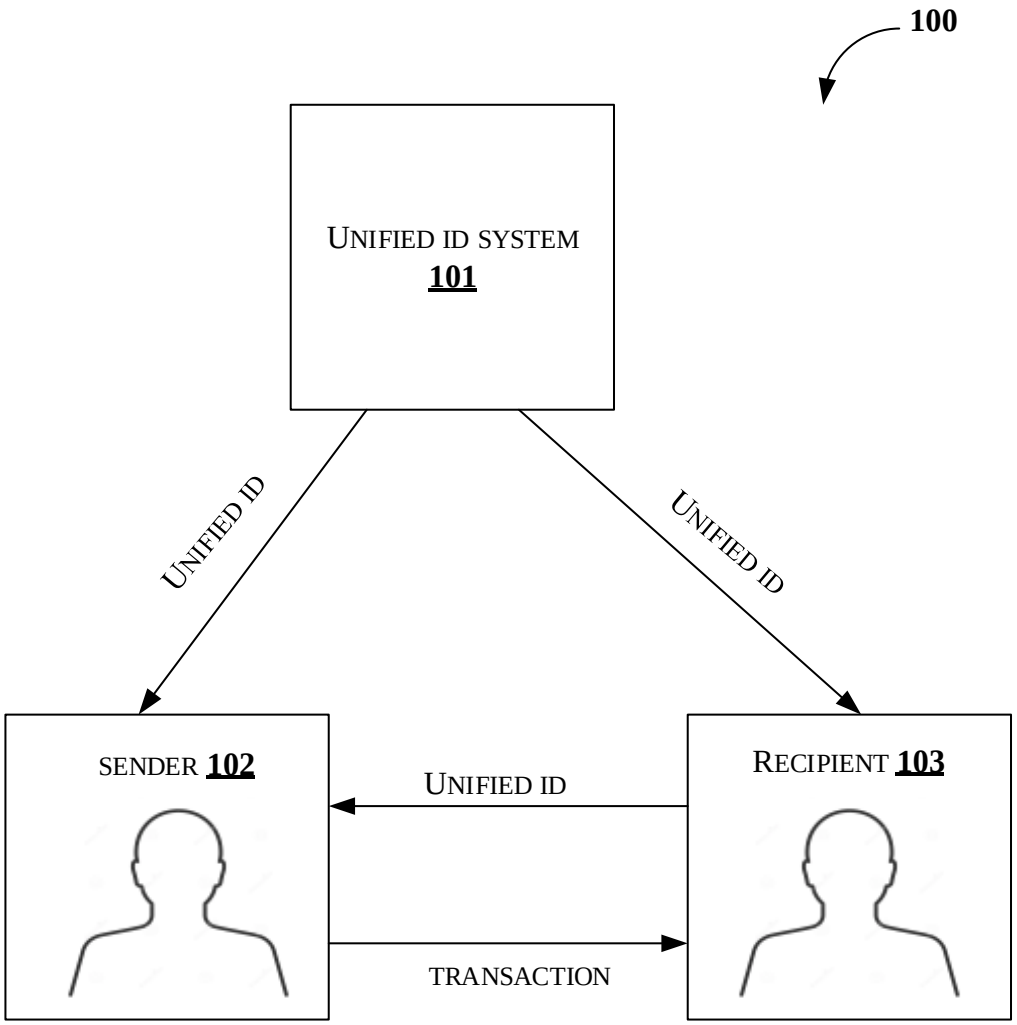
100
UNIFIED ID SYSTEM
101
UNIFIED ID
UNIFIED ID
SENDER 102
UNIFIED ID
RECIPIENT 103
TRANSACTION

