

COMPUTER SYSTEM AND COMPUTER-IMPLEMENTED METHOD FOR PROCESSING A PAYMENT TRANSACTION USING A WIFI ROUTER

Field of the invention

[0001] The present invention relates to a computer system and computer-implemented method for processing a payment transaction using a WiFi router, in particular, for processing a payment transaction between a merchant and a user using a merchant WiFi network.

Background of the invention

[0002] The payment industry has moved into a new era of electronic cashless payments. Card-not-present transactions are ubiquitous. They enable users to buy products over the internet in a quick and easy manner. Even in retail shops, digital payments are on the rise as consumers are encouraged to pay using mobile wallets in place of cash or physical payment cards.

[0003] Nonetheless, gaps remain in this almost seamless payment experience for the users. For example, retailers struggle to identify consumers as the consumers shop in-store and therefore are unable to provide a more personal shopping experience to the consumers. Moreover, most if not all mobile wallet's usage is still tied to a presence of an internet connection of the user's electronic device – an absence of such a connection renders mobile wallets useless for payment transactions.

[0004] It is therefore desirable to provide a system and method which help to ameliorate at least some of the problems discussed above, and/or to provide the public with a useful choice.

Summary of the invention

[0005] In accordance with a first aspect of the present invention, there is provided a WiFi router for processing a payment transaction between a merchant and a user using a merchant WiFi network connected to the router, the router comprising a computer processor and a data storage device, the data storage device storing instructions operable to cause the processor to:

receive, from a user electronic device, a connection request for connecting the user electronic device to the merchant WiFi network for paying the payment transaction, the connection request comprising a user device identifier associated with the user electronic device;

determine, using a merchant database, that the user electronic device is enrolled with the merchant for making payment using the merchant WiFi network based on a pairing between the user device identifier and a router identifier associated with the router;

transmit, to the user electronic device, a connection response indicating that the user electronic device is connected to the router for paying the payment transaction, the connection response comprising details of the payment transaction;

receive, from the user electronic device, a confirmation response for the merchant to proceed with the payment transaction;

retrieve, from the merchant database, payment instrument data associated with a user payment instrument in response to the confirmation response to proceed with the payment transaction, the payment instrument data comprises a payment account identifier; and

communicate, to a payment network server, a payment transaction request for processing the payment transaction, the payment transaction request comprising the payment transaction details and the payment instrument data.

[0006] Embodiments of the invention provide a WiFi router that can be used for processing a payment transaction between a merchant and a user using a merchant WiFi network. In particular, the WiFi router is configured to: (i) receive a connection request from a user electronic device, (ii) determine that the user electronic device is enrolled with the merchant for making payment using the merchant WiFi network, (iii) transmit a connection response indicating that the user electronic device is connected to the router for paying the payment transaction; (iv) receive a confirmation response to proceed with the payment transaction; (v) retrieve payment instrument data associated with a user payment instrument; and (vi) communicate a payment transaction request for processing the payment transaction. The WiFi router thereby provides a local network associated with the merchant for processing payment transactions between the merchant and the user. By integrating payment capabilities directly into the merchant WiFi network, a user would be able to pay through this channel and seamlessly connect to the merchant's payment system each time the user electronic device is within range of the WiFi network. Once the user has been enrolled to make payments using the merchant WiFi network, minimal user interaction is required to process the payment as the user electronic device is at least authenticated via the pairing of the user mobile electronic device with the merchant's WiFi router. Further, given that the payment transaction is processed using the merchant's WiFi router, it is possible to implement further layers of authentication if required for high value transactions (e.g. transactions with values above \$100 or any

amount set by the user or the issuer). This improves a shopping experience and convenience for the user. Moreover, a hardware requirement of the user electronic device for utilizing this payment route is low – the user electronic device is simply required to be capable of connecting to a WiFi network and to have a user interface for viewing and approving payment transactions. Moreover, the WiFi router as described may be provided in addition to existing functions of the WiFi router (e.g. providing an internet connection to the user electronic device etc.). Embodiments of the present invention thereby eliminate the requirements of a specific mobile application or an available internet connection on the user electronic device for processing the payment transaction.

[0007] The data storage device of the WiFi router may comprise instructions operative by the processor to: transmit, to the user electronic device, a payment approval response indicating whether the payment transaction is approved or refused.

[0008] The data storage device of the WiFi router may comprise instructions operative by the processor to perform an enrolment procedure, the enrolment procedure comprising:

transmitting, to the user electronic device, a pairing request for pairing a user device identifier with the router identifier;

receiving, from the user electronic device, a pairing response indicating the user's approval of said pairing; and

storing details of said pairing in the merchant database.

[0009] In accordance with a second aspect of the present invention, there is provided a computer-implemented method for processing a payment transaction between a merchant and a user using a merchant WiFi network connected to a router, the method comprising:

receiving, from a user electronic device, a connection request for connecting the user electronic device to the merchant WiFi network for paying the payment transaction, the connection request comprising a user device identifier associated with the user electronic device;

determining, using a merchant database, that the user electronic device is enrolled with the merchant for making payment using the merchant WiFi network based on a pairing between the user device identifier and a router identifier associated with the router;

transmitting, to the user electronic device, a connection response indicating that the user electronic device is connected to the router for paying the payment transaction, the connection response comprising details of the payment transaction;

receiving, from the user electronic device, a confirmation response for the merchant to proceed with the payment transaction;

retrieving, from the merchant database, payment instrument data associated with a user payment instrument in response to the confirmation response to proceed with the payment transaction, the payment instrument data comprises a payment account identifier; and

communicating, to a payment network server, a payment transaction request for processing the payment transaction, the payment transaction request comprising the payment transaction details and the payment instrument data.

[0010] The method may comprise:

transmitting, to the user electronic device, a payment approval response indicating whether the payment transaction is approved or refused.

[0011] The method may comprise performing an enrolment procedure, the enrolment procedure comprising:

transmitting, to the user electronic device, a pairing request for pairing a user device identifier with the router identifier;

receiving, from the user electronic device, a pairing response indicating the user's approval of said pairing; and

storing details of said pairing on the merchant database.

