April 2022

METHOD AND SYSTEM FOR SECURE THIRD-PARTY IDENTIFICATION

TODD MAZUREK
VISA

NEERAV BERRY
VISA

ANYA MILLER
VISA

METHOD AND SYSTEM FOR SECURE THIRD-PARTY IDENTIFICATION

VISA

INVENTORS:

TODD MAZUREK

NEERAV BERRY

ANYA MILLER

TECHNICAL FIELD

[0001] The present subject matter related to field of financial transactions, more particularly to secure third-party identification in online transactions.

BACKGROUND

[0002] Financial institutions, wallet providers, for example, Apple Pay, messaging platforms, FinTechs and other Customer Service Providers (CSP) offering bill payment services to their customers want to integrate with a number of third parties, e.g., billers, credit bureaus (e.g., Experian, TransUnion and Equifax in the US), accounting platforms (e.g., Quickbooks) and messaging platforms (e.g., Instagram), etc., in order to provide a rich bill pay experience. Consider a scenario where CSPs want to integrate with billers to get bills from and send bill payments to, with credit bureaus to provide payment histories to them to improve the customer's credit score and with accounting systems to exchange payment histories. With each third-party, the CSP needs to mutually identify the customer in a secure fashion.

[0003] The assumptions which are made when the CSPs want to integrate with a number of third parties are: a) The CSP has performed know-your-customer (KYC) authentication of the customer and possesses certain verified personal identifiable information (PII), such as name, email, phone, address, etc. Some of the PII may be generated by the CSP, for example bank account number. b) Each third-party possesses certain customer PII. Some of the PII may be generated by the third-party, for example billers typically generate a unique account number (biller account number) for each customer.

[0004] There are various stakeholders in a bill payment eco-system. For example, the stakeholders may be, a customer, a CSP and a third party. Each stakeholder has set of their own needs when it comes to protecting sensitive information from leaking and comes to mutual customer identification.

[0005] Each stakeholder has their set of needs/requirements. The customer wants to know what PII is being shared with each third-party and provide consent prior to the sharing. The customers are also concerned about breach of their private information held at the CSPs and third parties. Hence, customers prefer that the information exchanged between the CSP, and third parties is kept to the minimum required and, if there is a choice, the least sensitive set of

PII is exchanged (for example, the customers would prefer that the CSP share name, address, and year of birth rather than the full social security number). The customers prefer that the linking be done with data that CSP and each third-party already possess and if manual data entry is required, customers prefer to enter the least amount of information.

[0006] Further, the CSP needs to securely disclose customer information to third-parties. The CSPs would not like to disclose any PII that the third-party does not already have as the purpose of disclosing the PII is to mutually identify the customer, and not to provide new PII to the third-party. Hence, the CSP may wish to withhold account numbers (for example, bank account numbers, credit card details, etc.) from third parties.

[0007] Furthermore, another stakeholder, for example, a third-party biller, would like to withhold billing account numbers or other sensitive information from CSPs.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, serve to explain the disclosed principles. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. 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:

[0009] Fig. 1 illustrates an exemplary environment of a system for implementing embodiments consistent with the present disclosure.

[0010] Fig. 2 shows a flowchart illustrating a process for secure third-party identification and linking.

[0011] Fig. 3 illustrates a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[0012] 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

[0013] 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.

[0014] 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.

[0015] 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.

[0016] 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.

[0017] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to", unless expressly specified otherwise.

[0018] The present disclosure proposes a method and a system for securing third-party identification. The proposed system invokes its dynamic matching algorithm, which checks for matches between the Customer Service Provider (CSP) and the third-party entity profiles. The proposed system maintains a set of canonical customer identification attributes to facilitate matching between entities based on sensitivity and stability of the attributes. The proposed system provides a solution for linking the CSPs with third parties by sharing the least sensitive information with each other to identify a customer. According to the proposed system the information is obtained from the customer in case the information is not available with the CSP or the third party. The proposed system is adaptive and automatically updates entity profiles with each match. The information shared during the linking session is deleted.

[0019] **Fig. 1** illustrates an exemplary environment of a system for implementing embodiments consistent with the present disclosure. In an embodiment, the exemplary environment may include, without limiting to, a customer, a Customer Service Provider (CSP), a Bill Payment Network, and a third party (e.g., a biller).