FIGURE 1

2/6

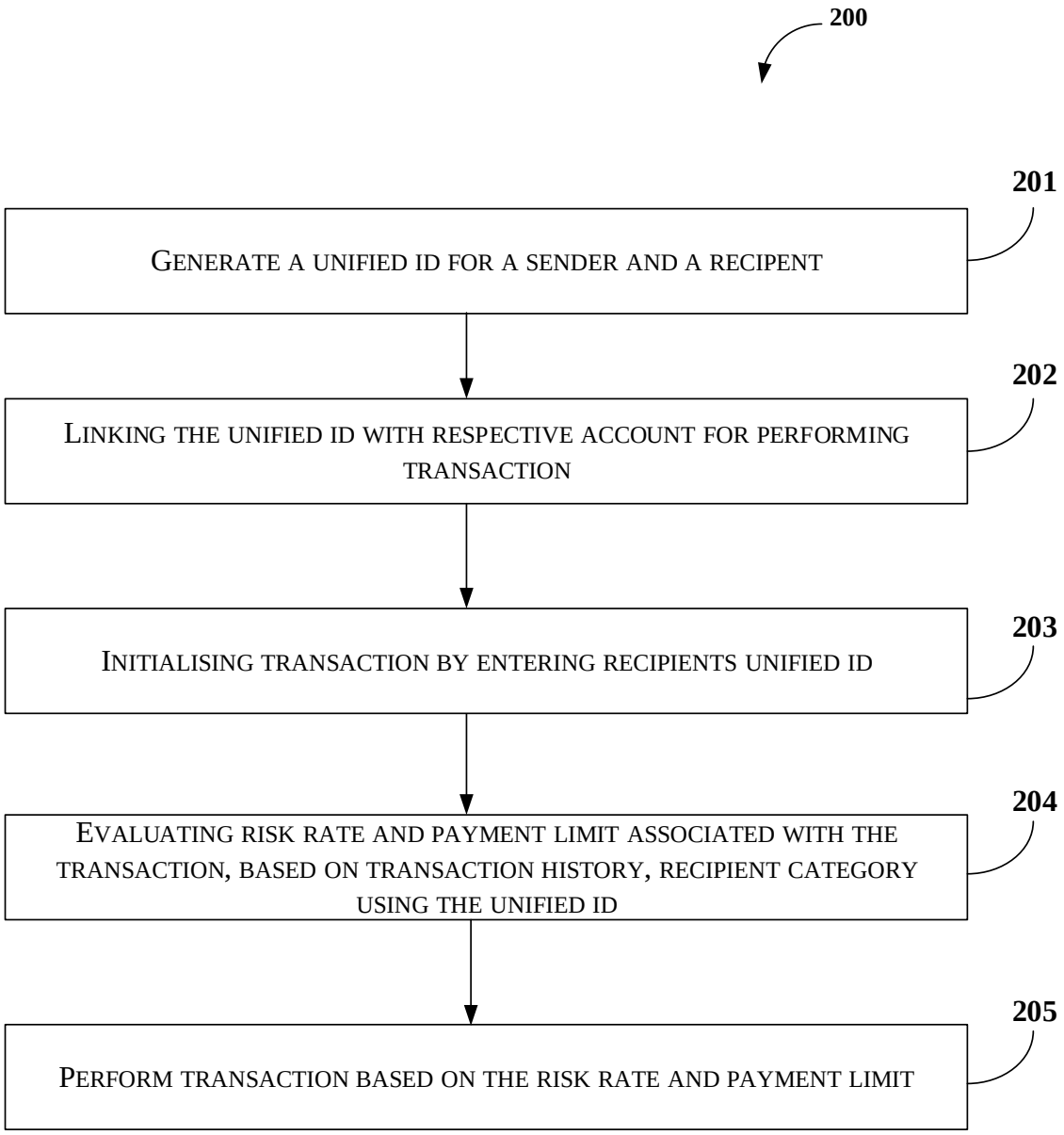
200
201
GENERATE A UNIFIED ID FOR A SENDER AND A RECIPENT
202
LINKING THE UNIFIED ID WITH RESPECTIVE ACCOUNT FOR PERFORMING TRANSACTION
203
INITIALISING TRANSACTION BY ENTERING RECIPIENTS UNIFIED ID
204
EVALUATING RISK RATE AND PAYMENT LIMIT ASSOCIATED WITH THE TRANSACTION, BASED ON TRANSACTION HISTORY, RECIPIENT CATEGORY USING THE UNIFIED ID
205
PERFORM TRANSACTION BASED ON THE RISK RATE AND PAYMENT LIMIT

