System and Method for Registering Payment Account Details on an Electronic Wallet for Subsequent Use

Field of the Invention

[0001] The present invention relates to a system and method for registering payment account details on an electronic wallet for subsequent use.

Background of the invention

[0002] It is common for people to own various types of payment cards or payment accounts with one or more financial institutions. The term payment card may comprise any suitable cashless payment mechanism, such as a credit card, a debit card, a prepaid card, a charge card, a membership card, a promotional card, a frequent flyer card, an identification card, a gift card or an electronic wallet.

[0003] Online transactions are prevalent and greater numbers of card owners are using electronic devices (e.g. mobile devices or personal computers) for transactions. In order to use an electronic device for a transaction, it is necessary for the card owner to manually input details of his/her payment cards or payment accounts, such as the name of the financial institution associated with the card, the card owner's name, the card/account code, a billing address, an issue date, an expiry date, a card verification value (CVV) and/or a personal identification number (PIN). This is time-consuming, manual input can be prone to errors and also the data entered may be inadvertently exposed for fraudulent use. There is also a risk of physical cards being lost or stolen, or card details like CVV or PIN becoming known to others and thus the security of the financial account associated with the payment card is compromised.

[0004] An electronic wallet can be used to store payment card or account details such that they only need to be entered once. However, the problems associated with entering payment card or account details, as outlined above, are still encountered in order to add a payment card or account to an electronic wallet in the first instance.

[0005] It is therefore desirable to have a system and method providing increased convenience for card owners and improvement to the security of financial accounts.

[0006] Consequently, there is a need for an improved system and method for registering payment account details on an electronic wallet for subsequent use.

Summary of the invention

[0007] In accordance with a first aspect of the present invention there is provided a data aggregator server for registering payment account details on an electronic wallet operating on an electronic device for subsequent use. The data aggregator server comprises a processor configured for:

a) receiving account information from a plurality of issuer servers, the account information comprising an account identifier and reference biometric data from a plurality of users;

b) receiving from an electronic wallet of a said user, registration biometric data and an identifier for the electronic wallet;

c) comparing the registration biometric data with the reference biometric data to identify the user and all the account information associated with the user; and

d) transmitting to the electronic device, using the identifier, the account information associated with the user for registration on the electronic wallet for subsequent use.

[0008] Embodiments of this aspect of the invention therefore provide a data aggregator server configured to aggregate account data across different financial institutions such that it can all be provided to a user's electronic wallet simply by matching biometric data provided by the user. Accordingly, the user does not need to manually enter any account details into their electronic wallet and therefore embodiments of this aspect of the invention provide a more efficient, more accurate and more secure method for registering account details on an electronic wallet for subsequent use.

[0009] The account identifier of the account information associated with the user may comprise a bank account code or a user's identity card code.

[0010] The reference biometric data and registration biometric data of the user may each comprise a face scan, an iris scan, a fingerprint or a heartbeat of the user or information derived therefrom. The reference biometric data and registration biometric data may be in the form of an image, a video, an image extracted from a video or a string of numbers and/or characters derived therefrom.

[0011] The reference biometric data and the registration biometric data may comprise information derived from actual biometric data such that actual biometric data is not received by the data aggregator server over the communication network. This ensures greater security for the actual biometric data which can either be verified locally (e.g. at each issuer server and on the electronic device of the user) or via an authentication server authorised to maintain records of actual biometric data.

[0012] The reference biometric data may be obtained by each of the plurality of issuer servers when a user requests to register his/her account details with the data aggregator server.

The user may register at each of the plurality of issuer servers in person (i.e. at each issuer institution associated with each issuer server).

[0013] The registration biometric data may be obtained from an image or video of the user taken from an electronic device (e.g. his/her electronic device). For example, the reference biometric data and registration biometric data may each comprise information pertaining to multiple points identified from a face scan.

[0014] In one embodiment, the form of the registration biometric data provided by the user should match the form of the reference biometric data that is stored in the data aggregator. For example, if an issuer server stores the reference biometric data as an image, the user should also provide an image corresponding to his/her registration biometric data for verification and access to his/her account information from that particular issuer server, at least. If an issuer server stores the fingerprint of the user as his/her reference biometric data, the user should provide his/her fingerprint as the registration biometric data for verification and access to his/her account information from that particular issuer server, at least. In other embodiments, the data aggregator server may aggregate all of the reference biometric data obtained from different issuer servers into a single account for each user such that access to all of the account information for a single user (from different issuer servers, i.e. different issuer institutions) may be provided if the user supplies registration biometric data in the same format as the registration biometric data from at least one of the issuer servers with which they have an account.

