May 2022

SYSTEM AND METHOD FOR TELEPHONIC PAYMENT CREDENTIAL COLLECTION

PATRICK FLANAGAN
Visa

VANESSA MAREN
Visa

TITLE: "SYSTEM AND METHOD FOR TELEPHONIC PAYMENT CREDENTIAL COLLECTION"

VISA

PATRICK FLANAGAN
VANESSA MAREN

TECHNICAL FIELD

[0001] The present disclosure relates to a system and a method for conducting network transactions. More particularly, the present disclosure relates to systems for authenticating and conducting business over data networks (such as the Internet) using a personal identifier such as a biometric.

BACKGROUND

[0002] The network transaction is a payment method in which the transfer of fund or money happens online over electronic fund transfer.

[0003] The network Authentication of a user and his credentials is the first line of defense. User authentication involves confirming the identity of a user and validating that a user is trusted and can use an electronic resource based on his credentials.

[0004] Consider a scenario where the user may communicate with the client for making and confirming the payment. The communication device associated with the user can interact with a client device over a communication network to initiate a transaction. For example, the user initiates a telephonic connection to the client device to initiate the transaction. In such cases, the user may orally provide the details relating to the payment device such as primary account number, expiration date, CVV field and so on, to the operator interacting with the client device. Further the operator may manually input the credentials to an application executing on the client device. Finally, the transaction is executed or completed. In such situations, the operator may incorrectly input credential data on the application executing on the client device or the operator may incorrectly hear a digit provided by the user which leads to an unsuccessful transaction and multiple attempts to execute the transaction, which causes lower computing network efficiency. To summarize, manual transcription by human operators is error prone causing billing mistakes and long phone calls to collect payment. Businesses and consumers still choose to pay by phone as billing details are best discussed/negotiated by humans. However, when it comes to taking the payment, the payee or payor prefer to conclude the payment

at the earliest, which might involve passing credentials over the phone, which is unsafe and also might be error prone.

[0005] Thus, there is a need for an efficient system and method to overcome such manual faults performed by the humans during the network transactions.

SUMMARY

[0006] According to some non-limiting embodiments, the present disclosure relates to a system and method for collecting the telephonic payment credential. The method of the present disclosure includes receiving, by a client device, a request to establish a connection with a communication device associated with a user. The connection can facilitate audio communication between the client device and the communication device. The method can also include establishing, by the client device, the connection with the communication device for initiation of a transaction with the user. The method can also include initiating, by the client device, an automated payment collection assistant (APCA) application executing on a server computer to be added to the connection between the client device and the communication device and after the first user of the communication device and a second user associated with the client device are in an oral conversation.

[0007] In the present disclosure, the APCA application can be configured to provide, for each field of a series of fields for a payment device, an audio prompt specifying each field of the series of fields for the payment device to the communication device. The APCA application can also be configured to detect, for each field of the series of fields for the payment device, an audio response provided by the communication device. The APCA application can also be configured to translate the audio responses for each field into a text-based series of fields for the payment device using a speech to text process. The APCA application can also be configured to authenticate the audio responses by comparing each audio response with a set of stored biometric voice data previously provided by the user.

[0008] The method can also include forwarding data relating to the transaction and the text-based series of fields for the payment device to a processing network configured to route the data

relating to the transaction and the text-based series of fields to an authorizing entity computer. The method can also include, responsive to obtaining an authorization response message from the authorizing entity computer, transmitting, by the client device, a message to the communication device indicating that the transaction is successful.

BRIEF DESCRIPTION OF THE DRAWINGS AND APPENDICES

[0009] Additional advantages and details of non-limiting embodiments are explained in greater detail below with reference to the exemplary embodiments that are illustrated in the accompanying schematic figures, in which:

[0010] FIG. 1 is a flow diagram for initiating a transaction using an automated and secure credential process according to an embodiment of the invention.

[0011] FIG. 2 is a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

DESCRIPTION OF THE DISCLOSURE

[0012] In the present document, the word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment or implementation of the present subject matter described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments.

[0013] While the disclosure is susceptible to various modifications and alternative forms, specific embodiment thereof has been shown by way of example in the drawings and will be described in detail below. It should be understood, however that it is not intended to limit the disclosure to the particular forms disclosed, but on the contrary, the disclosure is to cover all modifications, equivalents, and alternative falling within the spirit and the scope of the disclosure.

[0014] The terms “comprises”, “comprising”, or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a setup, device or method that comprises a list of components or steps does not include only those components or steps but may include other components or steps not expressly listed or inherent to such setup or device or method. In other words, one or more elements in a device or system or apparatus proceeded by “comprises… a” does not, without more constraints, preclude the existence of other elements or additional elements in the device or system or apparatus.

[0015] The terms "an embodiment", "embodiment", "embodiments", "the embodiment", "the embodiments", "one or more embodiments", "some embodiments", and "one embodiment" mean "one or more (but not all) embodiments of the invention(s)" unless expressly specified otherwise.

[0016] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to", unless expressly specified otherwise.

[0017] As used herein, the terms “communication” and “communicate” may refer to the reception, receipt, transmission, transfer, provision, and/or the like of information (e.g., data, signals, messages, instructions, commands, and/or the like). For one unit (e.g., a device, a system, a component of a device or system, combinations thereof, and/or the like) to be in communication with another unit means that the one unit is able to directly or indirectly receive information from and/or transmit information to the other unit. This may refer to a direct or indirect connection (e.g., a direct communication connection, an indirect communication connection, and/or the like) that is wired and/or wireless in nature. Additionally, two units may be in communication with each other even though the information transmitted may be modified, processed, relayed, and/or routed between the first and second unit. For example, a first unit may be in communication with a second unit even though the first unit passively receives information and does not actively transmit information to the second unit. As another example, a first unit may be in communication with a second unit if at least one intermediary unit (e.g., a third unit located between the first unit and the second unit) processes information received from the first unit and

communicates the processed information to the second unit. In some non-limiting embodiments, a message may refer to a network packet (e.g., a data packet and/or the like) that includes data. It will be appreciated that numerous other arrangements are possible.