FIGURE 2

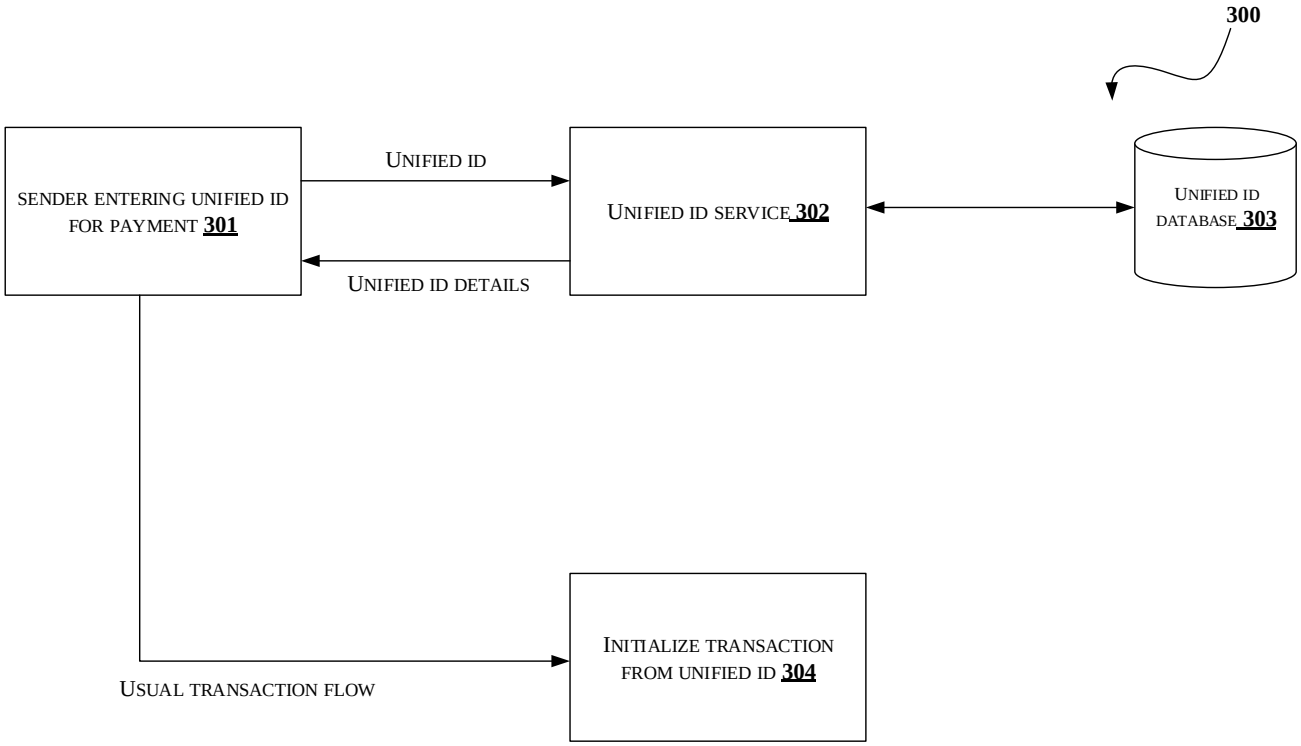
300
SENDER ENTERING UNIFIED ID FOR PAYMENT 301
UNIFIED ID
UNIFIED ID DETAILS
UNIFIED ID SERVICE 302
UNIFIED ID DATABASE 303
USUAL TRANSACTION FLOW
INITIALIZE TRANSACTION FROM UNIFIED ID 304

