(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 August 2019 (29.08.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/162879 A2

(51) International Patent Classification:
Not classified

(21) International Application Number:
PCT/IB2019/051429

(22) International Filing Date:
21 February 2019 (21.02.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

201811006836	22 February 2018 (22.02.2018)	IN
201811017690	10 May 2018 (10.05.2018)	IN
201811047475	14 December 2018 (14.12.2018)	IN

(71) Applicant: **DIZZI PAY HOLDINGS LTD.** [IL/IL]; Medinat Hayehudim 85, 46140 Herzliya (IL).

(72) Inventors: **ARORA, Pankaj**; 3B, Bliss Greens, opposite Prakash Towers, Peermuchula, Punjab, Zirakpur 140603 (IN). **BARUCH, Alfia**; 23 Haruv st., 60415 Or Yehuda (IL). **KUGEL, Yoram**; 58 Merino Dr. Alfredton Vic. 3350, AUSTRALIA, Alfredton, Victoria 3350 (AU). **SHAKED, Avi**; 28 hagderot, St. Savion, 56526 Savion (IL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

(54) Title: SYSTEM, APPARATUS, AND METHOD FOR INHIBITING PAYMENT FRAUDS

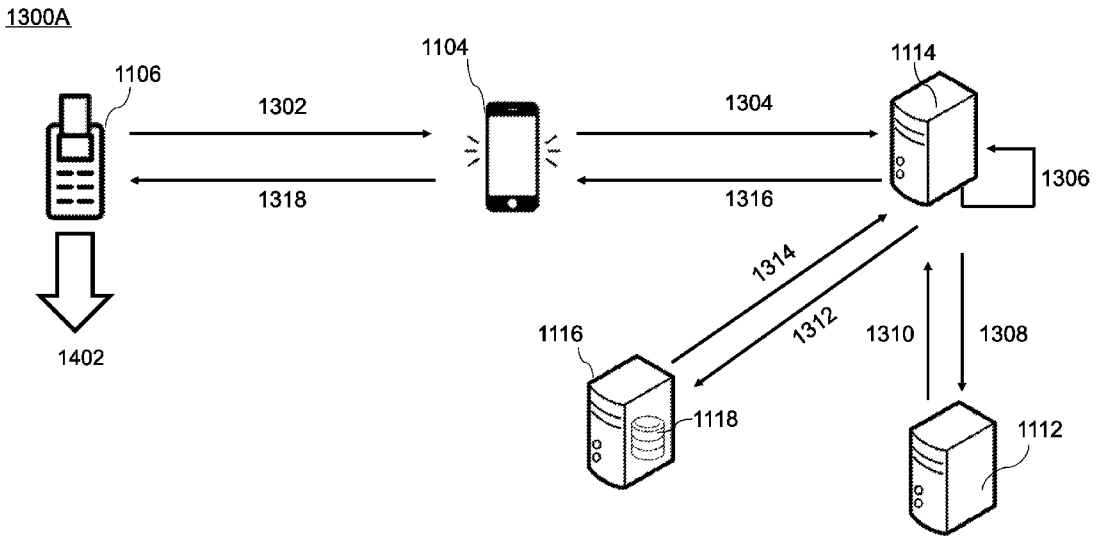


FIG. 13A

(57) Abstract: Embodiments of the present disclosure provides a system for enabling users to perform secure anonymous payments over web portals or over merchant POS devices. The users are not required to share their identities or their payment card details. Embodiments of the present invention enables the users to pay securely to anyone without sharing any personal or banking details with third parties.

WO 2019/162879 A2

[Continued on next page]

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

SYSTEM, APPARATUS, AND METHOD FOR INHIBITING PAYMENT FRAUDS

CROSS REFERNCE TO RELATED APPLICATIONS

[0001] This application claims benefit from Indian application number 201811006836 filed on February 22, 2018; from Indian application number 201811017690 filed on May 10, 2018 and from Indian application number 201811047475 filed on December 14, 2018. These documents are incorporated herein by reference in its entirety.

FIELD OF THE INVENTION

[0002] Embodiments of the present invention in general, concern a system, apparatus, and method for processing of transactions. More particularly, embodiments of the present invention concern to a system, apparatus, and method to process safe and secure transactions.

BACKGROUND OF THE INVENTION

[0003] Nowadays, use of credit cards and debit cards for monetary transactions is very common. Use of payment cards (i.e. prepaid cards, corporate cards, credit/debit cards, gift cards, etc.) provide ease to users in performing transactions as users are not required to remember details of their bank accounts. Instead, users are only required to remember a pass-code as an authentication factor for using their debit/credit cards. Obviously, it is an easier option than remembering a long bank account number.

[0004] However, debit/credit cards do not provide any security if a hacker has access to the pass-code as well as to the debit/credit card by cloning/skimming of the debit/credit card. Although, there is an option of reporting theft cases and getting fraud transaction reversed, but this option is a remedy after theft and not a preventive measure. Therefore, banks and financial institutions advice against sharing pass-codes and debit/credit card details with third parties.

[0005] There are millions of users who only have access to bank accounts but no access to debit/credit cards. In addition, there are many merchants who have access to systems for accepting magnetic cards and these merchants would like to bring the millions of potential customers to their stores or websites.

[0006] There are several websites and online banking stores that are currently not able to do business with millions of customers that have bank accounts but no access to debit or credit cards or even with access are unwilling or unable to access these sites.

[0007] Many customers who may have access to debit or credit cards do not want to use their debit or credit cards at the merchant side with a fear that their cards details can be stolen and used for illegal activities.

[0008] Many merchants have been registered by other wallets or have been registered by other services but still would just like to retain one receipt account e.g. access to a payment receipt machine from an authorized bank and not multiple wallets etc.

[0009] Nevertheless, despite of all education given by the banks and financial institutions, a huge amount of theft cases is still reported. Thieves and hackers have been successful in stealing debit/credit card details as well as pass-codes. A lot of solutions have been invented for preventing it, such as two-step authentication etc. However, hackers still have found ways to crack the two step authentication processes via identity theft.

[0010] Hence, it is apparent that a need exists for a technique that decimates the above-mentioned problems of the prior art and provides an improved method for preventing identity thefts and payment frauds.

[0011] The applicant has devised, tested and embodied the present invention to overcome the shortcomings of the state of the art and to obtain these and other purposes and advantages.

SUMMARY OF THE INVENTION

[0012] In order to improve the above-mentioned systems, a new technique has been devised to secure payment transactions and eliminate a number of challenges that exist in the cashless payment market by simplifying and virtualizing the payment process between a consumer and a merchant.

[0013] It is an object of the invention to provide a secure payment system, to protect identity of users from theft or hacking during merchant payments.

[0014] It is another object of the invention to provide ability for users to shop anywhere in the world without owning a card.

[0015] It is yet another object of the invention to protect identity of users if data collected by the merchant's during the transaction process is ever compromised.

[0016] It is yet another object of the invention to provide card based payment transactions between payer and payee, wherein the payer is not required to own a payment card to make the transactions.

[0017] It is another object of the invention to provide a payment platform that eliminates fraud concerns while shopping using bank payment platform.

[0018] It is another object of the invention to enable users to make payments anonymously.

[0019] It is another object of the invention to enable users to make payments without the need to share their actual card details.

[0020] It is another object of the invention to provide a payment platform to eliminate the chargeback and declines.

[0021] It is another object of the invention to provide a payment platform to eliminate card declines, wherein pre-notification to card issuer for every transaction is a sort of positive pay message to the card issuer which results in successful transactions for every authorization request.

[0022] It is another object of the invention to provide a payment platform that eliminates the need of cash based transactions and, thus accelerates the transition to a cashless economy.

[0023] To achieve these and other advantages, and in accordance with the purpose of the invention as embodied and broadly described, the invention provides a computer implemented method for processing transactions. The method utilizes a transaction processing engine to determine validity of an ongoing transaction. The transaction processing engine is configured to receive a plurality of notifications from a plurality of user devices, each of the plurality of notifications, received from a respective user device, comprises a virtual payment card associated with a corresponding ongoing transaction. The transaction processing engine is also configured to receive a plurality of verification requests from a plurality of merchant devices, wherein each of the plurality of verification requests, received from a respective merchant device, comprises a virtual payment card associated with a corresponding ongoing transaction. The transaction processing engine is further configured to compare the plurality of verification requests and the plurality of notifications to determine whether at least one verification request and at least one notification comprises same virtual payment card. The transaction processing engine is also configured to identify an ongoing transaction associated with the same virtual payment card of the at least one verification request and the at least one notification. Further, once the ongoing transaction associated with the same virtual payment card is identified, the transaction processing engine is configured to determine the validity of the identified ongoing transaction, wherein the identified ongoing transaction is determined to be valid when the at least one verification request and the at least one notification satisfy a predefined time criterion. The predefined time criterion is determined to be satisfied by the transaction processing engine when the at least one notification and the at least one verification request are received before lapse of a predefined time period, wherein the predefined time period is determined using a timestamp received in the at least one notification from the respective user device, the at least one verification request received from the respective merchant device or both.

[0024] The computer implemented method further enables executing following two steps concurrently in real-time prior to the comparison by the transaction processing engine, and determining, by the transaction processing engine, that the two steps are executed concurrently in real time using the timestamp received in the notification to determine the validity of the identified ongoing transaction:

associating, by the respective user device, the virtual payment card with the ongoing transaction, and transmitting, by the respective user device, the at least one notification to the transaction processing engine, wherein the at least one notification comprises the virtual payment card details and the timestamp associated with the ongoing transaction; and

transmitting, by the respective merchant device in communication with the respective user device, the at least one verification request to the transaction processing engine for the processing and verification of the ongoing transaction, wherein the verification request comprises the virtual payment card details associated with the ongoing transaction.

[0025] Further, the transaction processing engine is configured to receive merchant details incorporated in the at least one notification and the at least one verification request, and the identified ongoing transaction is determined to be valid when the merchant details are determined to be same, by the transaction processing engine, in the at least one notification and the at least one verification request. The merchant details comprise one or more of merchant identifier, merchant location, merchant name, merchant device ID, and merchant address.

[0026] Further, details of the virtual payment card received in the at least one verification request is provided to the respective merchant device by the respective user device using a contactless mode of communication, wherein the respective user device is performing the ongoing transaction with the respective merchant device, the respective merchant device is point-of-sale (POS) device, and the contactless mode of communication is one or more of a NFC, RFID, infrared, Bluetooth, and QR code scan.

[0027] The computer implemented method further utilizes the respective user device, the respective user device is configured to store in advance one or more virtual payment cards in a memory of the respective user device. The respective user device is configured to associate the virtual payment card, selected from the one or more virtual payment cards, with the ongoing transaction, and transmit the at least one notification to the transaction processing engine, wherein the at least one notification comprises the virtual payment card associated with the ongoing transaction. The respective user device is also configured to share the associated virtual payment card to the respective merchant device. Further, the respective user device is configured to receive merchant details from the respective merchant device, wherein the at least one notification further comprises the merchant details and/or the timestamp that are used by the transaction processing engine to determine the validity of the ongoing transaction.

[0028] The computer implemented method further utilizes the respective merchant device, the respective merchant device is configured to receive the virtual payment card associated with the ongoing transaction, from the respective user device, at initiation of the ongoing transaction. The respective merchant device is also configured to transmit the at least one verification request to the transaction processing engine, wherein the at least one verification request comprises the virtual payment card associated with the ongoing transaction.

[0029] It is yet another object of the invention to automatically fill payment details in corresponding one or more fields on a payment portal web interface, and submitting a request comprising the automatically filled details on the payment portal web interface to process an ongoing transaction. To achieve this object of the present invention, a user device is utilized, wherein the user device comprises one or more processors and a memory coupled to the one or more processors, the memory storing instructions which when executed by the one or more processors instruct the user device to perform acts comprising: receiving and displaying a payment portal web interface to make payment for an ongoing transaction; receiving an authorization to process the ongoing transaction; transmitting a request to a remote server to generate a virtual payment card corresponding to the ongoing transaction after receiving the authorization; receiving a response from the remote server, wherein the response comprises at least a virtual payment card generated by the remote server; identifying one or more fields on the payment portal web interface to be filled to process the ongoing transaction; extracting one or more details from the response received from the remote server corresponding to the one or more fields on the payment portal web interface; filling automatically the extracted one or more details in the corresponding one or more

fields on the payment portal web interface, and submitting a request comprising the automatically filled details on the payment portal web interface to process the ongoing transaction. According to an aspect, the authorization to process the ongoing transaction is provided manually by a user of the user device. According to another aspect, the memory of the user device further comprises instructions which when executed by the one or more processors instruct the user device to perform act comprising: providing automatically the authorization to process the ongoing transaction by automatically selecting a suitable payment method on the basis of previously stored user preferences or user purchase history, wherein one or more payment methods are displayed on the payment portal web interface. Also, the one or more details extracted from the response received from the remote server are virtual payment card number, virtual payment card expiry time, virtual payment card generation time, user name, CVV, and/or contact details. The request comprising the automatically filled details is submitted to a merchant acquirer server. Once the request comprising the automatically filled details is received by the merchant acquirer server, a verification request comprising the virtual payment card received from the automatically filled details is forwarded to a transaction processing engine to determine if the payment can be approved on the basis of a comparison, wherein the payment is approved when the virtual payment card details shared by the merchant acquirer server matches to the already stored information in a database of the transaction processing engine and the verification request is received form the merchant acquirer server before lapse of a predefined time period. The predefined time period is calculated using a timestamp provided by the user device at the initiation of the ongoing transaction. The user device is also configured to receive the notifications about the status of the ongoing transaction, wherein the status of the ongoing transaction can be success or the denial of the payment.

[0030] In accordance with another purpose of the invention as embodied and broadly described, the invention provides a computer implemented method for processing transactions. The computer implemented method utilizes a transaction processing engine, a card issuer, a financial institution, and a user device, a merchant device, and a merchant acquirer. The user device is configured to initiate an ongoing transaction with the merchant device. In one aspect, the merchant device is a point-of-sale device, and the user device and the merchant device are configured to communicate using a contactless mode of communication (e.g. NFC). In another aspect, the merchant device and/or the merchant acquirer is configured to provide payment portal web interface to the user device to process online transactions. In yet another aspect, the merchant device is configured to initiate an ongoing transaction with the user device.

[0031] Once transaction is initiated, the user device is configured to receive one or more details associated with the ongoing transaction from the merchant device, wherein the details can be, such as but not limited to, transaction amount, the payment time stamp, merchandise details, merchant ID, merchant name, merchant location, branch/outlet details, merchant address, merchant device ID, etc. Once the details associated with the ongoing transaction are received, the user device waits for an authorization to proceed further to process the transaction, wherein the authorization may be provided manually or automatically. Once the authorization is received, the user device transmits a notification associated with the ongoing transaction to a financial institution, the notification comprises details associated with the ongoing transaction, user account details and credentials, and/or a timestamp. The financial institution is configured to verify if associated user account can execute the ongoing transaction and/or if user account details/credentials are legitimate.

[0032] If output of the verification step comes out to be affirmative, then the financial institution is configured to transmit a request to a card issuer to dynamically generate a virtual payment card for the ongoing transaction and associate the generated virtual payment card with the ongoing transaction. In an aspect, the card issuer may be configured to select a virtual payment card from one or more pre-stored virtual payment cards and may associate the selected virtual payment card with the ongoing transaction. Thereafter, the virtual payment card associated with the ongoing transaction along with the one or more details associated with the ongoing transaction are stored in a database of the transaction processing engine, wherein the details comprises such as, but not limited to, a merchant device ID, merchant details, transaction amount, currency, USERID, State of the transaction (=approved/denied), virtual card details, timestamp, and card use status (=open/closed). Also, the virtual payment card associated with the ongoing transaction is provided to the user device, which thereby shares the same with the merchant device. In an aspect, the virtual payment card is shared with the merchant device using the contactless mode of communication, such as, and without limitation, NFC, RFID, Bluetooth, and/or Wi-Fi.

[0033] Thereafter, the merchant device is configured to transmit a verification request comprising the virtual payment card received from the user device and other ongoing transaction related details to the merchant acquirer, which thereby forwards the received details to the transaction processing engine. The transaction processing engine is configured to receive the verification request and compare the virtual payment card with the already stored information to determine if the received virtual payment card from the merchant device is same as that of the virtual payment card generated and stored in the database corresponding to the ongoing transaction. Once the match is found, it is determined that whether the verification request from the merchant device is received before lapse of a predefined time period, wherein the predefined time period is determined using the time stamp information received from the user device in the notification. Thus, using present invention, the user's financial institution, the card issuer, and/or the transaction processing engine are aware in advance of where and for what purpose the virtual payment card will be used, and thus transactions can be executed securely, and payment frauds are inhibited.

[0034] In accordance with yet another purpose of the invention as embodied and broadly described, the invention provides a computer implemented method for processing transactions. The computer implemented method utilizes a transaction processing engine to determine validity of cashless transactions. The transaction processing engine is configured to receive a request for processing an ongoing transaction from a user device. The transaction processing engine is configured to facilitate generation of a virtual payment card associated with the ongoing transaction. Also, the transaction processing engine is configured to facilitate sharing of the virtual payment card associated with the ongoing transaction with a user device, wherein the user device is configured to forward the associated virtual payment card with the merchant device. Further, the transaction processing engine is configured to receive a request for verification of the ongoing transaction, wherein the request for verification of the ongoing transaction comprises the virtual payment card from the merchant device. The transaction processing engine is further configured to determine if the virtual payment card received in the verification request from the merchant device is same as that of the virtual payment card that is previously generated and associated with the ongoing transaction. Once it is determined that the virtual payment card is same, the transaction processing engine is configured to determine validity of the ongoing transaction, wherein

the ongoing transaction is determined to be valid when a predefined time criterion is satisfied by the ongoing transaction, the predefined time criterion is satisfied or not is determined using the timestamp received in the request for processing the ongoing transaction from the user device.

[0035] It is to be understood that both the foregoing general descriptions and the following detailed description are exemplary and explanatory and are intended to provide further explanation of the invention as claimed.

[0036] Additional features and advantages of the invention will be set forth in the description which follows, and in part will be apparent from the description, or may be learned by practice of the invention. The objectives and other advantages of the invention will be realized and attained by the methods, systems, and apparatus particularly pointed out in the written description and claims hereof, as well as the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0037] The above and still further features and advantages of the present invention will become apparent upon consideration of the following detailed description of embodiments thereof, especially when taken in conjunction with the accompanying drawings, and wherein:

[0038] FIG. 1A and 1B illustrates exemplary environment 100 and 101 where various embodiments of the present invention are implemented;

[0039] FIG. 2 illustrates a block diagram of an electronic device 200, in accordance with an embodiment of the present invention;

[0040] FIG. 3 illustrates a flow diagram 300 of a method for anonymously paying to a merchant device (i.e. vendor device), in accordance with an embodiment of the present invention;

[0041] FIG. 4 illustrates a flow diagram 400 of a method for anonymously paying to a merchant device via a wallet service, in accordance with an embodiment of the present invention;

[0042] FIG. 5 illustrates a flow diagram 500 of another method for anonymously paying to a merchant device via a wallet service, in accordance with an embodiment of the present invention;

[0043] FIG. 6 illustrates a flow diagram 600 of another method for anonymously paying to a merchant device, in accordance with an embodiment of the present invention;

[0044] FIG. 7 illustrates a flow diagram 700 of a method for receiving anonymous payments from user devices, in accordance with an embodiment of the present invention;

[0045] FIG. 8 illustrates a flow diagram 800 of a method for generating a single-use virtual payment card, in accordance with an embodiment of the present invention;

[0046] FIG. 9 illustrates a flow diagram 900 of a method for anonymously paying over a payment portal web page, in accordance with an embodiment of the present invention; and

[0047] FIG. 10 illustrates a flow diagram 1000 of a method for refunding an anonymous user, in accordance with an embodiment of the present invention.

[0048] FIG. 11 illustrates exemplary environment 1100 where various embodiments of the present invention are implemented;

[0049] FIG. 12 schematically illustrates a flow diagram 1200 of a conventional payment system;

[0050] FIG. 13A schematically illustrates an exemplary flow diagram 1300A for generating as well as notifying a virtual payment card associated with an ongoing transaction to a transaction processing engine, according to first aspect of the present invention;

[0051] FIG. 13B schematically illustrates an exemplary flow diagram 1300B for generating as well as notifying a virtual payment card associated with an ongoing transaction to a transaction processing engine, according to second aspect of the present invention;

[0052] FIG. 13C schematically illustrates an exemplary flow diagram 1300C for generating as well as notifying a virtual payment card associated with an ongoing transaction to a transaction processing engine, according to third aspect of the present invention;

[0053] FIG. 13D schematically illustrates an exemplary flow diagram 1300D for generating as well as notifying a virtual payment card associated with an ongoing transaction to a transaction processing engine, according to fourth aspect of the present invention;

[0054] FIG. 13E schematically illustrates an exemplary flow diagram 1300E for generating as well as notifying a virtual payment card associated with an ongoing transaction to a transaction processing engine, according to fifth aspect of the present invention;

[0055] FIG. 13F schematically illustrates an exemplary flow diagram 1300F for generating as well as notifying a virtual payment card associated with an ongoing transaction to a transaction processing engine, according to sixth aspect of the present invention;

[0056] FIG. 14 schematically illustrates an exemplary flow diagram 1400 for verifying, by a merchant, information related to the ongoing transaction to determine the validity of the ongoing transactions, in accordance with an embodiment of the present invention;

[0057] FIG. 15 schematically illustrates a flow diagram 1500 for anonymously paying over an online payment portal, in accordance with another embodiment of the present invention; and

[0058] FIG. 16 schematically illustrates a flow diagram 1600 for anonymously paying at point of sale (POS), in accordance with another embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0059] Embodiments of the present invention are best understood by reference to the figures and description set forth herein. All the aspects of the embodiments described herein will be better appreciated and understood when considered in conjunction with the following description and the accompanying drawings. It should be understood, however, that the following descriptions, while indicating preferred embodiments and numerous specific details thereof, are given by way of illustration and not of limitation. Many changes and modifications may be made within the scope of the embodiments herein, without departing from the spirit and scope thereof, and the embodiments herein include all such modifications.

[0060] The terms "user", "consumer", "customer", "buyer", "shopper", "purchaser", "payer" and the plural form of these terms are used interchangeably throughout the specification to refer to those who would use the present invention to purchase the goods or services and make secure payments, unless specified otherwise.

[0061] The terms "merchant", "vendor", "payee", "retailer", "business owners" and the plural form of these terms are used interchangeably throughout the specification to refer to those who are the providers of the goods or services and to whom money is paid, unless specified otherwise.

[0062] The terms "software program", "service application", "computer program", "mobile application", "app", and the plural form of these terms are used interchangeably throughout the specification to refer to a set of computer executable instructions which are executed by the processing units to execute the various steps of the secure payment method of the present invention, unless specified otherwise.

[0063] The term "single use virtual payment card", "virtual payment card", "dynamically generated virtual payment card", "virtual card", "one-time use virtual payment card", and the plural form of these terms are used interchangeably throughout the specification to refer to a virtual payment card of the present invention, unless specified otherwise.

[0064] FIG. 1A illustrates an exemplary environment 100 where various embodiments of the present invention are implemented. The environment 100 includes a data server 102 connected to a plurality of devices 104-a-n and 106-a-m via a network 108, wherein the numbers n and m are arbitrary numbers representing same or different number of devices. Hereinafter, the devices 104-a-n may collectively be referred to as "user devices 104" and the vendor devices 106-a-m may collectively be referred to as "vendor devices 106".

[0065] Similar network environment 101 is illustrated in FIG. 1B wherein the user devices 104 are in communication with the data server 102 via the network 108. However, the user devices 104 are configured to communicate with the vendor devices 106 (not shown) via short range communication protocols, such as but not restricted to, NFC, RFID, Infrared, Bluetooth, etc.

[0066] Further, the user devices 104 may refer to electronic devices that may be utilized by individuals (consumers or customers) to access and communicate with the data server 102. In an embodiment of the present invention, the user devices 104 are portable wireless communication devices such as but not restricted to cell phones, tablets, laptops, wearables, smart watch etc. Further, the vendor devices 106 may refer to electronic devices that may be utilized by retailers or business owners to communicate with the data server 102. In an

embodiment, the service providers or vendors may also be able to directly communicate with the user devices 104.

[0067] Examples of the user devices 104 and the vendor devices 106 may include, but are not restricted to, a desktop computer, a laptop, a mobile/cell phone, a smart phone, a personal digital assistant (PDA), a tablet computer, and the like. The vendor devices 106 may also include POS devices. Further, the network 108 may include, but is not restricted to, a communication network such as Internet, Intranet, PSTN, Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN), and so forth.

[0068] In an exemplary embodiment of the present invention, the user devices 104 are installed with a service application (not shown). In an embodiment of the present invention, the service application may be implemented as a software application (or combination of software and hardware). Further, the service application installed in the user devices 104 is configured to connect the user devices 104 with multiple services offered by multiple service providers via the data server 102. The service application installed in the user devices 104 may also be configured to connect the user devices 104 with the vendor devices 106.

[0069] In an embodiment of the present invention, the service application is based on a web and application infrastructure that use some external support SDK. The service application may be configured to enable user devices 104 in performing secure transactions with vendor devices 106 without disclosing identities or payment account details. In another embodiment, the service application may be configured to enable user devices 104 in performing anonymous transactions with the vendor devices over the network. The functioning of the service application will be detailed further in conjunction with FIGS. 3-10 of the present application.