[0015] The account information may further comprise one or more of: a name, an address, a date of birth, a token and payment card details or other account details (e.g. for savings or checking accounts) associated with the account identifier.

[0016] The payment card associated with the account identifier may comprise one or more of a credit card, a debit card, a prepaid card, a charge card, a membership card, a promotional card, a frequent flyer card, an identification card, a gift card or a digital wallet.

[0017] The payment card details may comprise one or more of: the name of the issuer server associated with the card, the card owner's name, the card/account code, a billing address, a card verification value (CVV), a personal identification number (PIN), an issue date and an expiry date.

[0018] The data aggregator server may transmit updated account information to the electronic wallet of the user after receipt of updated account information from the plurality of issuer servers. For example, if the user acquires new payment cards or opens new accounts, these details may be automatically relayed from the issuer server to the data aggregator server and then on to the user's electronic wallet via the user's electronic device. Similarly, if the user cancels a payment card or closes an account, these changes may be

automatically relayed from the issuer server to the data aggregator server and then on to the user's electronic wallet via the user's electronic device and the details associated with the cancelled card or closed account may be automatically deleted from his/her electronic wallet. In addition, any change in information associated with a user's payment card or account (e.g. name, address, expiry date, etc.) may be automatically relayed from the issuer server to the data aggregator server and then on to the user's electronic wallet via the user's electronic device to update the relevant details therein. Such updates may be scheduled to take place immediately upon notification from an issuer server or they may be scheduled to take place periodically (e.g. hourly, daily or weekly).

[0019] In a second aspect, the present invention provides an electronic device for obtaining a user's payment account details on an electronic wallet for subsequent use. The electronic device may comprise a processor configured for:

a) transmitting registration biometric data and an identifier for the electronic wallet to a data aggregator server; and

b) receiving from the data aggregator server, using the identifier, account information associated with the user for registration on the electronic wallet for subsequent use.

[0020] Embodiments of this aspect therefore provide an electronic device configured to communicate with a data aggregator server to obtain a user's payment account details. The data communicated between the data aggregator server and the electronic device may be encrypted to ensure that the payment account details associated with the user are kept secure.

[0021] Embodiments of the invention may leverage a user's electronic device as a channel of communication for initiating and/or authorising payments.

[0022] In a third aspect, the present invention provides a computer-implemented method for registering payment account details on an electronic wallet operating on an electronic device for subsequent use, which comprises the steps of:

a) receiving account information from a plurality of issuer servers, the account information comprising an account identifier and reference biometric data from a plurality of users;

b) receiving from an electronic wallet of a said user, registration biometric data and an identifier for the electronic wallet;

c) comparing the registration biometric data with the reference biometric data to identify the user and all the account information associated with the user; and

d) transmitting to the electronic device, using the identifier, the account information associated with the user for registration on the electronic wallet for subsequent use.

[0021] Embodiments of this aspect therefore provide a computer-implemented method which may be performed by a data aggregator server to aggregate account data across different issuer servers such that it can all be provided to a user's electronic wallet simply by matching biometric data provided by the user. Accordingly, the user does not need to manually enter any account details into their electronic wallet and therefore embodiments of this aspect of the invention provide a more efficient, more accurate and more secure method for registering account details on an electronic wallet for subsequent use.

[0022] The above method may further comprise converting the registration biometric data to a string of numbers or characters if the registration biometric data obtained from the user is not formatted as a string of numbers or characters and the reference biometric data is formatted as a string of numbers or characters.

[0023] The method may further comprise the steps of:

a) for each user, identifying the account information, from the plurality of issuer servers, associated with a same user;

b) aggregating the identified account information into a user account profile; and

c) storing the user account profile in a database.

[0024] In a fourth aspect, the present invention provides a computer-implemented method for obtaining user's payment account details on an electronic wallet for subsequent use, which comprises the steps of:

a) transmitting, from a user's electronic device, registration biometric data and an identifier for the electronic wallet to a data aggregator server; and

b) receiving from the data aggregator server, using the identifier, account information associated with the user for registration on the electronic wallet for subsequent use.