[0018] A "communication device" may include any suitable device that can allow for communication with an external entity. A communication device may be a mobile device if the mobile device has the ability to communicate data to and from an external entity.

[0019] A “mobile device” may comprise any suitable electronic device that may be transported and operated by a user, which may also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network (e.g. 3G, 4G or similar networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network. Examples of mobile devices include mobile phones (e.g. cellular phones), PDAs, tablet computers, net books, laptop computers, personal music players, hand-held specialized readers, etc. Further examples of mobile devices include wearable devices, such as smart watches, fitness bands, ankle bracelets, rings, earrings, etc., as well as automobiles with remote communication capabilities. A mobile device may comprise any suitable hardware and software for performing such functions, and may also include multiple devices or components (e.g. when a device has remote access to a network by tethering to another device - i.e. using the other device as a modem – both devices taken together may be considered a single mobile device).

[0020] A “payment device” may include any suitable device that may be used to conduct a financial transaction, such as to provide payment credentials to a merchant. The payment device may be a software object, a hardware object, or a physical object. As examples of physical objects, the payment device may comprise a substrate such as a paper or plastic card, and information that is printed, embossed, encoded, or otherwise included at or near a surface of an object. A hardware object can relate to circuitry (e.g., permanent voltage values), and a software object can relate to non-permanent data stored on a device. A payment device may be associated with a value such as a monetary value, a discount, or

store credit, and a payment device may be associated with an entity such as a bank, a merchant, a payment processing network, or a person. A payment device may be used to make a payment transaction. Suitable payment devices can be hand-held and compact so that they can fit into a user's wallet and/or pocket (e.g., pocket-sized). Example payment devices may include smart cards, magnetic stripe cards, keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of mobile devices include pagers, payment cards, security cards, access cards, smart media, transponders, and the like. If the payment device is in the form of a debit, credit, or smartcard, the payment device may also optionally have features such as magnetic stripes. Such devices can operate in either a contact or contactless mode. In some embodiments, a mobile device can function as a payment device (e.g., a mobile device can store and be able to transmit payment credentials for a transaction).

[0021] A "credential" may be any suitable information that serves as reliable evidence of worth, ownership, identity, or authority. A credential may be a string of numbers, letters, or any other suitable characters, as well as any object or document that can serve as confirmation. Examples of credentials include value credentials, identification cards, certified documents, access cards, passcodes and other login information, etc.

[0022] A **"**value credential" may be information associated with worth. Examples of value credentials include payment credentials, coupon identifiers, information needed to obtain a promotional offer, etc.

[0023] "Payment credentials" may include any suitable information associated with an account (e.g. a payment account and/or payment device associated with the account). Such information may be directly related to the account or may be derived from information related to the account. Examples of account information may include a PAN (primary account number or "account number"), user name, expiration date, CVV (card verification value), dCVV (dynamic card verification value), CVV2 (card verification value 2), CVC3 card verification values, etc. CVV2 is generally understood to be a static verification value associated with a payment device. CVV2 values are generally visible to a user (e.g., a consumer), whereas CVV and dCVV values are typically embedded in memory or

authorization request messages and are not readily known to the user (although they are known to the issuer and payment processors). Payment credentials may be any information that identifies or is associated with a payment account. Payment credentials may be provided in order to make a payment from a payment account. Payment credentials can also include a user name, an expiration date, a gift card number or code, and any other suitable information.

[0024] An "application" may be computer code or other data stored on a computer readable medium (e.g. memory element or secure element) that may be executable by a processor to complete a task.

[0025] A "digital wallet" can include an electronic device that allows an individual to conduct electronic commerce transactions. A digital wallet may store user profile information, payment credentials, bank account information, one or more digital wallet identifiers and/or the like and can be used in a variety of transactions, such as but not limited to eCommerce, social networks, money transfer/ personal payments, mobile commerce, proximity payments, gaming, and/or the like for retail purchases, digital goods purchases, utility payments, purchasing games or gaming credits from gaming websites, transferring funds between users, and/or the like. A digital wallet may be designed to streamline the purchase and payment process. A digital wallet may allow the user to load one or more payment cards onto the digital wallet so as to make a payment without having to enter an account number or present a physical card.

[0026] A "digital wallet provider" may include an entity, such as an issuing bank or third party service provider, that issues a digital wallet to a user that enables the user to conduct financial transactions. A digital wallet provider may provide standalone user-facing software applications that store account numbers, or representations of the account numbers (e.g., payment tokens), on behalf of a cardholder (or other user) to facilitate payments at more than one unrelated merchant, perform person-to-person payments, or load financial value into the digital wallet. A digital wallet provider may enable a user to access its account via a personal computer, mobile device or access device. Additionally, a digital wallet provider may also provide one or more of the following functions: storing

multiple payment cards and other payment products on behalf of a user, storing other information including billing address, shipping addresses, and transaction history, initiating a transaction by one or more methods, such as providing a user name and password, NFC or a physical token, and may facilitate pass-through or two-step transactions.

[0027] A "token" may be a substitute value for a credential. A token may be a string of numbers, letters, or any other suitable characters. Examples of tokens include payment tokens, access tokens, personal identification tokens, etc.

[0028] A "payment token" may include an identifier for a payment account that is a substitute for an account identifier, such as a primary account number (PAN). For example, a token may include a series of alphanumeric characters that may be used as a substitute for an original account identifier. For example, a token "4900 0000 0000 0001" may be used in place of a PAN "4147 0900 0000 1234." In some embodiments, a token may be "format preserving" and may have a numeric format that conforms to the account identifiers used in existing transaction processing networks (e.g., International Organization for Standardization (ISO) 8583 financial transaction message format). In some embodiments, a token may be used in place of a PAN to initiate, authorize, settle or resolve a payment transaction or represent the original credential in other systems where the original credential would typically be provided. In some embodiments, a token value may be generated such that the recovery of the original PAN or other account identifier from the token value may not be computationally derived. Further, in some embodiments, the token format may be configured to allow the entity receiving the token to identify it as a token and recognize the entity that issued the token.