[0020] When a customer and/or a Customer Service Provider (CSP) offering bill payment services to their customers wants to integrate with third parties like billers, credit bureaus, accounting platforms, messaging platforms, etc., the Bill Presentment & Payment Network (BPPN) provides a scalable way of solving the customer identification problem by providing a network linking CSPs (directly and/or via their processors) on one side of the network with third parties on the other side. In an embodiment, a method for linking CSPs with third parties using the BPPN is disclosed. The method is performed by the system. When entities like CSPs and third parties are onboarded, the BPPN performs Know Your Customer (KYC) authentication on each participating entity so that the participating entities may trust each other. KYC authentication includes checking whether the entity is duly organized, obtaining contact information, obtaining the list of Personal Identifiable Information (PII) attributes maintained by the entity and obtaining assurances from the entity that it has processes to manage, safeguard and verify customer information, etc. The BPPN maintains a database of Canonical attributes which contains the information as shown in table 1. In the below table 1, each attribute has a name and format for each attribute (for example Social Security Number is a 9-digit number, ZIP code can be a 5 or a 9-digit number, etc.). A Canonical attribute may be a composite of other Canonical attributes (for example, birth date is a composite of birth year and birth month/date). Each attribute is assigned a sensitivity rating and stability rating, which defines

how sensitive and how stable the information is (for example Social Security Number is both highly sensitive and highly stable while Address is less sensitive and stable).

Attribute	Format	Sensitivity	Stability
Equipment ID	100 characters	1	1
Email	user@domain	1	2
Phone Number	Country Code-Number	1	1
First Name		1	5
Middle Name		1	5
Last Name		1	6
Name		2	6
Address ZIP	5 or 9 digits in the US	1	4
Address		3	3
Birth Month/Date	MM/DD	3	7
Birth Year	YYYY	4	7
Birth Date	MM/DD/YYYY	9	7
Mother's Maiden Name		8	7
Social security number	9-digit integer	10	6
Biller1 Account Number	10 digits	5	4
US Bank Account Number	6-17 digits	5	5

Table 1 Canonical Customer Attributes

[0021] In an embodiment, the BPPN maintains a matching profile for each entity as shown in table 2 below. In the table 2 below, the matching profile includes the set of attributes maintained by the entity for customer identification purposes. Each attribute has a name, format and range of values provided by the entity and is also mapped to the canonical attributes (for example, Account Number for a biller would be mapped to the Biller Account Number canonical attribute, name would be mapped to Salutation + First Name + Middle Name + Last Name attributes and Last 4 of Social would be mapped to last four digits of the Social Security Number canonical attribute). Each attribute in the matching profile is tagged as verified or not depending on whether the entity has verified that customer information attribute. The minimal

sequence of attributes required for identifying customers is also maintained for each entity. The minimal sequence is the equivalent of the set of identification questions a customer is asked when they call the entity, (for example, the CSP or the third party may ask "please give me your account number or your name and address, if you don't remember your account number."). The minimal sequence can be nested AND/OR expressions as shown in table 2 below. The matching profile can be updated programmatically by the Entity or via a portal provided by BPPN.

Attribute	**Canonical Attribute**	**Verified?**
Name	Name	Yes
Social Security Number	Social Security Number	Yes
Home Address	Address	Yes
Bank Account Number	US Bank Account Number	Yes
Email	Email	Yes
Phone	Phone	Yes

Sample CSP Minimum Matching Sequence:
(Name, Home Address, Bank Account Number and (Email or Phone)) or (Name, Home Address, Social Security Number and (Email or Phone))
Table 2 Sample CSP Matching Profile

[0022] When a customer and/or a CSP wants to link with a third-party the CSP calls the BPPN to initiate a customer linking session or vice versa when a third-party wants to link with a customer and/or a CSP the third party calls the BPPN to initiate a customer linking session. The BPPN's Linking Manager invokes its dynamic matching algorithm. According to the dynamic matching algorithm, the BPPN checks if there's a match between the CSP's matching profile and the third-party's matching profile. Specifically, the Dynamic Matching Algorithm computes combinations of CSP attributes that can match what the third-party requires to link with CSP. There may be one, multiple or no matches. The BPPN can perform extraction and aggregation (for example, if a third-party needs Year of Birth and CSP has the date of birth, then the BPPN can extract the year from the date of birth. Or, if a CSP has First, Middle and Last Name and a third-party requires Name then the BPPN can construct the name from first, middle and last name). If there are multiple matches the BPPN ranks them in an order from