[0025] Embodiments of this aspect therefore provide a computer-implemented method for an electronic wallet to communicate with a data aggregator server to obtain a user's payment account details. The data communicated between the data aggregator server and the electronic wallet may be encrypted to ensure that the payment account details associated with the user are kept secure.

[0026] The above method may further comprise requiring the user to blink when taking a video of him/herself to verify that the video is live before the registration biometric data is

obtained. The blinking of the user's eyes verifies that the user is actually present when taking a video or image of him/herself prior to obtaining and transmitting the registration biometric data. More specifically, requiring the blinking of the user's eyes prevents another person from impersonating the user, for example, by using a photograph of the user when obtaining the registration biometric data.

[0027] In a fifth aspect, the present invention provides a non-transitory computer-readable medium having stored thereon program instructions for causing at least one processor to perform the method according to the third or fourth aspects of the invention above.

[0028] Embodiments of the invention may be expressed as a network of communicating devices (i.e. a "computerized network"). It may further be expressed in terms of a software application downloadable into a computer device to facilitate the method. The software application may be a computer program product, which may be stored on a non-transitory computer-readable medium on a tangible data-storage device (such as a storage device of a server, or one within a communication device).

Brief description of the drawings

[0029] Embodiments of the invention will now be described by way of example only with reference to the following drawings, in which:

Figure 1 illustrates a computerised network of electronic devices in accordance with an embodiment of the invention;

Figure 2 shows an overview of a system for registering payment account details on an electronic wallet for subsequent use, in accordance with an embodiment of the invention;

Figure 3 illustrates a method for registering payment account details on an electronic wallet for subsequent use, in accordance with an embodiment of the invention;

Figure 4 shows a block diagram of technical architecture of a data aggregator shown in Figure 1 or 2, in accordance with an embodiment of the invention; and

Figure 5 shows a block diagram of technical architecture of a communication device shown in Figure 1 or 2, in accordance with an embodiment of the invention.

Detailed description of certain embodiments

[0030] Figure 1 illustrates a computerized network 20 of electronic devices in accordance with an embodiment of the invention. The network 20 comprises an electronic device in the form of a mobile device 22, connected via a communication network 24 to a data aggregator server 26. The mobile device 22 is associated with a user who wishes to

register financial account information on his/her electronic wallet operating on the mobile device 22 to perform transactions. In Figure 1, the mobile device 22 is depicted as a smartphone, however it may be constituted by any electronic communication device, such as a tablet computer, laptop or personal computer.

[0031] In general terms, the mobile device 22 can be considered to be a communication device (which is described below in more detail with reference to Figure 5). The mobile device 22 includes a screen 30 and an input device 32 (e.g. a keypad). The screen 30 may be touch sensitive, in which case a separate input device 32 may not be required and the screen alone may provide a user interface for the communication device. The mobile device 22 is able to communicate with the communication network 24 using respective communication interfaces (not shown). The communication device 22 may communicate with the communication network 24 via a wireless connection (e.g. GPRS, 3G, 4G, WIFI or Bluetooth) or a wired connection.

[0032] The user associated with the mobile device 22 maintains a payment account (e.g. a bank account or a credit card account) at a financial institution (e.g. issuer bank). He/she may be associated with more than one financial institution. In Figure 1, two financial institutions in the form of issuers 34 and 36 are depicted. Each issuer is associated with an issuer server (not shown). The issuer servers of each issuer 34 and 36 are connected to the data aggregator server 26 via the communication network 24 to transmit data relative to the payment accounts they hold. The mobile device 22 may also communicate with the data aggregator server 26 using the communication network 24.

[0033] As shown in Figure 1, a digital identity certification authority (DICA) server 250 and a digital integrated data processing (DIDP) server 252 are also connected to the data aggregator server 26 via the communication network 24. Both these servers 250, 252 may transfer data between the data aggregator server 26 and the mobile device 22 of the user as will be described in more detail below in relation to Figure 2.