[0012] The enrolment procedure may comprise:

transmitting, to the user electronic device, a payment instrument request in response to the user's approval of said pairing;

receiving, from the user electronic device, a payment instrument response comprising details of the user payment instrument;

transmitting, to the payment network server, the details of the user payment instrument for tokenization of the user payment instrument;

receiving, from the payment network server, a payment token associated with the user payment instrument; and

storing, on the merchant database, the payment token against the user device identifier.

[0013] The enrolment procedure may comprise:

transmitting, to the user electronic device, a password input request comprising a request for the user to retrieve a password from a merchant payment terminal;

receiving, from the user electronic device, a password input response comprising a password input; and

verifying that the password input matches the password, the payment instrument request is transmitted to the user electronic device if the password input is verified.

[0014] The enrolment procedure may comprise:

transmitting, to the user electronic device, a network password input request comprising a request for a network password;

receiving, from the user electronic device, a network password input response comprising a network password input; and

verifying that the network password input matches the network password, the payment instrument request is transmitted to the user electronic device if the network password input is verified.

[0015] The enrolment procedure may comprise receiving, from the user electronic device, authorization to use the payment token for processing the payment transaction.

[0016] The payment details may comprise a payment amount associated with the payment transaction.

[0017] The payment token may be generated by the payment network server. The payment network server may be associated with a Banknet payment network operated by Mastercard®. The payment token may be requested by the issuer institution.

[0018] The payment token may be associated with the user device identifier and the router identifier so that the payment token is valid only for payment transactions made through the user electronic device and the router.

[0019] The user device identifier and/or the router identifier may comprise a media access control (MAC) address. The user device identifier and/or the router identifier may be included in one or more 3DS field.

[0020] In accordance with a third aspect of the present invention, a non-transitory computer-readable medium having stored thereon program instructions for causing at least one processor to perform the preceding method.

[0021] The present invention aims to provide a new and useful computer system and computer-implemented method for processing a payment transaction between a merchant and a user using a merchant WiFi network to improve convenience and a shopping experience for a user.

Brief description of the drawings

[0022] Non-limiting embodiments of the invention will now be described for the sake of example only, with reference to the following drawings in which:

Fig. 1 shows a computer system for processing a payment transaction between a merchant and a user using a merchant WiFi network in accordance with an embodiment of the invention;

Fig. 2 shows steps of a method for processing the payment transaction between the merchant and the user using the merchant WiFi network facilitated by the computer system of Fig. 1;

Fig. 3 shows steps of a method for enrolling the user for payment using the merchant WiFi network facilitated by the computer system of Fig. 1;

Fig. 4 shows further steps of the method for enrolling the user for payment according to Fig. 3;

Fig. 5 shows steps of a first method for authenticating the merchant during enrollment of the user for payment using the merchant WiFi network facilitated by the computer system of Fig. 1;

Fig. 6 shows steps of a second method for authenticating the merchant during enrollment of the user for payment using the merchant WiFi network facilitated by the computer system of Fig. 1;

Fig. 7 shows an illustration of the steps of the method for enrolling the user for payment using the merchant WiFi network according to Figs. 3 and 4;

Fig. 8 shows an illustration of the steps of the first and second methods for authenticating the merchant during enrollment of the user for payment using the merchant WiFi network according to Figs. 5 and 6;

Fig. 9 shows an illustration of the steps of the method for processing the payment transaction between the merchant and the user using the merchant WiFi network according to Fig. 2; and

Fig. 10 shows schematically a hardware structure of the WiFi router which may be used in the computer system of Fig. 1 to implement a method in accordance with an embodiment of the invention.

Detailed description of the embodiments

[0023] Note that the term “payment instrument” refers to any form or mode of payment which is associated with a financial account (e.g. a current account, a saving account, a trading account etc.) or is associated with 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 prepaid card, a gift card, and/or any other payment device that may hold payment account information, such as mobile phones, Smartphones, personal digital assistants (PDAs), key fobs, transponder devices, NFC-enabled devices, and/or computers.

[0024] Note that the term “institution” is used here in a sense which is not necessarily limited to organizations which are legally constituted as banks, since in some jurisdictions other organizations may be permitted to maintain financial accounts such as a payment card account. An institution may comprise a financial technology company, a telecommunication company, a financial institution or any form of a payment service provider.

[0025] As used in this application, the terms “component,” “module,” “system,” “apparatus,” “interface,” or the like are generally intended to refer to a computer-related entity, either hardware, a combination of hardware and software, software, or software in execution. For example, a component or a module may be, but is not limited to being, a process running on a processor, a processor, an object, an executable, a thread of execution, a program, and/or a computer. By way of illustration, both an application running on a controller and the controller can be a component or a module. One or more components/modules may reside within a process and/or thread of execution and a component may be localized on one computer and/or distributed between two or more computers.

[0026] Furthermore, the claimed subject matter may be implemented as a method, apparatus, or article of manufacture using standard programming and/or engineering techniques to produce software, firmware, hardware, or any combination thereof to control a computer to implement the disclosed subject matter. For instance, the claimed subject matter may be implemented as a computer-readable medium embedded with a computer executable program, which encompasses a computer program accessible from any computer-readable storage device or storage media. For example, computer readable media can include but are not limited to magnetic storage devices (e.g., hard disk, floppy disk, magnetic strips . . .), optical disks (e.g., compact disk (CD), digital versatile disk (DVD) . . .), smart cards, and flash memory devices (e.g., card, stick, key drive . . .).

[0027] Fig. 1 shows a computer system 100 for processing a payment transaction between a merchant and a user using a merchant WiFi network in accordance with an embodiment of the invention. The computer system 100 comprises a WiFi router 104 which acts as an access point for providing the merchant WiFi network. The WiFi router 104 is associated with the merchant who provides goods and/or services for the user. The WiFi router 104 is connected to a payment network such as the Banknet payment network operated by Mastercard®. As shown in Fig. 1, the WiFi router 104 is in communication with a user electronic device 102 and a merchant payment terminal 106. Therefore, the WiFi network provides a communication channel between the user electronic device 102 and the merchant payment terminal 106. The user electronic device 102 is associated with the user and is capable of at least processing the payment transaction between the merchant and the user as described in Fig. 2. The user electronic device 102 may be a mobile phone, a laptop/notebook, a desktop, a tablet, a personal digital assistant (PDA), a key fob, a transponder device, a NFC-enabled device, and/or a computer. The merchant payment terminal 106 is a Point-of-Sale (POS) terminal but may be other devices associated with the merchant which is capable of processing the payment transaction using the merchant WiFi network. In an embodiment, the POS is a mobile application associated with a merchant device which can be used to communicate over the merchant WiFi network with the user electronic device 102. The mobile application may be provided as a firmware together with the WiFi router 104.