highest to lowest as follows. The matches using verified data from both entities are ranked the highest. Matches which use the least sensitive data are second. Matches which use the most stable data are third. The last are the matches using unverified data from the CSP with verified data from the third-party. If there are no matches, the BPPN identifies the least sensitive set of attributes that the CSP is missing. The BPPN asks the CSP to obtain missing data from the customer. The data obtained from the customer that is not independently verified is considered unverified data. If required, the CSP asks customer for missing data and provides it to the BPPN. The linking manager then initiates a linking session with the third-party. The linking manager provides the matching data to the third-party. If the third-party finds a unique match with the data provided, the third-party provides a status and may provide a unique ID for future identification of the same customer with that third-party. If the third-party does not find a unique match with the data provided, then the third-party may provide a set of step-up authentication parameters to finish the match. If the third-party wants to provide a set of step-up authentication parameters to finish the match, then the process of ranking the matches is repeated to see if there's a match with data the CSP along with the data can be obtained from the customer. If the third-party does not provide step-up authentication parameters to finish the match, then the linking manager provides the matching data for the next matching option till all the matching options are exhausted. Once a customer is uniquely identified by the third-party, the third-party provides a status and may provide a unique ID for future identification of the same customer with that third-party. The BPPN transmits the information provided by the third-party to the CSP. The BPPN updates the third-party profile as it learns about success of matches and step-up authentication. This makes the system adaptive. An implementation of BPPN can start with empty Entity Profiles for third parties where profiles are learned and updated with each match. The BPPN deletes all the information shared during the linking session. The present disclosure helps in providing a dynamic and adaptive customer identification when a CSP wants to link with a third party or vice versa. The linking is done on a customer-by-customer basis, and only the least sensitive information is shared between a CSP and a third party. The BPPN is adaptive as it learns and updates the profile of the third-party with each match.

[0023] In an embodiment, the below tables 3A-3D show an exemplary matching scenario based on the attributes available for matching. The minimum matching for sample biller 1 and sample CSP in the below table 3A is name and last four digits of social security number. Hence, these are the attributes that BPPN will send from sample CSP to sample biller 1. For sample biller 2

in table 3B and sample CSP there is no match. The BPPN could ask the sample CSP to get meter number or biller account number. Since the meter number is less sensitive, the BPPN will ask for it rather than the biller account number. In table 3C the sample biller 3 has two matching options (i) Name, email and phone or (ii) Name and social security number. Since email and phone are less sensitive than social security number, BPPN will send those. For sample credit bureau in table 3D there are two matching options (i) Name and address or (ii) Social security number. The BPPN will send name and address since it is less sensitive information. However, sample credit bureau may find that for this customer there are two names at the same address, (e.g., if a father and son have same name and reside at the same address). In that case the sample credit bureau would request year of birth as a step-up authentication parameter to uniquely identify the customer. Hence, BPPN would request the Sample CSP for the year of birth.

Attribute	**Canonical Attribute**	**Verified?**
Name	Name	Yes
Social Security Number	Social Security Number	Yes
Service Address	Address	Yes
Biller Account Number		Yes

Sample Biller1 Minimum Matching Sequence:
(Name and Service Address) or (Name and Last four digits of Social Security Number) or Biller Account Number

Table 3A – Sample biller 1

Attribute	**Canonical Attribute**	**Verified?**
Name	Name	Yes
Meter Number	Equipment ID	Yes
Biller Account Number		Yes

Sample Biller2 Minimum Matching Sequence:
(Name and Meter Number) or Biller Account Number

Table 3B – Sample biller 2

Attribute	Canonical Attribute	Verified?
Name	Name	Yes
Social Security Number	Social Security Number	Yes
Service Address	Address	Yes
Biller Account Number		Yes
Email	Email	Yes
Phone	Phone	Yes

Sample Biller3 Minimum Matching Sequence:
(Name and Service Address) or Biller Account Number or (Name, Email and Phone) or (Name and Last Four of Social Security Number)

Table 3C – Sample biller 3

Attribute	Canonical Attribute	Verified?
Name	Name	Yes
Social Security Number	Social Security Number	Yes
Home Address	Address	Yes
Date of Birth	Date of Birth	Yes
Mother's Maiden Name	Mother's Maiden Name	Yes

Sample Credit Bureau Minimum Matching Sequence:
(Name and Address) or Social Security Number