[0029] "Tokenization" is a process by which data is replaced with substitute data. For example, a payment account identifier (e.g., a primary account number (PAN)) may be tokenized by replacing the primary account identifier with a substitute number (e.g. a token) that may be associated with the payment account identifier. Further, tokenization may be applied to any other information that may be replaced with a substitute value (i.e., token).

Tokenization may be used to enhance transaction efficiency, improve transaction security, increase service transparency, or to provide a method for third-party enablement.

[0030] [0001] A "token provider" or "token service system" can include a system that services payment tokens. In some embodiments, a token service system can facilitate requesting, determining (e.g., generating) and/or issuing tokens, as well as maintaining an established mapping of tokens to primary account numbers (PANs) in a repository (e.g. token vault). In some embodiments, the token service system may establish a token assurance level for a given token to indicate the confidence level of the token to PAN binding. The token service system may include or be in communication with a token vault where the generated tokens are stored. The token service system may support token processing of payment transactions submitted using tokens by de-tokenizing the token to obtain the actual PAN. In some embodiments, a token service system may include a tokenization computer alone, or in combination with other computers such as a transaction processing network computer. Various entities of a tokenization ecosystem may assume the roles of the token service provider. For example, payment networks and issuers or their agents may become the token service provider by implementing the token services according to embodiments of the present invention.

[0031] [0002] A "token domain" may indicate an area and/or circumstance in which a token can be used. Examples of the token domain may include, but are not limited to, payment channels (e.g., e-commerce, physical point of sale, etc.), POS entry modes (e.g., contactless, magnetic stripe, etc.), and merchant identifiers to uniquely identify where the token can be used. A set of parameters (i.e. token domain restriction controls) may be established as part of token issuance by the token service provider that may allow for enforcing appropriate usage of the token in payment transactions. For example, the token domain restriction controls may restrict the use of the token with particular presentment modes, such as contactless or e-commerce presentment modes. In some embodiments, the token domain restriction controls may restrict the use of the token at a particular merchant that can be uniquely identified. Some exemplary token domain restriction controls may require the verification of the presence of a token cryptogram that is unique to a given

transaction. In some embodiments, a token domain can be associated with a token requestor.

[0032] [0003] "Token expiry date" may refer to the expiration date/time of the token. The token expiry date may be passed among the entities of the tokenization ecosystem during transaction processing to ensure interoperability. The token expiration date may be a numeric value (e.g. a 4-digit numeric value). In some embodiments, the token expiry date can be expressed as a time duration as measured from the time of issuance.

[0033] A "token request message" may be an electronic message for requesting a token. A token request message may include information usable for identifying a payment account or digital wallet, and/or information for generating a payment token. For example, a token request message may include payment credentials, mobile device identification information (e.g. a phone number or MSISDN), a digital wallet identifier, information identifying a tokenization service provider, a merchant identifier, a cryptogram, and/or any other suitable information. Information included in a token request message can be encrypted (e.g., with an issuer-specific key).

[0034] A "token response message" may be a message that responds to a token request. A token response message may include an indication that a token request was approved or denied. A token response message may also include a payment token, mobile device identification information (e.g. a phone number or MSISDN), a digital wallet identifier, information identifying a tokenization service provider, a merchant identifier, a cryptogram, and/or any other suitable information. Information included in a token response message can be encrypted (e.g., with an issuer-specific key).

[0035] A "user" may include an individual. In some embodiments, a user may be associated with one or more personal accounts and/or mobile devices. The user may also be referred to as a cardholder, account holder, or consumer.

[0036] A "resource provider" may be an entity that can provide a resource such as goods, services, information, and/or access. Examples of resource providers include merchants, access devices, secure data access points, etc. A "merchant" may typically be an entity that

engages in transactions and can sell goods or services, or provide access to goods or services.

[0037] An "acquirer" may typically be a business entity (e.g., a commercial bank) that has a business relationship with a particular merchant or other entity. Some entities can perform both issuer and acquirer functions. Some embodiments may encompass such single entity issuer-acquirers. An acquirer may operate an acquirer computer, which can also be generically referred to as a "transport computer".

[0038] An "authorizing entity" may be an entity that authorizes a request. Examples of an authorizing entity may be an issuer, a governmental agency, a document repository, an access administrator, etc. An "issuer" may typically refer to a business entity (e.g., a bank) that maintains an account for a user. An issuer may also issue payment credentials stored on a user device (or "communication device"), such as a cellular telephone, smart card, tablet, or laptop to the consumer.

[0039] An "access device" may be any suitable device that provides access to a remote system. An access device may also be used for communicating with a merchant computer, a transaction processing computer, an authentication computer, or any other suitable system. An access device may generally be located in any suitable location, such as at the location of a merchant. An access device may be in any suitable form. Some examples of access devices include POS or point of sale devices (e.g., POS terminals), cellular phones, PDAs, personal computers (PCs), tablet PCs, hand-held specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like. An access device may use any suitable contact or contactless mode of operation to send or receive data from, or associated with, a user mobile device. In some embodiments, where an access device may comprise a POS terminal, any suitable POS terminal may be used and may include a reader, a processor, and a computer-readable medium. A reader may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include radio frequency (RF) antennas, optical scanners, bar code readers, or magnetic stripe readers to interact with a payment device and/or mobile device. In some embodiments, a cellular

phone, tablet, or other dedicated wireless device used as a POS terminal may be referred to as a mobile point of sale or an "mPOS" terminal.