[0034] Figure 2 illustrates a system 240 for registering payment account details on an electronic wallet for subsequent use in accordance with one embodiment of the invention. Figure 2 is intended to illustrate example communication paths between the various different servers and devices in the system 240. However, it should be understood that, in accordance with Figure 1, the various servers (i.e. issuer servers, data aggregator server, DICA server and DIDP server) and devices (i.e. electronic device) communicate with each other by sending data over the communications network 24.

[0035] In this embodiment, a data aggregator server 248 is connected to three financial institutions denoted as bank 1 issuer server (242), bank 2 issuer server (244) and bank 3

issuer server (246). The data aggregator server 248 receives account information from each of these financial institutions for a plurality of users. The account information comprises an account identifier (e.g. a bank account code, a user's identity card code) and reference biometric data (e.g. a face scan, an iris scan, a fingerprint or heartbeat or information derived therefrom) from a user. The data aggregator server 248 stores the account information in a database (not shown).

[0036] The bank account code and the user's identity card code may comprise numbers or characters.

[0037] The data aggregator server 248 is connected to the digital identity certification authority (DICA) server 250. The digital identity certification authority (DICA) server 250 transmits data between the data aggregator server 248 and an electronic device 254 of the user (which may be a mobile device or other device such as a personal computer or piece of electronic equipment).

[0038] The digital identity certification authority (DICA) server 250 is in communication with the digital integrated data processing (DIDP) server 252 over the communication network 24. The DICA 250 and DIDP 252 may each be independently operated servers. The digital integrated data processing (DIDP) server 252 transmits data between the digital identity certification authority (DICA) server 250 and the electronic device 254.

[0039] In use, the user transmits or receives data between his or her electronic device 254 and the data aggregator server 248 directly. In another embodiment, the user transmits or receives data through the digital identity certification authority (DICA) server 250 or the digital integrated data processing (DIDP) server 252.

[0040] Figure 3 shows a method 100 for registering payment account details on an electronic wallet operating on the electronic device 254 for subsequent use in accordance with an embodiment of the invention. The method 100 comprises the following steps performed by a processor of a data aggregator server 248:

Step 102: receiving account information from a plurality of issuer servers 242, 244, 246, the account information comprising an account identifier and reference biometric data from a plurality of users;

Step 104: receiving from an electronic wallet of a user, via the electronic device 254, registration biometric data and an identifier for the electronic wallet;

Step 106: comparing the registration biometric data with the reference biometric data to identify the user and all the account information associated with the user; and

Step 108: transmitting to the electronic device 254, using the identifier, the account information associated with the user for registering on the electronic wallet for subsequent use.

[0041] In this embodiment, the user visits each of the financial institutions associated with the bank 1 issuer server (242), bank 2 issuer server (244) and bank 3 issuer server (246) in person to register his/her account information and reference biometric data with the data aggregator server 248. The account information associated with the user may comprise his/her name, his/her address, his/her date of birth, token, payment card details of payment cards or other account details associated with the user. The system may not only register payment card details, it may also register different types of bank accounts which the user has access to, such as savings accounts, current accounts, etc.

[0042] The payment card/account details may comprise one or more of a name of the financial institution or issuer server associated with the payment card/account, a card/account owner's name, a card/account code, a billing address, a token, a card verification value (CVV), a personal identification number (PIN), an issue date and an expiry date.

[0043] The data aggregator server may transmit updated account information to the electronic wallet of the user, via the electronic device 254, after receipt of updated account information from the plurality of issuer servers 242, 244, 246. For example, if the user acquires new payment cards or opens new accounts, these details may be automatically relayed from the issuer server 242, 244, 246 to the data aggregator server 248 and then on to the user's electronic wallet via the electronic device 254. Similarly, if the user cancels a payment card or closes an account, these changes may be automatically relayed from the issuer server 242, 244, 246to the data aggregator server 248 and then on to the user's electronic wallet and the details associated with the cancelled card or closed account may be automatically deleted from his/her electronic wallet. In addition, any change in information associated with a user's payment card or account (e.g. name, address, expiry date etc.) may be automatically relayed from the issuer server 242, 244, 246to the data aggregator server 248 and then on to the user's electronic wallet to update the relevant details therein. Such updates may be scheduled to take place immediately upon notification from an issuer server 242, 244, 246or they may be scheduled to take place periodically (e.g. hourly, daily or weekly).