[0070] FIG. 2 illustrates a block diagram of an electronic device 200 (such as the user device 104, as explained earlier in conjunction with FIG. 1 of the present invention), in accordance with an embodiment of the present invention. As depicted from the figure, the electronic device 200 comprises a processor 202, a memory 206 for data storage, and a network interface module 204 for connecting the electronic device 200 with a network (such as the network 108 defined in conjunction with FIG. 1 of the present invention). The processor 202 may comprise one or more than one processor. The network interface module 204 may be a hardware, a software, or a combination thereof.

[0071] The memory 206 further comprises a database 210 and an instruction set 208. The memory 206 may either be a primary memory or a secondary memory. For example, but not restricted to, random access memory (RAM), cache memory, hard disk drive (HDD), solid state drive (SSD), compact disk (CD), portable memories, and like.

[0072] The instruction set 208 stored in the memory 206 uses the processor 202 to perform actions, e.g., receiving, storing, processing, and transmitting data stored in the memory 206. More specifically, the instruction set 208 stored in the memory 206 uses the processor 202 to perform actions that are defined further in conjunction with FIG. 3-10 of the present invention.

[0073] FIG. 3 illustrates a flow diagram 300 of a method for anonymously paying to a merchant device (i.e. vendor device), in accordance with an embodiment of the present invention. The present invention enables users to securely make cashless transactions at point-of-sale (POS) without owning a bank issued payment card, for example and without limitation, a credit card and/or a debit card.

[0074] Herein, a user device (such as the user device 104) is installed with a service application that enables the user device to pay anonymously to merchants. In an embodiment, the service application represents a third-party service provider.

[0075] Referring flowchart 300, at step 302, a request from a POS device is received by a user device to pay 'X' amount of money. The user device may have a service application installed for facilitating secure and anonymous transactions. In one embodiment, the request from the POS device may be received using short range communication protocol such as, but not limited to, NFC, Bluetooth, and RFID. In an alternate embodiment, the service application of the user device may initiate the payment request.

[0076] At step 304, service application may request the user to approve the payment requested by the POS device. Once the user approves the payment request, the process proceeds to Step 306, otherwise the payment request is declined if the user disapproves the request.

[0077] At step 306, the service application may request the user to pay the 'X' amount of money from user's bank account or via any other suitable means such as, but not restricted to, cash, demand draft, cheque, credit card, debit card, net-banking, mobile banking, wallets, etc. The user may select a suitable payment method or the service application may be configured to automatically select the suitable payment method depending on the user preferences. Once the suitable payment method is selected, the service application transmits a request to the associated financial institution for the approval of the transaction.

[0078] At step 308, the service application may receive confirmation from its bank account corresponding to reception of 'X' amount of money from the user's bank account.

[0079] Thereafter, at step 310, the service application may request a remote server to generate a virtual payment card of the 'X' amount of money. The remote server may represent servers of financial institutions and/or a card issuing authority.

[0080] At step 312, the service application may receive the virtual payment card details from the remote server and the same is shared with the POS device. In an embodiment, the virtual card may be shared using the NFC protocol. However, similar short-range protocols may also be used such as Bluetooth, RFID readers, infrared etc. Further, it is imperative that the virtual card details are shared securely with the merchant device. The virtual card details may be shared in form of secured tokens via NFC protocol. Encryption of the data may further be considered. Thereafter, the service application may receive an acknowledgment from the POS device on successful payment transaction and the same will be displayed to the user at step 314.

[0081] This will complete the transaction process without sharing details corresponding to user's bank account or payment card details. This way, the merchant device will never have access to the user information and the

user will never have access to the shared payment card. Thereby, payment security will automatically be ensured due to anonymity in payment transactions.

[0082] FIG. 4 illustrates a flow diagram 400 of a method for anonymously paying to a merchant device via a wallet service, in accordance with an embodiment of the present invention. Herein, a user device (such as the user device 104) is considered to be installed with a service application that enables the user device to pay anonymously to merchants. In an embodiment, the service application represents a third-party service provider. The user device may use NFC protocol to initiate a payment with a merchant's POS device.

[0083] Thereafter, the service application may request the user to load merchant requested balance in a wallet of the third-party service provider. On successful loading of the payment in the wallet, the service application will deduct the loaded money from the wallet and request a remote financial institution or a card issuer to generate a single-use payment card of the merchant requested amount. The generated payment card details will then be shared with the merchant device for payment in a secured manner.

[0084] Referring now to the flowchart 400, at step 402, a POS device may request a user device to pay 'X' amount of money. This action may trigger a service application installed in the user device. The service application may be configured to facilitate secure and anonymous transactions for protecting identity frauds.

[0085] Further, on receiving request from the POS device, the service application may first determine whether a user has a pre-subscribed wallet service available or not (with the third-party service provider). If the user is found to have an active wallet registered with the third-party service provider, then the service application may determine, at step 404, if personal wallet of the user has at least the 'X' amount of money available as requested by the POS device.

[0086] Thereafter, if the service application determined that the user does not have sufficient balance in the wallet then, at step 406, the service application will request the user to pay the 'X' amount of money from user's bank account in real time. After receiving payment confirmation at step 408, the service application may add the same amount of money in the wallet of the user (at step 410).

[0087] At step 412, the service application will request a remote server of a financial institute to generate a single-use virtual payment card of 'X' amount of money. Thereafter, at step 414, the service application may deduct the 'X' amount of money from the personal wallet of the user and the user may be notified accordingly. The service application may then use the single-use virtual payment card details for paying the requested 'X' amount of money to the POS device. The service application, in one embodiment, may share the card details via NFC protocol with the POS device in a secure token form.

[0088] FIG. 5 illustrates a flow diagram 500 of another method for anonymously paying a merchant device via a wallet service, in accordance with an embodiment of the present invention. Herein, a user device (such as the user device 104) is installed with a service application that enables the user device to pay anonymously to merchants.

[0089] In an embodiment, the service application represents a third-party service provider. The user device may use NFC protocol to initiate a payment with a merchant's POS device. Thereafter, the service application may first check if the user already has sufficient balance in his/her wallet (wallet may be pre-registered with the third service provider).

[0090] If the wallet is determined to be having sufficient balance, then the service application will deduct the loaded money from the wallet and request a remote financial institution to generate a single-use payment card of the merchant requested amount. The generated payment card details will then be shared with the merchant device for payment in the secured manner. This way, the merchant device never had access to the user information and the user never had access to the shared payment card. This ensures payment security by minimizing payment fraud chances due to anonymity.

[0091] Referring now to the flowchart 500, at step 502, a POS device may request a user device to pay 'X' amount of money. This action may trigger a service application installed in the user device. The service application may be configured to facilitate secure and anonymous transactions for protecting identity frauds. The service application may then request a user to confirm if the user is willing to proceed with the requested transaction, at step 504.

[0092] Further, on receiving approval from the user to proceed with the transaction, the service application, at step 506, may first determine whether the user has a pre-subscribed wallet service available or not (with the third-party service provider). If the user is found to have an active wallet registered with the third-party service provider, then the service application may determine if the personal wallet of the user has at least the 'X' amount of money available or not, as requested by the POS device.

[0093] If the wallet of the user is determined to be having sufficient balance, then at step 508, the service application may deduct the 'X' amount of money from the user's wallet. Thereafter, at step 510, the service application may request a remote server of a financial institution to dynamically generate a one-time use virtual payment card of 'X' amount in real-time. The service application may then receive the virtual payment card details from the remote server and share the same with the POS device via a NFC protocol in a secured manner, at step 512. Thereafter, the service application may receive an acknowledgment from the POS device on successful payment transaction and the same will be displayed to the user at step 514.

[0094] FIG. 6 illustrates a flow diagram 600 of another method for anonymously paying to a merchant device, in accordance with an embodiment of the present invention. Herein, a user device (such as the user device 104) is installed with a service application that enables the user device to pay anonymously to merchants.

[0095] Referring now to the flowchart 600, at step 602, a request from a POS device may be received by a user device to pay a 'X' amount of money. At step 604, the payment request from a user may be authenticated as explained in conjunction to figure 3 of the present invention. At step 606, a virtual payment card may be requested from a remote server for payment of the 'X' amount of money.

[0096] Thereafter, at step 608, the details corresponding to the requested virtual payment card may be received. The details corresponding to the virtual payment card may include the virtual card number, amount etc. Further, at step 610, the virtual payment card details may be shared with the POS device as explained in conjunction to figure 3 of the present invention. At step 612, acknowledgment for successful payment may be received and the same will be displayed to the user at step 614.

[0097] FIG. 7 illustrates a flow diagram 700 of a method for receiving anonymous payments from user devices, in accordance with an embodiment of the present invention. Herein, a merchant device (such as the vendor device 106) in form of a POS device is receiving anonymous payments from user devices (such as the user devices 104). The user devices are installed with a service application that facilitates the user devices in making anonymous payments. In an embodiment, the service application represents a third-party service provider.

[0098] The merchant device may use NFC protocol to initiate a payment with the user device. Thereafter, the merchant device will receive details of a payment card which is transferred to a financial institution such as a bank for authentication and payment purposes. On successful payment acknowledgment from the financial institution the merchant device will further acknowledge to the user device. This way the merchant device never received information corresponding to the user or user's payment card. The merchant device only received a single-use dynamically generated payment card that had no information related to the user. Therefore, neither the merchant or any intruder had access to the user information, which minimizes payment fraud possibilities.

[0099] In case the merchant device may need to refund the payment to the user, the merchant device may have the option to either transfer the money back to the single-use payment card or may also have an option to refund the money to the third-party service provider with information on the payment time stamp, payment amount, and/or on the payment card details. The third-party service provider can back track the user from the payment time stamp, payment amount, and from the payment card details and can refund the money back directly to the user from its bank account or wallet service. This way only the third-party service provider had access to the user's information and the merchant never had such access.

[00100] Referring now to the flowchart 700, at step 702, availability of a user device may be detected by a POS merchant device for payment of 'X' amount of money. The availability may be determined by any short-range protocol such as NFC, RFID, WiFi, Infrared, Bluetooth, etc.

[00101] At step 704, the POS device may request the available user device to initiate transaction of the 'X' amount by transferring the payment amount details to the user device. Thereafter, at step 706, the POS device may receive from the user device, details corresponding to a payment card which may be used by the POS device to initiate transaction of the 'X' amount. The POS device may then transfer the payment card details to a financial institute's remote server at step 708 for authentication of the payment card details. After successful authentication, the POS device may receive acknowledgment from the remote server at step 710. Thereafter, at step 712, the POS device will notify the user device corresponding to the success of the payment transaction.

[00102] FIG. 8 illustrates a flow diagram 800 of a method for generating a single-use virtual payment card, in accordance with an embodiment of the present invention. Herein, a user device (such as the user device 104) is

considered to be installed with a service application that enables the user device to pay anonymously to merchants. In an embodiment, the service application represents a third-party service provider. The user device may use NFC protocol to initiate a payment with a merchant's POS device. Thereafter, the service application may request a remote financial institution to generate a single-use payment card of the merchant requested amount. The generated payment card will then be shared with the merchant device for payment in a secured manner.

[00103] Referring now to the flowchart 800, at step 802, a user device may request a remote server of a financial institution to generate a dynamic single-use virtual payment card of 'X' amount. The user device may then receive details corresponding to the generated card at step 804. The generated card details may then be shared with a POS device by the user device to initiate a payment transaction at step 806. At step 808, the user device may receive acknowledgment from the POS device corresponding to success of the payment transaction.

[00104] FIG. 9 illustrates a flow diagram 900 of a method for anonymously paying using a payment portal web page, in accordance with an embodiment of the present invention. In an embodiment, a user device may have an option to pay a merchant over a web interface. The user device may use a service application to open an integrated web browser for accessing payment portal of a merchant or vendor. The service application may automatically detect the payment portal web page and may offer the user to select anonymous payment option.

[00105] If the user selected the anonymous payment option, then the service application may request a financial institution to generate a single-use payment card and then will automatically fill in the details of the single-use payment card on behalf of the user. The user may then proceed with the payment process without requiring to share his/her personal payment information.

[00106] The service application may receive payments from the user's pre-registered wallet. In case the user does not have a wallet registered with the third-party service provider or does not have sufficient balance in the wallet then the service application may first request the user to pay same amount to the third service provider in real time or to load similar balance in the its registered wallet. This way the service provider received money from the user and transferred the money to the merchant on user's behalf by protecting identity and payment information of the user.

[00107] Referring now to the flowchart 900, at step 902, the service application may detect if the user has navigated to a payment portal web page. At step 904, the service application will request the user to confirm if the user is willing to allow the service application to pay anonymously on the payment portal page. If the user approves for anonymous payment, then at step 906, the service application may request a remote server of a financial institution for generating a single use virtual payment card that can be shared over the payment portal page.

[00108] At step 908, the service application receives the requested virtual payment card from the remote server and at step 910 the service application automatically fills the information on the payment portal page, without requiring any effort from the user. The service application may then automatically submit the details on the portal page to initiate the transaction.

[00109] In an embodiment of the present invention, the service application may use web scripts to automatically detect web portal IP addresses or domain URLs and may automatically run scripts to auto-fill payment details with user's permission and skip all web pages to load at user end that demands payment information. This way user will never encounter payment portal requests and will never be able to access the payment card details shared by the service application with the web portals on behalf of the user.

[00110] This way, the user escaped from a need of sharing his/her bank or card details with the payment portal page and therefore minimized identity fraud possibilities. This way, the merchants and intruders will never receive user information and the user and intruder will never have access to the dynamically generated payment card information. This type of anonymity will enhance payment transaction security and reliability.

[00111] FIG. 10 illustrates a flow diagram 1000 of a method for paying refunds to an anonymous user, in accordance with an embodiment of the present invention. Herein, a user device (such as the user device 104) is installed with a service application that enables the user device to pay anonymously to merchants. In an embodiment, the service application represents a third-party service provider. The user device may use NFC protocol to initiate a payment with a merchant's POS device. Thereafter, the service application may request the user to pay merchant requested amount from user's bank account to the third-party service provider.

[00112] On receiving confirmation, the service application will request a remote financial institution or a card issuing authority (i.e. card issuer) to generate a single-use payment card of the merchant's requested amount. The generated payment card will then be shared with the merchant device for payment. This way, the merchant device will never have access to the user information and the user will never have access to the shared payment card.

[00113] However, this anonymity does not deprive the user from receiving refunds from the merchant. The merchant still has the details of the single-use payment card that was used to pay initially. Therefore, the merchant still has the option to use the same card details to process refunds. In an embodiment, the single-use virtual payment card has the capability to receive money. This way the financial institution who generated the single-use virtual payment card will receive refunded money. The financial institution then will determine from its databases account details of owner of the single-use virtual payment card. As described previously, the owner of the single-use virtual payment card is the third-party service provider.

[00114] This way money will be received by the third-party service provider and then the service provider will check from its own database to determine bank account details of the user for whom the single-use virtual payment card was requested from the financial institution. After recognizing the user, the third-party service provider will refund the amount to the pre-registered bank details of the recognized user. This way, despite of being anonymous to the merchant and the financial institution, the present invention facilitates the user to pay and receive refunds in hassle free manner.

[00115] Referring back to the flowchart 1000, at step 1002, a refund notification from a financial institution (e.g., a remote financial institution or a card issuing authority as described above) is received by a service provider (e.g., the third-party service provider as described above). The financial institution may have received

the refund amount from a merchant in reference to a virtual card (e.g., the single-use virtual payment card as described above) previously generated by the financial institution. The financial institution may then have learned from its database that the virtual card was previously requested by the service provider.

[00116] Thereafter, at step 1004, the service provider searches within its own database to identify a user for which the virtual card was generated by the financial institution. After learning the identity of the user, the service provider further determines, at step 1006, bank account details of the user from its database. After determining the bank account details, the service provider then transfers the refunded amount to the user's bank account at step 1008. Finally, at step 1010, the service provider notifies the user corresponding to the refund via suitable means such as SMS, email, notification, etc.

[00117] FIG. 11 illustrates an exemplary environment 1100 where various embodiments of the present invention are implemented, according to another aspect of the present invention. The environment 1100 includes a plurality of user devices 1104a-1104n (also referred as "1104") connected to a plurality of vendor devices 1106a-1106m (also referred as "1106") via a network 1102, wherein the numbers "n" and "m" are arbitrary numbers representing same or different number of devices. The environment 1100 also includes a merchant acquirer 1108, a payment network 1110, a card issuer 1112, an issuing financial institution 1114 (i.e. issuing bank), and a transaction processing engine 1116. The transaction processing engine 1116 also comprises a database 1118 to store any data which is required to execute the payment requests in accordance with the present invention.

[00118] Further, the user devices 1104 may refer to electronic devices that may be utilized by individuals (consumers or customers) to access and communicate with the vendor devices 1106 using the communication network. In an embodiment of the present invention, the user devices 1104 are portable wireless communication devices such as but not restricted to cell phones, tablets, laptops, wearables, smart watch etc. Further, the vendor devices 1106 may refer to electronic devices that may be utilized by retailers or business owners to communicate with the user devices 1104 over the communication network 1102. The vendor devices 1106 may be configured to provide various functionalities such as, but not limited to, transmit the payment requests, receive the payments related information from the user, provide an online purchase interface, and/or provide a cashless payment interface to the users. The vendor devices 1106 can be such as, but not limited to, merchant web server hosting the merchant's online shopping portal, Point-of-Sale (POS) devices, or any other similar devices that can be used by the merchant to initiate or receive the payments, etc.

[00119] The user devices 1104 and the vendor device 1106 may be configured to communicate with each other using the communication protocols such as, but not limited to, NFC, RFID, Infrared, Bluetooth, etc. In one embodiment, the user devices 1104 may also engage with the vendor device 1106 by scanning of a matrix/QR code.

[00120] Further, the network 1102 may include, but is not restricted to, a communication network such as Internet, Intranet, PSTN, Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN), and so forth.

[00121] In one example, the secure transaction process of the present invention is implemented at least in part using suitable application programs, which can be hosted on one or more of the following:

[00122] processing system of the user devices 1104a-1104n;

[00123] processing system of the financial institution 1114 (i.e. issuing bank);

[00124] processing system of the card issuer 1112; and/or

[00125] processing system of the transaction processing engine 1116.

[00126] The functioning of the suitable application programs will be detailed further in conjunction with FIGS. 13-16 of the present application.

[00127] In an exemplary embodiment of the present invention, the user devices 1104 are installed with a service application (not shown). In an embodiment of the present invention, the service application may be implemented as a software application (or combination of software and hardware). Further, the service application installed in the user devices 1104 is configured to implement the secure transactions between the user devices 1104 and the multiple service providers 1106 (i.e. vendors) via the network 1102. The service application installed in the user devices 1104 may also be configured to connect the user devices 1104 with the vendor devices 1106.

[00128] In an embodiment of the present invention, the service application is based on a web and application infrastructure that uses some external support SDK. The service application may be configured to enable user devices 1104 in performing secure transactions with vendor devices 1106 without disclosing identities or payment account details. In another embodiment, the service application may be configured to enable user devices 1104 in performing anonymous transactions with the vendor devices 1106 over the network.

[00129] It should be noted that the secure payment environment 1100 shown in FIG. 11 is simplified for the better illustration of the present invention and therefore the environment 1100 should be considered not to limit the scope of the present invention. Further, some devices, modules or the network elements may be either omitted or may be further added in the secure payment environment 1100 without departing from the scope of the present invention.

[00130] FIG. 12 illustrates a flow diagram of a conventional payment system 1200. In the conventional cashless payment systems, a request for the payment is initiated either by a user or by a merchant or a party operating on behalf of the merchant.

[00131] In the conventional method shown herein, the user swipes his credit/debit card through a reader device installed at the point-of-sale (POS) to transmit a request.

[00132] The request transmitted to a vendor POS payment system, in step 1202 includes account details of a user's financial instrument that has been selected for the processing of the payment. In one example, if the user swipes the credit card or debit card for the processing of the payment, the card details comprising such as, but

not limited to, the card number, card expiry date, card holder name, contact details, etc. are transmitted to the merchant side payment system.

[00133] This is the biggest disadvantage of the traditional cashless payment methods as the user account details or the actual card details are shared with the merchant payment system which can be collected by the third parties and may be used for the fraudulent activities.

[00134] Referring back to FIG. 12, at step 1204, the user account details acquired by the merchant POS payment system are transmitted to a merchant acquirer. The details transmitted to the merchant acquirer includes the card details payment amount, currency details, etc.

[00135] At step 1206, the merchant acquirer routes the received details to a payment network. The payment network is responsible for processing the transactions.

[00136] In step 1208, the payment network forwards the processed transaction request to a card issuer to authenticate the card details shared by the user. The processing systems at the card issuing party processes the received request and routes the same to an issuing bank for the approval of the transaction, as illustrated in step 1210.

[00137] On receiving the transaction details, the processing systems at the issuing bank (i.e. financial institution) checks the authenticity of the received transaction details and if sufficient balance exists in the user account to process the payment request.

[00138] Once the issuing financial institution determines that the received transaction request is legitimate and authentic, the user account is debited, and a confirmation is sent to the merchant using the inverse process, as shown in the steps 1212 to 1220 to complete the transaction process.

[00139] As discussed above in reference to FIG. 12, in the traditional payment methods, the user account details or the card details are exposed to the merchants, and therefore a major risk exists as these details are prone to theft or use for illegal activities.

[00140] There exist many such examples where millions of card holders data (e.g. usernames and passwords) have been stolen from the merchants in the past. For example, in Dec 2013, US retail giant Target Corporation had announced that upto 70 million customer's personal data including the card numbers, names, postal addresses, phone numbers and email addresses was stolen from the company's database.

[00141] Also, the traditional cashless payment processes make it mandatory for the user to use their credit cards/debit cards for doing the payment at the point-of-sale. However, many of the users do not have credit/debit cards or many user who have financial institution issued cards (credit cards, debit cards, prepaid cards, gift cards, etc.) do not want to use their cards at the point-of-sale for making the payment due to the fear that their personal details (card details, name, etc.) can be exposed to the merchants/retailers, and thus can be used by unauthorized person without their permission.

[00142] The unique payment process as mentioned in the present invention addresses the problems described above, and therefore the present invention makes it very difficult to the unauthorized person to use the user account details and/or the credit card/debit cards details of the user for the illegal and fraudulent activities. Also, the present invention eradicates the problem of having a credit card/debit card at the point-of-sale for making the cashless payments. Therefore, users who may not have bank issued cards (debit cards, credit cards, gift cards, prepaid cards, etc.) may also use the present invention for making the cashless payments.

[00143] Some examples of the present invention are discussed below, however, it will be appreciated that the following examples should not be considered to limit to the scope of the present invention, and numerous other examples may be possible within the scope of the present invention.

[00144] FIG. 13A-13F schematically illustrates the various aspects of the present invention to generate a single use virtual payment card associated with an ongoing transaction, and notify payment details comprising the single use virtual payment card to a transaction processing engine.

[00145] FIG. 13A schematically illustrates the steps to generate a single-use virtual payment card and notify the same to a transaction processing engine for anonymously paying to a merchant according to first aspect of the present invention. The present invention enables a user to make payment transactions at the point of sale without owning a credit/debit card. According to this aspect of the invention, a few steps of the present invention for generating the single-use virtual payment card are executed by processing system of a user device 1104 and some other steps are performed at least in part using processing systems of at least a financial institution 1114 (i.e. issuing bank), such as suitably programmed computer systems of the financial institution.

[00146] In one example, the process of generating the single-use virtual payment card is implemented at least in part using suitable service applications which is executed by the user device 1104 and/or a vendor device 1106, and in part using the suitably programmed processing system hosted by one or more of the financial institutions 1114 (i.e. issuing bank), a transaction processing engine 1116, and/or a card issuer 1112.

[00147] In another example, the process of generating the single-use virtual payment card is implemented using the suitably programmed service application running on the user devices 1104. In yet another example, the process of generating the single-use virtual payment card is implemented using the suitably programmed processing system hosted by the financial institution 1114. In yet another example, the process of generating the single-use virtual payment card is implemented using the suitably programmed processing system hosted by the card issuer 1112. In yet another example, the process of generating the single-use virtual payment card is implemented using the suitably programmed processing system hosted by the transaction processing engine 1116.

[00148] FIG. 13A shows a system flow diagram 1300A of transactions between a user terminal 1104 (i.e. user device) and a vendor terminal 1106. The user device 1104 is configured with a service application which when executed by the processor of the user device 1104 facilitates the user device in making anonymous payments.

[00149] According to the preferred embodiment of the invention, the user terminal 1104 (i.e. user device) and the vendor terminal 1106 are configured to communicate with each other using contactless mode of communication, wherein the contactless mode of communication can be such as, but not limited to, Near-Field Communication (NFC).

[00150] A request for the payment transaction can either be initiated by the user device 1104 or by the vendor device 1106. As shown, at step 1302, the vendor device 1106 sends a request using NFC interface to initiate a contactless payment with the user device 1104.

[00151] In this aspect, NFC is used as a communication interface between the user device 1104 and the vendor device 1106, however, other similar short-range protocols such as Bluetooth, RFID, infrared, matrix code (QR code) scanning, etc. may also be used without limitation.