[0040] An "authorization request message" may be an electronic message that requests authorization for a transaction. In some embodiments, it is sent to a transaction processing computer and/or an issuer of a payment card to request authorization for a transaction. An authorization request message according to some embodiments may comply with ISO 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a user using a payment device or payment account. The authorization request message may include an issuer account identifier that may be associated with a payment device or payment account. An authorization request message may also comprise additional data elements corresponding to "identification information" including, by way of example only: a service code, a CVV (card verification value), a dCVV (dynamic card verification value), a PAN (primary account number or "account number"), a payment token, a user name, an expiration date, etc. An authorization request message may also comprise "transaction information," such as any information associated with a current transaction, such as the transaction amount, merchant identifier, merchant location, acquirer bank identification number (BIN), card acceptor ID, information identifying items being purchased, etc., as well as any other information that may be utilized in determining whether to identify and/or authorize a transaction.

[0041] An "authorization response message" may be a message that responds to an authorization request. In some cases, it may be an electronic message reply to an authorization request message generated by an issuing financial institution or a transaction processing computer. The authorization response message may include, by way of example only, one or more of the following status indicators: Approval -- transaction was approved; Decline -- transaction was not approved; or Call Center -- response pending more information, merchant calls the toll-free authorization phone number. The authorization response message may also include an authorization code, which may be a code that a credit card issuing bank returns in response to an authorization request message in an electronic message (either directly or through the transaction processing computer) to the merchant's access device (e.g. POS equipment) that indicates approval of the transaction. The code

may serve as proof of authorization. As noted above, in some embodiments, a transaction processing computer may generate or forward the authorization response message to the merchant.

[0042] A "server computer" may include a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The server computer may be coupled to a database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers. The server computer may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers.

[0043] An "automated payment collection assistant (APCA)" can include an application/service executing on a computing device configured to prompt a speech input from a user providing payment device details (e.g., payment credentials), convert the speech input into text-based fields, and authenticate the speech input. The APCA can join an interaction (e.g., a phone or voice over IP (VoIP) call) between a communication device and a client device and obtain the payment device details audibly from the user. Responsive to authenticating the speech of the user (e.g., by comparing the speech input with a stored voice print of the user), a text-based version of the payment device details can be provided to a processing network for authentication of a transaction using the payment device details.

[0044] The present embodiments relate to automated and secure credential acquisition and voice verification. When a user, via a communication device, interacts with a client (e.g., a resource provider) via a communication network, an automated payment collection assistant (APCA) can be joined to a call/messaging session between the user and client to obtain payment credentials from the user.

[0045] For instance, the APCA can prompt the user for payment device fields (e.g., PAN, expiration date, CVV, zip) and the user can verbally provide responses (e.g., in multi-digit fields). The APCA can perform a speech to text process to translate the verbal input into

text-based fields that can be used in a subsequent transaction. Further, the speech input provided by the input can be compared with stored speech data (e.g., a voice print) of the user to determine whether the speech input corresponds with the stored speech data.

[0046] Responsive to authenticating the speech input, the transaction can be initiated using the obtained payment credentials using a card not present (CNP) authentication procedure. For instance, the transaction data can be forwarded to an issuer via a processing network. Responsive to initiation of the transaction, a payment success message can be forwarded to the communication device (e.g., via a SMS message).

[0047] The present disclosure overcomes the errors occurred during the manual transcription performed by the human operators. The present disclosure also reduces the time and enhances the speed for the transaction process between the client and the user. Also, the present disclosure ensures authentication of the user in a secure manner for a secure transaction.

[0048] FIG. 1 is a flow diagram for initiating a transaction using an automated and secure credential acquisition process. As shown in FIG. 1, a system for initiating a transaction using an automated and secure credential acquisition process can include a user mobile device 101 (hereinafter referred to as communication device 101) (e.g., a mobile phone), a client device (e.g., a computing device associated with a resource provider), and an APCA application executing on a server computer. The communication device 101, client device, and APCA application 102 can communicate via one or more communication networks (e.g., a cellular network, the Internet).

[0049] At S105, the communication device 101 associated with the user can initiate or receive a call to the client device. This can include dialing a customer service phone number for the client or selecting a link to establish a connection to the client device (e.g., via the internet).

[0050] At S110, a call can be inbound to client device via a communication channel. This can include inbounding a telephone call (or an internet-enabled connection) to the client device.

[0051] At S115, a connection can be established between client device and communication device 101. In some instances, prior to establishing the connection to the client device, an automated data retrieval service can obtain account details relating to the user (e.g., a username, phone number associated with the user).

[0052] At S120, during a conversation between the user and the resource provider, a request to initiate a transaction (or to make a payment) can be made. For instance, the client can specify a payment amount for the user to provide to the client. The request can be made during an oral conversation between a first user of the communication device 101 and a second user associated with the client device.

[0053] At S125, the user and client can agree to begin collecting payment details for the user. This can include a request for data relating to a payment device (e.g., credit card, debit card), such as a primary account number (PAN), expiration date, CVV, zip code, etc.

[0054] [0004] At S130, the APCA 102 can join the call between the user and client. The APCA 102 can be dialed into the call between the user and client as a conference call. For instance, the client can call a specific conference number and a code to instruct the APCA 102 to join the call. In some instances, the APCA 102 can automatically join the call between the user and client responsive to a triggering event (e.g., a detection that payment device details are about to be provided by the user).

[0055] At S135, the APCA 102 can provide a request for payment amount confirmation from the user. For instance, the APCA 102 can provide an audio prompt for the user to audibly provide payment device details.

[0056] At S140, the APCA 102 can prompt for payment device details, such as a PAN, expiration data, CVV, ZIP, etc. The APCA 102 can prompt for each field and subsequently provide time for the user to provide corresponding data (e.g., by audibly providing a series of digits).

[0057] At S145, the user can provide an audible (e.g., speech) response to provide the fields prompted by the APCA 102.