FIGURE 3A

4/6

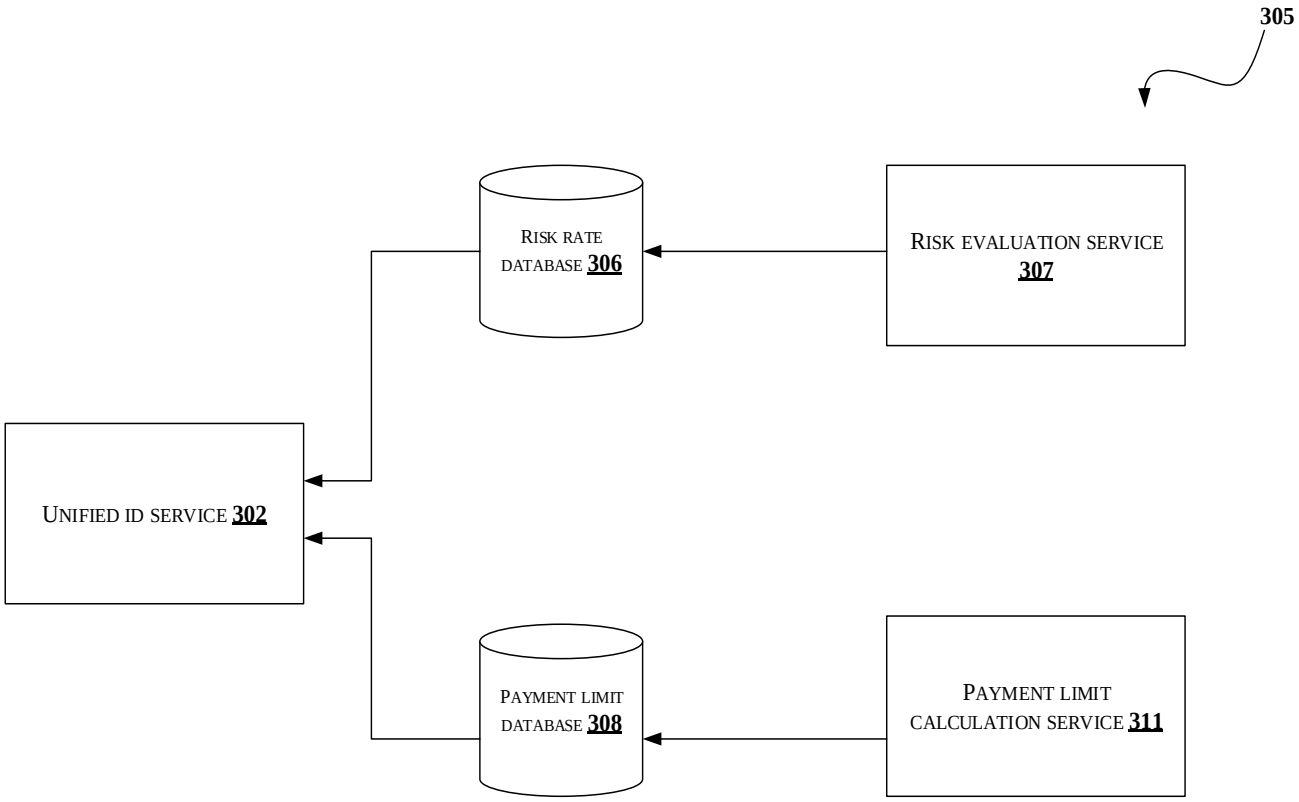
305
RISK RATE DATABASE 306
RISK EVALUATION SERVICE 307
UNIFIED ID SERVICE 302
PAYMENT LIMIT DATABASE 308
PAYMENT LIMIT CALCULATION SERVICE 311