[00152] The request for the payment transaction comprises transaction details and the information to identify the vendor device 1106 at the Point of Sale (POS). Transaction details includes information related to the initiated transaction such as, but not limited to, transaction amount, and/or the payment time stamp, merchandise details, etc. The information to identify the vendor device can be such as, but not limited to a vendor device ID, wherein the vendor device ID indicates any code, number, indicia, symbol, or other identifier that may be associated with the merchant device 1106 (i.e. vendor device) and/or the corresponding merchant or the business entity. In one embodiment, the information to identify the vendor may also indicate (without limitation) merchant/vendor name, branch/outlet details, POS device ID, and the corresponding location of the merchant and/or the POS device, etc.

[00153] Optionally, the transaction request, at step 1302, may also comprise identity of the user device 1104 to identify the target user device 1104, wherein the identity of the user device comprises unique user-device ID, unique service application ID, phone number, IMEI number, IP address, etc. associated with the user device.

[00154] It should be noted that the transaction request, at step 1302, does not include any information related to user's financial instrument. In other words, the transaction request does not include one or more of the credit card/debit card details, bank details, account number, password, mPIN, etc.

[00155] The user device 1104 receives the transaction request from the vendor device 1106 and the service application running on the user device ensures the secure transactions between the user device and the vendor device without disclosing identities of user's financial instrument or payment account details.

[00156] The service application receives the payment amount and requests the user of the device to authenticate/approve the transaction.

[00157] If approved by the user, at step 1304, the service application running on the user device 1104 transmits the request to a remote financial institution 1114 to dynamically generate a single-use payment card of the merchant requested amount. The request sent at step 1304 comprises information related to the initiated transaction such as, but not limited to, user account details, user ID, password, requested transaction amount, vendor details, vendor terminal ID, currency, and/or transaction time stamp.

[00158] In the preferred embodiment of the invention, the user account details and account credentials are pre-associated with the service application and transmitted automatically to the financial institution once the user approves the transaction. In another embodiment, the user manually selects or enters target account details of the target financial institution when authorizing the transaction request. In another embodiment, one or more account details of one or more financial institutions can be pre-saved in the service application, wherein the user can select the target financial institution's account details while authorizing the transaction request. In yet another embodiment of the invention, the service application may be linked to a pre-subscribed wallet service to execute the transactions.

[00159] The remote financial institution's computing environment 1114 comprises one or more servers that are configured to carry out the functions of the present invention. More specifically, one or more servers of the remote financial institution are installed with a computer program code which when executed by one or more processors of the remote financial institution 1114 provides secure transactions according to the embodiments of the present invention.

[00160] At step 1306, a computer program code running on the servers of the financial institution 1114 receives the encrypted details shared by the service application of the user device and verifies the initiated transaction request. The step of verification of the transaction includes determining whether the details shared by the user device 1104 are valid or not. Once the financial institution 1114 has obtained the user credentials, the financial institution will compare the provided credentials with the pre-stored user account details to authenticate the transaction request. If the account details are found to be legitimate, thereafter the server of the financial institution 1114 is configured to compare the requested transaction amount with the available amount in the user account to determine whether there is enough balance amount in the associated user financial account to execute the initiated transaction request. If the output of the verification step comes out to be affirmative, then the sever of the financial institution 1114 is configured to temporarily debit the requested amount from the user's financial account. In one embodiment, the sever of the financial institution 1114 is further configured to create debit request on-hold status for the requested amount.

[00161] Thereafter, at step 1308, the financial institution's server 1114 is configured to transmit a request to the card issuer 1112 to dynamically generate a virtual payment card for the requested amount of transaction. The virtual payment card is a single use virtual payment card which becomes invalid immediately after it is used. In one embodiment, the single use virtual payment card becomes invalid if a predefined time has lapsed after the generation of the card. According to one embodiment of the invention, the predefined time is less than equal to 360 seconds. In accordance to another embodiment of the invention, the predefined time is less than equal to 180 seconds.

[00162] At step 1310, processing system of the card issuer 1112 receives a request to generate a virtual payment card for the requested amount. On reception of details of the transaction, the card issuer 1112 generates a single use virtual payment card and shares the details of the generated virtual payment card with the processing systems of the financial institution 1114.

[00163] In an embodiment, the financial institution computing system 1114 may be capable to dynamically generate a virtual payment card and may transmit the dynamically generated virtual card details to the service application of the user device 1104 directly. In that case, process as shown in steps 1108 and 1110 will not be required anymore.

[00164] Referring back to FIG. 13A, at step 1312, on reception of the virtual payment card details, the computer program code running on the financial institution's servers 1114 is configured to transmit a command to a transaction processing engine 1116 to make a record regarding the ongoing transaction. The data stored in database 1118 of the transaction processing engine 1116 at this step is used thereafter to validate and secure the transactions, and protect the user against fraudulent actions (as explained in connection with the description of FIG. 14). The command to the transaction processing engine 1116 includes the information related to the transaction request, wherein the information comprises such as, but not limited to, a vendor device ID, merchant details, transaction amount, currency, USERID, State of the transaction (=approved/denied), virtual card details, timestamp, and card use status (=open/closed).

[00165] If the transaction is denied by the financial institution (at step 1306), in that case the step 1312 may not be initiated and the transaction failure status may be returned to the merchant and/or customer. However, if the transaction is approved by the financial institution at step 1306, in that case the status of the virtual payment card will be saved as "open" in the database 1118 of the transaction processing engine 1116. The timestamp data is used to maintain the information about the session time. The timestamp data along with status information also helps to differentiate between an open session and a closed session, wherein the open session is a session that may receive the future activities. In one embodiment, the single use virtual payment card becomes invalid if the card is not used within a predefined time.

[00166] The transaction processing engine 1116 stores the information corresponding to the ongoing transaction in response to the command and sends a confirmation to the financial institution 1114. At step 1314, the computer program code running on the financial institution's computing environment 1114 receives the confirmation from the transaction processing engine 1116 that the data has been stored and is ready to be used for verification of the further activities related to the transaction.

[00167] On receipt of the confirmation from the transaction processing engine 1116, at step 1316, the computer program code running on the financial institution's computing environment 1114 transmits the virtual card details to the user device 1104.

[00168] Thereafter, at step 1318, the service application running on the user device 1104 receives the dynamically generated single use virtual payment card details from the financial institution server 1114 and the same is shared with the POS computer system informing that the virtual card token has been generated, and the method thereby proceeds further to step 1402 as illustrated in FIG. 14.

[00169] It should be considered that in one embodiment of the invention, step of sharing the virtual payment card between the financial institution 1114 and the user device 1104 (i.e. step 1316) may execute in parallel to

the steps of storing the data in the payment processing engine (i.e. step 1312) to expedite the transaction processing speed.

[00170] In an embodiment, the virtual card may be shared between the user device 1104 and the vendor device 1106 using the NFC protocol. However, similar short-range protocols may also be used such as Bluetooth, RFID readers, infrared, matrix code (QR code) scanning, etc. Further, it is imperative that the virtual card details are shared securely with the merchant device (i.e. vendor device). The virtual card details may be shared in the form of secured tokens via NFC protocol. Encryption of the data may further be considered.

[00171] One of the advantages of the present invention over the traditional prior art systems is that the virtual card issuing party knows in advance, before generating the virtual card, about the purpose for which the virtual card is being generated. As the virtual card is generated on-the-fly, and the target merchant details along with the purpose of the card are also known in advance, therefore, the present invention provides an additional layer of security over the conventional payment methods and thus the financial institutions release the money to the requesting party only when the previously provided details (while generating the virtual card) matches with the newly received details, and therefore the unique payment process mentioned in the present invention is very difficult to defraud.

[00172] FIG. 13B illustrates a flow chart 1300B for generating a single-use virtual payment card and notifying the same to a transaction processing engine for anonymously paying to a merchant, according to another aspect of the present invention. According to this aspect, the process of generating the single-use virtual payment card is implemented using a suitably programmed service application running on a user device 1104. Therefore, the service application running on the user device 1104 executes the process of generating the single use virtual payment card and recording of the payment data in a transaction processing engine 1116. In other words, the service application of the user device 1104 coordinates with a financial institution 1114, a card issuer 1112, and the transaction processing engine 1116 for executing the secure transaction process of the present invention.

[00173] The process starts at step 1322, wherein a request for the payment transaction is initiated. As shown, the vendor device 1106 sends a request using the Near-Field Communication Interface to initiate a contactless payment with the user device 1104, wherein the request comprises transaction details and the information to identify vendor device at the Point of Sale (POS). In an alternate embodiment of the invention, the user can also initiate the transaction by sending a transaction request to the vendor device 1106 using the user device 1104.

[00174] Transaction details transmitted at step 1322 includes information related to the initiated transaction such as, but not limited to, transaction amount, and/or the payment time stamp, merchandise details, vendor ID, POS terminal ID, vendor details, vendor location, etc.

[00175] The service application of the user device 1104 is configured to receive the transaction request from the vendor device 1106. In one embodiment, the transaction request is received using NFC interface of the user device. In other embodiments, other various types of short-range communication techniques known in the art are used to receive the transaction request.

[00176] Optionally, on receipt of the transaction request, the service application may be programmed to provide user with an option to accept or reject the transaction request. On approval, the service application may request the user to pay the requested amount of money from the user's bank account or via any other suitable means such as, but not restricted to, cash, demand draft, cheque, credit card, debit card, net-banking, mobile banking, wallets, prepaid card, P2P transfer mechanism, etc. The service application may also be configured to be associated with one or more financial accounts of the user for the execution of the payments without the user to add the account details manually. In one embodiment, the execution of this step depends on parameters such as, but not limited to, transaction amount, financial institution, user settings and preferences, etc.

[00177] It should be noted that in the above example the user is provided with an option to select the payment method for the execution of the ongoing transaction request., however, the suitable payment method can also be determined automatically by the service application as per the user preference and/or the purchase history. In one example, the user account details (account number, card details, etc.) are pre-saved at the service application and the same are transmitted automatically to the financial institution for the verification once the user approves the transaction. In an alternate embodiment, the user may select a suitable payment mode and the process proceeds to step 1324. In yet another embodiment, the user manually enters the target account details of the target financial institution when authorizing the transaction request. In yet another embodiment, one or more account details of one or more financial institutions can be pre-saved in the service application, wherein the user can select the target financial institution's account details while authorizing the transaction request. In yet another embodiment of the invention, the service application may be linked to a pre-subscribed wallet service to execute the transactions. If the user is found to have an active wallet registered, then the service application may determine if the personal wallet of the user has sufficient balance available as requested by the POS device. Thereafter, if the service application determined that the user does not have sufficient balance in the wallet then the service application may request the user to pay the amount from user's bank account in real time.

[00178] Once the suitable payment method is selected and approved, at step 1324 the service application running on the user device 1104 executes the transaction as per the suitable payment method. In this embodiment, the service application transmits the request to the user selected financial institution servers 1114 to determine if the selected financial account of the user is capable to execute the ongoing transaction. The request sent at step 1324 comprises information for example, and without limitation, user account details, user ID, password, requested transaction amount, vendor details, vendor terminal ID, and/or transaction time stamp.

[00179] At step 1326, the service application receives confirmation from the selected financial institution or the third-party wallet service provide whether the account details shared by the user device are valid or not and if there is sufficient balance in the user account.

[00180] If the output of the verification step comes out to be affirmative, thereafter, at step 1328, the service application may request the remote server of the card issuing authority 1112 (i.e. card issuer) to generate a virtual payment card of the requested amount of money.

[00181] At step the 1330, the service application may receive the virtual payment card details from the remote server of the card issuing authority 1112 (i.e. card issuer). The virtual payment card is a single use virtual

payment card which becomes invalid immediately after it is used. Further, the single use virtual payment card of the present invention cannot be used for a purpose other than for which it has been generated. In one embodiment, the single use virtual payment card becomes invalid if a predefined time has lapsed after the generation of the card.

[00182] In an alternate embodiment, the financial institution computing system 1114 may be capable to generate a virtual payment card and may transmit the virtual card details to the service application directly in step 1326. In yet another embodiment, the financial institution 1114 may directly communicate with the card issuing authority 1112 which may generate the virtual card and provide the card details to the financial institution 1114. Thereafter, the financial institution 1114 may provide the card details to the service application in step 1326. Therefore, the steps 1328 and 1330 are not required in case of these two embodiments.

[00183] Once the virtual payment card has been received, the service application is configured to supply a command to a transaction processing engine 1116 to make a record regarding the ongoing transaction, at step 1332. The command sent to the transaction processing engine 1116 includes the information related to the transaction, wherein the information comprises for example, and without limitation, one or more of a vendor device ID, merchant details, transaction amount, currency, USERID, State of the transaction (=bank approval/denial), Virtual Card details, timestamp, and status of the card (=open/closed).

[00184] The data stored in the transaction processing engine 1116 at this step is used thereafter to validate and secure the transactions, and protect the user against fraudulent actions. For example, a virtual card generated for purchasing a merchandize from the merchant "A", may not be used for making the payment to merchant "B". Transaction processing engine also effectively limit the use of the virtual payment card of the present invention is such a way that the same card cannot be used at a location different from the location mentioned in the transaction request. The transaction processing engine 1116 along with single use virtual payment card also ensures that the card can be used within a limited time duration, thus making the cashless payments more secure, and thereby protecting the user from the fraudulent activities.

[00185] At step 1334, the service application receives a confirmation from the transaction processing engine 1116 that the data has been stored and is ready to be used for verification of the further activities related to the transaction.

[00186] On receipt of the confirmation from the transaction processing engine 1116, at step 1336, the service application running on the user device 1104 transmits the virtual card details to the POS system, and the method thereby proceeds to step 1402 as illustrated in FIG. 14.

[00187] It will be appreciated that the transaction shown herein is between the user device and the POS system, however, the present invention may encompass other types of payment methods such as, but not limited to, online shopping and purchases. Also, in some circumstances NFC or other short-range communication between the user device and the POS system may not be required. The process may start directly when a user purchases a product online and initiates the transaction.

[00188] In any event, it will be appreciated that the present invention payment facilitates the transactions between the users and the vendors without requiring actual card or account details to be exchanged between the payee and the payer.

[00189] FIG. 13C illustrates a flow diagram 1300C for generating a single-use virtual payment card and notifying the same to a transaction processing engine for anonymously paying to a merchant, according to third aspect of the present invention. According to this aspect of the invention, a transaction processing engine 1116 runs under the control of a card issuer 1112. According to this aspect of the invention, the card issuer 1112 coordinates with a suitably programmed service application of a user device 1104 to generate the virtual payment card.

[00190] As shown herein, a transaction request is received by the service application of the user device 1104, at step 1342. At step 1344, a suitable payment method is determined and the user device 1104 requests the financial institution 1114 to verify the corresponding account details. At step 1346, the user device receives a response from the financial institution 1114 confirming if the suitable payment method can be used for the execution of the transaction. If the response received at step 1346 is denied, then the transaction is failed, and a payment failure response is sent to the merchant and/or the user. However, if a positive response is received from the financial institution server 1114, the method proceeds to next step 1348 where the service applications transmits a request to the card issuer computing environment 1112 to generate a single use virtual payment card. The card issuer computing system 1112 processes the received request and makes the decision regarding the generation of the virtual payment card. If the output of the decisioning steps comes out to be positive, then the card issuer generates a single use virtual payment card corresponding to the transaction request. At step 1350, the card issuer 1112 server sends a command to the transaction processing engine 1116 to make a record of the virtual payment card and the transaction request. The transaction processing engine 1116 associates the virtual payment card details and the details received in the transaction request (e.g. merchant details, currency, location of the merchant, purpose of the transaction, timestamp, etc.) and stores the associated details in the database 1118. At step 1352, the transaction processing engine 1116 transmits an acknowledgement to the card issuer that the data has been stored in the database 1118. At step 1354, the card issuer processing system 1112 transmits the details of the virtual payment card to the user device 1104. The user device 1104 is configured to receive the details of the dynamically virtual payment card and share the received card details with the merchant side POS system as shown in step 1356, and the method thereby proceeds to step 1402 as illustrated further in FIG. 14.

[00191] It should be noted that the virtual payment card details are encrypted for the secure transmission between the various devices over the network. It should also be considered that the step of sharing the virtual payment card between the card issuer and user device (i.e. step 1354) may execute in parallel to the steps of storing the data in the payment processing engine (i.e. step 1350) to expedite the transaction processing speed.

[00192] FIG. 13D illustrates a flow diagram 1300D for generating a single-use virtual payment card and notifying the same to a transaction processing engine for anonymously paying to a merchant according to fourth aspect of the present invention. According to this aspect of the invention, a transaction processing engine 1116

runs under the control of a card issuer 1112, and the card issuer 1112 coordinates with a financial institution 1114 for the generation of the dynamic virtual payment card.

[00193] The process of FIG. 13D begins at step 1362, where a service application of a user device 1104 is configured to receive a transaction request. The service application then determines a suitable payment method either automatically or by facilitating the user to make the selection. Once the suitable payment method is determined, the service application of the user device 1104 transmits a request to the financial institution processing system 1114, wherein the request comprises the selected payment method details along with the details of the transaction request, as shown at step 1364. The suitably programmed processing system of financial institution 1114 receives the request and determines whether the selected payment method (e.g. selected user account) can execute the transaction. If deemed positive, the process proceeds to next step 1366, where a request to generate a virtual payment card is sent to the card issuer 1112, wherein the request sent at this step comprises, for example and without limitation, merchant details, merchant device ID (POS device ID), merchant location, currency, requested amount, timestamp, state of the transaction, etc. The suitably programmed processing system of the card issuer 1112 processes the received request and dynamically generates a virtual payment card corresponding to the transaction request, and forwards the details of the virtual payment card along with the corresponding transaction request details to the transaction processing engine 1116, as shown in step 1368.

[00194] The transaction processing engine 1116 associates the virtual payment card details (card number, expiry details, timestamp, card use status, etc.) and the details received in the transaction request (e.g. merchant details, vendor device ID, currency, location of the merchant, purpose of the transaction, timestamp, requested amount, etc.) and stores the associated details in the database 1118. In an alternate embodiment of the invention, the card issuer 1112 associates the virtual payment card details with the details received in the transaction request.

[00195] At step 1370, the transaction processing engine 1116 transmits an acknowledgement to the card issuer 1112 that the data has been stored in the database 1118. At step 1372, the card issuer processing system 1112 transmits the details of the virtual payment card to the financial institution which forwards the details further to the user device 1104, at step 1374. It should be considered that the step of sharing the virtual payment card between the card issuer and financial institution (i.e. step 1372) may execute in parallel to the steps of storing the data in the payment processing engine (i.e. step 1368) to expedite the transaction processing speed.

[00196] The user device 1104 is configured to receive the details of the dynamically virtual payment card and share the received card details with the merchant side POS system as shown in step 1376, and the method thereby proceeds to step 1402 as illustrated further in FIG. 14.

[00197] It should be noted that the virtual payment card details are encrypted for the secure transmission between the various devices over the network.

[00198] FIG. 13E illustrates a flow diagram 1300E for generation of a single-use virtual payment card and notifying the same to a transaction processing engine for anonymously paying to a merchant, according to fifth aspect of the present invention.

[00199] In one embodiment of this aspect of the invention, at least one virtual payment card is pre-generated and pre-saved in a service application of a user device 1104 in an inactive state. In yet another embodiment of this aspect of the invention, the service application is configured to generate an inactive virtual payment card which is activated by a card issuer 1112 by sending an activation request. The flow diagram of FIG. 13 illustrates various steps for activating an inactive virtual payment card and recording transaction data in a transaction processing engine 1116, in accordance to an embodiment of the invention.

[00200] The process begins at step 1382, where the service application of the user device 1104 receives a transaction request from a merchant POS device 1106. In an alternate embodiment, the service application may initiate the transaction request directly.

[00201] According to an embodiment of this aspect of the invention, the service application of the user device is configured to store various pre-generated virtual payment cards. In an embodiment of the invention, each of the pre-generated virtual payment cards may have an associated maximum purchase limit. The service application evaluates the received transaction request and associates a pre-generated and pre-saved virtual payment card with the transaction request, wherein the service application associates the virtual payment card with the transaction request using a random selection method. In an alternate embodiment, the service application is configured to select the pre-generated virtual payment card using a selection criterion, wherein the selection criteria may depend on parameters such as, but not limited to, merchant type, merchant location, transaction amount, currency, and/or timestamp information.

[00202] According to another embodiment of this aspect of the invention, the service application is configured to generate a random virtual payment card on-the-fly and associate the randomly generated virtual payment card with the ongoing transaction request, upon the reception of the transaction request at step 1382. In the preferred embodiment of the invention, the virtual payment card generated by the service application is in inactive state and may not be used for the execution of the transaction until activated, however, various other modifications in this should be recognized by the person skilled in the art.

[00203] Once the virtual payment card is associated with the transaction request, in step 1384, the service application transmits a request to the card issuer 1112 for activating the virtual payment card that is associated with the ongoing transaction request. The request to activate the card comprises virtual payment card details along with the transaction request details such as, but not limited to, merchant details, item details, merchant device ID, merchant location, currency, requested amount, and/or timestamp.

[00204] The card issuer processing system 1112 processes the received details and verifies if the received details are valid or not. If the verification step deems to be valid, then the card issuer 1112 activates the virtual payment card, wherein value of the virtual payment card is equivalent to the amount requested by the merchant.

[00205] In step 1386, the card issuer 1112 transmits a command to the transaction processing engine 1116 to store the information regarding the ongoing transaction for further processing of the transaction.

[00206] Thereby, the transaction processing engine 1116 stores the information received from the card issuer 1112 in the database 1118 and sends a confirmation to the card issuer 1112, as shown in step 1388. The information stored by the transaction processing engine 1116 comprises for example and without limitation, a vendor device ID, merchant details, transaction amount, currency, USERID, State of the transaction (=approved/denied), virtual card details, timestamp, and card use status (=open/closed).

[00207] In step 1390, the card issuer 1112 transmits an acknowledgement to the service application that the virtual payment card has been activated. The card issuer 1112 may also send one or more authentication parameters to the service application to control the usage of the virtual payment card.

[00208] The service application of the user device 1104 receives the information provided by the card issuer 1112 and sends the virtual card details to the merchant POS system, as shown in step 1391.

[00209] In one embodiment of the invention, step 1386, 1388 of storing data in the transaction processing engine 1116 and step 1390 of sharing the data with the service application of the user device 1104 may be executed concurrently to reduce latency and therefore, to ensure the fast processing of the transactions.

[00210] The embodiment as described in the FIG. 13E may be further modified, wherein the service application may be configured to activate the virtual payment card.

[00211] In another variation to this aspect of the invention, the service application may be configured to directly communicate with the transaction processing engine 1116 to speed up the processing of the transactions.

[00212] FIG. 13F illustrates a flow diagram 1300F for generating a single-use virtual payment card and notifying the same to a transaction processing engine for anonymously paying to a merchant, according to sixth aspect of the present invention. In accordance to this aspect of the invention, a transaction processing engine 1116 is configured to coordinate with various other processing systems of the anonymous payment environment 1100 of the present invention to facilitate generation of the single use virtual payment card.

[00213] In first embodiment of this aspect of the invention, the transaction processing engine 1116 is configured to receive a transaction request form a service application running on a user device 1104 and thereby the transaction processing engine 1116 is configured to generate a single use virtual payment card.

[00214] According to the first embodiment of this aspect of the present invention, the process begins at step 1392, where a service application running on a user device 1104 is configured to receive a transaction request from a merchant POS device 1106, wherein the received transaction request comprises information such as, but not limited to, payment amount, currency, merchant details (POS terminal ID, merchant name, franchise name), merchant location, time stamp (time when the transaction started), and/or purpose of the transaction.

[00215] The service application determines a suitable payment method either automatically or by facilitating the user to make the selection. Once the suitable payment method is determined, the service application of the user device 1104 transmits a request, as shown in step 1393, to the transaction processing engine 1116 to generate a single use virtual payment card, wherein the request transmitted to the transaction processing engine 1116

comprises the selected payment method details along with the details as received in the transaction request received in step 1392.

[00216] The transaction processing engine 1116 is configured to receive and process the request sent by the service application in the previous step 1393. The transaction processing engine 1116 is further configured to transmit the user selected payment method details to a corresponding financial institution 1114 for the verification purposes to determine that if the selected payment method is capable to execute the ongoing transaction of the user account, as shown in step 1394. The suitably programmed financial institution 1114 determines whether the selected payment method details are valid or not. If the account details are found to be legitimate, thereafter the server of the financial institution 1114 is configured to compare the requested transaction amount with the available amount in the user account to determine whether there is enough balance amount in the associated user financial account to execute the initiated transaction request. If the output of the verification step comes out to be affirmative, then the financial institution 1114 sends the transaction approval confirmation to the transaction processing engine 1116, in step 1395.

[00217] In step 1396, the transaction processing engine 1116 is further configured to transmit the request to the card issuer 1112 for the generation of the single use virtual payment card corresponding to the ongoing transaction. The suitably configured processing system of the card issuer 1112 receives the request to generate the virtual payment card for the requested amount from the transaction processing engine 1116 and on reception of details of the transaction, the card issuer processing system 1112 generates a single use virtual payment card corresponding to the ongoing transaction and shares the details of the generated single use virtual payment card with the transaction processing engine 1116.