[0058] In some instances, at S150, the APCA 102 can request an invoice number verbally. One or more invoice numbers can be associated with the transaction to track the completion of payment for various invoices relating to the user.

[0059] At S155, the APCA 102 can process and confirm responses provided by the user using a speech to text process. For instance, each field can be populated using digits provided by the user in a text form by translating audible responses by the user into a text-based field.

[0060] At S160, the user, via the communication device 101, can provide enrollment data. The enrollment data can enroll a phone number (or other identifier, such as an email address or username) and a payment device with a voice print. The voice print can include a user providing an audio input providing the speech of the user (e.g., by the user following a script). The voice print can include a biometric sample uniquely identifying the voice of the user. The enrollment data can be provided by the user at any point in time (e.g., prior to providing the payment device details). In some instances, the enrollment data can be dynamically generated based on previous interactions with the user and recording user speech during the previous interactions.

[0061] At S165, the user can provide the enrollment data to be compared with the input speech providing the payment device details.

[0062] At S170, the APCA 102 can analyze responses by performing a speaker verification process. The verification process can include comparing speech input by user and stored speech (e.g., the voice print) to determine a similarity between the speech and the voice print. This can include comparing a known portion of stored speech (e.g., a voice input of a first digit) provided in the voice print with a similar portion of the speech input provided by the user. A similarity metric or score can be generated indicative of a similarity between the voice input provided by the user and the voice print included in the enrollment data. The user can be verified responsive to the similarity metric/score exceeding a threshold score/metric. In some other embodiments of the present disclosure, the APCA 102 may authenticate the user by sending a One Time Password (OTP) to the communication device 101 and further the user may prove to be authentic by entering the received OTP.

[0063] At S175, an authorization identifier, a result (e.g., a similarity score, transaction details), a user phone number, and provided payment device details can be provided to issuer. The issuer can authorize the transaction using the transaction details. The data can be provided to the issuer via a processing network and/or a card not present (CNP) gateway.

[0064] At S180, a CNP gateway can perform a CNP authorization process with the processing network. The CNP authorization process can include routing transaction details across a processing network to authenticate the transaction.

[0065] At S185, a CNP authorization process can be performed with the CNP gateway to execute the transaction. The CNP authorization process can include verifying the transaction details provided by the client device and the APCA 102.

[0066] At S190, the client device can identify that the transaction is complete.

[0067] At S195, the client device can send an SMS message to the user via an SMS interface at the client device.

[0068] At S200, the client device can send a SMS message to an SMS application on the communication device 101.

[0069] In some instances, a method for telephonic payment credential collection is provided. The method can include receiving a request to establish a connection with a communication device 101 associated with a user. The connection can facilitate audio communication (e.g., a phone call, a VoIP call) between the client device and the communication device 101. The client device can establish the connection with the communication device 101 for initiation of a transaction with the user. For instance, the user, via communication device 101, can contact the client device to provide a payment to the client device.

[0070] The client device can initiate an automated payment collection assistant (APCA) application 102 executing on a server computer to be added to the connection between the client device and the communication device 101. For instance, the client device can dial a conference number and a specific code to instruct the APCA 102 to join a call between the

client device and communication device 101. The APCA 102 can prompt the user for payment device details and authenticate the speech of the user.

[0071] The APCA 102 can provide, for each field of a series of fields for a payment device, an audio prompt specifying each field of the series of fields for the payment device to the communication device 101. The series of fields can include details relating to a payment device, such as a PAN, an expiration date, a CVV, a zip code, etc. The audio prompt can include an instruction to provide a specific payment device detail (e.g., the PAN).

[0072] The APCA 102 can detect, for each field of the series of fields for the payment device, an audio response provided by the communication device 101. For instance, after providing a given prompt, the APCA 102 can record a voice response by the user providing a series of digits for a payment device field.

[0073] The APCA 102 can translate the audio responses for each field into a text-based series of fields for the payment device using a speech to text process. For instance, each field can be populated into a text-based series of fields specifying details of the payment device.

[0074] The APCA 102 can authenticate the audio responses by comparing each audio response with a set of stored biometric voice data previously provided by the user. For instance, this can include deriving a similarity score based on a similarity between each audio response and the set of stored biometric voice data previously provided by the user. This can also include determining whether the similarity score exceeds a threshold score. The audio responses can be authenticated responsive to determining that the similarity score exceeding a threshold score.

[0075] Data relating to the transaction (e.g., transaction amount, invoice number, resource provider identifier) and the text-based series of fields for the payment device can be forwarded to a processing network configured to route the data relating to the transaction and the text-based series of fields to an authorizing entity computer. This can include forwarding the details to an issuer via a CNP authorization procedure.

[0076] Responsive to obtaining an authorization response message from the authorizing entity computer (indicating that a transaction is successful), a message can be transmitted to the communication device 101 indicating that the transaction is successful.

[0077] FIG. 2 is a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[0078] In some embodiments, FIG. 2 illustrates a block diagram of an exemplary computer system 200 for implementing embodiments consistent with the present disclosure. In some embodiments, the computer system 200 may be an APCA 102 to collect telephonic payment credential. The processor 202 may include at least one data processor for executing program components for executing user or system-generated business processes. A user may include a person, a person using a device such as those included in this disclosure, or such a device itself. The processor 202 may include specialized processing units such as integrated system (bus) controllers, memory management control units, floating point units, graphics processing units, digital signal processing units, etc.

[0079] The processor 202 may be disposed in communication with input devices 311 and output devices 212 via I/O interface 201. The I/O interface 201 may employ communication protocols/methods such as, without limitation, audio, analog, digital, stereo, IEEE-1393, serial bus, Universal Serial Bus (USB), infrared, PS/2, BNC, coaxial, component, composite, Digital Visual Interface (DVI), high-definition multimedia interface (HDMI), Radio Frequency (RF) antennas, S-Video, Video Graphics Array (VGA), IEEE 802.n /b/g/n/x, Bluetooth, cellular (e.g., Code-Division Multiple Access (CDMA), High-Speed Packet Access (HSPA+), Global System For Mobile Communications (GSM), Long-Term Evolution (LTE), WiMax, or the like), etc.