[0028] The acquirer server 108, the payment network server 110 and the issuer server 112 forms a conventional payment architecture for processing the payment transaction between the user and the merchant. As shown in Fig. 1, the WiFi router 104 is in communication with the acquirer server 108. The acquirer server 108 is operated by an acquiring institution at which the merchant maintains an account to receive funds. The acquirer server 108 is in turn in communication with the payment network server 110 which is also in communication with the issuer server 112. The issuer server 112 is associated with an issuer institution which maintains payment accounts for the user. The payment network server 110 facilitates payment transactions between the merchant and the user by communicating relevant transactions (e.g. payment requests, authentications etc.) between the acquirer server 108 and the issuer server 112. The issuer server 112 is in communication with the user electronic device 102 at least for the purpose of authentication the user for processing the payment transaction.

[0029] Moreover, a merchant database 114 is operationally connected to the WiFi router 104. The merchant database 114 serves at least to store enrolment information of the

user, and payment instrument data associated with a user payment instrument for processing the payment transaction. The enrolment information includes a user device identifier associated with the user electronic device 102 and a router identifier associated with the WiFi router 104. The enrolment information also provides for other enrolment details such as a date and time of the enrolment, expiry date of the enrolment (if any) etc. The payment instrument data comprises at least a payment account identifier. The payment account identifier comprises a user account number (e.g. a user payment card number) or a token associated with the user payment card. The payment instrument data may comprise details associated with the user (a user name, a user's date of birth etc.) and/or other relevant details associated with the payment account identifier (e.g. a card verification code (CVC), an expiry date of the user payment card etc.). A payment terminal database 116 is in communication with the merchant payment terminal 106. The payment terminal database 116 is operative to store payment transaction details. The payment transaction details include a transaction amount, a transaction date and time, a type of the payment instrument used, a payer of the payment transaction etc. A payment network database 118 is in communication with the payment network server 110. The payment network database 118 is operative to store at least pairing details between the user electronic device 102 and the WiFi router 104. In some embodiments, the payment network database 118 stores the payment instrument data as described above in place of or in conjunction with the merchant database 114. Although the merchant database 114, the payment terminal database 116 and the payment network database 118 are shown as external databases in Fig. 1, these databases 114, 116, 118 may form part of the WiFi router 104, the merchant payment terminal 106 and the payment network server 110 respectively. In some embodiments, the merchant database 114, the payment terminal database 116 and the payment network database 118 may also be integrated as a single entity which is connected to the WiFi router 104.

[0030] Embodiments of the present invention aim to provide a means for processing a payment transaction between a merchant and a user using a merchant WiFi network. In particular, the WiFi router 104 provides a local network associated with the merchant for processing payment transactions between the merchant and the user. By integrating payment capabilities directly into the merchant WiFi network, a user would be able to pay through this channel and seamlessly connect to the merchant's payment system each time the user electronic device 102 is within range of the merchant WiFi network. This improves a shopping experience and convenience for the user. Moreover, a hardware requirement of the user electronic device for utilizing this payment route is low – the user

electronic device is simply required to be capable of connecting to a WiFi network and to have a user interface for viewing and approving payment transactions.

[0031] In order to facilitate the above, the WiFi router 104 is configured to: (i) receive a connection request from the user electronic device 102, (ii) determine that the user electronic device 102 is enrolled with the merchant for making payment using the merchant WiFi network, (iii) transmit a connection response indicating that the user electronic device 102 is connected to the WiFi router 104 for paying the payment transaction; (iv) receive a confirmation response to proceed with the payment transaction; (v) retrieve payment instrument data associated with a user payment instrument; and (vi) communicate a payment transaction request for processing the payment transaction. The user electronic device 102 is enrolled with the merchant for making payment using the merchant WiFi network based on a pairing between the user device identifier and the router identifier associated with the WiFi router 104. The user device identifier and the router identifier may each be a media access control (MAC) address uniquely associated with its respective device. Therefore, the pairing between the user electronic device 102 and the WiFi router 104 is unique and provides a form of identification of the user on the merchant WiFi network. The pairing record may be stored in a secure element associated with the WiFi router 104 and/or it may be stored at the payment network database 118. The aforementioned token and the pairing record may be generated and communicated using the 3DS2.0 type of framework.

[0032] Although the WiFi router is described in a manner that is specific to processing payment transactions, it should be appreciated that the WiFi router may be used by the user for other purposes such as for accessing the internet. In an embodiment, the user may be connected to the internet via the steps of (i) to (iii) above. When a payment is to be made or completed, then steps (iv) to (vi) may be performed by the WiFi router 104. For example, when the user is connected to the WiFi router, the following may happen: (i) if the user is new, a registration screen will show up; or (ii) if payment is pending for this user, the payment screen will show up (e.g. in relation to step (iv) above). The user is also allowed to access the internet in the meantime.

[0033] More specifically, the present embodiment builds upon the IEEE 802.11 protocol for implementing wireless local area networks (LANs). The 802.11 protocol has been the standard for interoperability between connected devices and access points (e.g. routers) within a wireless LAN or WiFi network. Access points (APs) are bridges that provide communication between mobile stations (e.g. the user electronic device 102 and/or the merchant payment terminal 106). Prior to making a connection between a mobile station

and an access point, the mobile station is required to be in an appropriate connection state. In particular, for embodiments of the present invention, the mobile station such as the user electronic device 102 is required to be in an authenticated and associated state with the WiFi router 104 before the payment transaction between the user and the merchant can be processed.

[0034] In order to process the payment transaction using the merchant WiFi network, the user electronic device 102 searches for available WiFi networks within its proximity. The user can select, via the user electronic device 102, a desired WiFi network for connection among the available WiFi networks. The user electronic device 102 transmits an initial connection request comprising at least the user electronic device 102 supported data rates. Upon receipt of the initial connection request, the WiFi router 104 is configured to determine if the user electronic device 102 has a compatible supported data rate. If the user electronic device 102 has a compatible data rate, an initial connection response is transmitted from the WiFi router 104 to the user electronic device 102. The initial connection response may comprise the WiFi router 104 supported data rates, encryption types if required, and other 802.11 capabilities of the WiFi router 104. The user can then request to make a connection with the WiFi router 104 with the user electronic device 102.