[00218] On reception of the single use virtual payment card details generated by the card issuer 1112, the suitably programmed transaction processing engine is configured to associate the single use virtual payment card details with the ongoing transaction details and store the associated details in a database 118, as shown in step 1397, wherein the transaction details comprises such as, but not limited to, payment amount, currency, merchant details (POS terminal ID, merchant name, franchise name), merchant location, time stamp (time when the transaction started), and/or purpose of the transaction. The single use virtual payment card details stored in the database 1118 comprises such as, but not limited to, virtual card number, timestamp (time when card was generated), card expiry time, card use status (=open/closed), etc.

[00219] Once aforementioned details are stored in the database 1118, the transaction processing engine 1116 is configured to share the single use virtual card details with the service application which further transmits the single use virtual card details to the merchant POS system, as shown is step 1398 and 1399 respectively.

[00220] In second embodiment of this aspect (sixth aspect) of the invention, the transaction processing engine 1116 is configured to receive details of an inactive single use virtual payment card from a service application running on a user device 1104 in step 1393, and in response the transaction processing engine 1116 is configured to facilitate activation of the received inactive single use virtual payment card. In this embodiment, on reception of the inactive virtual payment card from the service application, the transaction processing engine 1116 determines whether sufficient balance exist in associated user account to execute the transaction. In one

embodiment, the transaction processing engine 1116 sends an account verification request to the financial institution 1114 to determine if sufficient balance exists in associate user account to execute the transaction. After confirming that the user account can execute the transaction, the transaction processing engine 1116 transmits a request to the card issuer 1112 to activate the inactive virtual payment card. Upon reception of the confirmation from the card issuer 1112 regarding the card activation, the transaction processing engine 1116 is configured to associate and store the virtual payment card along with the ongoing transaction request for the further processing of the transaction request. In one variation to this embodiment, the steps 1394 and 1395 as mentioned in FIG. 13F may be negated, where the transaction processing engine 1116 may be directly configured for doing the user account verification. Optionally, in another variation, the transaction processing engine 1116 may be configured to activate the inactive virtual payment card itself and therefore, the steps as mentioned in FIG. 1396 and 1397 may be negated in that case.

[00221] Also, according to third embodiment of this aspect (sixth aspect) of the invention, the transaction processing engine 1116 may be configured to dynamically generate an inactive virtual payment card corresponding to the ongoing transaction on reception of the transaction request from the service application (at step 1393). The transaction processing engine 1116 may be further configured to facilitate activation of the dynamically generated inactive virtual payment card by transmitting a request to the card issuer 1112.

[00222] Therefore, as shown in the aforementioned specifications, the present invention can be used by users to make cashless transactions irrespective of whether they have financial institution issued payment cards (such as, and without limitation, credit cards/debit cards, prepaid cards, and/or gift cards). Also, as the user account details are not exposed with the merchant and dynamically generated virtual payment cards are used for making the payments, therefore the present invention facilitates a secure payment method to protect user data from theft or hacking during cashless payments.

[00223] It should be noted that in all above aspects related to generation of a virtual payment card, generation of a single use virtual payment card is disclosed according to preferred embodiment of the invention. However, a variety of modifications in this may be possible, wherein dynamically generated virtual payment card can be used more than one time to execute the transaction within a specified time period without departing from the scope and spirit of the present invention. In an exemplary embodiment according to this variation, user may specify number of times a virtual payment card may be used at a merchant side. In this case, the transaction processing engine 1116 also maintains a virtual payment card use counter in the database 1118 in addition to aforementioned information to determine number of times the card has been used, and to reject the transaction in case the virtual payment card use counter has been overflowed.

[00224] FIG. 14 illustrates a flow diagram 1400 to utilize the dynamically generated virtual payment card (as generated in FIG. 13A-13F) for making the payment to the vendor. Process starts at step 1402, where a payment request is transmitted to a merchant acquirer 1108, wherein the payment request includes one or more of details of the virtual payment card (as generated in FIG. 13A-13F), payment amount, currency, merchant details (POS terminal ID, merchant name, or location), time stamp (time when the transaction started at step(s) 1302, 1322, 1342, 1362, 1382, 1392 and/or the time when the virtual card was generated). The merchant acquirer 1108 is the

merchant's financial institution, which facilitates transactions on behalf of the merchant and also transmits notifications to the merchant about the status of the transactions. It should be noted that the functionalities of the merchant acquirer 1108 are implemented using a suitably programmed computer implemented system.

[00225] The processing system at the merchant acquirer 1108 receives the transactions request and processes it and routes the same to a payment network 1110, at step 1404. The payment network 1110 is responsible for processing the transactions. The payment network 1110 may be implemented by an entity who has defined the protocols to facilitate the execution of the transactions. The payment network 1110 ensures processing and execution of the activities related to the implementation of the transactions such as, authorization, clearings, settlements, etc. The payment network 1110 also selects the suitable communication and data network for the execution of the transaction.

[00226] In step 1406, the payment network 1110 forwards the processed transaction request to the issuer 1112 (i.e. card issuer) of the dynamically generated virtual card for the approval of the previously generated single use virtual payment card. The processing subsystems at the card issuing party 1112 (i.e. card issuer) processes the received request and forwards the processed request to the issuing bank 1114 (i.e. financial institution) for the approval of the transaction, as illustrated in step 1408.

[00227] A suitably programmed processing systems of the issuing bank 1114 (i.e. financial institution) processes the received transaction request and transmits a request along with the transaction details to the transaction processing engine 1116, at step 1410.

[00228] On receiving the transaction details, a suitably configured processing systems at the transaction processing engine 1116 verifies the authenticity of the received transaction details by checking if the record exists for the received transaction details in the database 1118. Therefore, the transaction processing engine 1116 is configured to compare the received transaction details with previously stored details in the database 1118.

[00229] Therefore, the transaction processing engine 1116 compares the received virtual card details with the previously saved virtual card details in the database 1118 (i.e. saved at step 1312 of the process described in FIG. 13A or the step 1332 of the process described in FIG. 13B or the step 1350 of the process described in FIG. 13C or the step 1368 of the process described in FIG. 13D, the step 1386 of the process described in FIG. 13E or the step 1397 of the process described in FIG. 13F).

[00230] The transaction processing engine 1116 also matches the merchant details and the time-stamps to determine if the single use virtual card is being used with the same merchant and within the limited time period. In addition to this, the transaction processing engine also determines the status of the card, wherein if the status of the card is open it is determined that the virtual card is being used for the first time and is therefore valid.

[00231] Once the transaction processing engine 1116 determines that the received transaction process is legitimate and authentic, a confirmation is sent to the merchant using the inverse process, as shown in step 1412. This will complete the transaction process without sharing the actual card or account details of the user, and therefore enhances the security of the online and digital transactions, protects the user data, and inhabits the

fraudulent transactions. Also, as the single use virtual payment card is used for making the payments, therefore even if the data is compromised over the network and is stolen during the transmissions over the network, the account details stolen cannot be used by the unauthorized person or the hackers. Therefore, the present invention facilitates a payment system which is very difficult to defraud. Also, the multilevel checks for the execution of a single transaction (e.g. comparing the merchant details, virtual card, timestamps, location information, POS terminal ID, merchandize details, etc.) ensures that transaction is not being made by the unauthorized person at an unidentified place and therefore the present invention provides an additional level of protection against fraudulent and illegal use.

[00232] Therefore, the above discussed process of the present invention is in contrast with other conventionally known payment methods of the prior art where the actual account details and the card details are shared with the vendor/merchant or the financial institution or any other third party operating on behalf of the merchant to execute the payments. In contrast, in the present invention, transactions are executed anonymously using the single use payment card which is generated in real time and on the fly to ensure the secure transactions.

[00233] The secure transaction method disclosed in the present invention is a two-step method, wherein in a first step a virtual card is dynamically generated corresponding to a transaction request and the generated virtual payment card along with other transaction related details are stored in a transaction processing engine, and in a second step the dynamically generated virtual card details are verified to authenticate the transaction request. Further, the target merchant details along with the purpose of the transaction are associated to the dynamically generated virtual payment card, and these details are recorded in the database and used further to authenticate the transaction. Thereby, using the present invention, the payment is released to the requesting party only when the transaction details in the transaction request matches to the previously provided details that were used for the generation of the virtual payment card. If the output of this comparison step is invalid, then the transactions are declined.

[00234] It shall be apparent to the person skilled in the art that the invention as described in reference of FIG.13 & FIG. 14 is used to execute cashless transactions at the point of sale (POS), but it shall not be considered limiting and many changes and modifications may be made within the scope of the embodiments herein, without departing from the spirit and scope thereof, and the embodiments herein include all such modifications. Thereby, the present invention can also be modified to execute the cashless e-commerce transactions or online payment portals (e.g. web portal) transactions.

[00235] A further illustrative example of a payment method will now be described to showcase how the payment method of the present invention can be used in making payments on an online payment portal. An example of the online purchasing system 1500 in accordance to one embodiment of the present invention is described with reference to FIG. 15.

[00236] According to this embodiment of the invention, a service application running on a user device is configured to request a remote server to generate a single-use payment card and then automatically fill in details of the single-use payment card on behalf of a user on an online shopping portal. Therefore, the user does not

need to enter the card details manually for the execution of the payment. The user may therefore execute the payment request without requiring to share his/her personal payment information.

[00237] The process starts at step 1502, where a user accesses a website by sending a request from a user device and thereby receiving a response from a remote web server, wherein the website is under the control of a third party (e.g. merchant/retailer) and is hosted by the merchant's web server. The website provides the details about the goods and services that are available for the online purchase by the customers. The website provides the functionality to browse through the available goods and services, where the user can make selection of the desired goods or services for the purchase and proceed to checkout page to complete the purchase of the item.

[00238] In one example, the user access merchant's website using a web browser of the user device. In another example, a merchant application program may be installed in the user device to access the merchant web portal. In yet another example, the service application installed on the user device can provide the functionality of the web browser, using which the user can access online merchant web portal. In yet another embodiment, the functionalities of the service application can be provided using a plug-in, desktop based software application, or an add-on for the browser.

[00239] In step 1504, the user transmits a purchase request to the merchant's web server regarding the details of the goods or services selected by the user in the previous step. The details of the selected goods or services comprises such as, but not limited to, product name, brand name, amount, supplementary information such as color, size, material type, or any other product specific information. Additionally, the received request at the merchant web server may also contain user information to identify the user and shipping address.

[00240] The merchant web server processes the received request to determine the availability of the user selected item. The merchant web server may also compare the received user information with the user profile information to determine if the purchase request can be executed or not. On confirmation, the merchant web server routes the purchase request to a merchant acquirer's server, in step 1506.

[00241] On the reception of the payment request, the merchant acquirer server provides a payment web interface to the user device for making the payment for the desired item(s), in step 1508. The payment web interface may display various options available for making the payment for the item(s).

[00242] In one embodiment, the merchant acquirer web server may be hosted by the financial institution of the merchant. In another embodiment, the merchant acquirer web server may be hosted by a third party responsible for executing the payments on behalf of the merchant. In yet another embodiment, the functionalities of the merchant acquirer server and the merchant web server may be hosted by a single entity and/or a single server may be capable to execute the operations as performed by the merchant web server and the acquirer server.

[00243] In one embodiment, the service application running on the user device may detect the payment portal web page and may offer the user to select the suitable payment option. In another embodiment, the service application may automatically detect the payment portal web page and automatically selects the suitable payment method on the basis of the previously stored user preferences or the user purchase history. The service

application may also receive payments from the user's pre-registered wallet. In case the user does not have a wallet registered with the third-party service provider or does not have sufficient balance in the wallet then the service application may first request the user to pay same amount to the third-party service provider in real time.

[00244] When a suitable payment method is selected and/or the user approves the request, a request is transmitted to a remote server to generate a virtual payment card, as shown in step 1510.

[00245] In step 1512, the remote server authenticates the user account details associated with the selected payment method and verifies that the user account has sufficient balance to execute the payment. If the authentication step is deemed valid then a virtual payment card is generated for the ongoing payment request.

[00246] In one embodiment, the remote server is hosted by the financial institution. In another embodiment of the invention, the remote server may be hosted by the card issuer. In yet another embodiment, the remote server represents one or more servers of the financial institution and one or more servers of the card issuer operating together in coordination to generate the virtual payment card. In yet another embodiment, the remote server represents one or more servers of a third party responsible for the verification of the transaction request.

[00247] At step 1514, the remote server transmits the details of the virtual payment card to the transaction processing engine, which saves the received details in the transaction processing engine database for the future processing of the card. The information saved by the transaction processing engine includes one or more of the virtual card number, timestamp information, merchant details, product details, currency information, customer details, merchant location information, merchant web server address, etc. At step 1516, the remote server receives the acknowledgement from the transaction processing engine that the entry about the generated virtual card has been saved in the database.

[00248] In one embodiment, the functionalities of the transaction processing engine and the remote server may be integrated and hosted within a single computing device.

[00249] At step 1518, the service application receives the requested virtual payment card from the remote server. At step 1520, the service application is configured to automatically fill the information about the virtual payment card on the payment portal page, without requiring any effort from the user. The service application may then automatically submit the details on the portal page to initiate the transaction, as shown in step 1522. Once the virtual payment card is received by the merchant acquirer server, the same can be shared with the payment network 1110 and the issuer financial institution for the execution of the payment, wherein the payment information received from the merchant acquirer server is compared with the already stored payment information in the transaction processing engine to determine if the payment can be approved on the basis of the comparison, wherein the payment is approved when the information shared by the merchant acquirer server matches to the already stored information in the database of the transaction processing engine within a predefined time period. The service application is also configured to receive the notifications about the status of the transaction request, wherein the status of the transaction request can be success or the denial of the payment.

[00250] In an embodiment of the present invention, the service application may use web scripts to automatically detect web portal IP addresses or domain URLs and may automatically run scripts to auto-fill payment details with user's permission and skip all web pages to load at the user end that demands payment information. This way the user accessing the online payment page will not require to manually enter the payment card details for the processing of the transaction.

[00251] This way, the user is escaped from a need of sharing his/her bank or card details with the payment portal and therefore minimizes fraud possibilities. Also, the merchants and intruders will never receive user information and the user and intruder will never have access to the dynamically generated payment card information. This type of anonymity will enhance payment transaction security and reliability. Also, the user who does not own a bank issued card (e.g. credit card and/or debit card) can make cashless card based transactions using the techniques mentioned in the present invention.

[00252] FIG. 16 schematically illustrates a flow diagram 1600 for anonymously paying to a vendor at the point-of-sale, in accordance with another embodiment of the present invention. According to this embodiment of the present invention, following two sub-steps are executed concurrently in real-time:

1. associating, by a user device 1104, a virtual payment card with an ongoing transaction, and transmitting, by the user device 1104, a notification to a transaction processing engine 1116, wherein the notification comprises at least the virtual payment card details and a time stamp associated with the ongoing transaction; and

2. transmitting, by a vendor device 1106, a verification request to the transaction processing engine 1116 for the processing and verification of the ongoing transaction, wherein the verification request comprises at least the virtual payment card details associated with the ongoing transaction.

[00253] According to a preferred embodiment of the invention, the transaction processing engine 1116 gets the notification about the ongoing transaction from the user device 1104 before the transaction processing engine 1116 gets the verification request from the vendor device 1106, wherein the notification about the ongoing transaction from the user device 1104 comprises a first information and the verification request from the vendor device 1106 comprises a second information. The first information and the second information further comprise one or more parameters related to the ongoing transaction. In one embodiment, the first information and the second information comprise at least details about the virtual payment card. In another embodiment, the first information also comprises at least the time stamp information. In yet another embodiment, the first information and the second information may comprise of additional transaction details apart from the virtual payment card such as, and without limitation, merchant name, merchant type, merchant location, date and/or time of transaction, transaction amount, and/or currency details.

[00254] In an embodiment, the user device 1104 is suitably programmed to transmit the notification about the ongoing transaction to the transaction processing engine 1116 prior to the transmission of the verification request by the vendor device 1106 to the transaction processing engine 1116 for quick processing of the transactions,, wherein the notification about the ongoing transaction comprises the first information, and the verification request comprises the second information.

[00255] In another embodiment, the method may be configured to wait for a predefined time before declining the transaction if the transaction processing engine 1116 gets the verification request from the vendor device 1106 before the transaction processing engine 1116 gets the notification from the user device 1104 or vice-versa, wherein the verification request from the vendor device 1106 comprises the second information and the notification from the user device 1104 comprises the first information. The method is configured to approve the transaction only when the first information and the second information is received at the transaction processing engine 1116 within the predefined time, and at least a portion of details of the first information matches with at least a portion of details of the second information. In a preferred embodiment, the aforementioned portion of details of the first information and the second information comprises details about the virtual payment card. In another embodiment, the first information also comprises the time stamp information along with virtual payment card details. The time stamp is the time at which the virtual payment card is shared with the vendor device 1106 by the user device 1104 (i.e. the time when the transaction is initiated).

[00256] In an embodiment, the time stamp information shared by the user device 1104 with the transaction processing engine 1116 is used to determine whether the predefined time period has been lapsed or not. In another embodiment, the time at which either of the notification or verification request is received first at the transaction processing engine 1116 is used as a reference to determine whether the predefined time period has been lapsed or not. In an embodiment, the predefined time period is less than equal to 180 seconds. According to another embodiment, the predefined time period is less than equal to 360 seconds.

[00257] If either of the first information and or the second information is not received by the transaction processing engine 1116 within the predefined time period, then the transaction is declined. In other words, it is important that both the first information and the second information are received within the predefined time, and at least the portion of the details present in the first information and the second information is matched for a successful transaction to take place.

[00258] The user device 1104 is configured with the service application that facilitates the user device 1104 in making anonymous payments. The flow 1600 starts when the user device 1104 configured with the service application is brought near to the vendor device 1106, wherein the user device 1104 is configured to share the details of the virtual payment card with the vendor device 1106, as shown in step 1602. According to the preferred embodiment of the invention, the user device 1104 and the vendor device 1106 are configured to communicate with each other using a contactless mode of communication, wherein the contactless mode of communication can be such as, but not limited to, Near-Field Communication (NFC).

[00259] According to an embodiment, one or more virtual payment cards are pre-generated and/or pre-saved in the service application of the user device 1104 and the service application is configured to select and associate a virtual payment card with the ongoing transaction. According to another embodiment, the service application is configured to generate a random virtual payment card on-the-fly at the initiation of the transaction and associate the randomly generated virtual payment card with the ongoing transaction.

[00260] In another exemplary embodiment of the present invention, the service application running on the user device 1104 is configured to request and store the one or more virtual payment cards generated by an issuing

bank 1114 and/or a card issuer 1112 in advance. The service application running on the user device 1104 may be configured to periodically request and securely store the one or more virtual payment cards in the memory of the user device 1104.

[00261] In yet another embodiment, the service application running on the user device 1104, may be configured to check the availability of the virtual payment cards. If there are no virtual payment cards available for the transaction, the service application may be configured to either generate or request the issuing bank 1114 and/or the card issuer 1112 for the virtual payment cards in real time.

[00262] In an embodiment of the invention, the virtual payment card generated by the service application may not be used for the execution of the transaction until validated by comparing the first information and the second information, however, various other modifications in this should be recognized by the person skilled in the art.

[00263] Further, in one of the exemplary embodiments, the security of the transactions may be further improved by restricting the usage of the virtual payment cards. For example, each of the pre-generated or requested virtual payment cards may have an associated maximum purchase limit, vendor related restrictions, expiry duration, location related restrictions, or a combination thereof.

[00264] Additionally, and without limitation, the user device 1104 is suitably configured to receive transaction details from the vendor device 1106 on the merchant side, as shown in step 1604. However, it should be noted that the step 1604 is an optional step and the method 1600 may be suitably implemented without the execution of this step (i.e. 1604). In one embodiment, the step 1604 may be executed before the execution of the step 1602, therefore the user device 1104 may be configured to receive the transaction details first and then it may share a virtual payment card with the vendor device 1106. In another embodiment, the method 1600 may be suitably implemented to execute step 1602 concurrently with the step 1604 at the same time. Thereby the user device 1104 may be configured to receive the transaction details and share the virtual payment card with the vendor device 1106 at the same time. However, it should be noted that these two steps are executed simultaneously in real-time without any significant delay. According to this embodiment, the service application on the user device 1104 processes the received transaction details (i.e. at step 1604) and associates the virtual payment card with the ongoing transaction, wherein the service application associates the virtual payment card with the ongoing transaction using a random selection method. In an alternate embodiment, the service application is configured to select the pre-generated virtual payment card using a selection criterion, wherein the selection criterion may depend on parameters such as, but not limited to, merchant type, merchant name, merchant location, date and/or time of transaction, item/product details, currency details, and/or transaction amount.

[00265] According to some exemplary embodiments, when the NFC transaction starts, and the user device 1104 and the contactless vendor device 1106 start to exchange data between each other. The best point during the transaction to notify the transaction processing engine 1116 will be when the contactless vendor device 1106 is sending a GENERATE AC command to the user device 1104. The GENERATE AC command that the contactless vendor device 1106 sends to the user device 1104, commands the user device 1104 to generate an application cryptogram (AC). At that point, all the transaction details are known to the user device 1104, wherein

the transaction details comprise one or more of the transaction amount, merchant details, item details, merchant device ID, currency, and/or merchant location.

[00266] It should be noted that while performing the GENERATE AC command, the user device 1104 is suitably programmed to decide if it approves the transaction offline, declines the transaction, or decides to go for online authorization. If the user device 1104 decides to go for online authorization, then the contactless vendor device 1106 will go online, and transaction processing engine 1116 and/or issuing bank 1114 will get the verification request through the vendor device 1106. But in some cases, although the user device 1104 approves the transaction offline or even if the user device 1104 declined the transaction totally, it is still possible that the contactless vendor device 1106 may go online for online authorization. Therefore, according to this aspect of the invention, user device 1104 may be configured to notify the transaction processing engine 1116 and/or issuing bank 1114 no matter what is the result of the GENERATE AC command.

[00267] Once the virtual payment card is associated with the ongoing transaction, the service application transmits the notification to the issuing bank 1114 for notifying the details of at least the virtual payment card and the time stamp (timestamp defining the time at which the virtual payment card was shared with the vendor device 1106 and/or the time at which the virtual payment card was associated with the ongoing transaction by the user device), as shown in step 1606. The notification from the user device 1104 to the issuing bank 1114 may also comprises optional transaction details apart from the virtual payment card and the time stamp, wherein optional transaction details comprises such as, but not limited to, merchant details, item details, merchant device ID, merchant location, currency and/or requested amount. Therefore, at this step the user device 1104 sends all the details to the issuing bank 1114.

[00268] The issuing bank 1114, upon reception of the aforementioned details, commands to the transaction processing engine 1116 to store the information regarding the ongoing transaction for further processing of the transaction, as shown in step 1608.

[00269] Thereby, the transaction processing engine 1116 stores the information received from the issuing bank 1114 in a database 1118 and may send a confirmation to the issuing bank 1114. The information stored by the transaction processing engine 1116 comprises at least the virtual payment card and the time stamp information at which the virtual payment card was shared with the vendor device 1106. Further, in an embodiment, the transaction processing engine 1116 optionally stores the additional information regarding the transaction, for example and without limitation, a vendor device ID, merchant details, merchant location, item/product details, transaction amount, currency, USERID, State of the transaction (=approved/denied), card expiry date/time, virtual card details, virtual card number, and card use status (=open/closed).

[00270] While the user device 1104 is sharing the notification about the ongoing transaction with the transaction processing engine 1116, the vendor device 1106 is configured to transmit the verification request to the transaction processing engine 1116 simultaneously. Thereby, the vendor device 1106 transmits at least the received virtual payment card details to a merchant acquirer 1108 which in turn shares this information with a payment network 1110, as shown in step 1610 and 1612 respectively. Optionally, the vendor device 1106 is configured to transmit additional transaction details along with the virtual payment card details with the merchant

acquirer 1108, wherein the additional transaction details comprises one or more of vendor device ID, merchant details, item/product details, merchant location, transaction amount, currency information, etc.

[00271] At step 1614, the payment network 1110 is configured to transmit at least the virtual payment card details to the card issuer 1112, which further forwards these details to the issuing bank 1114, at step 1616.

[00272] At step 1618, upon reception of at least the virtual payment card from the card issuer 1112, the issuing bank 1114 determines whether sufficient balance exist in associated user account to execute the transaction or if there's any fraudulent activity reported with the associated user's bank account.

[00273] After confirming that the user account can execute the transaction, suitably programmed processing systems of the issuing bank 1114 (i.e. financial institution) processes the received virtual payment card details and the optional transaction details and transmits these details to the transaction processing engine 1116, as shown in step 1620. On receiving at least, the virtual payment card details, the suitably configured processing systems at the transaction processing engine 1116 verifies the authenticity of the virtual payment card details by checking if the record exists for the received virtual payment card details in the database 1118. The transaction processing engine 1116 compares the virtual payment card details, received at step 1620, with the previously notified virtual payment card details, received at step 1608, and determines if both the virtual payment card details match with each other. The transaction processing engine 1116 also determines whether at least the virtual payment card shared by the vendor device 1106 and the user device 1104 is received within the predefined time period, wherein the lapse of the predefined time period is determined using the time stamp shared by the user device 1104. If it is determined that the predefined time period has been lapsed, then the transaction is declined, and a transaction decline receipt is transmitted to vendor device 1106 and/or user device 1104.