[0044] In this embodiment, the reference biometric data is a face scan. From the face scan, a predefined number of features (e.g. 72 points) on specific locations on the user's face are determined and converted into a string of numbers or characters. In other embodiments, the number of points may be varied. The string of numbers or characters is stored as the

reference biometric data of the user. The reference biometric data is encrypted and stored in the database associated with the data aggregator server 248.

[0045] The three issuer servers 242, 244, 246 and the data aggregator server 248 form a circle of trust, in which confidential and trusted information is communicated between the issuer servers and the data aggregator server 248. The digital identity certification authority (DICA) server 250 receives aggregated identity assertions from the circle of trust and consolidates a final assertion of the identity and information associated with the user.

[0046] In one implementation, the digital integrated data processing (DIDP) server 252 and the digital identity certification authority (DICA) server 250 may be implemented as a distributed ledger system. In this implementation, once the digital identity certification authority (DICA) server 250 has consolidated its final assertion of the identity and information associated with the user, digitalized enrolment data along with certification records are written to the distributed ledger system in the digital integrated data processing (DIDP) server 252.

[0047] An electronic wallet application (or other payment application) is installed in the electronic device 254. When the user wishes to register financial account information on his/her electronic wallet to perform a transaction, he/she launches the electronic wallet application on his/her electronic device 254 to take a video of his/her face. The video is encrypted into a string of numbers or characters, which is sent to the digital integrated data processing (DIDP) server 252. The encrypted string of numbers or characters constitutes the registration biometric data of the user.

[0048] In this embodiment, the user is required to blink his/her eyes when taking the video of him/herself to verify that the video is live before the registration biometric data is obtained. The blinking of the user's eyes verifies that the user is actually present when taking a video or image of him/herself prior to obtaining and transmitting the registration biometric data. More specifically, requiring the blinking of the user's eyes prevents another person from impersonating the user, for example, by using a photograph of the user as a still image which could be transmitted as the registration biometric data.

[0049] The registration biometric data of the user is transmitted to the digital identity certification authority (DICA) server 250, before reaching the data aggregator server 248. The data aggregator server 248 comprises a scoring and data engine. The registration biometric data is compared with the reference biometric data in the data aggregator server 248 by the scoring and data engine to identify the user.

[0050] The form of the registration biometric data provided by the user should match the form of the reference biometric data that is stored in the data aggregator server. For example, if

an issuer server stores the reference biometric data as an image, the user should also provide an image corresponding to his/her registration biometric data for verification and access to his/her account information from that particular financial institution, at least. If an issuer server stores the fingerprint of the user as his/her reference biometric data, the user should provide his/her fingerprint as the registration biometric data for verification and access to his/her account information from that particular financial institution, at least. In some embodiments, the data aggregator server may aggregate all of the reference biometric data obtained from different issuer servers into a single account for each user such that access to all of the account information for a single user (from different financial institutions) may be provided if the user supplies registration biometric data in the same format as the registration biometric data from at least one of the issuer servers with which they have an account.

[0051] In some embodiments, the reference biometric data and the registration biometric data comprise information derived from actual biometric data such that actual biometric data is not sent over the communication network to the data aggregator server 248. This ensures greater security for the actual biometric data which can either be verified locally (e.g. at each issuer server 242, 244, 246 and on the electronic device 254 of the user) or via an authentication server (e.g. DICA server 250) authorised to maintain records of actual biometric data.

[0052] Once the identity of the user is obtained, the account information (or at least one part of it) associated with the user is retrieved from the database associated with the data aggregator server 248 and transmitted to the electronic device 254 of the user through the digital identity certification authority (DICA) server 250 and the digital integrated data processing (DIDP) server 252. The account information may comprise payment card details of payment cards associated with the user. The payment card details or other account details will be displayed on the electronic device 254. The user only has to select the desired payment card/account for a subsequent transaction and does not need to enter all of the account information manually.

[0053] In some embodiments, the payment card or account details may be tokenized for added security. The data aggregator server 248 may transmit the token associated with the payment card/account to the user's electronic device 254. In the event that the user's electronic device 254 is lost or hacked, no-one will be able to retrieve the payment card/account details from the token stored in the electronic device 254.

[0054] After the user selects the desired payment card, he/she may be required to enter a CVV for authentication. Once authentication is successful, the user is able to make

payments using the payment card/account details on the electronic device 254 via electronic wallet.