[0035] The user electronic device 102 then attempts a low-level 802.11 authentication with the WiFi router 104 by sending a low-level 802.11 authentication frame to the WiFi router 104. This sets an initiating authentication to an open setting with a sequence 0x0001. In response to the initiating authentication frame, the WiFi router is configured to respond to the user electronic device 102 with a payment authentication frame which is set to open and indicating a sequence of 0x0002. Once the user electronic device 102 is authenticated, the user electronic device 102 is configured to begin an association process with the WiFi router 104. In particular, the user electronic device 102 can be 802.11 authenticated to multiple WiFi routers 104. This speeds up a subsequent association process when the user electronic device 102 moves between different WiFi routers 104. However, the user electronic device 102 can only be actively associated and transferring data through a single WiFi router 104 at a time.

[0036] In embodiments where the user electronic device 102 is authenticated to multiple WiFi routers 104, the user then selects, via the user electronic device 102, the WiFi router 104 the user electronic device 102 is to be associated with. If only one WiFi router 104 is available, the user electronic device 102 will be configured to associate with the WiFi router 104. In any case, the user electronic device 102 is configured to transmit an

association request to the selected WiFi router 104. The association request contains a chosen payment encryption type (if required) and other compatible 802.11 capabilities. If the elements in the association request match the capabilities of the WiFi router 104, the WiFi router 104 will create an Association ID for the user electronic device 102 and respond with an association response comprising a success message granting payment network access to the user electronic device 102. The user electronic device 102 is successfully associated with the WiFi router 104 at this point and payment transactions can be processed between the user and the merchant using the associated merchant WiFi network.

[0037] In embodiments of the present invention, the WiFi router 104 is configured to commence processing the payment transaction using the Secure Remote Commerce (SRC) framework. For example, an SRC initiator can integrate and display SRC Marks as part of the 802.11 connection authentication page (e.g. a pop-up page/event in the user electronic device 102 for completing an authentication process for connecting to the WiFi router 104). An SRC initiator is an entity or a platform which supports checkout and/or a secure retrieval of payment data from the SRC System. An example of an SRC initiator is a merchant payment service provider. The WiFi router 104 is configured to be identified and associated uniquely to a router identifier or a merchant identifier (MID). Moreover, the WiFi router 104 can be configured to retain a connection record between the user electronic device 102 and the WiFi router 104. The connection record is associated with the user device identifier and the router identifier, and may include the media access control (MAC) addresses uniquely associated with each of the respective devices. The WiFi router 104 is associated or in communication with any number of merchant payment terminals 106 for processing payment transactions. Notably, in embodiments of the present invention, the software or application layer required for processing the payment transaction resides with the WiFi router 104. Therefore, this reduces a need for the user electronic device 102 to install or store the necessary applications for processing the payment transaction. In particular, user electronic devices 102 which do not provide a graphical user interface can still be connected to the WiFi router 104 for processing the payment transaction without a conventional step-by-step checkout as is prevalent in common mobile payment processes or applications.

[0038] To begin processing the payment transaction, the user proceeds to the merchant payment terminal 106 (e.g. a mobile application, a kiosk at a physical store location, a smart speaker etc.) to initiate a transaction request. As described above, the user electronic device 102 is already connected to the merchant WiFi network at this point for making payment through the merchant WiFi network. In some embodiments, the user

electronic device 102 is connected as the payment transaction is being processed at the merchant payment terminal 106. In some embodiments, the merchant initiates a step-up authentication such that at the point of purchase, the user has been authenticated by e.g. a biometric or a PIN using the user electronic device 102. This step-up authentication may be implemented by the issuer institution (e.g. in the form of a SMS one-time password via a 3DS platform, or in the form of a biometric input using an issuer application associated with the issuer institution). Upon receiving the transaction request, the WiFi router 104 is configured to identify the user electronic device 102 (e.g. via the user device identifier), and to retrieve the stored data associated with the user payment instrument. More than one user payment instruments may be stored in association with the WiFi router 104 and/or the merchant. In this case, the user is prompted to select one of the user payment instruments for paying the payment transaction. Unknown users (e.g. a user who has successfully enrolled with the WiFi router 104 and/or the merchant for the first time) are prompted to provide additional data to help with identification. The application provided at the merchant payment terminal 108 is also configured to allow the user to add data associated with a new user payment instrument with the WiFi router 104.

[0039] In some embodiments, the user approaches the merchant payment terminal 106 for making a purchase prior to connecting to the merchant WiFi network. In these cases, the details of the payment transaction can be transmitted together with the connection response to the user electronic device 102 for processing the payment transaction.

[0040] The WiFi router 104 is configured to verify the user credentials (e.g. using 3D secure) for making payment using the selected user payment instrument. For example, an authentication of the user can be carried out using a one-time-password sent by the merchant to a pre-determined user contact (e.g. a mobile number or a user electronic mail address) to verify that the user is entitled to use the selected payment instrument to make the purchase. This verification step is optional. In some embodiments, for example in transactions associated with a small payment amount (e.g. a predetermined payment amount of less than \$100), this verification step is skipped to facilitate quicker processing of payment transactions.

[0041] The WiFi router 104 is configured to request a confirmation from the user electronic device 102 to process the payment transaction. The confirmation can be requested either before or after the above described verification step. The WiFi router 104 is configured to receive a confirmation response from the user electronic device 102 to indicate whether the merchant is approved to proceed with the payment transaction.

Once the confirmation response indicating that the payment transaction is to proceed is received, the WiFi router 104 is configured to communicate a payment transaction request for processing the payment transaction to a payment network (e.g. the payment network server 110). The payment transaction request comprises the payment transaction details and the payment instrument data associated with the user payment instrument for processing the payment transaction. The payment transaction request is communicated from the WiFi router 104 to the payment network server 110 via the acquirer server 108, or it can be communicated to the payment network server 110 directly. The payment transaction request is subsequently processed in a conventional way, similar to that for processing a card-not-present payment transaction.