[00274] In another scenario, the verification request from the vendor device 1106 may be received by the transaction processing engine 1116 before the reception of the notification from the user device 1104. In that case, the transaction processing engine 1116 is configured to record the details received in the verification request in the database 1118 and a predefined wait time counter is initiated. If the notification about the ongoing transaction is not received within the predefined wait time, then the transaction processing engine 1116 is configured to decline the transaction.

[00275] Optionally, the transaction processing engine 1116 also matches the merchant details to determine if the virtual payment card is being used with the same merchant and within the limited time period. Alternatively, the transaction processing engine 1116 may also determine the status of the card before approving the transaction, wherein if the status of the card is open it is determined that the virtual card is being used for the first time and is therefore valid. However, various other modifications in this should be recognized by the person skilled in the art.

[00276] The transaction processing engine 1116, after determining whether the ongoing transaction is legitimate and not, transmits a message to the vendor device 1106 using an inverse process to report the success or the denial of the transaction, as shown in step 1622. Additionally, a message indicating successful/un-successful

processing of the transaction may be conveyed by the transaction processing engine 1116 to the user by using the user device 1104.

[00277] Further in one of the unique embodiments, the card issuer 1112 can be configured to perform functions of the issuing bank 1114 as mentioned herein. In other words, the card issuer 1112 can be configured to record at least the details of virtual payment card and time stamp received from the user device 1104 in the transaction processing engine 1116, and facilitate the authentication of the transaction by comparing at least the virtual payment card details received from the vendor device 1106 and the user device 1104. According to this embodiment, the card issuer 1112 can be configured to receive the notification about the ongoing transaction from the service application of the user device 1104, wherein the notification about ongoing transaction comprises one or more of the virtual payment card, the time stamp, and/or other details associated with the ongoing transaction. The card issuer 1112 can be further configured to transmit a command to the transaction processing engine 1116 to store the information regarding the ongoing transaction in the database 1118 for further verification of the transaction. Further, the card issuer 1112 can also be configured to receive at least the virtual payment card details from the vendor device 1106 and facilitate the comparison of at least the virtual card details received from the user device 1104 and the vendor device 1106 for the authentication of the ongoing transaction.

[00278] Similarly, in an alternate embodiment, the present invention may be configured to operate without the card issuer 1112 and the issuing bank 1114 may be configured to perform additional functions of the card issuer 1112. According to an embodiment, the functionalities of the card issuer 1112 and the issuing bank 1114 may be integrated and hosted within a single computing device.

[00279] In another variation of the invention, the vendor device 1106 and the user device 1104 may be configured to communicate with the transaction processing engine 1116 to speed up the processing of the transactions, and therefore the issuing bank 1114 and card issuer 1112 may not be required according to this implementation of the invention.

[00280] The secure transaction method disclosed in this embodiment of the present invention is a single-step method, which further comprises two sub-steps that are executed concurrently in real-time to ensure fast and secure processing of the cashless transactions. First sub-step is about associating a virtual payment card with an ongoing transaction and notifying at least the virtual payment card and a timestamp to a transaction processing engine, wherein these details are further recorded in a database of the transaction processing engine. In a second sub-step, which is executed simultaneously while the first sub-step is being executed, at least details of the virtual payment card are transmitted to the transaction processing engine by a vendor device. The transaction processing engine compares the information received from the vendor device and the information received from the user device. The transaction processing engine also determines that whether both of the information are received within a predefined time period. Therefore, by using the present invention, the payment is released only when the information received from the vendor device matches to the information provided by the user device within the predefined time period. If the output of this comparison step is invalid, then the transaction is declined.

[00281] It shall be apparent to the person skilled in the art that the invention is described in reference to cashless transactions at the point of sale (POS), but it shall not be considered limiting and many changes and modifications may be made within the scope of the embodiments herein, without departing from the spirit and scope thereof, and the embodiments herein include all such modifications. Thereby, the present invention can also be modified to execute the cashless e-commerce transactions or online payment portals (e.g. web portal) transactions.

[00282] Therefore, the present invention presents a new system and method for providing secure and fast cashless transactions without the risk of exposing the user account details to the merchant or any other third parties involved during the processing of the transactions over computer networks. The solution proposed by the present invention combats the user account theft that captures the user account details during the execution of the cashless transactions over the internet.

[00283] Although the present disclosure has been described in terms of certain preferred embodiments, various features of separate embodiments can be combined to form additional embodiments not expressly described. Moreover, other embodiments apparent to those of ordinary skill in the art after reading this disclosure are also within the scope of this invention. Furthermore, not all of the features, aspects and advantages are necessarily required to practice the present disclosure. Thus, while the above detailed description has shown, described, and pointed out novel features of the invention as applied to various embodiments, it will be understood that various omissions, substitutions, and changes in the form and details of the apparatus or process illustrated may be made by those of ordinary skill in the technology without departing from the spirit of the invention. The inventions may be embodied in other specific forms not explicitly described herein. The embodiments described above are to be considered in all respects as illustrative only and not restrictive in any manner.

CLAIMS:

1. A computer implemented method for processing transactions, the computer implemented method comprising:

receiving, by a remote server, a request for processing an ongoing transaction from a user device;

facilitating, by the remote server, generation of a first virtual payment card associated with the ongoing transaction;

facilitating, by the remote server, storage of the first virtual payment card associated with the ongoing transaction in a database;

facilitating, by the remote server, sharing of the first virtual payment card associated with the ongoing transaction with a merchant device;

receiving, by the remote server, a request for verification of the ongoing transaction from the merchant device, wherein the request for verification of the ongoing transaction comprises a second virtual payment card from the merchant device;

facilitating, by the remote server, comparison of the second virtual payment card with the first virtual payment card stored in the database; and

determining, by the remote server, validity of the ongoing transaction, wherein the ongoing transaction is determined to be valid when the first virtual payment card is determined to be same as that of the second virtual payment card on the basis of the comparison, and a predefined time criterion is satisfied by the ongoing transaction.

2. The computer implemented method of claim 1 further comprises:

initiating the ongoing transaction between the user device and the merchant device in a contactless mode of communication, wherein the contactless mode of communication is near field communication (NFC), infrared, RFID, Wi-Fi, Bluetooth, and/or QR code scan.

3. The computer implemented method of claim 1, wherein the request for processing the ongoing transaction from the user device further comprises a timestamp to determine whether the predefined time criterion is satisfied by the ongoing transaction.

4. The computer implemented method of claim 1 further comprises:

receiving, by the remote server, one or more of the following merchant details along with the second virtual payment card received in the request for verification of the ongoing transaction from the merchant device: merchant identifier, merchant location, merchant name, brand name, merchant device ID, and merchant address.

5. The computer implemented method of claim 1, wherein the predefined time criterion is satisfied by the ongoing transaction if the second virtual payment card is received before lapse of a predefined time period, wherein the predefined time period is determined using a timestamp received in the request for processing the ongoing transaction from the user device.

6. The computer implemented method of claim 1, wherein both of the request for processing the ongoing transaction from the user device and the request for verification of the ongoing transaction from the merchant device further comprises merchant details, wherein the ongoing transaction is determined to be valid when the merchant details are determined to be same, wherein the merchant details comprises one or more of merchant identifier, merchant location, merchant name, brand name, merchant device ID, and merchant address.

7. The computer implemented method of claim 1, further comprises; facilitating, by the remote server, transmission of a confirmation to the merchant device and/or the user device when the ongoing transaction is determined to be valid.

8. The computer implemented method of claim 1, wherein the remote server is hosted on or running under control of a financial institution and/or a card issuer.

9. The computer implemented method of claim 1 further comprises:

determining, by the remote server, whether there is enough balance in a financial account, associated with a user of the user device, to execute the ongoing transaction before facilitating the generation of the first virtual payment card.

10. The computer implemented method of claim 1 further comprises:

facilitating, by the remote server, determination of use status of the first virtual payment card and the second virtual payment card, wherein the ongoing transaction is determined to be valid when the use status of both the first virtual payment card and the second virtual payment card is determined to be used for first time.

11. The computer implemented method of claim 1, wherein the step of facilitating, by the remote server, sharing of the first virtual payment card with a merchant device further comprises:

transmitting, by the remote server, the first virtual payment card to the user device; and

sharing, by the user device, the virtual payment card with the merchant device using a contactless mode of communication.

12. The computer implemented method of claim 1, wherein the merchant device is a point-of-sale (POS) device.

13. The computer implemented method of claim 1, wherein the ongoing transaction is an online purchase request initiated using a payment portal web interface.

14. The computer implemented method of claim 1, wherein the ongoing transaction is executed anonymously without sharing actual user account details with the merchant device and/or a merchant acquirer.

15. A computer implemented method for processing an ongoing transaction between a user device and a merchant device, the computer implemented method comprising:

receiving, by the user device, a suitable payment method for executing the ongoing transaction;

transmitting, by the user device, an authorization request to a financial institution associated with the suitable payment method;

receiving, by the user device, a response corresponding to the authorization request, the response facilitating, the user device, to determine whether the suitable payment method is able to execute the ongoing transaction;

transmitting, by the user device, a request for generation of a virtual payment card associated with the ongoing transaction to a remote server when it is determined that the suitable payment method is able to execute the ongoing transaction;

receiving, by the user device, a virtual payment card generated by the remote server;

facilitating, by the user device, storage of the received virtual payment card along with a timestamp in a database;

sharing, by the user device, the received virtual payment card with the merchant device; and

receiving, by the user device, a response regarding validity of the ongoing transaction, wherein the virtual payment card and the timestamp is used to determine validity of the ongoing transaction.

16. The computer implemented method of claim 15 further comprises:

initiating the ongoing transaction with between the user device and the merchant device using a contactless mode of communication, wherein the contactless mode of communication is near field communication (NFC), infrared, RFID Wi-Fi, Bluetooth, and/or QR code scan.

17. The computer implemented method of claim 15 further comprises:

receiving, by the user device, merchant details from the merchant device using a contactless mode of communication, wherein the merchant details comprises merchant identifier, merchant location, merchant name, brand name, merchant device ID, and merchant address; and

facilitating, by the user device, storage of the merchant details received from the merchant device in the database along with the virtual payment card and the timestamp.

18. The computer implemented method of claim 15, wherein the timestamp is used to determine a predefined time criterion, wherein the ongoing transaction is determined to be valid when the predefined time criterion is determined to be satisfied by the ongoing transaction.

19. The computer implemented method of claim 15 further comprises

transmitting a verification request, by the merchant device, to a transaction processing engine, wherein the verification request comprises the virtual payment card shared by the user device with the merchant device using a contactless mode of communication.

20. The computer implemented method of claim 15, wherein the merchant device is a point-of-sale (POS) device.

21. The computer implemented method of claim 15 further comprises:

determining, by a transaction processing engine, validity of the ongoing transaction, wherein the ongoing transaction is determined to be valid when the virtual payment card stored in the database by the user device

is same as that of the virtual payment card received in a verification request from the merchant device and a predefined time criterion is satisfied by the ongoing transaction; and

transmitting, by the transaction processing engine, the response regarding the validity of the ongoing transaction to the user device.

22. The computer implemented method of claim 15, wherein the predefined time criterion is satisfied by the ongoing transaction if the verification request is received from the merchant device before lapse of a predefined time period, wherein the predefined time period is determined using the timestamp received in the request for processing the ongoing transaction from the user device.

23. The computer implemented method of claim 15, wherein the remote server is hosted on or running under control of the financial institution and/or a card issuer.

24. The computer implemented method of claim 15 further comprises:

comparing, by a transaction processing engine, merchant details received in the verification request from the merchant device with merchant details received from the user device to determine whether the merchant details are same; and

determining, by the transaction processing engine, validity of the ongoing transaction, wherein the ongoing transaction is determined to be valid when the merchant details are determined to be same.

25. The computer implemented method of claim 15, wherein the user device is configured to facilitate a user to select the suitable payment method manually.

26. The computer implemented method of claim 15, wherein the user device is configured to select automatically the suitable payment method on the basis of previously stored user preferences or user purchase history.

27. The computer implemented method of claim 15, wherein the response corresponding to the authorization request facilitate the user device to determine whether there is enough balance in a financial account associated with a user of the user device to execute the ongoing transaction before facilitating the generation of the virtual payment card.

28. The computer implemented method of claim 15 further comprises:

determining, by a transaction processing engine, use status of the virtual payment card wherein the ongoing transaction is determined to be valid when the use status of the virtual payment card is determined to be used for first time.

29. The computer implemented method of claim 15, wherein the ongoing transaction is an online purchase request initiated using a payment portal web interface.

30. The computer implemented method of claim 15, wherein the ongoing transaction is executed anonymously without sharing actual user account details with the merchant device and/or a merchant acquirer.

31. A computer implemented method for processing transactions, the computer implemented method comprising:

receiving, by a transaction processing engine, a request for processing an ongoing transaction from a user device;

facilitating, by the transaction processing engine, generation of a first virtual payment card associated with the ongoing transaction;

facilitating, by the transaction processing engine, sharing of the first virtual payment card associated with the ongoing transaction with a merchant device;

receiving, by the transaction processing engine, a request for verification of the ongoing transaction, wherein the request for verification of the ongoing transaction comprises a second virtual payment card from the merchant device;

comparing, by the transaction processing engine, the second virtual payment card with the first virtual payment card; and

determining, by the transaction processing engine, validity of the ongoing transaction, wherein the ongoing transaction is determined to be valid when the first virtual payment card is determined to be same as that of the second virtual payment card on the basis of the comparison, and a predefined time criterion is satisfied by the ongoing transaction.

32. The computer implemented method of claim 31 further comprises:

initiating the ongoing transaction between the user device and the merchant device in a contactless mode of communication, wherein the contactless mode of communication is near field communication (NFC), infrared, RFID Wi-Fi, Bluetooth, and/or QR code scan.

33. The computer implemented method of claim 31, wherein the request for processing the ongoing transaction from the user device further comprises a timestamp to determine whether the predefined time criterion is satisfied by the ongoing transaction.

34. The computer implemented method of claim 31, wherein the predefined time criterion is satisfied by the ongoing transaction if the first virtual payment card and the second virtual payment card are received before lapse of a predefined time period, wherein the predefined time period is determined using a timestamp received in the request for processing the ongoing transaction from the user device.

35. The computer implemented method of claim 31 further comprises:

receiving, by the transaction processing engine, two or more of the following transaction details in the request for processing the ongoing transaction from the user device: merchant address, item details, merchant device ID, merchant location, merchant name, currency details, and/or a timestamp; and

storing, by the transaction processing engine, the received transaction details along with the virtual payment card associated with the ongoing transaction in a database.

36. The computer implemented method of claim 31 further comprises:

receiving, by the transaction processing engine, one or more of the following transaction details along with the second virtual payment card received in the request for verification of the ongoing transaction from the merchant device: item details, currency details, merchant address, merchant device ID, merchant name, and/or merchant location.

37. The computer implemented method of claim 31, wherein both of the request for processing the ongoing transaction from the user device and the request for verification of the ongoing transaction from the merchant device further comprises merchant details, wherein the ongoing transaction is determined to be valid when the merchant details are determined to be same by the transaction processing engine, wherein the merchant details comprises one or more of merchant identifier, merchant location, merchant name, brand name, merchant device ID, and merchant address..

38. The computer implemented method of claim 31, further comprises: facilitating, by the transaction processing engine, transmission of a confirmation to the merchant device and/or the user device when the ongoing transaction is determined to be valid.

39. The computer implemented method of claim 31, wherein the virtual payment card is generated by a remote server, wherein the remote server is hosted on or running under control of a financial institution associated with a user of the user device and/or a card issuer.

40. The computer implemented method of claim 31 further comprises:

facilitating, by the transaction processing engine, determination of whether there is enough balance in a financial account, associated with a user of the user device, to execute the ongoing transaction before facilitating the generation of the first virtual payment card.

41. The computer implemented method of claim 31 further comprises:

facilitating, by the transaction processing engine, determination of use status of the first virtual payment card and the second virtual payment card, wherein the ongoing transaction is determined to be valid when the use status of both the first virtual payment card and the second virtual payment card is determined to be used for first time.

42. The computer implemented method of claim 31, wherein the step of facilitating, by the transaction processing engine, sharing of the first virtual payment card with a merchant device further comprises:

transmitting, by the transaction processing engine, the first virtual payment card to the user device; and

sharing, by the user device, the virtual payment card with the merchant device using a contactless mode of communication.

43. The computer implemented method of claim 31, wherein the ongoing transaction is executed anonymously without sharing actual user account details with the merchant device and/or a merchant acquirer.

44. The computer implemented method of claim 31, wherein the ongoing transaction is an online purchase request initiated using a payment portal web interface.

45. A computer implemented method for processing transactions, the computer implemented method comprising:

receiving and displaying, by a user device, a payment portal web interface to make payment for an ongoing transaction;

receiving an authorization, by the user device, to process the ongoing transaction;

transmitting, by the user device, a request to a remote server to generate a virtual payment card corresponding to the ongoing transaction after receiving the authorization;

receiving, by the user device, a response from the remote server, wherein the response comprises at least a virtual payment card generated by the remote server;

identifying, by the user device, one or more fields on the payment portal web interface to be filled to process the ongoing transaction;

extracting, by the user device, one or more details from the response received from the remote server corresponding to the one or more fields on the payment portal web interface; and

filling automatically, by the user device the extracted one or more details in the corresponding one or more fields on the payment portal web interface, and submitting a request comprising the automatically filled details on the payment portal web interface to process the ongoing transaction.

46. The computer implemented method of claim 45, wherein the payment portal web interface is hosted on a third-party web server, the payment portal web interface providing various payment options to a user of the user device.

47. The computer implemented method of claim 45, wherein the authorization to process the ongoing transaction is provided manually by a user of the user device.

48. The computer implemented method of claim 45 further comprises

providing automatically the authorization to process the ongoing transaction by automatically selecting a suitable payment method on a basis of previously stored user preferences or user purchase history, wherein one or more payment methods are displayed on the payment portal web interface.

49. The computer implemented method of claim 45, wherein the one or more details extracted from the response received from the remote server are one or more of virtual payment card number, virtual payment card expiry time, virtual payment card generation time, user name, CVV, and/or contact details.

50. The computer implemented method of claim 45, wherein the request to the remote server to generate the virtual payment card further comprises a timestamp, wherein the timestamp is used to determine validity of the ongoing transaction.

51. The computer implemented method of claim 45, wherein the remote server is hosted on or running under control of a financial institution and/or a card issuer.

52. The computer implemented method of claim 45, wherein the request comprising the automatically filled details on the payment portal web interface to process the ongoing transaction is submitted to a merchant acquirer server.

53. The computer implemented method of claim 45 further comprises:

receiving, by a transaction processing engine, the virtual payment card generated by the remote server and a timestamp, wherein the timestamp is received from the user device;

storing, by the transaction processing engine, the virtual payment card and the timestamp in a database corresponding to the ongoing transaction;

receiving, by the transaction processing engine, a verification request for the ongoing transaction from a merchant acquirer server, wherein the verification request comprises the virtual payment card provided to the merchant acquirer server by the user device in the request comprising the automatically filled details;

comparing, by the transaction processing engine, the virtual payment card provided by the merchant acquirer server in the verification request and the virtual payment card stored in the database for the ongoing transaction;

determining, by the transaction processing engine, on the basis of the comparison whether the virtual payment card stored in the database for the ongoing transaction and the virtual payment card received from the merchant acquirer server are same; and

determining, by the transaction processing engine, validity of the ongoing transaction, wherein the ongoing transaction is determined to be valid when the virtual payment card is determined to be same, and the verification request from the merchant acquirer server is received before lapse of a predefined time period, wherein the predefined time period is determined using the timestamp received from the user device.

54. The computer implemented method of claim 45, wherein the ongoing transaction is executed anonymously without sharing actual user account details with a merchant acquirer server.

55. The computer implemented method of claim 45 further comprises:

facilitating, by the remote server, determination of whether there is enough balance in a financial account, associated with a user of the user device, to execute the ongoing transaction before the generation of the virtual payment card.

56. A computer implemented method for processing transactions, the computer implemented method comprising:

receiving, by a transaction processing engine, a plurality of notifications from a plurality of user devices, wherein each of the plurality of notifications comprises a virtual payment card associated with a corresponding ongoing transaction;

receiving, by the transaction processing engine, a plurality of verification requests from a plurality of merchant devices, wherein each of the plurality of verification requests comprises a virtual payment card associated with a corresponding ongoing transaction;

comparing, by the transaction processing engine, the plurality of verification requests and the plurality of notifications to determine whether at least one verification request and at least one notification comprises same virtual payment card;

identifying, by the transaction processing engine, an ongoing transaction associated with the same virtual payment card of the at least one verification request and the at least one notification; and

determining, by the transaction processing engine, validity of the identified ongoing transaction;

wherein the identified ongoing transaction is determined to be valid when the at least one verification request and the at least one notification satisfy a predefined time criterion.

57. The computer implemented method of claim 56 further comprises executing following two steps concurrently in real-time prior to the comparison by the transaction processing engine:

associating, by a respective user device, the virtual payment card with the ongoing transaction, and transmitting, by the respective user device, the at least one notification to the transaction processing engine, wherein the at least one notification comprises the virtual payment card and a timestamp associated with the ongoing transaction; and

transmitting, by a respective merchant device in communication with the respective user device, the at least one verification request to the transaction processing engine for the processing and verification of the ongoing transaction, wherein the verification request comprises the virtual payment card associated with the ongoing transaction.

58. The computer implemented method of claim 57 further comprises:

determining, by the transaction processing engine, that the two steps are executed concurrently in real time using the timestamp received in the at least one notification to determine the validity of the identified ongoing transaction.

59. The computer implemented method of claim 56, wherein the at least one notification and/or the at least one verification request further comprises a timestamp to determine whether the predefined time criterion is satisfied by the ongoing transaction.

60. The computer implemented method of claim 56, wherein the predefined time criterion is satisfied by the ongoing transaction when the at least one notification and the at least one verification request are received before lapse of a predefined time period, wherein the predefined time period is determined using a timestamp received in the at least one notification from a respective user device, the at least one verification request received from a respective merchant device or both.

61. The computer implemented method of claim 56, wherein when the identified ongoing transaction is determined to be valid, a successful receipt of the processing of the ongoing transaction is transmitted, by the transaction processing engine, to a respective user device, a respective merchant device, an acquirer of a merchant of the respective merchant device, and a financial institution of a user of the respective user device.

62. The computer implemented method of claim 56, wherein the at least one notification and the at least one verification request further comprises merchant details, wherein the identified ongoing transaction is determined to be valid when the merchant details are determined to be same, by the transaction processing engine, in the at least one notification and the at least one verification request.

63. The computer implemented method of claim 62, wherein the merchant details comprise one or more of merchant identifier, merchant location, merchant name, brand name, merchant device ID, and/or merchant address.

64. The computer implemented method of claim 56, wherein details of the virtual payment card received in the at least one verification request is provided to a respective merchant device by a respective user device using a contactless mode of communication, wherein the respective user device is performing the ongoing transaction with the respective merchant device.

65. The computer implemented method of claim 64, wherein the respective merchant device is a point-of-sale (POS) device and the contactless mode of communication is one or more of NFC, RFID, infrared, Bluetooth, and/or QR code scan.

66. The computer implemented method of claim 56 further comprises:

storing, by a respective user device, one or more virtual payment cards in a memory of the respective user device;

associating, by the respective user device, the virtual payment card, selected from the one or more virtual payment cards, with the ongoing transaction; and

transmitting, by the respective user device, the at least one notification to the transaction processing engine, wherein the at least one notification comprises the virtual payment card associated with the ongoing transaction.

67. The computer implemented method of claim 56 further comprises:

receiving merchant details by a respective user device, from a respective merchant device, during initiation of the ongoing transaction; and

incorporating the merchant details, by the respective user device, in the at least one notification before transmitting the at least one notification to the transaction processing engine.

68. The computer implemented method of claim 56 further comprises:

receiving, by a respective merchant device, the virtual payment card associated with the ongoing transaction, from a respective user device, at initiation of the ongoing transaction; and

transmitting, by the respective merchant device, the at least one verification request to the transaction processing engine, wherein the at least one verification request comprises the virtual payment card associated with the ongoing transaction.

69. The computer implemented method of claim 56, wherein the plurality of merchant devices are point-of-sale (POS) devices.

70. The computer implemented method of claim 56 further comprises:

storing, by the transaction processing engine, the plurality of notifications and the plurality of verification requests in a database prior to the comparison by the transaction processing engine.

71. The computer implemented method of claim 56, wherein the ongoing transaction is executed anonymously without sharing actual user account details with a respective merchant device and/or a merchant acquirer.