FIGURE 3B

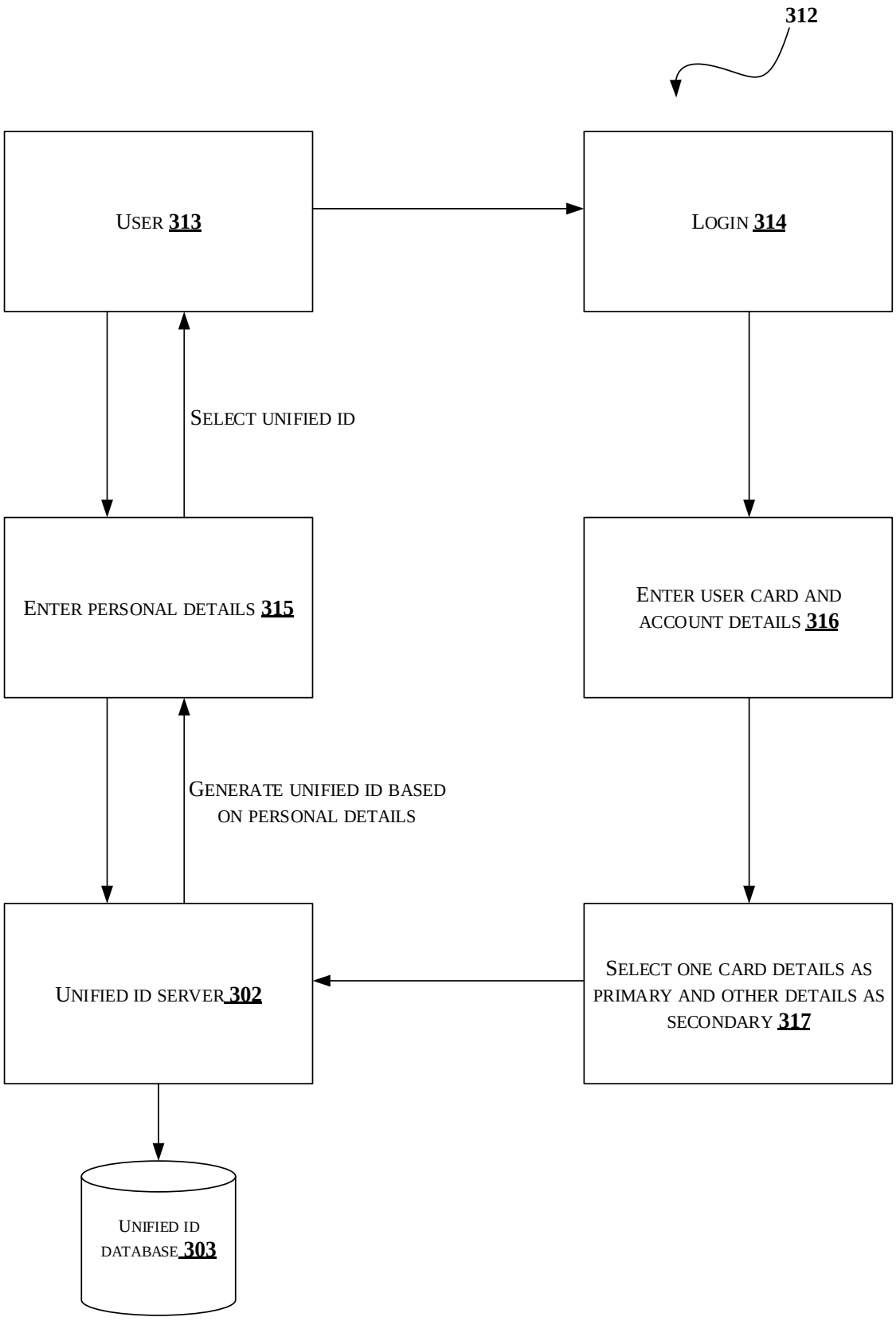
312
USER 313
LOGIN 314
SELECT UNIFIED ID
ENTER PERSONAL DETAILS 315
ENTER USER CARD AND ACCOUNT DETAILS 316
GENERATE UNIFIED ID BASED ON PERSONAL DETAILS
UNIFIED ID SERVER 302
SELECT ONE CARD DETAILS AS PRIMARY AND OTHER DETAILS AS SECONDARY 317
UNIFIED ID DATABASE 303