[0042] In some embodiments, the issuer server 112, after having received the payment transaction request, is configured to authenticate the user prior to authorizing the payment transaction request. The authentication may involve sending a dynamic password to the user or using a predetermined password or any other means. If authentication of the user fails, the enrolled connection to the WiFi router 104 may be terminated or blacklisted. This aids in minimizing fraudulent transactions. In some embodiments, this further authentication step is a requirement by the merchant in order to complete the payment transaction.

[0043] The WiFi router 104 is configured to receive a notification that the payment transaction is successful once the issuer server 112 has authorized the payment transaction. The WiFi router 104 is then configured to transmit a payment approval response indicating whether the payment transaction is approved or refused to the user electronic device 102 and/or the merchant payment terminal 106.

[0044] In order to process payment transactions using the merchant WiFi network as described above, the user electronic device 102 has to be enrolled with the WiFi router 104 of the merchant. The enrolment process is described in relation to Figs. 3 to 8. Embodiments of the present invention provide encryption protocols which are to be followed to ensure that no fraudulent emulations of access points exist that can deceive users into logging onto fraudulent WiFi networks for gaining access to user payment credentials. For example, using the SRC framework, the WiFi router 104 is configured to generate a private key-public key pair during an enrolment of the user electronic device 102. The public key is transmitted to the user electronic device 102 and is preferably stored in a secure element of the user electronic device 102. The private key-public key pair may also be compliant with the EMVCo latency standards. The private key-public key pair may be configured to function as an authorization token to communicate with

the SRC initiator securely on behalf of the user (e.g. similar to the Open Authorization (OAuth) standard). In embodiments, the SRC initiator supports WebAuthn standard for logging in the SRC initiator portal and the WiFi router 104 is configured to register itself as one of the secure tokens for the user. Upon enrolment, the WiFi router 104 is configured to log onto the SRC initiator on behalf of the user using the pre-authorized/enrolled private key-public key pair. The user may revoke this private key-public key pair at any time using the SRC initiator portal. Embodiments of the present invention provide registration of access points using a centralized database and/or a blockchain so that only registered and certified/verified access points or routers that are on-boarded with this WiFi payment scheme are able to process payment transactions as described above. Registration of access points can be done in a similar conventional manner as the enrollment of payment terminals (e.g. POS terminals).

[0045] Although only one user electronic device 102, only one WiFi router 104, only one merchant payment terminal 106, only one acquirer server 108 and only one issuer server 112 are shown in Fig. 1, a plurality of user electronic devices 102, a plurality of WiFi routers 104 associated with respective merchants, a plurality of merchant payment terminals 106 associated with respective merchants, a plurality of acquirer servers 108 associated with respective acquiring institutions and a plurality of issuer servers 112 associated with respective issuing institutions may form part of the computer system 100. Accordingly, a plurality of merchant databases 114 and/or a plurality of payment terminal databases 116 associated with respective merchants may form part of the computer system 100. Each user may be associated with more than one WiFi routers 104 for use in processing payment transactions as described above.

[0046] Communication between the WiFi router 104 and the servers 108, 110, 112 and databases 114, 116 may take place via any type of system, for example, a virtual private system (VPN), the Internet, a local area and/or wide area system (LAN and/or WAN), and so on. The merchant payment terminal 106 may be in communication with the WiFi router 104 using the WiFi local network or directly using a LAN cable.

[0047] Fig. 2 shows steps of a method 200 for processing the payment transaction between the merchant and the user using the merchant WiFi network facilitated by the computer system of Fig. 1. The method 200 is carried out using the WiFi router 104.

[0048] In a step 202, the WiFi router 104 is configured to receive a connection request from the user electronic device 102 for connecting the user electronic device 102 to the merchant WiFi network for paying the payment transaction. The connection request comprises at least a user device identifier associated with the user electronic device. The

user device identifier uniquely identifies the user electronic device 102. In an embodiment, the user device identifier is a layer 2 (data link) address (e.g. MAC address) of the user electronic device 102.

[0049] In a step 204, the WiFi router 104 is configured to determine, using the merchant database 114, that the user electronic device is enrolled with the merchant for making payment using the merchant WiFi network based on a pairing between the user device identifier and a router identifier associated with the WiFi router 104.

[0050] In a step 206, the WiFi router 104 is configured to transmit a connection response to the user electronic device 102 indicating that the user electronic device 102 is connected to the WiFi router 104 for paying the payment transaction. The connection response comprises the details of the payment transaction. The details of the payment transaction include a payment amount associated with the payment transaction, methods or modes of payment, user payment instrument details, a time and date of the payment transaction, name of the merchant etc. The connection response comprises one or more of the above listed details. In some embodiments, the connection response includes one or more of the following: (i) a response that the payment instrument has been successfully paired with the router inclusive of all security features, (ii) a notification of any transactions charged against the authorized payment instrument (e.g. credit, debit, prepaid), (iii) a notification of any reconnection to the WiFi network (e.g. in the form of “welcome back, you are now paired with our network and express checkout payment”), and (iv) a notification of any previous termination (either initiated by the user or the merchant) of the pairing. The connection response may comprise a confirmation request requesting the user to confirm that the user wishes to proceed with processing the payment transaction. In some embodiments, the confirmation request can be transmitted from the WiFi router 104 to the user electronic device 102 separately from the connection response. In embodiments where the user has registered more than one user payment instruments with the WiFi router 104, the user is prompted to select one of the more than one user payment instruments to be used for processing the payment transaction.

[0051] In a step 208, the WiFi router 104 is configured to receive a confirmation response for the merchant to proceed with the payment transaction from the user electronic device 102. The confirmation response indicates if the user wishes to proceed with processing the payment transaction.

[0052] In a step 210, the WiFi router 104 is configured to retrieve payment instrument data associated with the user payment instrument from the merchant database 114 in

response to the confirmation response to proceed with the payment transaction. The payment instrument data may comprise a payment account identifier (for example, a payment card number or a token associated with the payment card number). In embodiments where there is more than one registered user payment instruments with the merchant database 114, the WiFi router 104 is configured to retrieve the payment instrument data associated with the selected user payment instrument as indicated by the user.