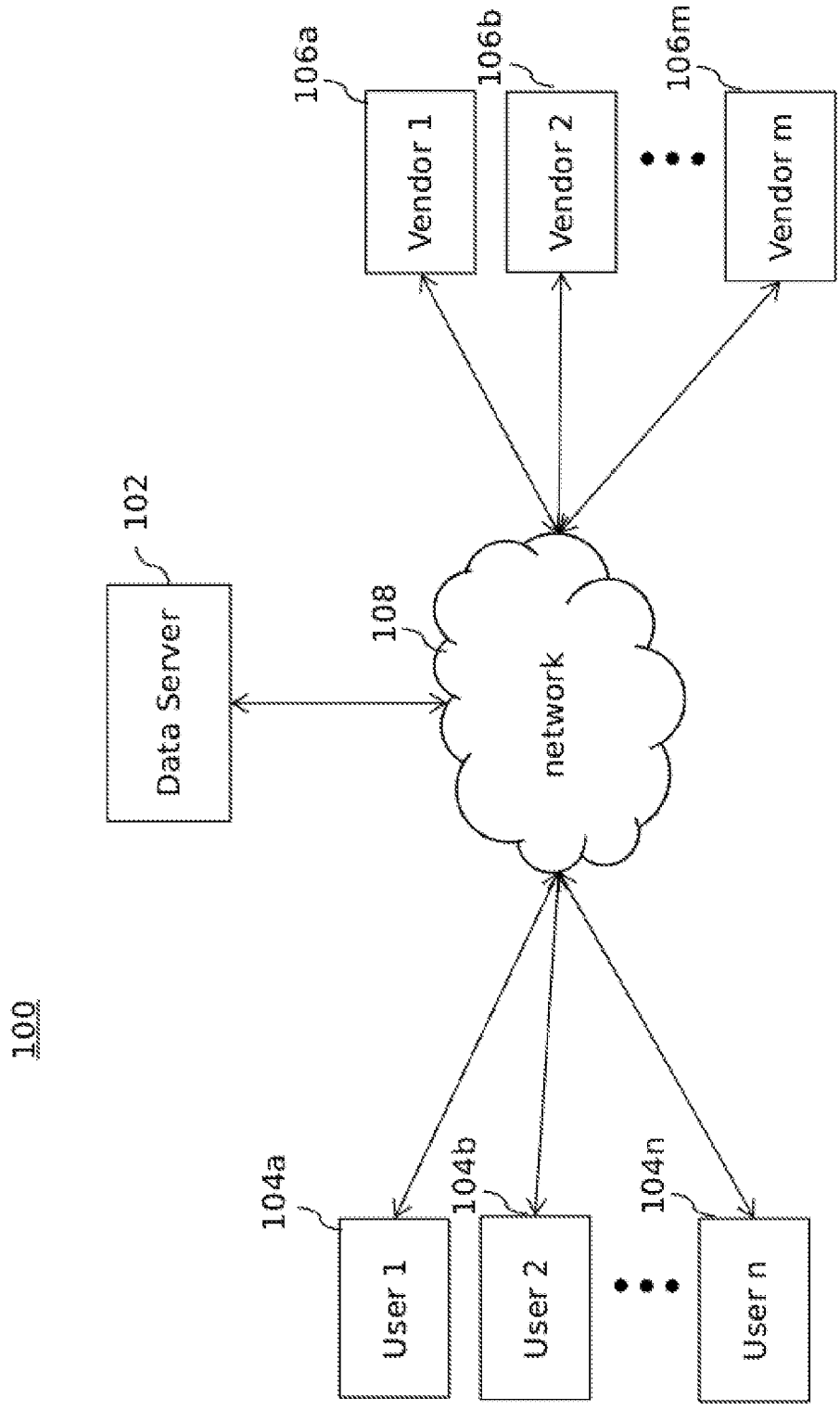

100
Data Server
102
network
108
Vendor 1
106a
Vendor 2
106b
Vendor m
106m
User 1
104a
User 2
104b
User n
104n

FIG. 1A

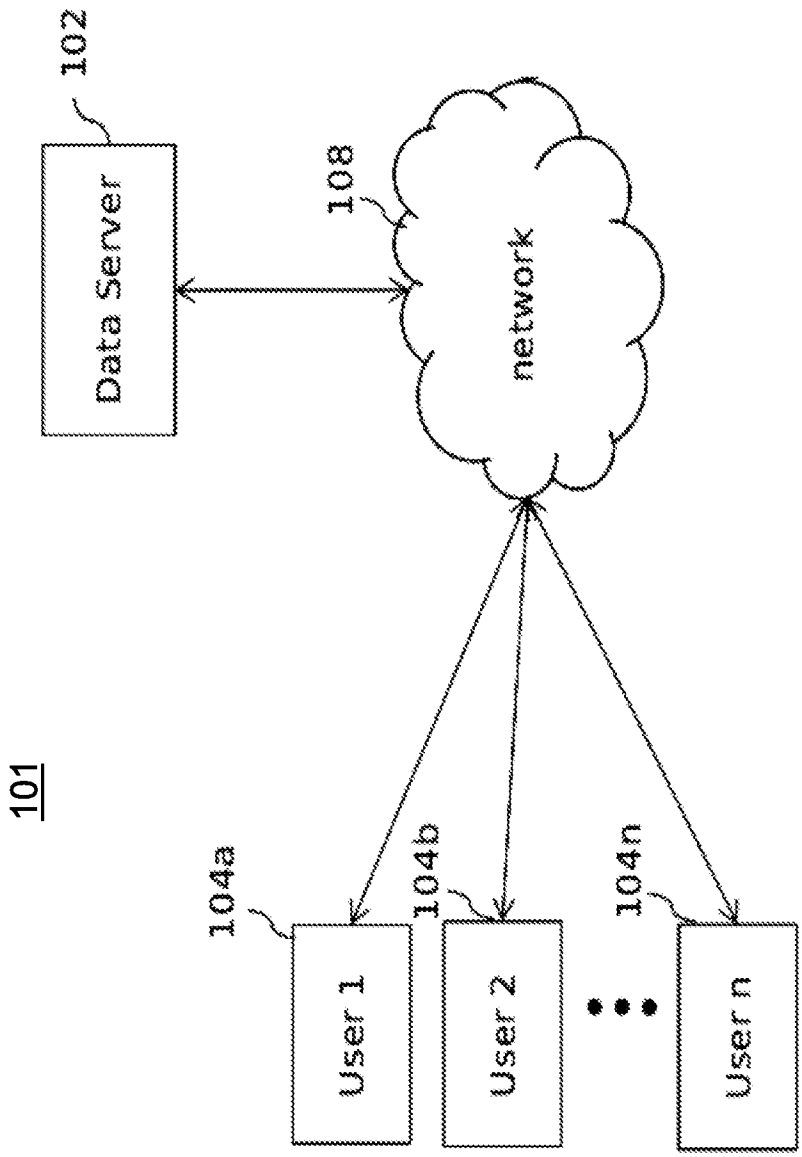

101
102
Data Server
108
network
104a
User 1
104b
User 2
104n
User n

FIG. 1B

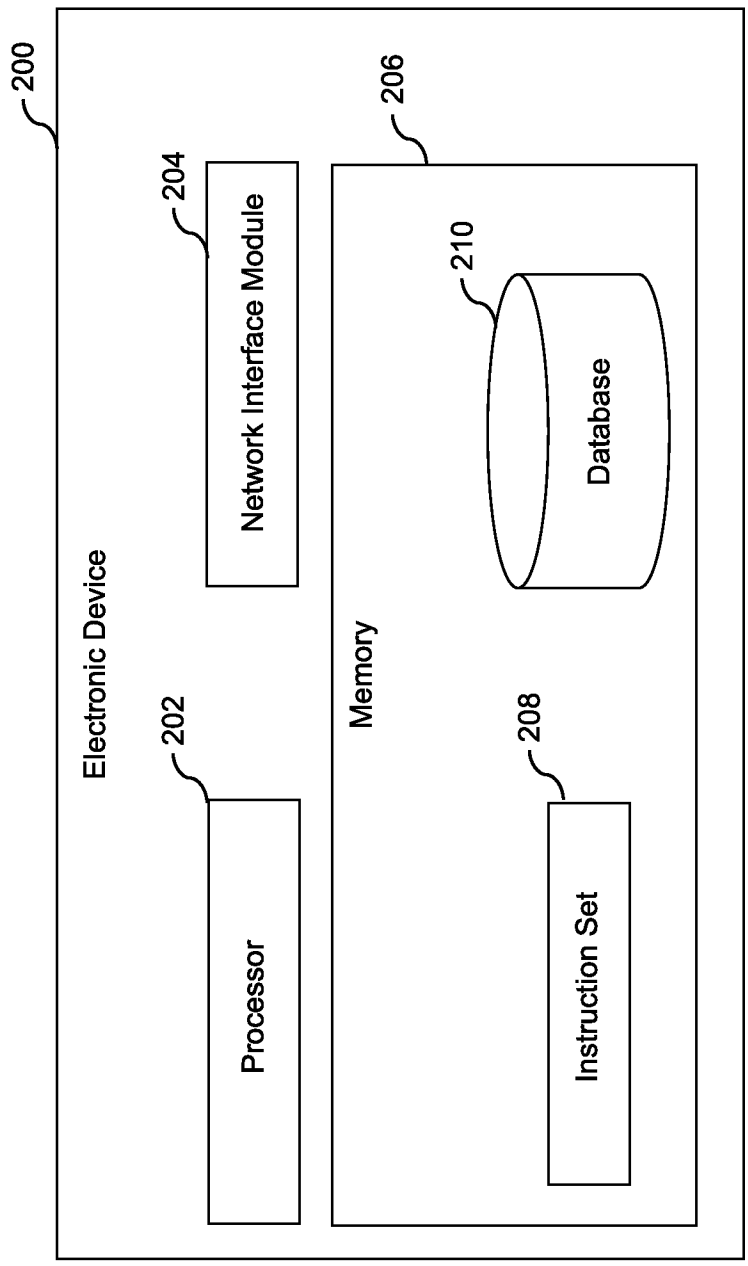

200
Electronic Device
202
Processor
204
Network Interface Module
206
Memory
208
Instruction Set
210
Database

FIG. 2

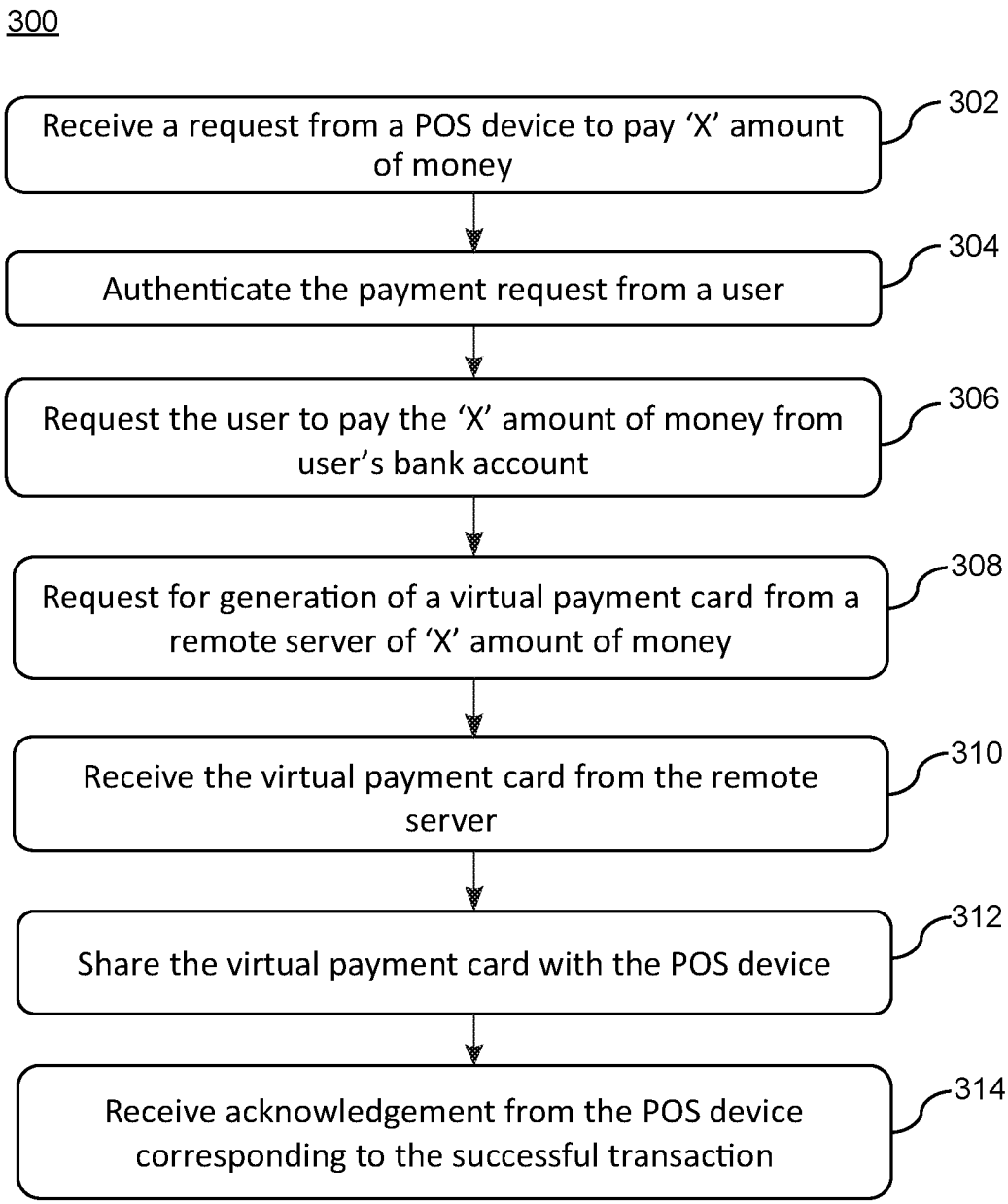

300
Receive a request from a POS device to pay 'X' amount of money
302
Authenticate the payment request from a user
304
Request the user to pay the 'X' amount of money from user's bank account
306
Request for generation of a virtual payment card from a remote server of 'X' amount of money
308
Receive the virtual payment card from the remote server
310
Share the virtual payment card with the POS device
312
Receive acknowledgement from the POS device corresponding to the successful transaction
314

FIG. 3

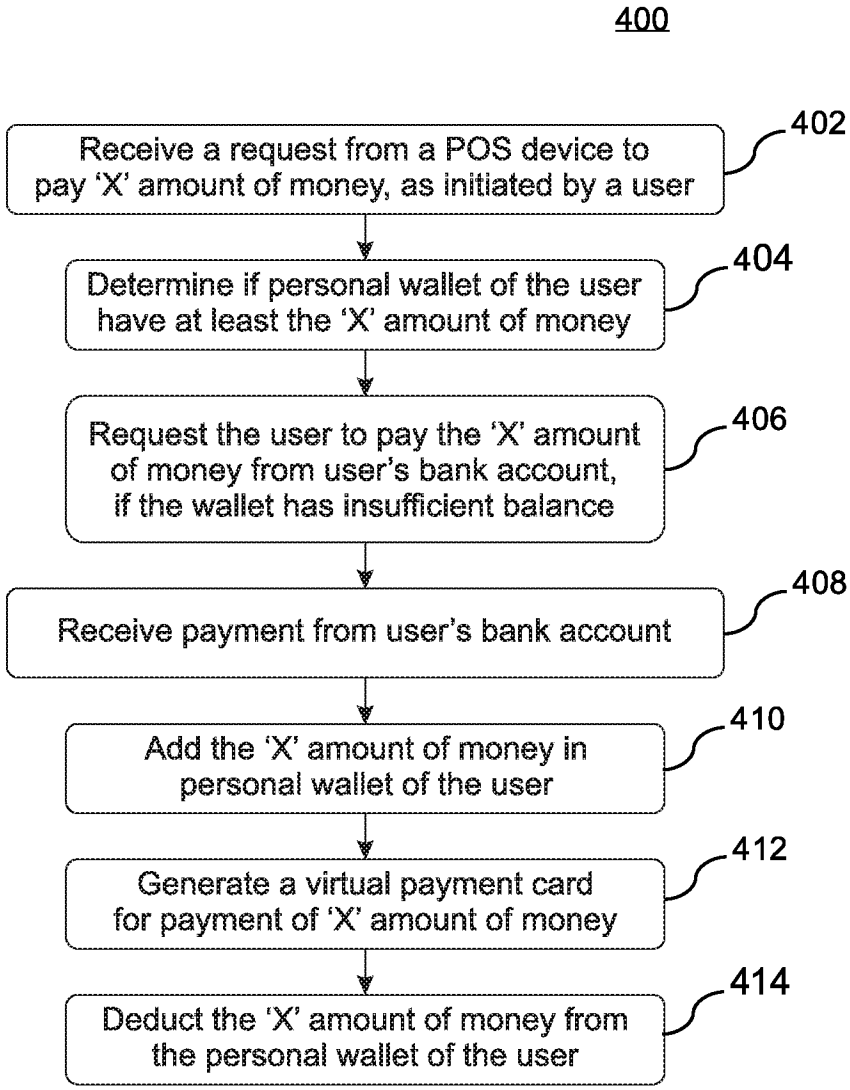

400
Receive a request from a POS device to pay 'X' amount of money, as initiated by a user
402
Determine if personal wallet of the user have at least the 'X' amount of money
404
Request the user to pay the 'X' amount of money from user's bank account, if the wallet has insufficient balance
406
Receive payment from user's bank account
408
Add the 'X' amount of money in personal wallet of the user
410
Generate a virtual payment card for payment of 'X' amount of money
412
Deduct the 'X' amount of money from the personal wallet of the user
414

FIG. 4

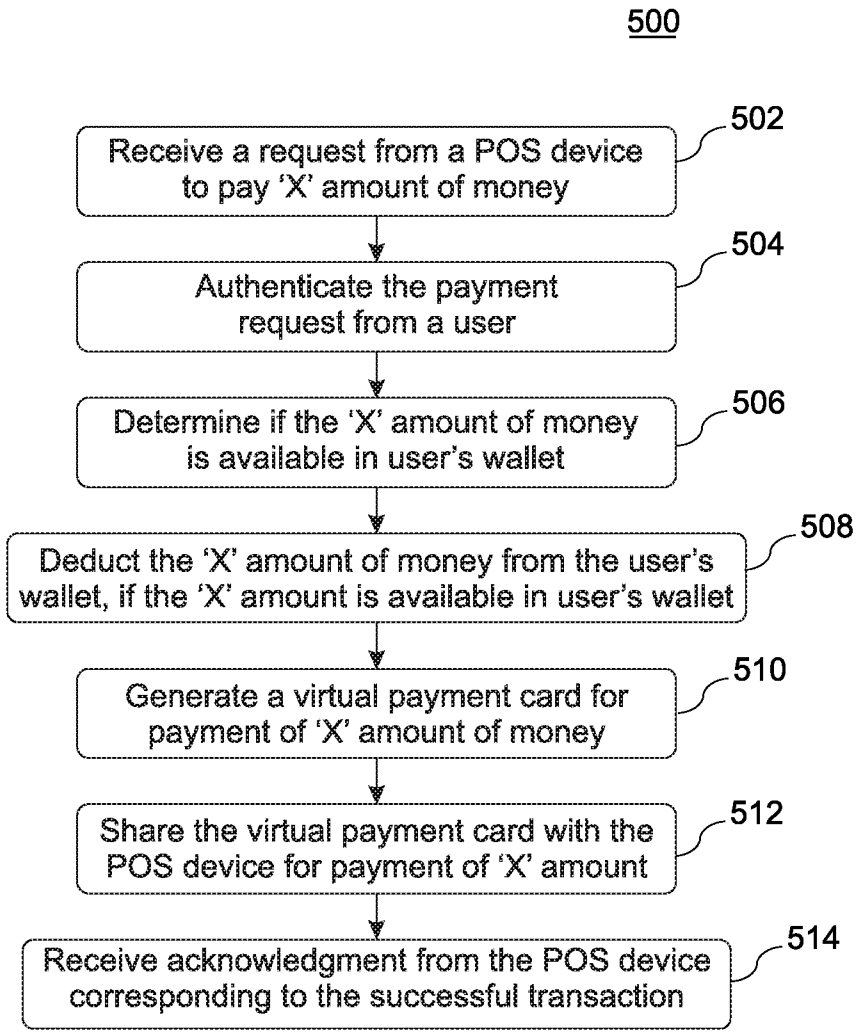

500
Receive a request from a POS device to pay 'X' amount of money
502
Authenticate the payment request from a user
504
Determine if the 'X' amount of money is available in user's wallet
506
Deduct the 'X' amount of money from the user's wallet, if the 'X' amount is available in user's wallet
508
Generate a virtual payment card for payment of 'X' amount of money
510
Share the virtual payment card with the POS device for payment of 'X' amount
512
Receive acknowledgment from the POS device corresponding to the successful transaction
514

FIG. 5

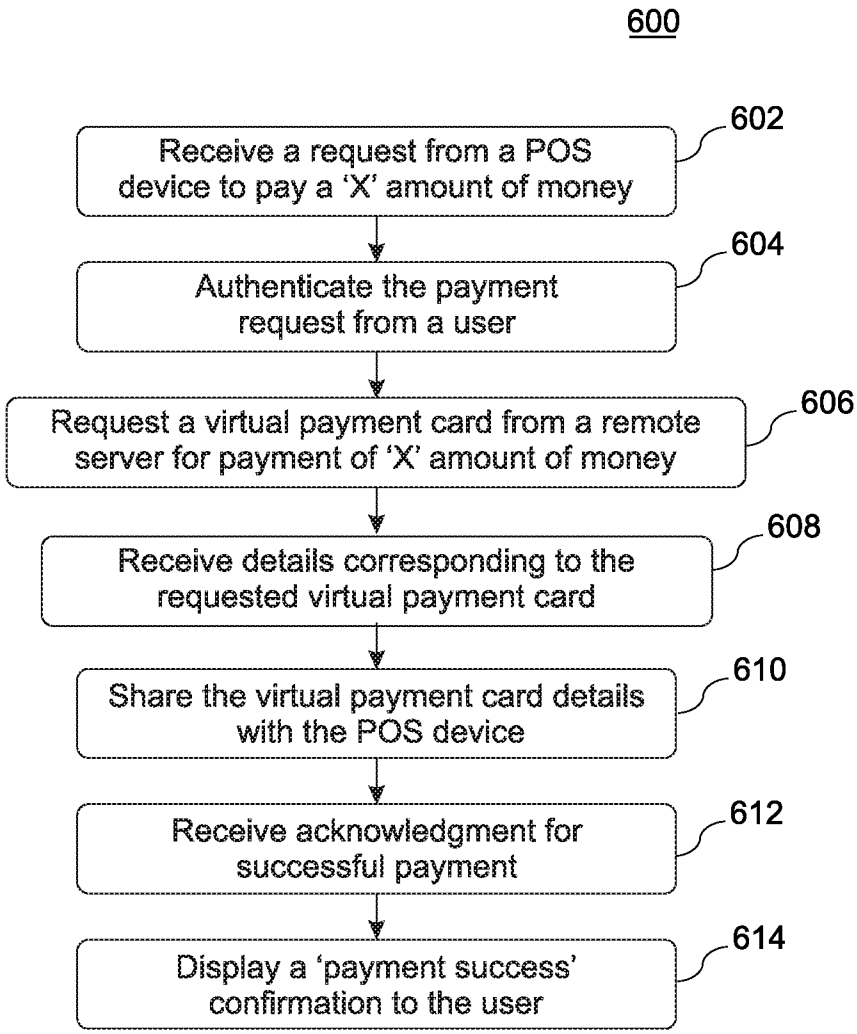

600
Receive a request from a POS device to pay a 'X' amount of money
602
Authenticate the payment request from a user
604
Request a virtual payment card from a remote server for payment of 'X' amount of money
606
Receive details corresponding to the requested virtual payment card
608
Share the virtual payment card details with the POS device
610
Receive acknowledgment for successful payment
612
Display a 'payment success' confirmation to the user
614

FIG. 6

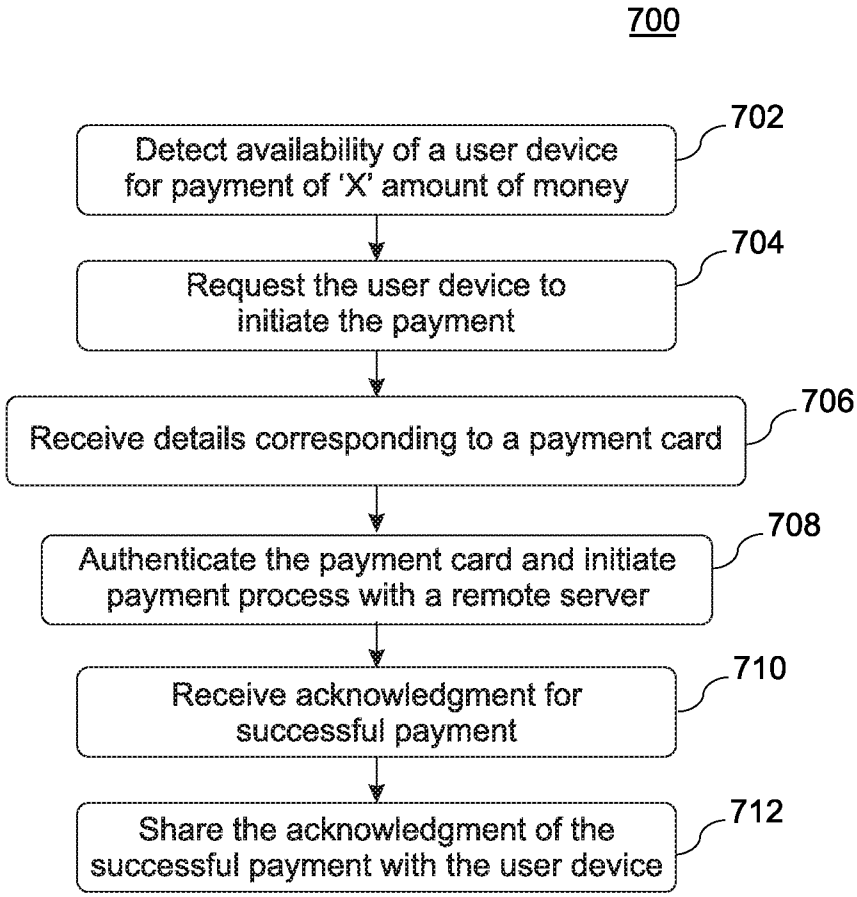

700
Detect availability of a user device for payment of 'X' amount of money
702
Request the user device to initiate the payment
704
Receive details corresponding to a payment card
706
Authenticate the payment card and initiate payment process with a remote server
708
Receive acknowledgment for successful payment
710
Share the acknowledgment of the successful payment with the user device
712