[0080] Using the I/O interface 201, the computer system 200 may communicate with the input devices 211 and the output devices 212.

[0081] In some embodiments, the processor 202 may be disposed in communication with a communication network 209 via a network interface 203. The network interface 203 may communicate with the communication network 209. The network interface 203 may

employ connection protocols including, without limitation, direct connect, Ethernet (e.g., twisted pair 10/100/1000 Base T), Transmission Control Protocol/Internet Protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc. Using the network interface 203 and the communication network 209, the computer system 200 may communicate with a user mobile device 101, a client device 213 and a VISA NET 103. The communication network 209 can be implemented as one of the different types of networks, such as intranet or Local Area Network (LAN), Closed Area Network (CAN) and such. The communication network 309 may either be a dedicated network or a shared network, which represents an association of the different types of networks that use a variety of protocols, for example, Hypertext Transfer Protocol (HTTP), CAN Protocol, Transmission Control Protocol/Internet Protocol (TCP/IP), Wireless Application Protocol (WAP), etc., to communicate with each other. Further, the communication network 209 may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, etc. In some embodiments, the processor 302 may be disposed in communication with a memory 205 (e.g., RAM, ROM, etc. not shown in FIG.2) via a storage interface 203. The storage interface 203 may connect to memory 205 including, without limitation, memory drives, removable disc drives, etc., employing connection protocols such as Serial Advanced Technology Attachment (SATA), Integrated Drive Electronics (IDE), IEEE-1393, Universal Serial Bus (USB), fibre channel, Small Computer Systems Interface (SCSI), etc. The memory drives may further include a drum, magnetic disc drive, magneto-optical drive, optical drive, Redundant Array of Independent Discs (RAID), solid-state memory devices, solid-state drives, etc.

[0082] The memory 205 may store a collection of program or database components, including, without limitation, a user interface 206, an operating system 207, a web browser 308 etc. In some embodiments, the computer system 200 may store user/application data, such as the data, variables, records, etc. as described in this disclosure. Such databases may be implemented as fault-tolerant, relational, scalable, secure databases such as Oracle or Sybase.

[0083] The operating system 207 may facilitate resource management and operation of the computer system 200. Examples of operating systems include, without limitation, APPLE®

MACINTOSH® OS X®, UNIX®, UNIX-like system distributions (E.G., BERKELEY SOFTWARE DISTRIBUTION® (BSD), FREEBSD®, NETBSD®, OPENBSD, etc.), LINUX® DISTRIBUTIONS (E.G., RED HAT®, UBUNTU®, KUBUNTU®, etc.), IBM®OS/2®, MICROSOFT® WINDOWS® (XP®, VISTA®/7/8, 10 etc.), APPLE® IOS®, GOOGLE™ ANDROID™, BLACKBERRY® OS, or the like. The User interface 206 may facilitate display, execution, interaction, manipulation, or operation of program components through textual or graphical facilities. For example, user interfaces may provide computer interaction interface elements on a display system operatively connected to the computer system 200, such as cursors, icons, checkboxes, menus, scrollers, windows, widgets, etc. Graphical User Interfaces (GUIs) may be employed, including, without limitation, Apple® Macintosh® operating systems' Aqua®, IBM® OS/2®, Microsoft® Windows® (e.g., Aero, Metro, etc.), web interface libraries (e.g., ActiveX®, Java®, Javascript®, AJAX, HTML, Adobe® Flash®, etc.), or the like.

[0084] In some embodiments, the computer system 200 may implement the web browser 208 stored program components. The web browser 208 may be a hypertext viewing application, such as MICROSOFT® INTERNET EXPLORER®, GOOGLE™ CHROME™, MOZILLA® FIREFOX®, APPLE® SAFARI®, etc. Secure web browsing may be provided using Secure Hypertext Transport Protocol (HTTPS), Secure Sockets Layer (SSL), Transport Layer Security (TLS), etc. Web browsers 308 may utilize facilities such as AJAX, DHTML, ADOBE® FLASH®, JAVASCRIPT®, JAVA®, Application Programming Interfaces (APIs), etc. In some embodiments, the computer system 200 may implement a mail server stored program component. The mail server may be an Internet mail server such as Microsoft Exchange, or the like. The mail server may utilize facilities such as Active Server Pages (ASP), ACTIVEX®, ANSI® C++/C#, MICROSOFT®, .NET, CGI SCRIPTS, JAVA®, JAVASCRIPT®, PERL®, PHP, PYTHON®, WEBOBJECTS®, etc. The mail server may utilize communication protocols such as Internet Message Access Protocol (IMAP), Messaging Application Programming Interface (MAPI), MICROSOFT® exchange, Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), or the like. In some embodiments, the computer system 200 may implement a mail client stored program component. The mail client may be a mail viewing application, such as APPLE®

MAIL, MICROSOFT® ENTOURAGE®, MICROSOFT® OUTLOOK®, MOZILLA® THUNDERBIRD®, etc.

[0085] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer-readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer-readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term "computer-readable medium" should be understood to include tangible items and exclude carrier waves and transient signals, i.e., non-transitory. Examples include Random Access Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, Compact Disc (CD) ROMs, Digital Video Disc (DVDs), flash drives, disks, and any other known physical storage media.

[0086] Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. Accordingly, the disclosure of the embodiments of the disclosure is intended to be illustrative, but not limiting, of the scope of the disclosure.

[0087] With respect to the use of substantially any plural and/or singular terms herein, those having skill in the art can translate from the plural to the singular and/or from the singular to the plural as is appropriate to the context and/or application. The various singular/plural permutations may be expressly set forth herein for sake of clarity.

[0088] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on

or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0089] The above description is illustrative and is not restrictive. Many variations of the invention may become apparent to those skilled in the art upon review of the disclosure.