[0053] In a step 212, the WiFi router 104 is configured to communicate a payment transaction request to the payment network server 110 for processing the payment transaction. The payment transaction request is communicated from the WiFi router 104 (e.g. associated with a merchant server) via the acquirer server 108 or via a SRC initiator or directly with the payment network server 110. The payment transaction request comprises the payment transaction details and the payment instrument data for processing the payment transaction. As described above, the issuer server 112 may be configured to authenticate the user associated with the user electronic device 102 prior to authorizing the payment transaction request. Once the payment transaction has been authorized, the WiFi router 104 is configured to receive a notification of the same from the issuer server 112. The WiFi router 104 is then configured to transmit a payment approval response indicating whether the payment transaction is approved or refused to the user electronic device 102.

[0054] Fig. 3 shows steps of a method 300 for enrolling the user for payment using the merchant WiFi network facilitated by the computer system of Fig. 1. The method 300 is carried out using the WiFi router 104 and may be performed prior to or at the time of processing the payment transaction as described in Fig. 2.

[0055] In a step 302, the WiFi router 104 is configured to transmit a pairing request for pairing the user device identifier with the router identifier to the user electronic device 102. The pairing request may be transmitted via a captive portal associated with the merchant WiFi network. A captive portal is a web page which is displayed to newly connected users of a WiFi network before they are granted broader access to network resources. A captive portal provides a means to authenticate the users prior to granting permission for them to connect to the WiFi network. The user device identifier and the router identifier is each uniquely associated with the user electronic device 102 and the WiFi router 104 respectively. The user device identifier and/or the router identifier may be a MAC address.

[0056] In a step 304, the WiFi router 104 is configured to receive a pairing response indicating the user's approval of said pairing from the user electronic device 102.

[0057] In a step 306, the WiFi router 104 is configured to store details of said pairing in the merchant database 114 in response to the pairing response in the step 304. The details of the pairing include at least the user device identifier and the router identifier. In an embodiment where the method is implemented in the SRC technical framework, the details of the pairing include at least the user's SRC profile. The details of the pairing may include the date and/or time of the pairing request, a name of the user and other relevant details (e.g. identification (ID) number, contact details, birthday etc.) of the user. Although in the present embodiment the details of said pairing between the user electronic device 102 and the WiFi router 104 is stored in the may be stored in a secure element of the WiFi router 104 or the payment network server database 118.

[0058] Fig. 4 shows further steps in a method 400 for enrolling the user for payment using the merchant WiFi network facilitated by the computer system of Fig. 1. The method 400 is carried out by the WiFi router 104 after the method 300 as described in relation to Fig. 3.

[0059] In a step 402, the WiFi router 104 is configured to transmit a payment instrument request to the user electronic device 102 in response to the user's approval of said pairing. The payment instrument request comprises a request for the user to include payment instrument details to be used for processing payment transactions.

[0060] In a step 404, the WiFi router 104 is configured to receive a payment instrument response comprising details of the user payment instrument from the user electronic device 102. The details of the user payment instrument may include a user account number (e.g. a user payment card number), details associated with the user (a user name, a user's date of birth etc.) and/or other information such as a card verification coded (CVC), an expiry date of the payment card etc.

[0061] In a step 406, the WiFi router 104 is configured to transmit the details of the user payment instrument to the payment network server 110 for tokenization of the user payment instrument. In some embodiments, in order to issue a payment token for the tokenization request, the user is authenticated. The user may be authenticated by the payment network server 110 or the issuer server 112 using a one-time-password which is sent to the user electronic device 102 or by using predetermined passwords or by providing correct answers to predetermined security questions. In some embodiments, the payment network server 110 forwards the details of the user payment instrument to

the issuer server 112 for generating the payment token associated with the user payment instrument.

[0062] In a step 408, the WiFi router 104 is configured to receive the payment token associated with the user payment instrument from the payment network server 110. The payment token may be any string of numbers, alphabets or alphanumeric associated with the user payment instrument and which replaces the details associated with the user payment instrument for use in processing the payment transaction.

[0063] In a step 410, the WiFi router 104 is configured to store, on the merchant database 114, the payment token against the user device identifier.

[0064] Fig. 5 shows steps of a first method 500 for authenticating the merchant during enrollment of the user for payment using the merchant WiFi network facilitated by the computer system of Fig. 1. The method 500 is carried out by the WiFi router 104 and may be performed in addition to the methods 300, 400 during the enrollment of the user.

[0065] In a step 502, the WiFi router 104 is configured to transmit a password input request to the user electronic device 102. The password input request comprises a request for the user to retrieve the password from the merchant payment terminal 106. In an embodiment, an identity of the user electronic device 102 (e.g. a name associated with the user electronic device 102) is displayed at the merchant payment terminal 106 once the password is received. The user can then retrieve the relevant password at the merchant payment terminal 106 using the identity of the user electronic device 102. In an embodiment, the password may be a one-time password (OTP). The OTP may be generated by the issuing institution associated with the user payment instrument provided in the step 404. The OTP may be generated in compliance with the 3DS standard. In an embodiment, the OTP may be generated if and when the thresholds for transaction are breached.

[0066] In a step 504, the WiFi router 104 is configured to receive a password input response comprising a password input from the user electronic device 102. The user is prompted to enter the password retrieved from the merchant payment terminal 106 as the password input and transmits it to the WiFi router 104 for verification.

[0067] In a step 506, the WiFi router 104 is configured to verify that the password input matches the generated password. The payment instrument request as described in the step 402 is transmitted to the user electronic device if the password input is verified. In

this way, a successful verification of the password input authenticates the merchant and ensures that the enrollment process is performed correctly.

[0068] The above method 500 aids in authenticating an identity of the merchant since the password is randomly and uniquely generated for each enrollment process, and is securely transmitted to the merchant payment terminal 106.

[0069] Fig. 6 shows steps of a second method 600 for authenticating the merchant during enrollment of the user for payment using the merchant WiFi network facilitated by the computer system of Fig. 1. The method 600 is carried out by the WiFi router 104 and may be performed in addition to the methods 300, 400 during the enrollment of the user.