FIG. 7

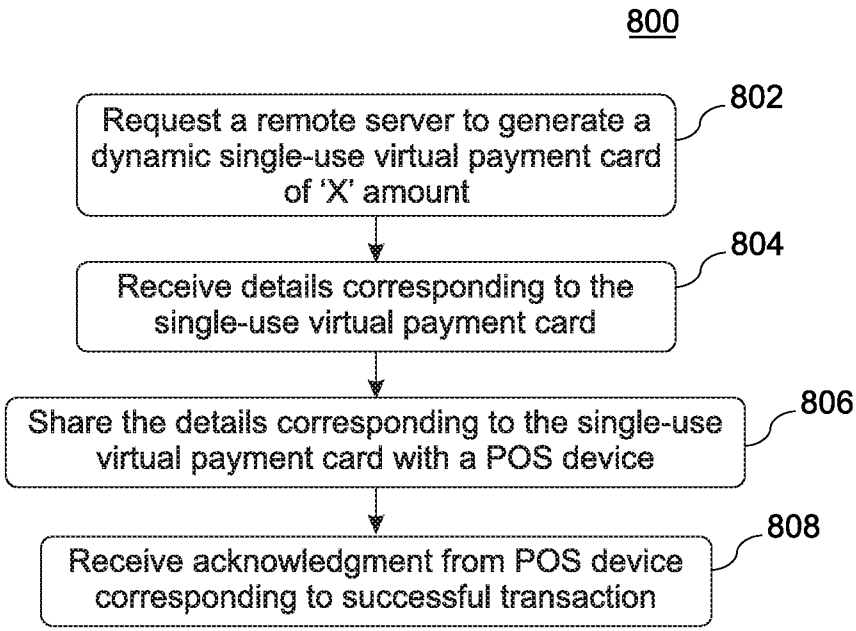

800
Request a remote server to generate a dynamic single-use virtual payment card of 'X' amount
802
Receive details corresponding to the single-use virtual payment card
804
Share the details corresponding to the single-use virtual payment card with a POS device
806
Receive acknowledgment from POS device corresponding to successful transaction
808

FIG. 8

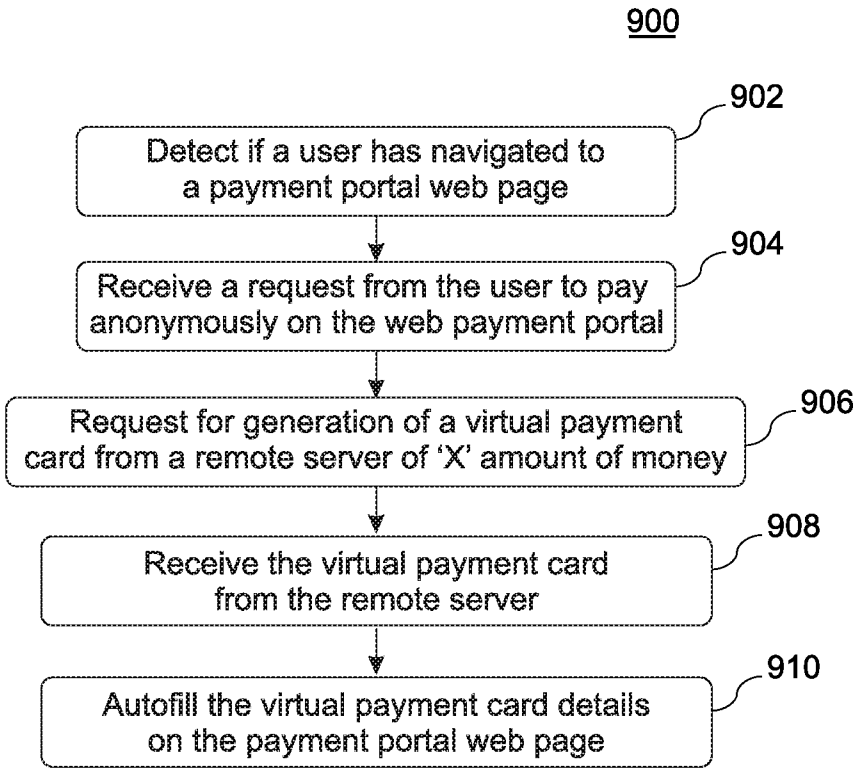

900
902
Detect if a user has navigated to a payment portal web page
904
Receive a request from the user to pay anonymously on the web payment portal
906
Request for generation of a virtual payment card from a remote server of 'X' amount of money
908
Receive the virtual payment card from the remote server
910
Autofill the virtual payment card details on the payment portal web page

FIG. 9

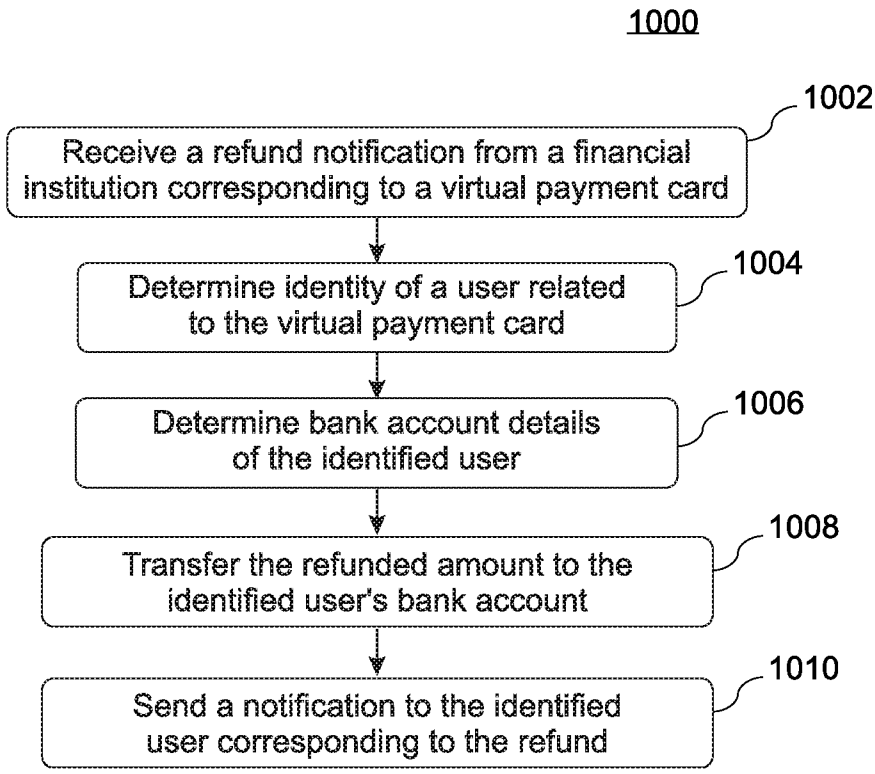

1000
1002
Receive a refund notification from a financial institution corresponding to a virtual payment card
1004
Determine identity of a user related to the virtual payment card
1006
Determine bank account details of the identified user
1008
Transfer the refunded amount to the identified user's bank account
1010
Send a notification to the identified user corresponding to the refund

FIG. 10

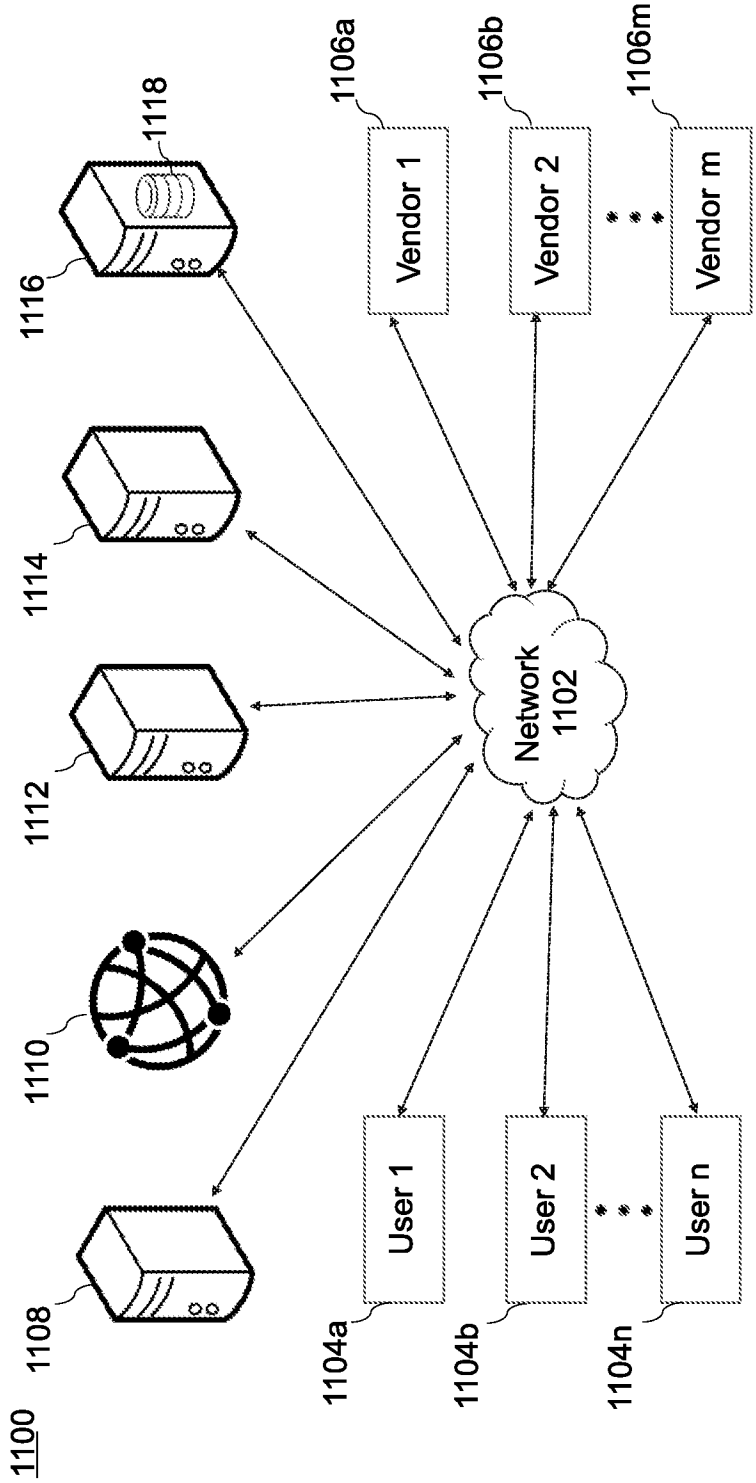

1100
1108
1110
1112
1114
1116
1118
Network
1102
Vendor 1
Vendor 2
Vendor m
1106a
1106b
1106m
User 1
User 2
User n
1104a
1104b
1104n

FIG. 11

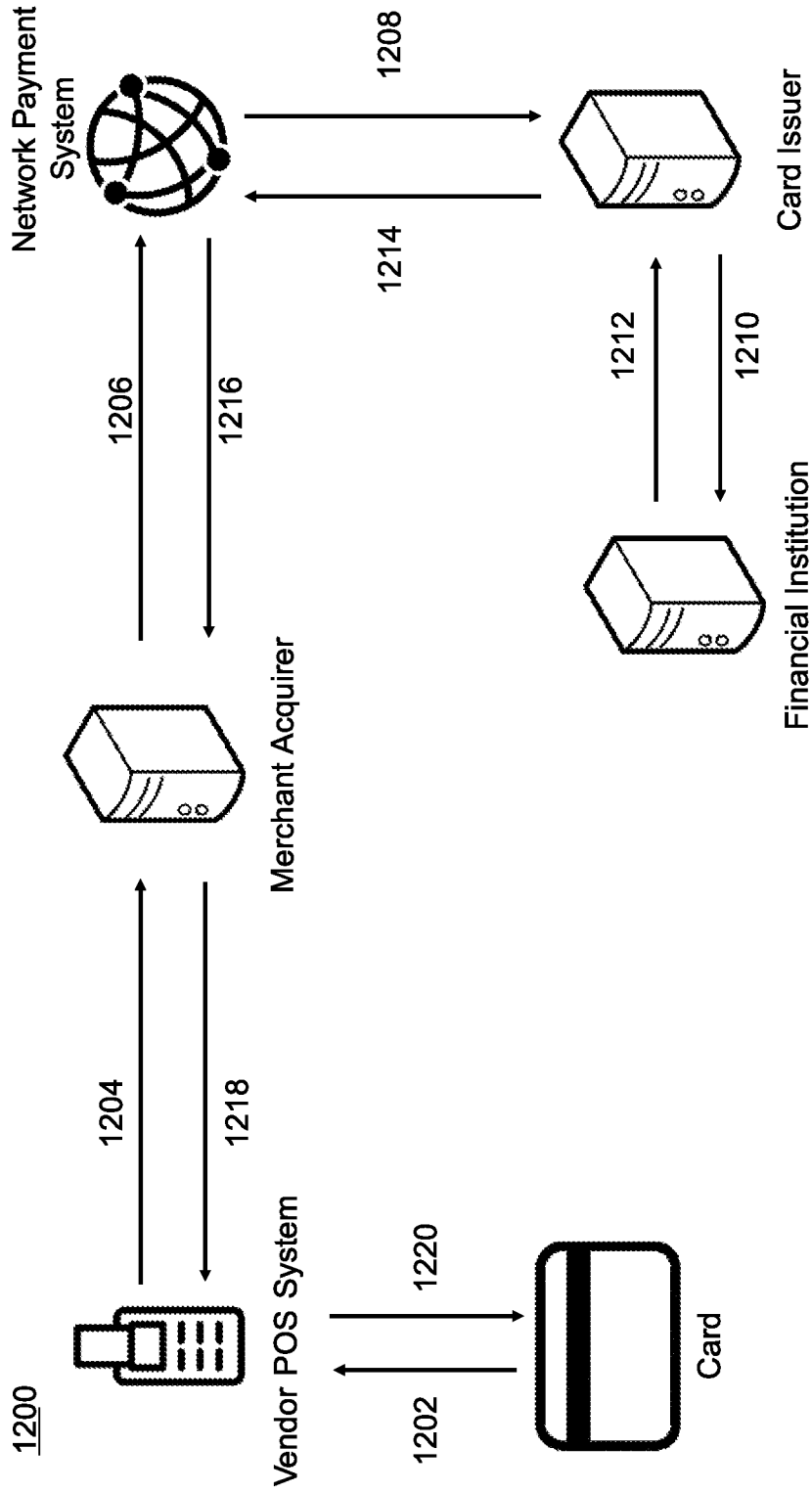

1200
Vendor POS System
Merchant Acquirer
Network Payment System
Financial Institution
Card Issuer
Card
1202
1204
1206
1208
1210
1212
1214
1216
1218
1220