[0090] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0091] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0092] All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

[0093] Although the invention has been described in detail for the purpose of illustration based on what is currently considered to be the most practical and preferred embodiments, it is to be understood that such detail is solely for that purpose and that the invention is not limited to the disclosed embodiments, but, on the contrary, is intended to cover modifications and equivalent arrangements that are within the spirit and scope of the invention. For example, it is to be understood that the present invention contemplates that, to the extent possible, one or more features of any embodiment can be combined with one or more features of any other embodiment.

ABSTRACT

SYSTEM AND METHOD FOR TELEPHONIC PAYMENT CREDENTIAL COLLECTION

Embodiments of the invention are directed to methods and systems for telephonic payment credential collection. A user, via a communication device 101, can establish a telephonic connection to a client device (e.g., associated with a resource provider) to initiate a transaction. The client device can join an automated payment collection assistant (APCA) application 102 to prompt the user for fields relating to a payment device, translate the fields into text, and authenticate the speech of the user (e.g., by comparing the voice of the user with a stored biometric voice print previously provided by the user). Data relating to the transaction and the payment device details can be forwarded to a processing computer for authentication of the transaction. Responsive to authenticating the transaction, a message can be sent to the communication device 101 indicating that the transaction is successful.

FIG. 1

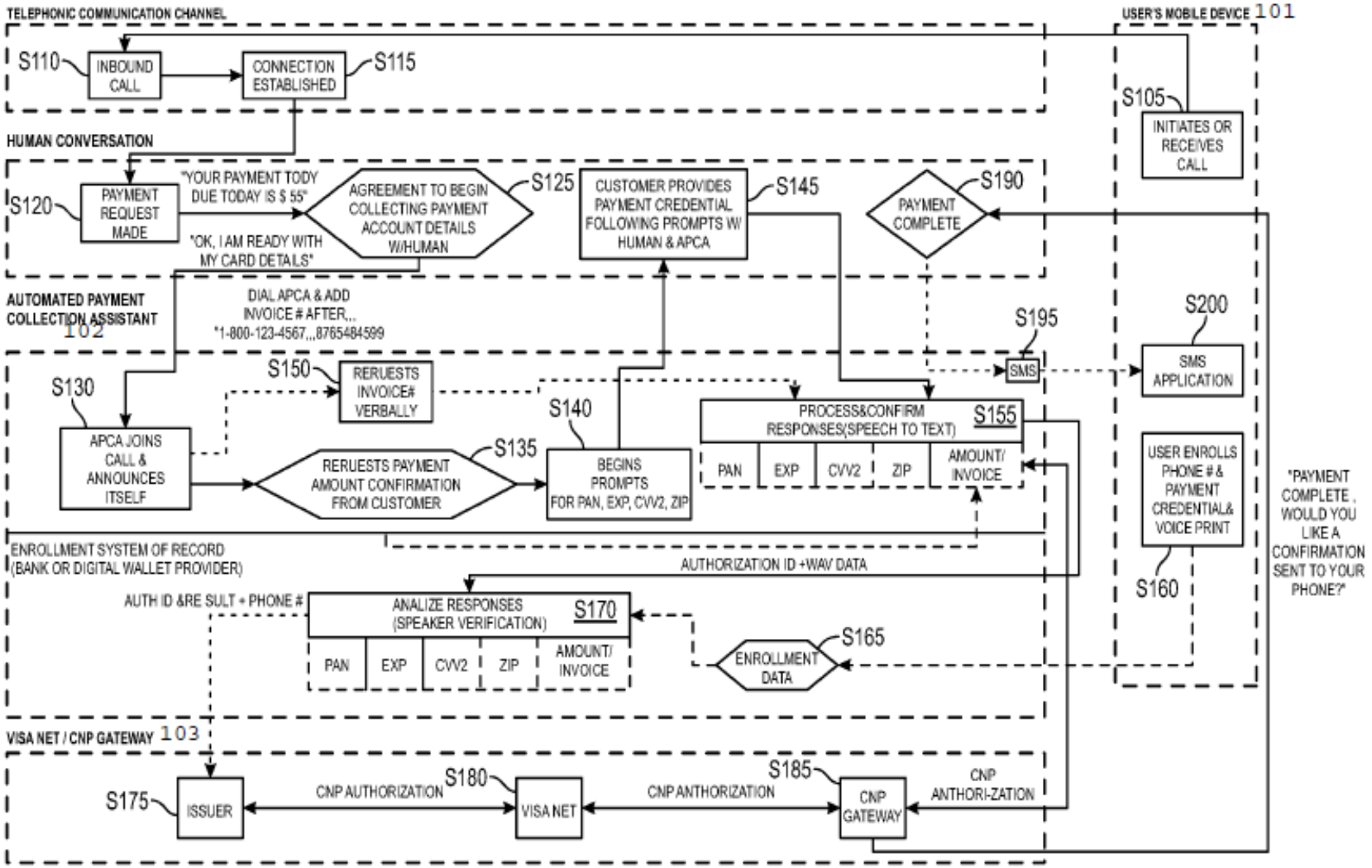
TELEPHONIC COMMUNICATION CHANNEL
USER'S MOBILE DEVICE 101
S110
INBOUND CALL
CONNECTION ESTABLISHED
S115
S105
INITIATES OR RECEIVES CALL
HUMAN CONVERSATION
S120
PAYMENT REQUEST MADE
"YOUR PAYMENT TODY DUE TODAY IS $ 55"
"OK, I AM READY WITH MY CARD DETAILS"
AGREEMENT TO BEGIN COLLECTING PAYMENT ACCOUNT DETAILS W/HUMAN
S125
CUSTOMER PROVIDES PAYMENT CREDENTIAL FOLLOWING PROMPTS W/ HUMAN & APCA
S145
PAYMENT COMPLETE
S190
AUTOMATED PAYMENT COLLECTION ASSISTANT 102
DIAL APCA & ADD INVOICE # AFTER,,, "1-800-123-4567,,,876548599
S195
SMS
S200
SMS APPLICATION
S150
RERUESTS INVOICE# VERBALLY
S130
APCA JOINS CALL & ANNOUNCES ITSELF
S140
PROCESS&CONFIRM RESPONSES(SPEECH TO TEXT)
S155
PAN
EXP
CVV2
ZIP
AMOUNT/ INVOICE
S135
RERUESTS PAYMENT AMOUNT CONFIRMATION FROM CUSTOMER
BEGINS PROMPTS FOR PAN, EXP, CVV2, ZIP
USER ENROLLS PHONE # & PAYMENT CREDENTIAL& VOICE PRINT
S160
"PAYMENT COMPLETE , WOULD YOU LIKE A CONFIRMATION SENT TO YOUR PHONE?"
ENROLLMENT SYSTEM OF RECORD (BANK OR DIGITAL WALLET PROVIDER)
AUTHORIZATION ID +WAV DATA
AUTH ID &RE SULT + PHONE #
ANALIZE RESPONSES (SPEAKER VERIFICATION)
S170
PAN
EXP
CVV2
ZIP
AMOUNT/ INVOICE
S165
ENROLLMENT DATA
VISA NET / CNP GATEWAY 103
S175
ISSUER
CNP AUTHORIZATION
S180
VISA NET
CNP ANTHORIZATION
S185
CNP GATEWAY
CNP ANTHORI-ZATION