[0070] In a step 602, the WiFi router 104 is configured to transmit a network password input request to the user electronic device 102. The network password input request comprises a request for a network password. The network password may be any string of numbers or alphanumeric. The network password may be randomly generated by the WiFi router 104 or is predetermined by the merchant. In any case, the network password is uniquely associated with the merchant and the WiFi router 104. An example of a network password is a password associated with the network name (SSID) of the WiFi router 104.

[0071] In a step 604, the WiFi router 104 is configured to receive a network password input response from the user electronic device 102. The network password input response comprises a network password input. Similar to connecting to the merchant WiFi network, the user may be prompted by the WiFi router 104 to enter the network password again in this step 604.

[0072] In a step 606, the WiFi router 104 is configured to verify that the network password input matches the network password. The payment instrument request as described in the step 402 is transmitted to the user electronic device if the network password input is verified. In this way, a successful verification of the network password input authenticates the merchant and ensures that the enrollment process is performed correctly.

[0073] Fig. 7 illustrates the steps for enrolling the user for payment using the merchant WiFi network.

[0074] Once the user electronic device 102 is connected to the merchant WiFi network, the user electronic device 102 is configured to transmit a pairing request to the WiFi router 104 in a step 702. The pairing request comprises a request for pairing or associating the

user device identifier with the router identifier. The user device identifier and the router identifier may be a layer 2 (data link) address (e.g. a MAC address) which is uniquely associated with the user electronic device 102 and the WiFi router 104 respectively. In a step 704, the WiFi router 104 is configured to receive a pairing response from the user electronic device 102 indicating the user's approval of said pairing. Once the user's approval for the pairing is received in the step 704, the WiFi router 104 is configured to store details of said pairing on the merchant database 114 in response to the pairing response in a step 706. The details of the pairing include at least the user device identifier and the router identifier. The details of the pairing may further include the date and/or time of the pairing request, a name of the user and/or other relevant details (e.g. identification (ID) number, contact details, birthday etc.) of the user. In a step 708, the WiFi router 104 is configured to transmit a payment instrument request to the user electronic device 102 in response to the user's approval of said pairing received in the step 704. The payment instrument request comprises a request for the user to include payment instrument details to be used for processing payment transactions with the merchant. In a step 710, the WiFi router 104 is configured to receive a payment instrument response comprising details of the user payment instrument from the user electronic device 102. The details of the user payment instrument may include a user account number (e.g. a user payment card number), details associated with the user (a user name, a user's date of birth etc.) and/or other information such as a card verification coded (CVC), an expiry date of the payment card etc. Upon receipt of the details of the user payment instrument, the WiFi router 104 is configured to transmit the details of the user payment instrument to the payment network server 110, e.g. via the acquirer server 108 (not shown in Fig. 7), for tokenization of the user payment instrument. Tokenization of the user payment instrument may be carried out by the payment network server 110 or the issuer server 112.

[0075] In a step 714, the payment network server 110 is configured to generate a payment token associated with the user payment instrument in response to the tokenization request. In an embodiment where the present method is implemented using the SRC technical framework, the token is generated by a SRC system. A SRC system is an entity which orchestrate all activities between participants of the SRC framework/program. An SRC system may comprise a payment scheme or a payment network (e.g. Mastercard®). In some embodiments, the user is authenticated prior to the generation of the payment token. The payment token may be any string of numbers, alphabets or alphanumeric associated with the user payment instrument and which replaces the details associated with the user payment instrument for use in processing

the payment transaction. In a step 716, the WiFi router 104 is configured to receive the generated payment token associated with the user payment instrument from the payment network server 110 (or the issuer server 112). Upon receipt of the payment token, the WiFi router 104 is configured to store the payment token against the user device identifier in the merchant database 114. In some embodiments, once the enrollment is successful, the user electronic device 102 is configured to store the router identifier. Connection with the WiFi router 104 for payment is available only if the router identifier is the same as that at the time of enrollment.

[0076] Fig. 8 illustrates the steps of two different methods 802, 804 for authenticating the merchant during enrollment of the user for payment using the merchant WiFi network. Each of the methods 802, 804 can be used in conjunction with the steps as described above in Fig. 7. In particular, either one of the methods 802, 804 can be incorporated in the enrollment process prior to requesting from the user electronic device 102 the details of the user payment instrument in the step 708.

[0077] Under the SRC framework, the WiFi router 104 is configured to generate a private key-public key pair during an enrolment of the user electronic device 102. The public key is transmitted to the user electronic device 102 and is preferably stored in a secure element of the user electronic device 102. The private key-public key pair may also be compliant with the EMVCo latency standards. The private key-public key pair may be configured to function as an authorization token to communicate with the SRC initiator securely on behalf of the user (e.g. similar to the Open Authorization (OAuth) standard). In embodiments, the SRC initiator supports WebAuthn standard for logging in the SRC initiator portal and the WiFi router 104 is configured to register itself as one of the secure tokens for the user. This aforementioned process may take place once the user has authenticated himself/herself using the methods 802 and 804 as described below. In an embodiment, the user logs in to his SRC profile before authorizing the merchant to associate the private key-public key pair for authentication via the WebAuthn. It may therefore involve an input from the user's device when logging in through the captive portal for the first time.

[0078] In the method 802, the WiFi router 104 is configured to transmit a password input request to the user electronic device 102 to request the user to retrieve a password from the merchant payment terminal 106 in a step 806. The password may be a predetermined password associated with the merchant and it may be received using a captive portal associated with the merchant WiFi network. In some embodiments, the password may be a one-time password (OTP). The OTP may be generated by the

issuing institution associated with the user payment instrument provided in the step 404. The OTP may be generated in compliance with the 3DS standard. In an embodiment, the OTP may be generated if and when the thresholds for transaction are breached. Upon receipt of the password input request, the user is to retrieve the password from the merchant payment terminal 106 and to input it at the user electronic device 102 as a password input in response to the password input request in a step 808. In some embodiments, there is a predetermined time-limit for a validity of the generated password within which the user is required to retrieve the password from the merchant payment terminal 106 and to transmit it to the WiFi router 104 to complete the verification process. The predetermined time limit may be determined by the merchant, and it can be 1 minute, 2 minutes, 3 minutes, 5 minutes, 10 minutes, 30 minutes, 1 hour or any other suitable time range. In a step 810, the user electronic device 102 is configured to transmit a password input response comprising the password input to the WiFi router 104. Upon receipt of the password input response, the WiFi router 104 is configured verify that the password input matches the generated password in a step 812.