[0055] In all of the servers and devices of this embodiment, different application programming interfaces (APIs) are used, each with its own function. For example, a privacy API is used to ensure the privacy of the data communications transmitted over the communication network. User data may be anonymized such that it is not possible to reveal the identity of the user through the user data alone.

[0056] One advantage of this embodiment is that the user is not required to manually input his/her account information in his/her electronic device when he/she needs to perform a transaction using an electronic wallet. This saves time and reduces the risk of errors during data input.

[0057] Another advantage of this embodiment is that by requiring the user to blink his/her eyes when taking a video of him/herself with his/her electronic device, the security of the financial accounts associated with the user is enhanced as it is not possible for someone to use a still photograph of the user as the registration biometric data.

[0058] Figure 4 is a block diagram showing a technical architecture of the data aggregator server 26, 248. The issuer servers of each issuer 34 or 36 may also have this technical architecture.

[0059] The technical architecture includes a processor 422 (which may be referred to as a central processor unit or CPU) that is in communication with memory devices including secondary storage 424 (such as disk drives), read only memory (ROM) 426, random access memory (RAM) 428. The processor 422 may be implemented as one or more CPU chips. The technical architecture may further comprise input/output (I/O) devices 430, and network connectivity devices 432.

[0060] The secondary storage 424 is typically comprised of one or more disk drives or tape drives and is used for non-volatile storage of data and as an over-flow data storage device if RAM 428 is not large enough to hold all working data. Secondary storage 424 may be used to store programs which are loaded into RAM 428 when such programs are selected for execution.

[0061] In this embodiment, the secondary storage 424 has a processing component 424a comprising non-transitory instructions operative by the processor 422 to perform various operations of the method of the present disclosure. The ROM 426 is used to store instructions and perhaps data which are read during program execution. The secondary

storage 424, the RAM 428, and/or the ROM 426 may be referred to in some contexts as computer readable storage media and/or non-transitory computer readable media.

[0062] I/O devices 430 may include printers, video monitors, liquid crystal displays (LCDs), plasma displays, touch screen displays, keyboards, keypads, switches, dials, mice, track balls, voice recognizers, card readers, paper tape readers, or other well-known input devices.

[0063] The network connectivity devices 432 may take the form of modems, modem banks, Ethernet cards, universal serial bus (USB) interface cards, serial interfaces, token ring cards, fiber distributed data interface (FDDI) cards, wireless local area network (WLAN) cards, radio transceiver cards that promote radio communications using protocols such as code division multiple access (CDMA), global system for mobile communications (GSM), long-term evolution (LTE), worldwide interoperability for microwave access (WiMAX), near field communications (NFC), radio frequency identity (RFID), and/or other air interface protocol radio transceiver cards, and other well-known network devices. These network connectivity devices 432 may enable the processor 422 to communicate with the Internet or one or more intranets. With such a network connection, it is contemplated that the processor 422 might receive information from the network, or might output information to the network in the course of performing the above-described method operations. Such information, which is often represented as a sequence of instructions to be executed using processor 422, may be received from and outputted to the network, for example, in the form of a computer data signal embodied in a carrier wave.

[0064] The processor 422 executes instructions, codes, computer programs, scripts which it accesses from hard disk, floppy disk, optical disk (these various disk based systems may all be considered secondary storage 424), flash drive, ROM 426, RAM 428, or the network connectivity devices 432. While only one processor 422 is shown, multiple processors may be present. Thus, while instructions may be discussed as executed by a processor, the instructions may be executed simultaneously, serially, or otherwise executed by one or multiple processors.

[0065] Although the technical architecture is described with reference to a computer, it should be appreciated that the technical architecture may be formed by two or more computers in communication with each other that collaborate to perform a task. For example, but not by way of limitation, an application may be partitioned in such a way as to permit concurrent and/or parallel processing of the instructions of the application. Alternatively, the data processed by the application may be partitioned in such a way as to permit concurrent and/or parallel processing of different portions of a data set by the two or more computers. In an embodiment, virtualization software may be employed by the technical architecture

420 to provide the functionality of a number of servers that is not directly bound to the number of computers in the technical architecture 420. In an embodiment, the functionality disclosed above may be provided by executing the application and/or applications in a cloud computing environment. Cloud computing may comprise providing computing services via a network connection using dynamically scalable computing resources. A cloud computing environment may be established by an enterprise and/or may be hired on an as-needed basis from a third party provider.