Table 3D – Sample credit bureau profile attributes

[0024] **Fig. 2** shows a flowchart illustrating a process for secure third-party identification. **At block 201**, the method comprises calling the Bill Presentment and Payment Network (BPPN) to initiate customer linking session. For example, a customer wants to link with a third-party bill pay application, the Customer Service Provider (CSP) calls the BPPN to initiate the linking session with the third-party. The BPPN maintains a set of attributes based on how sensitive and how stable the attributes are. The BPPN also performs Know Your Customer (KYC) authentication for each entity the BPPN onboards so that the participating entities may trust each other. **At block 203**, the method comprises invoking a dynamic matching algorithm. The dynamic matching algorithm checks for matches between the CSP and the third-party entity

profiles. The entity profile includes the set of customer identification attributes maintained by each entity (for example, name, address, email, phone, etc.). The Entity Profile identifies which attributes are verified by the entity and includes a matching sequence. If there's one match proceed to the next step. If there are multiple matches the BPPN ranks the match that use verified data on both sides first, then by sensitivity (least sensitive gets a higher ranking) then by stability (most stable gets a higher ranking) and lastly by utilizing some unverified data from the CSP. Matching options utilizing unverified data held by the third-party side are disregarded. If there are no matching options, the matching algorithm identifies the least sensitive set of attributes that the CSP needs to obtain from the customer and then asks the customer to provide the missing data. **At block 205**, the method comprises initiating a linking session with third party. **At block 207,** the method comprises providing the matching data by the BPPN issuer identified **at block 203**. If the third-party finds a unique match with the data provided, proceed to the next step. If not, the third-party may provide step-up authentication attributes or it may not. If it does not, the BPPN sends the attributes from the next matching option identified **at block 203** to the third-party. If step-up attributes are provided by the third-party follow the same process as **block 203** to see if those attributes are available or can be obtained from the customer. **At block 209,** the method comprises providing a status and a unique ID to each customer for future identification. **At block 211,** the method comprises transmitting the information provided by the third party to the CSP. **At block 213,** the method comprises updating the third-party profiles as the BPPN learns with every match. This makes the BPPN adaptive, if an implementation of BPPN starts with empty entity profiles for third parties, the profiles are learned and updated with each match. Finally, **at block 215,** all the information shared during the linking session is deleted.

[0025] Computer System

[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 securing third-party identification. 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 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.

[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 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.

[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.

[0035] 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. 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.

[0036] 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.

[0037] 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.).

[0038] 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.

[0039] 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.

[0040] 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.

[0041] 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.

METHOD AND SYSTEM FOR SECURE THIRD-PARTY IDENTIFICATION

ABSTRACT

The present disclosure relates to a method and system for two parties, such as a Customer Service Provider and a biller, to authenticate a mutual customer. The present invention uses a dynamic matching algorithm to check and match the customer information available from each party, without either party disclosing new information about the customer to the other. The method also comprises maintaining a set of canonical customer identification attributes to facilitate matching between entities based on sensitivity and stability of the attribute. The present disclosure provides a solution for authenticating customers by sharing the least sensitive information with each other to identify a customer. The method also comprises obtaining the information from customer in case there is no match. The system is also updated at the same time which makes the system adaptive. The information shared during the linking session is deleted.

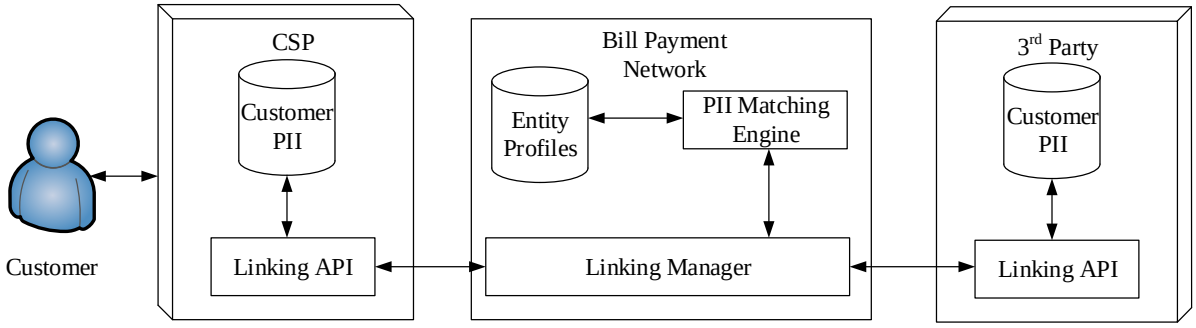
CSP
Customer PII
Linking API
Customer
Bill Payment Network
Entity Profiles
PII Matching Engine
Linking Manager
3rd Party
Customer PII
Linking API