FIG. 1

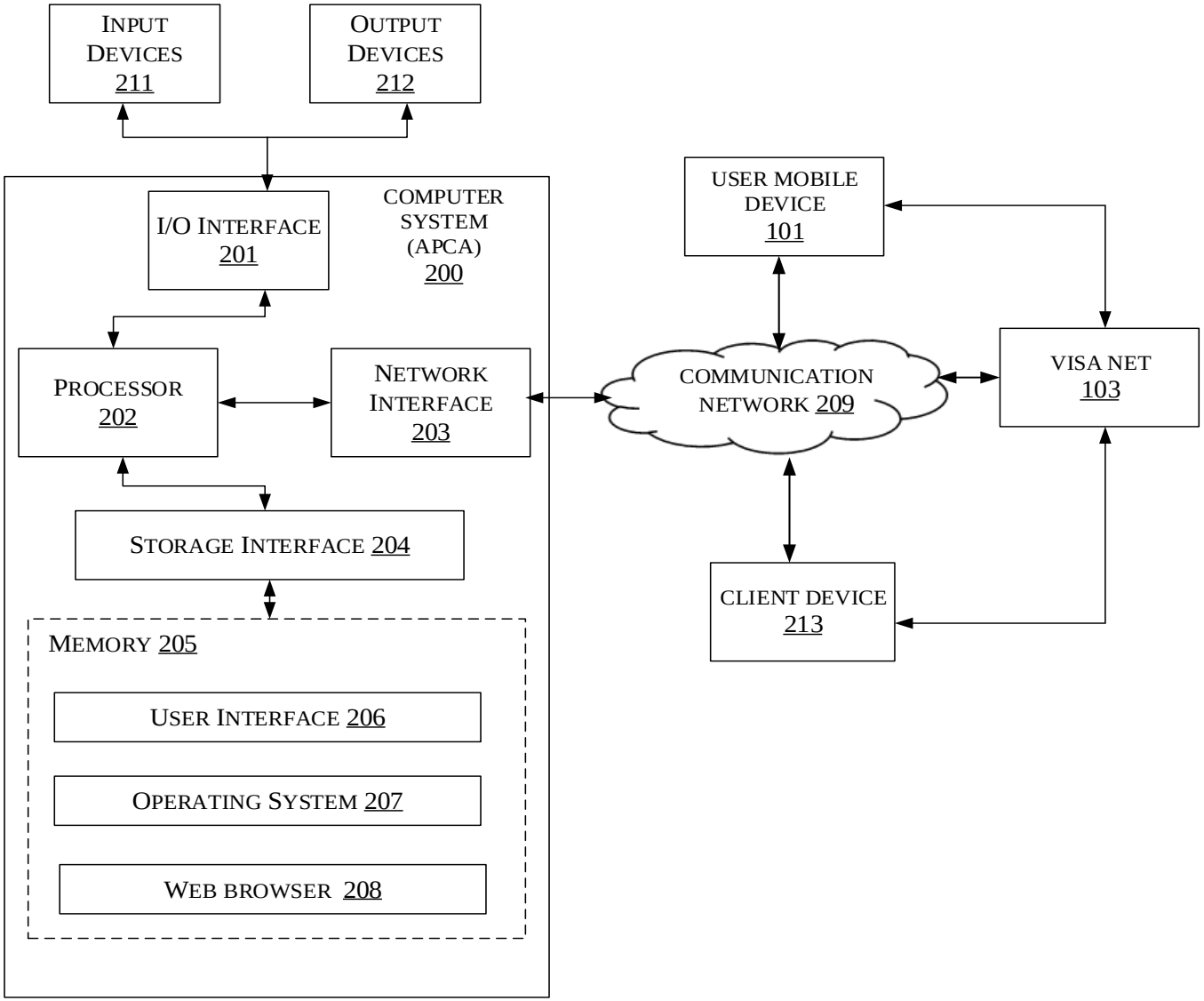
INPUT DEVICES 211
OUTPUT DEVICES 212
I/O INTERFACE 201
COMPUTER SYSTEM (APCA) 200
PROCESSOR 202
NETWORK INTERFACE 203
STORAGE INTERFACE 204
MEMORY 205
USER INTERFACE 206
OPERATING SYSTEM 207
WEB BROWSER 208
USER MOBILE DEVICE 101
COMMUNICATION NETWORK 209
VISA NET 103
CLIENT DEVICE 213

FIG. 2