[0066] It is understood that by programming and/or loading executable instructions onto the technical architecture, at least one of the CPU 422, the RAM 428, and the ROM 426 are changed, transforming the technical architecture in part into a specific purpose machine or apparatus having the novel functionality taught by the present disclosure. It is fundamental to the electrical engineering and software engineering arts that functionality that can be implemented by loading executable software into a computer can be converted to a hardware implementation by well-known design rules.

[0067] Figure 5 is a block diagram showing a technical architecture of the mobile device 22 and electronic device 254.

[0068] The technical architecture includes a processor 322 (which may be referred to as a central processor unit or CPU) that is in communication with memory devices including secondary storage 324 (such as disk drives or memory cards), read only memory (ROM) 326, random access memory (RAM) 328. The processor 322 may be implemented as one or more CPU chips. The technical architecture further comprises input/output (I/O) devices 330, and network connectivity devices 332.

[0069] The I/O devices comprise a user interface (UI) 330a. In the case of the customer mobile device 28, a camera 330b and a geolocation module 330c may also be provided. The UI 330a may comprise a touch screen, keyboard, keypad or other known input device. The camera 330b allows a user to capture images and save the captured images in electronic form. The geolocation module 330c is operable to determine the geolocation of the communication device using signals from, for example global positioning system (GPS) satellites.

[0070] The secondary storage 324 is typically comprised of a memory card or other storage device and is used for non-volatile storage of data and as an over-flow data storage device if RAM 328 is not large enough to hold all working data. Secondary storage 324 may be used to store programs which are loaded into RAM 328 when such programs are selected for execution.

[0071] In this embodiment, the secondary storage 324 has a processing component 324a, comprising non-transitory instructions operative by the processor 322 to perform various operations of the method of the present disclosure. The ROM 326 is used to store instructions and perhaps data which are read during program execution. The secondary storage 324, the RAM 328, and/or the ROM 326 may be referred to in some contexts as computer readable storage media and/or non-transitory computer readable media.

[0072] The network connectivity devices 332 may take the form of modems, modem banks, Ethernet cards, universal serial bus (USB) interface cards, serial interfaces, token ring cards, fiber distributed data interface (FDDI) cards, wireless local area network (WLAN) cards, radio transceiver cards that promote radio communications using protocols such as code division multiple access (CDMA), global system for mobile communications (GSM), long-term evolution (LTE), worldwide interoperability for microwave access (WiMAX), near field communications (NFC), radio frequency identity (RFID), and/or other air interface protocol radio transceiver cards, and other well-known network devices. These network connectivity devices 332 may enable the processor 322 to communicate with the Internet or one or more intranets. With such a network connection, it is contemplated that the processor 322 might receive information from the network, or might output information to the network in the course of performing the above-described method operations. Such information, which is often represented as a sequence of instructions to be executed using processor 322, may be received from and outputted to the network, for example, in the form of a computer data signal embodied in a carrier wave.

[0073] The processor 322 executes instructions, codes, computer programs, scripts which it accesses from hard disk, floppy disk, optical disk (these various disk based systems may all be considered secondary storage 324), flash drive, ROM 326, RAM 328, or the network connectivity devices 332. While only one processor 322 is shown, multiple processors may be present. Thus, while instructions may be discussed as executed by a processor, the instructions may be executed simultaneously, serially, or otherwise executed by one or multiple processors.

[0074] Whilst most electronic wallets currently operate on mobile devices, it will be understood by those skilled in the art that electronic wallets may exist on other electronic devices such as non-mobile devices or equipment such as personal computers, refrigerators, televisions, etc. An electronic wallet may be integrated into these non-mobile devices and a user may access the electronic wallet for transactions from the comfort of his/her home or office.

[0075] Whilst the foregoing description has described specific embodiments, it will be understood by those skilled in the art that many variations of the embodiments can be made in accordance with the appended claims.