Fig. 1

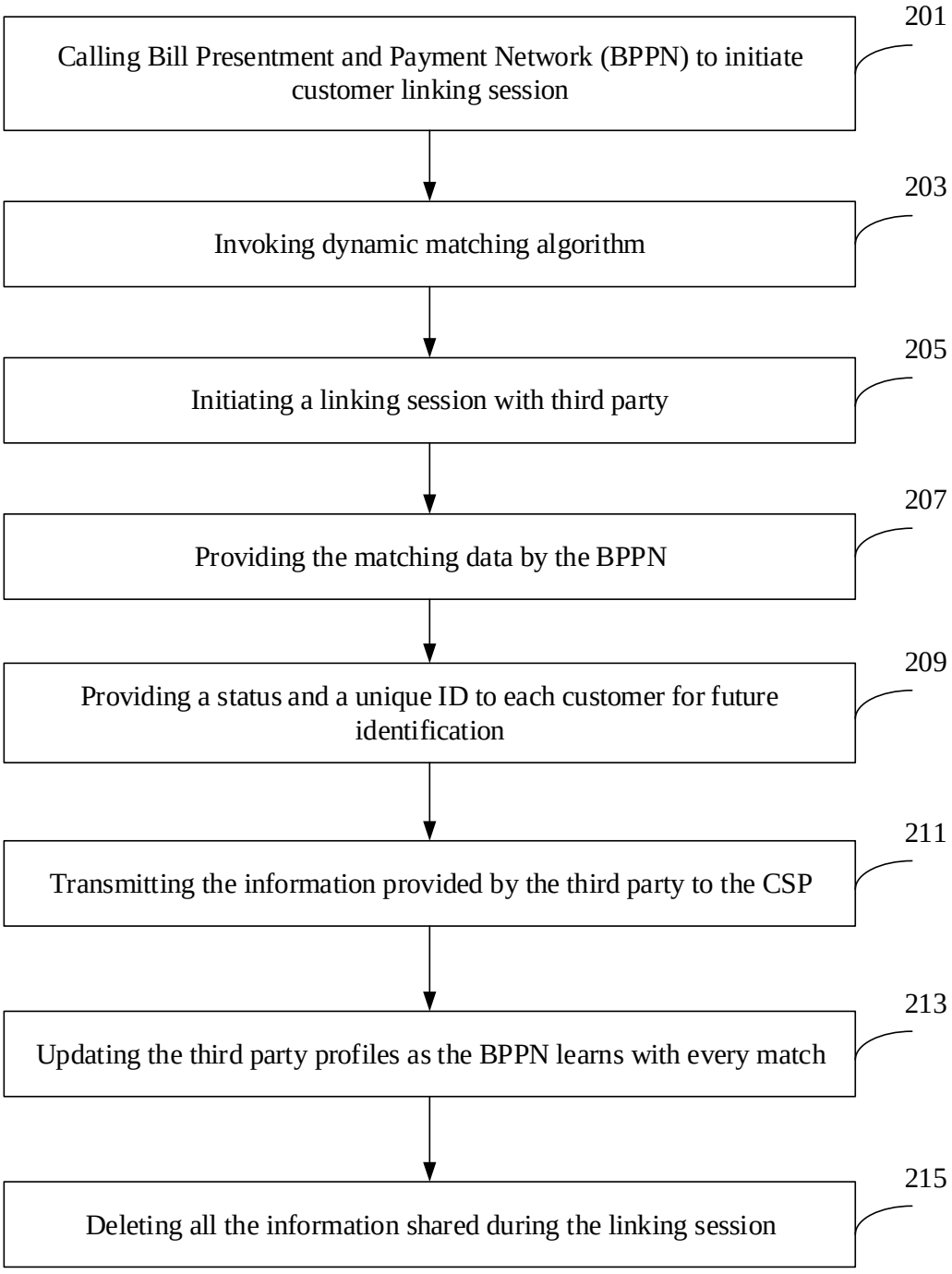
201
Calling Bill Presentment and Payment Network (BPPN) to initiate customer linking session
203
Invoking dynamic matching algorithm
205
Initiating a linking session with third party
207
Providing the matching data by the BPPN
209
Providing a status and a unique ID to each customer for future identification
211
Transmitting the information provided by the third party to the CSP
213
Updating the third party profiles as the BPPN learns with every match
215
Deleting all the information shared during the linking session