FIGURE 3C

6/6

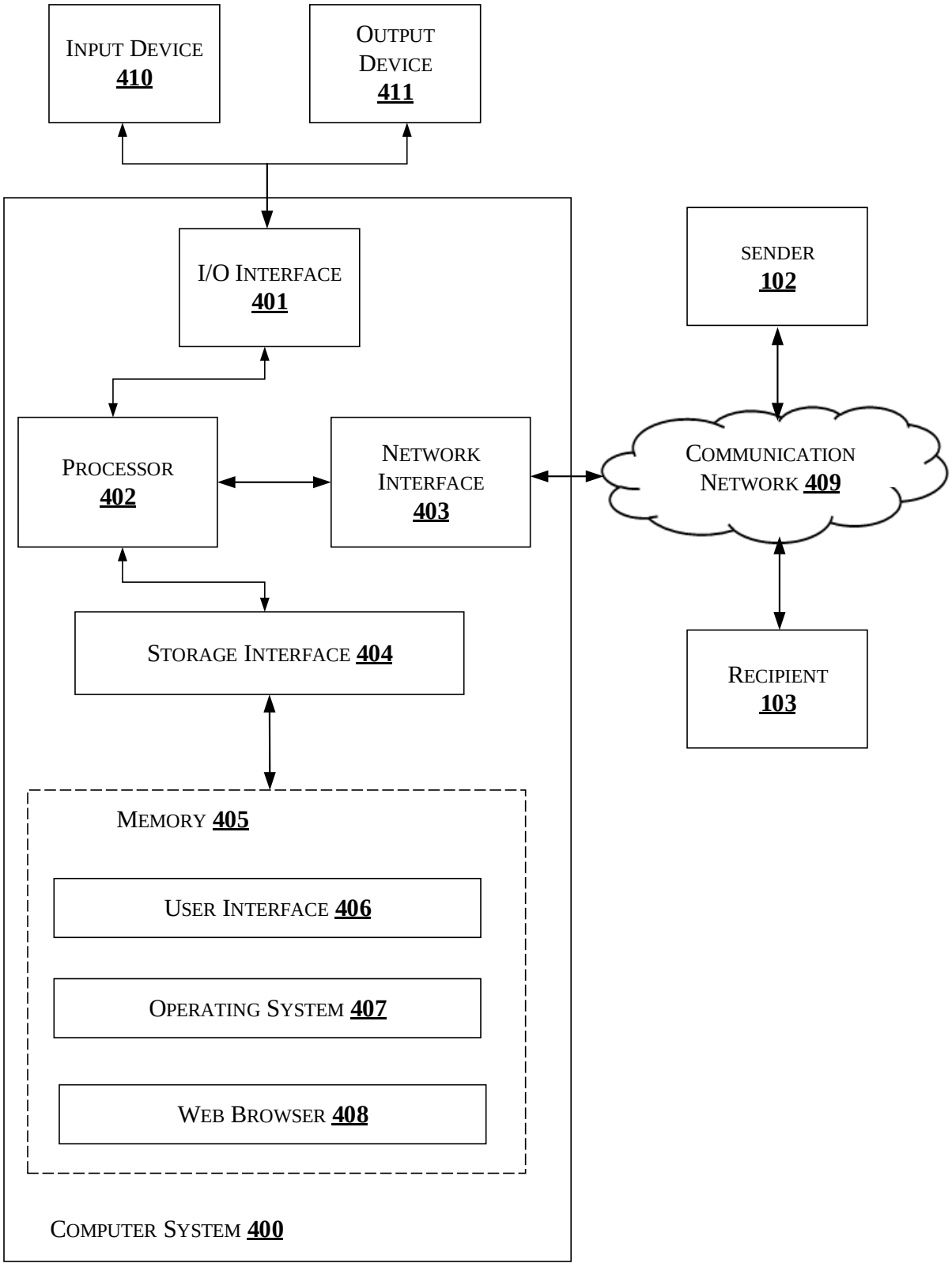
INPUT DEVICE
410
OUTPUT DEVICE
411
I/O INTERFACE
401
PROCESSOR
402
NETWORK INTERFACE
403
STORAGE INTERFACE 404
MEMORY 405
USER INTERFACE 406
OPERATING SYSTEM 407
WEB BROWSER 408
COMPUTER SYSTEM 400
SENDER
102
COMMUNICATION NETWORK 409
RECIPIENT
103

FIGURE 4