Claims

1. A data aggregator server for registering payment account details on an electronic wallet operating on an electronic device for subsequent use, comprising a processor configured for:

    a) receiving account information over a communication network from a plurality of issuer servers, the account information comprising an account identifier and reference biometric data from a plurality of users;

    b) receiving from the electronic device of a said user, registration biometric data and an identifier for the electronic wallet;

    c) comparing the registration biometric data with the reference biometric data to identify the user and all the account information associated with the user; and

    d) transmitting to the electronic device, using the identifier, the account information associated with the user for registration on the electronic wallet for subsequent use.

2. The data aggregator server of claim 1, wherein the account identifier comprises a bank account code or a user's identity card code.

3. The data aggregator server of claim 1 or 2, wherein the reference biometric data and registration biometric data each comprise a face scan, an iris scan, a fingerprint or a heartbeat of the user or information derived therefrom.

4. The data aggregator server of claim 3, wherein the reference biometric data and the registration biometric data comprise said information such that actual biometric data is not received by the data aggregator server over the communication network.

5. The data aggregator server of any preceding claim, wherein the reference biometric data and registration biometric data each comprise at least one of an image, a video, an image extracted from a video or a string of numbers or characters derived therefrom.

6. The data aggregator server of any preceding claim, wherein the reference biometric data is obtained by each of the plurality of issuer servers when a user requests to register his/her account details with the data aggregator server.

7. The data aggregator server of any preceding claim, wherein the registration biometric data is obtained from an image or video of the user taken from an electronic device.

8. The data aggregator server of any preceding claim, wherein the registration biometric data comprises information pertaining to multiple points identified from a face scan.

9. The data aggregator server of any preceding claim, wherein the registration biometric data provided by the user is in a form that matches that of the reference biometric data stored in the data aggregator to identify the user.

10. The data aggregator server of any preceding claim, wherein the account information further comprises one or more of: a name, an address, a date of birth, a token and payment card details of a payment card or other account details associated with the account identifier.

11. The data aggregator server of claim 9, wherein the payment card comprises one or more of a credit card, a debit card, a prepaid card, a charge card, a membership card, a promotional card, a frequent flyer card, an identification card, a gift card or a digital wallet.

12. The data aggregator server of claim 9, wherein the payment card details comprise one or more of: a name of the issuer server associated with the payment card, a card owner's name, a card/account code, a billing address, a card verification value (CVV), a personal identification number (PIN), an issue date and an expiry date.

13. The data aggregator server of any preceding claim, configured to transmit updated account information to the electronic wallet of the user after receipt of updated account information from one or more of the plurality of issuer servers.

14. An electronic device for obtaining a user's payment account details on an electronic wallet for subsequent use, comprising a processor configured for:

    a) transmitting registration biometric data and an identifier for the electronic wallet to a data aggregator server; and

    b) receiving from the data aggregator server, using the identifier, account information associated with the user for registration on the electronic wallet for subsequent use.

15. A computer-implemented method for registering payment account details on an electronic wallet operating on an electronic device for subsequent use, comprising the steps of:

    a) receiving account information from a plurality of issuer servers, the account information comprising an account identifier and reference biometric data from a plurality of users;

    b) receiving from an electronic wallet of a said user, registration biometric data and an identifier for the electronic wallet;

c) comparing the registration biometric data with the reference biometric data to identify the user and all the account information associated with the user; and

d) transmitting to the electronic device, using the identifier, the account information associated with the user for registration on the electronic wallet for subsequent use.

16. The method of claim 14, further comprising converting the registration biometric data to a string of numbers or characters if the registration biometric data obtained from the user is not formatted as a string of numbers or characters and the reference biometric data is formatted as a string of numbers or characters.

17. The method of claim 14 or 15, further comprising the steps of:

a) for each user, identifying the account information from the plurality of issuer servers associated with a same user;

b) aggregating the identified account information into a user account profile; and

c) storing the user account profile in a database.

18. A computer-implemented method for obtaining user's payment account details on an electronic wallet for subsequent use, comprising the steps of:

a) transmitting, from a user's electronic device, registration biometric data and an identifier for the electronic wallet to a data aggregator server; and

b) receiving from the data aggregator server, using the identifier, account information associated with the user for registration on the electronic wallet for subsequent use.

19. The method of claim 17, further comprising requiring the user to blink when taking a video of him/herself to verify that the video is live before the registration biometric data is obtained.

20. A non-transitory computer-readable medium having stored thereon program instructions for causing at least one processor to perform the method according to any one of claims 14 to 18.