Fig. 2

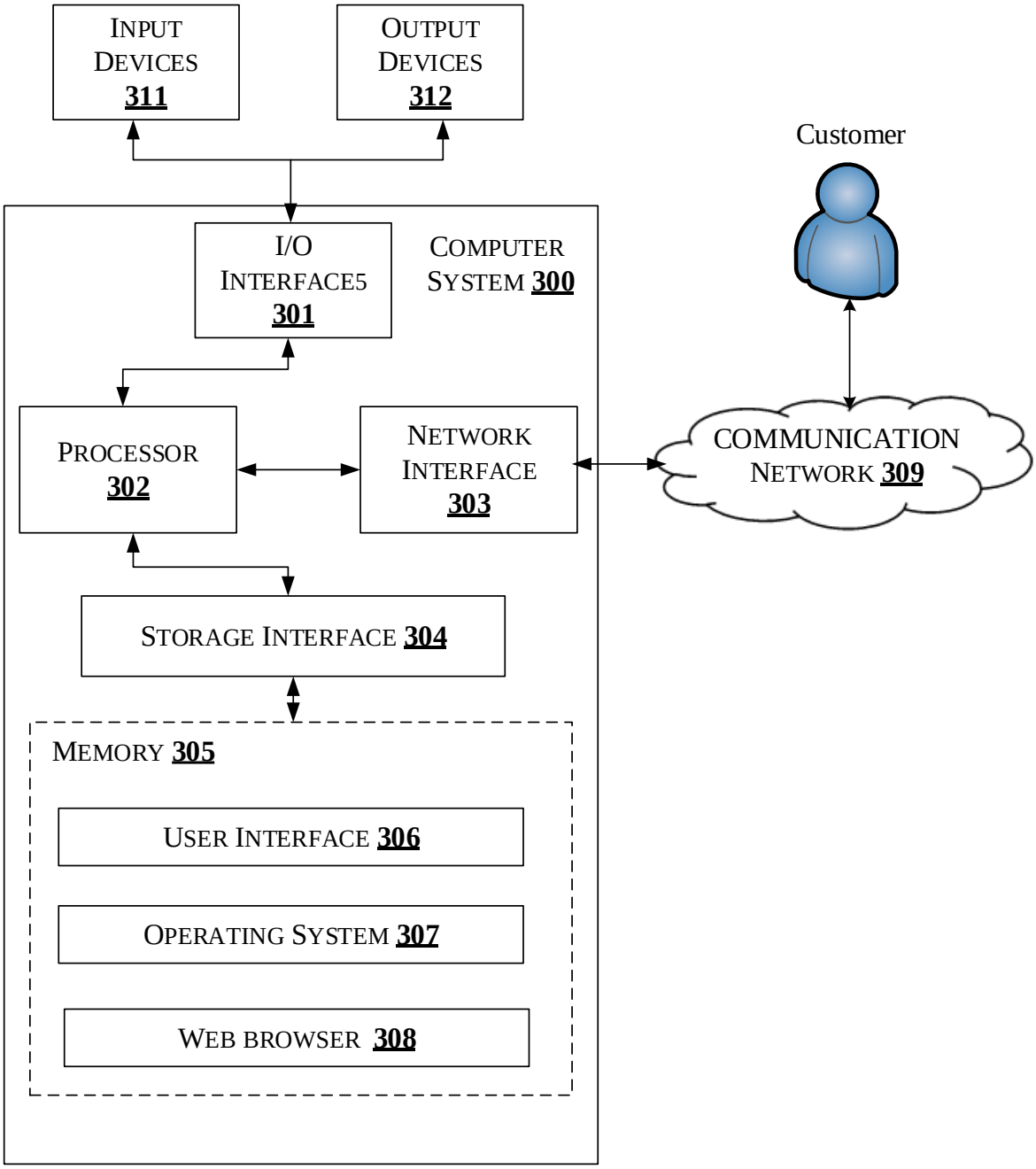
INPUT DEVICES 311
OUTPUT DEVICES 312
Customer
I/O INTERFACE5 301
COMPUTER SYSTEM 300
PROCESSOR 302
NETWORK INTERFACE 303
COMMUNICATION NETWORK 309
STORAGE INTERFACE 304
MEMORY 305
USER INTERFACE 306
OPERATING SYSTEM 307
WEB BROWSER 308

Fig. 3