FIG. 12

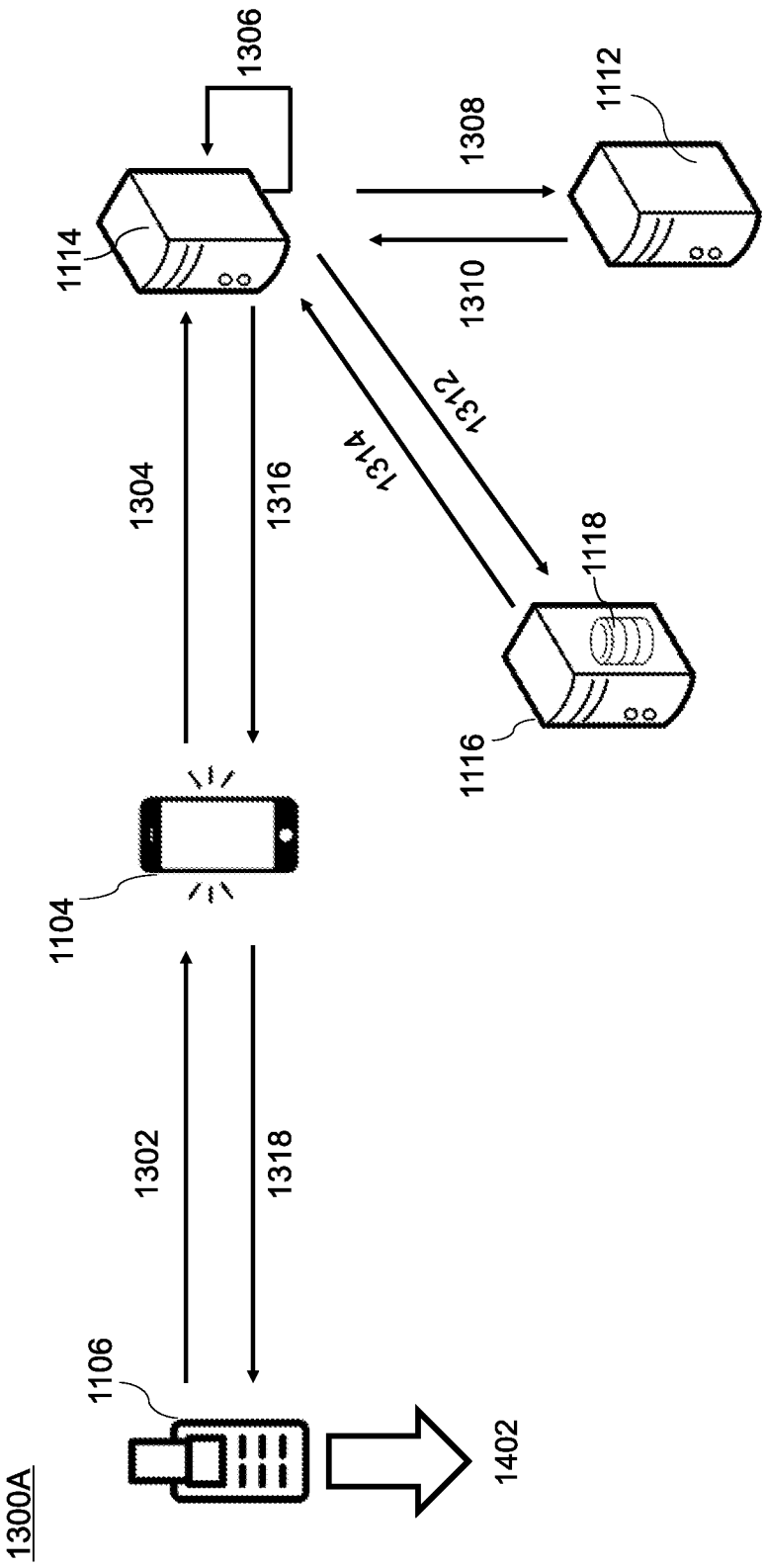

1300A
1106
1402
1302
1318
1104
1304
1316
1114
1306
1308
1310
1112
1312
1314
1118
1116

FIG. 13A

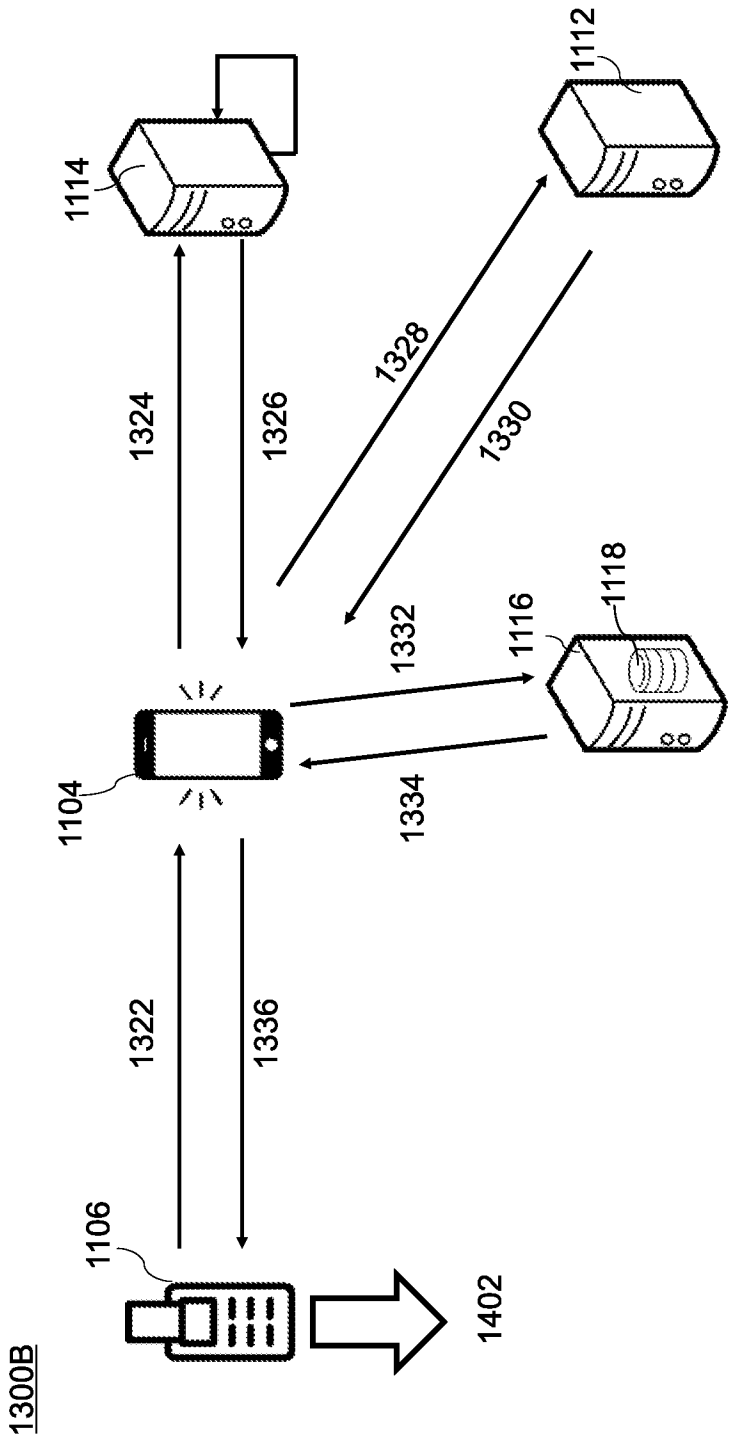

1300B
1106
1322
1336
1402
1104
1334
1332
1116
1118
1324
1326
1328
1330
1114
1112

FIG. 13B

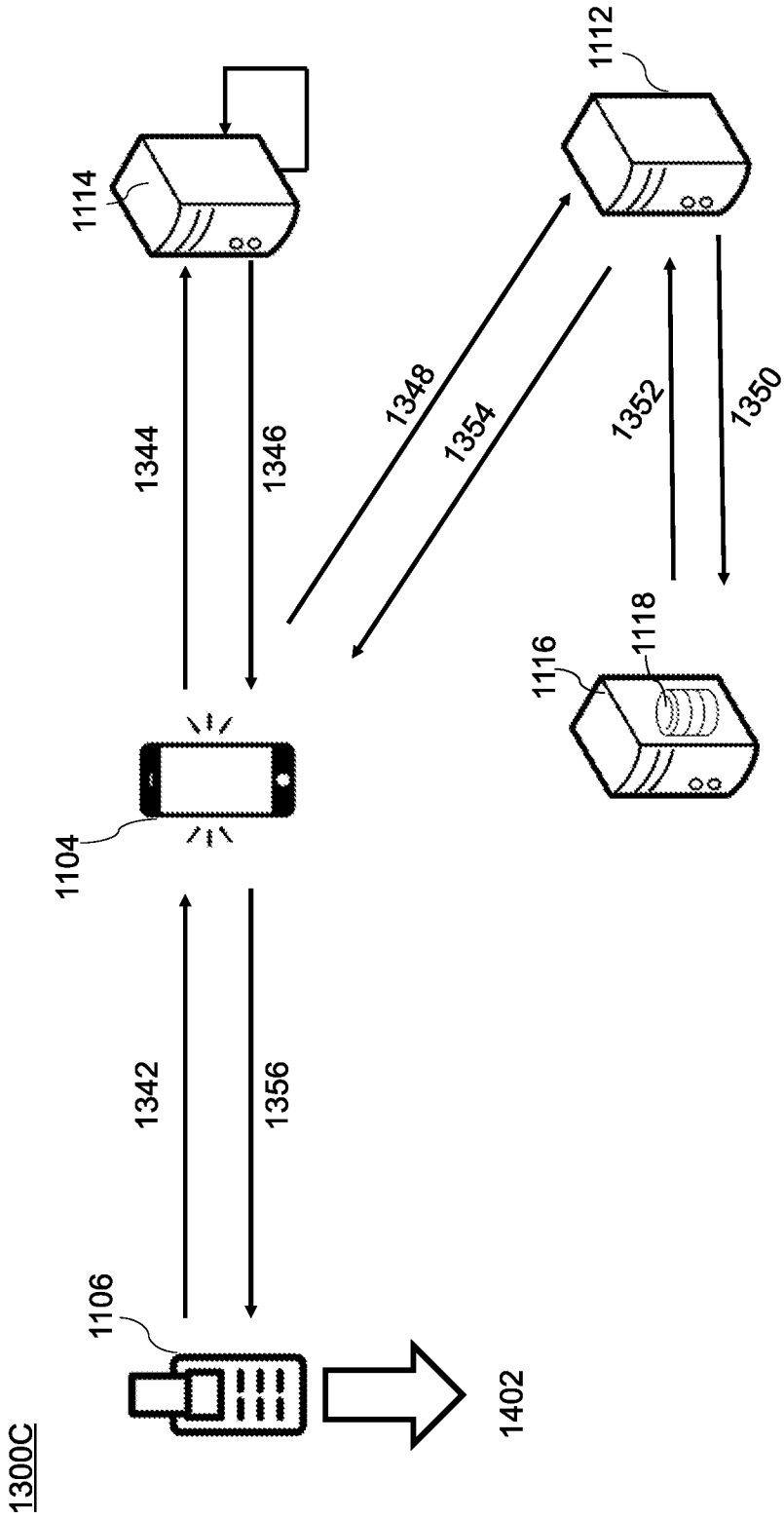

1300C
1106
1342
1356
1402
1104
1344
1346
1114
1348
1354
1112
1352
1350
1116
1118

FIG. 13C

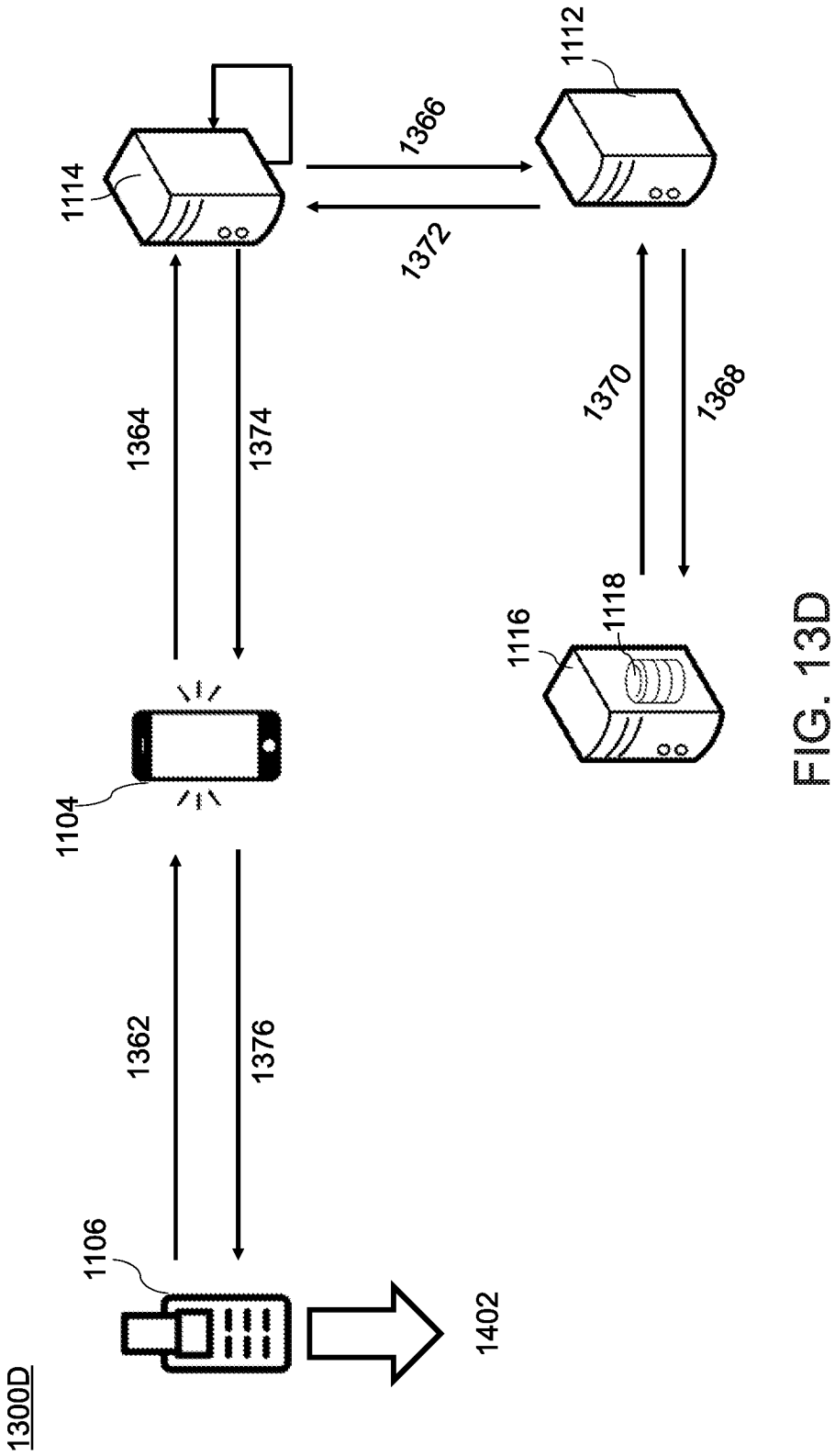

1300D
1106
1402
1362
1376
1104
1364
1374
1114
1366
1372
1112
1370
1368
1116
1118

FIG. 13D

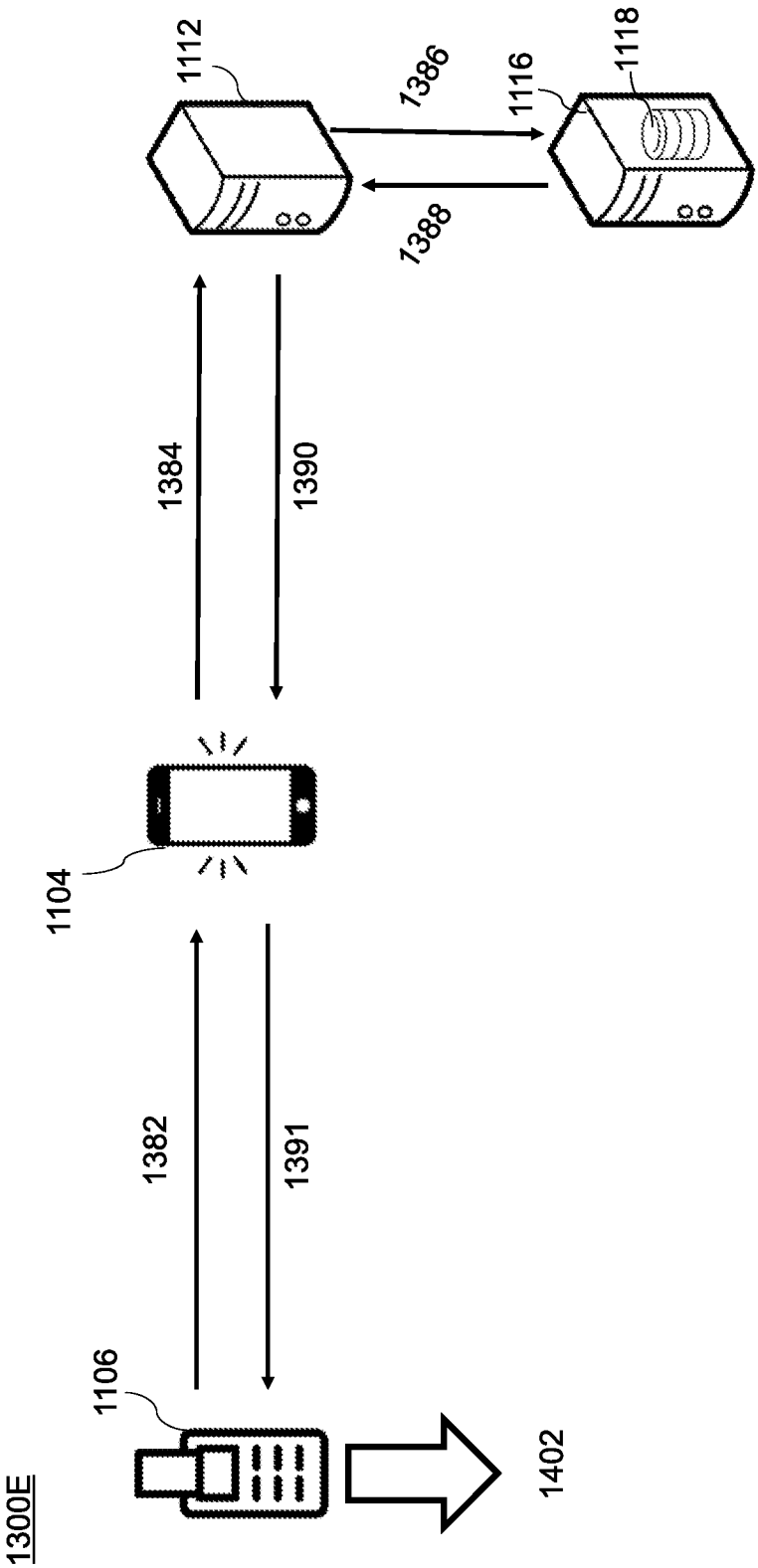

1300E
1106
1402
1382
1391
1104
1384
1390
1112
1386
1116
1118
1388

FIG. 13E

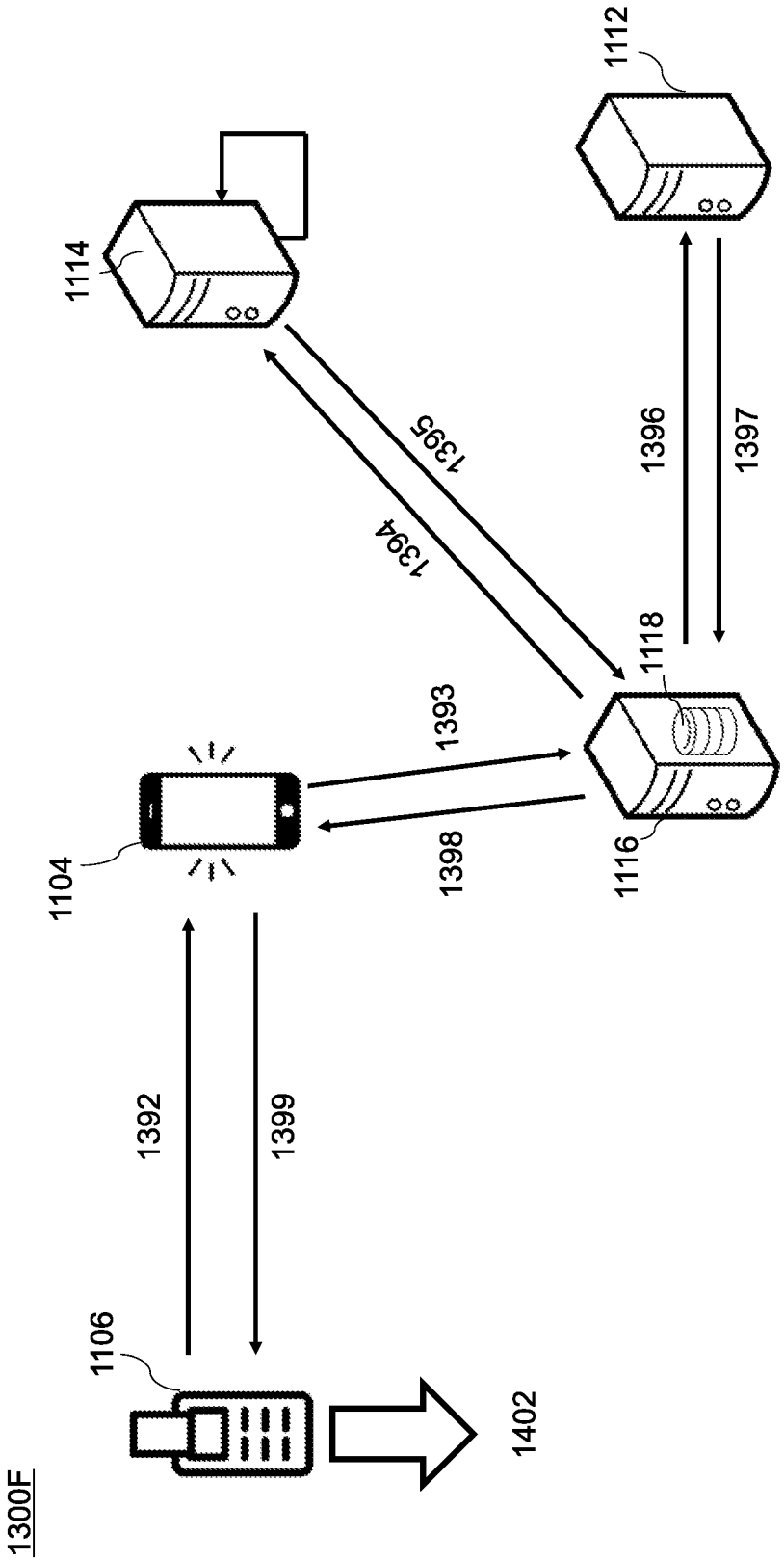

1300F
1106
1402
1392
1399
1104
1393
1398
1116
1118
1394
1395
1396
1397
1114
1112

FIG. 13F

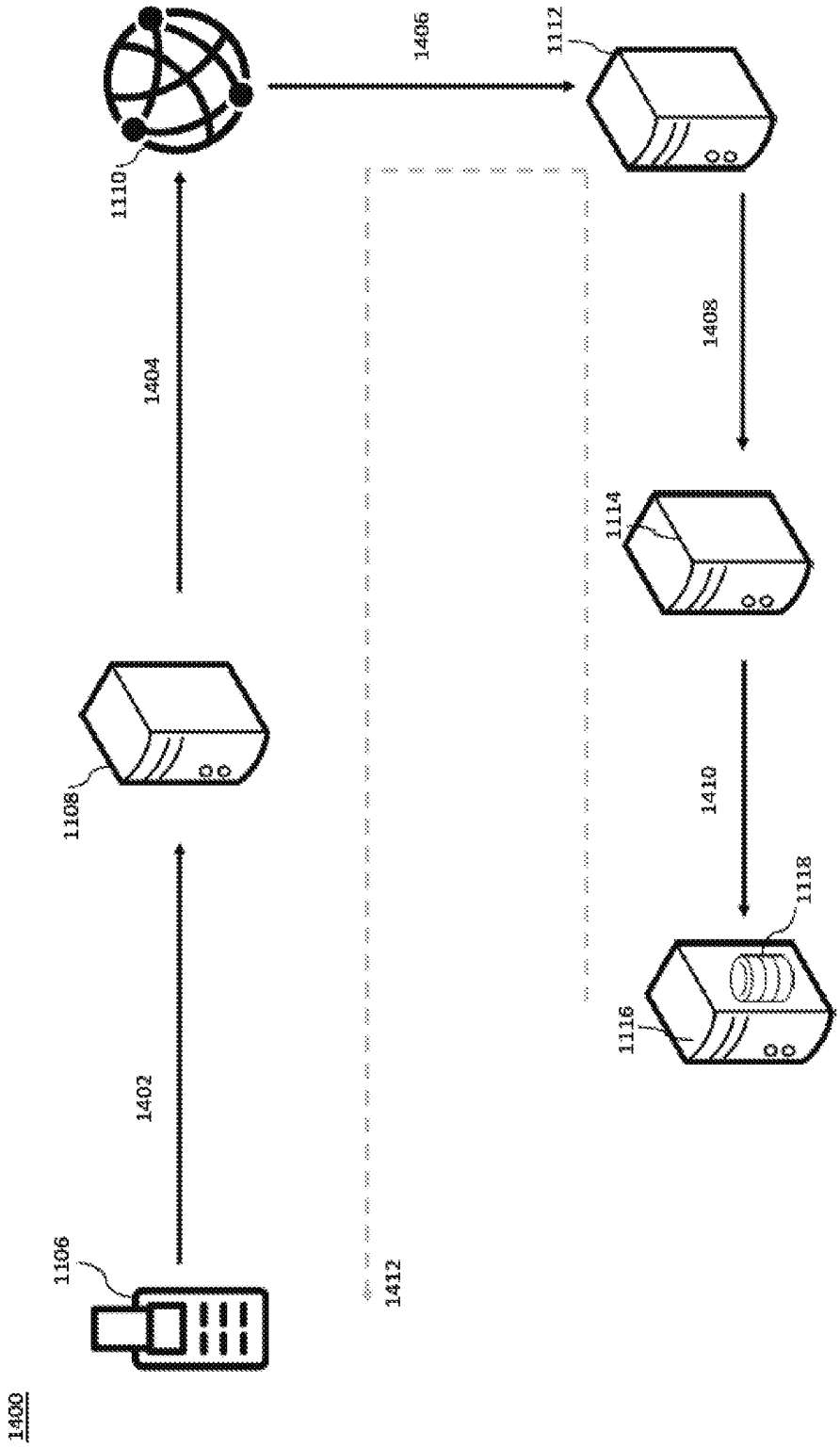

1400
1106
1402
1108
1404
1110
1406
1112
1408
1114
1410
1116
1118
1412

FIG. 14

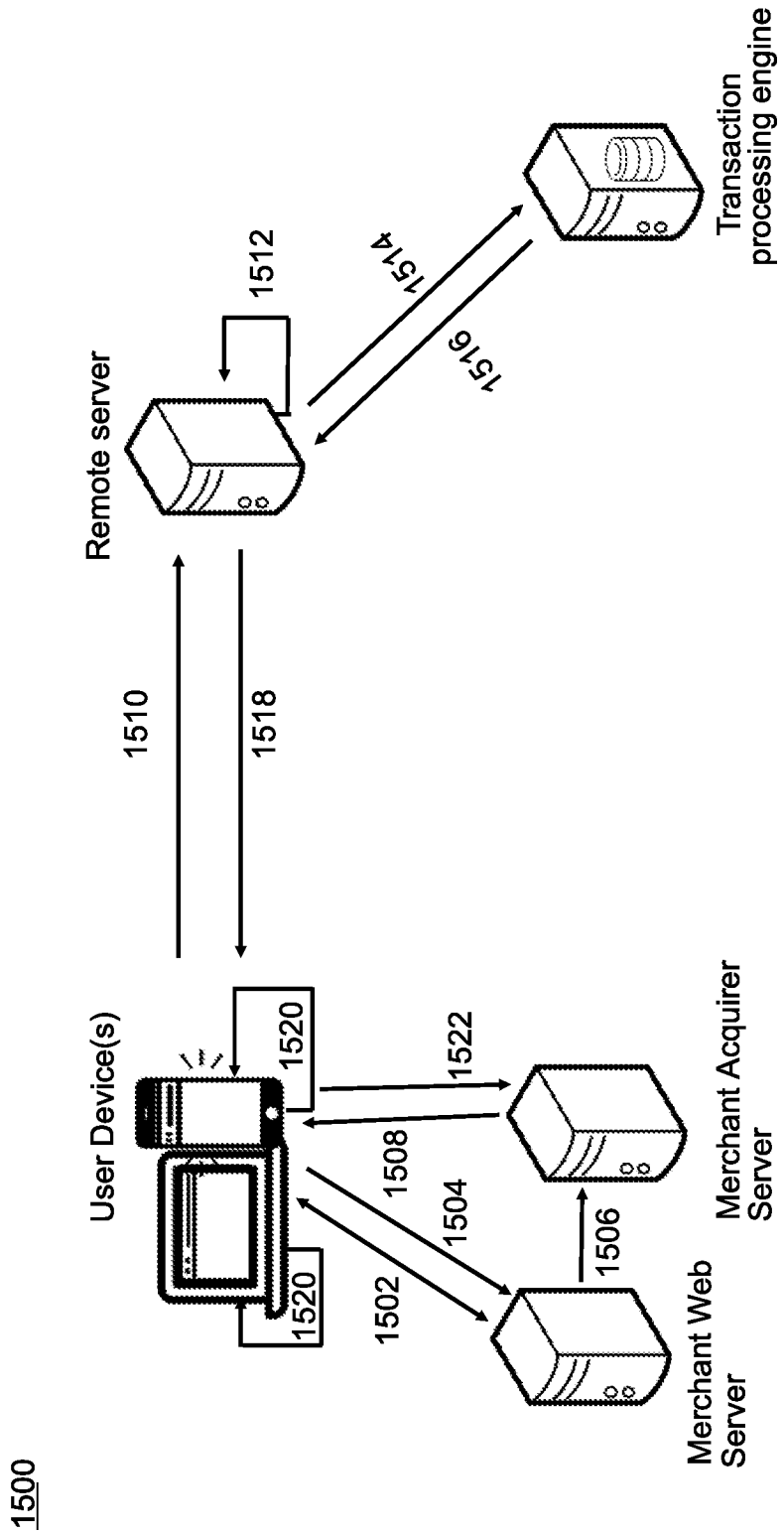

1500
User Device(s)
1520
1520
1502
1504
1506
1508
Merchant Web Server
Merchant Acquirer Server
1522
1510
1518
Remote server
1512
1514
1516
Transaction processing engine

FIG. 15

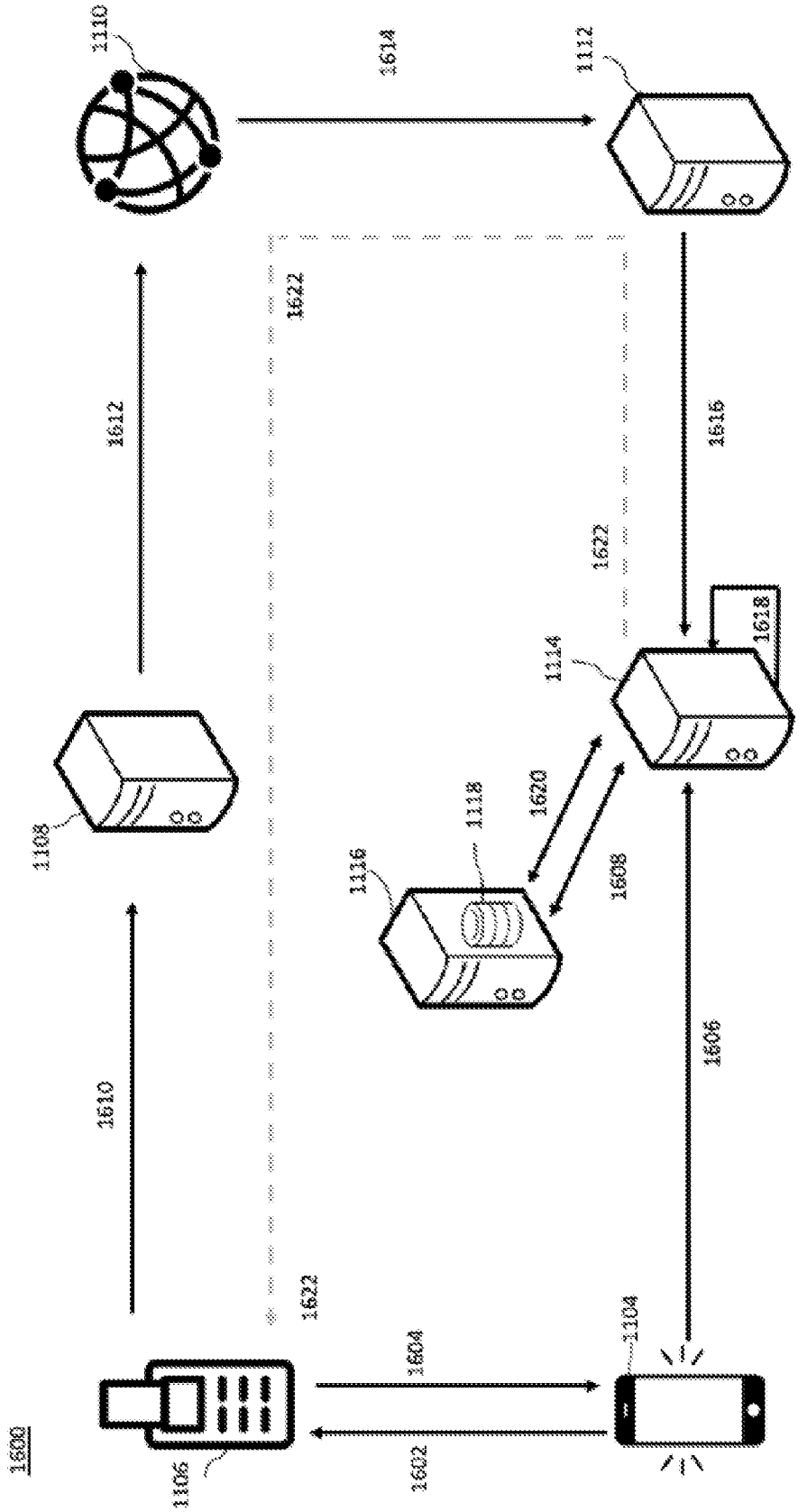

1600
1602
1604
1606
1608
1610
1612
1614
1616
1618
1620
1622
1622
1622
1102
1104
1106
1108
1110
1112
1114
1116
1118

FIG. 16