[0079] In the method 804, the WiFi router 104 is first configured to transmit a password input request to the user electronic device 102 in a step 814. The password input request comprises a request for a network password. The user electronic device 102 is configured to transmit a password input response comprising a network password input to the WiFi router 104 in a step 816. The network password is typically a password associated with the merchant WiFi network. In a step 818, the WiFi router 104 is configured to verify that the network password input matches the network password. In some embodiments, the WiFi router 104 is configured to use the network password which the user has already entered for securely connecting to the merchant WiFi network for verifying the merchant so that the method 804 is done automatically without any active input from the user (e.g. in the background of the enrollment process).

[0080] Fig. 9 illustrates the steps of the method 900 for processing the payment transaction between the merchant and the user using the merchant WiFi network.

[0081] In order to initiate the payment transaction, the user electronic device 102 is required to be first connected to the merchant WiFi network. Typically, the user enters a physical store associated with the merchant and finds the merchant WiFi network on a list of WiFi networks available to be connected on the user electronic device 102. In a step 902, the user electronic device 102 transmits a connection request to the WiFi router 104 for connecting the user electronic device 102 to the merchant WiFi network. The connection request comprises at least a user device identifier associated with the user electronic

device. In a step 904, the WiFi router 104 is configured to determine, using the merchant database 114, whether the user electronic device 102 is enrolled with the merchant for making payment using the merchant WiFi network. The user electronic device 102 is enrolled with the merchant if there exists a pairing between the user device identifier and the router identifier (the pairing process is described in Fig. 4). Once it is determined that the user electronic device 102 is enrolled, the WiFi router 104 is configured to transmit a connection response indicating that the user electronic device 102 is connected to the router 104 for processing the payment transaction to the user electronic device 102 in a step 906. The connection response comprises at least the details of the payment transaction. The details of the payment transaction include a payment amount associated with the payment transaction, methods or modes of payment, user payment instrument details, a time and date of the payment transaction, name of the merchant etc.

[0082] In some embodiments, the details associated with the payment transaction is not comprised in the connection response. In these cases, an optional step 908 (shown as a dotted line arrow) is performed. Once the user electronic device 102 is connected to the WiFi router 104 for making payment, the payment transaction is initiated by the user at the merchant payment terminal 106. The application available at the merchant payment terminal 106 displays all the user electronic devices which are paired for payments and connected to the merchant WiFi network. The merchant selects the user electronic device 102 from the list of available user electronic devices 102 to initiate the transaction request. In the optional step 908, the merchant payment terminal 106 is configured to transmit a transaction request to the WiFi router 104. The transaction request comprises the details of the payment transaction for processing the payment transaction.

[0083] In any case, a confirmation request inviting the user to confirm that the user wishes to proceed with processing the payment transaction is transmitted from the WiFi router 104 to the user electronic device 102 in a step 910. In embodiments where the user has registered more than one user payment instruments with the WiFi router 104, the user is prompted to select one of the user payment instruments to be used for processing the payment transaction. In some embodiments, the confirmation request comprises a portion of the details of the user payment instruments (e.g. last 4 digits of a payment card number) for the user to select the user payment instrument to be used for processing the payment transaction. The confirmation request may include a tip amount field for the user to offer a tip to the merchant. In a step 912, the user electronic device 102 is configured to transmit a confirmation response to the WiFi router 104 to indicate if the user wishes to proceed with processing the payment transaction. In embodiments where more than one user payment instruments are registered with the WiFi router 104,

the confirmation response comprises an indication of the selected user payment instrument for use in paying the payment transaction.

[0084] If the confirmation response is received by the WiFi router 104 indicating that the user wishes to proceed with processing the payment transaction, the WiFi router 104 is configured to retrieve the payment instrument data associated with the user payment instrument from the merchant database 114 in a step 914. In embodiments where there are more than one registered user payment instruments with the merchant database 114, the WiFi router 104 is configured to retrieve the payment instrument data associated with the selected user payment instrument as indicated by the user. Once the data associated with the user payment instrument is retrieved in the step 914, the WiFi router 104 is configured to transmit a payment transaction request for processing the payment transaction to the payment network server 110. The payment transaction request can be transmitted via the acquirer server 108 or directly to the payment network server 110. The payment transaction request comprises the payment transaction details and the payment instrument data for processing the payment transaction. The payment network server 110 then forwards the payment transaction request to the issuer server 112 for authorizing the payment transaction. In some embodiments, the issuer server 112 is configured to authenticate the user prior to authorizing the payment transaction request. Once the payment transaction has been authorized (e.g. if the user has been authenticated), the issuer server 112 is configured to transmit a payment transaction response to the payment network server 110 which in turn forwards it to the WiFi router 104 in a step 918. The payment transaction response comprises an indication of whether the payment transaction is approved or refused. Once the WiFi router 104 has received the payment transaction response in the step 918, the WiFi router 104 is configured to transmit the transaction response to the merchant payment terminal 106 in a step 920 and to communicate the results for the payment transaction to the user electronic device 102 in a step 922.

[0085] Fig. 10 is a block diagram showing a technical architecture of the WiFi router 104.

[0086] The technical architecture includes a processor 1002 (which may be referred to as a central processor unit or CPU) that is in communication with memory devices including secondary storage 1004 (such as disk drives), read only memory (ROM) 1006, and random access memory (RAM) 1008. The processor 1002 may be implemented as one or more CPU chips. The technical architecture may further comprise input/output (I/O) devices 1010, and system connectivity or network devices 1012.

[0087] The secondary storage 1004 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 1008 is not large enough to hold all working data. Secondary storage 1004 may be used to store programs which are loaded into RAM 1008 when such programs are selected for execution.

[0088] In some embodiments, the secondary storage 1004 has a processing component 1004a comprising non-transitory instructions operative by the processor 1002 to perform various operations of the method of the present disclosure. The ROM 1006 is used to store instructions and perhaps data which are read during program execution. The secondary storage 1004, the ROM 1006, and/or the RAM 1008 may be referred to in some contexts as computer readable storage media and/or non-transitory computer readable media.

[0089] I/O devices 1010 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 input devices.

[0090] The system connectivity or network devices 1012 may take the form of modems, modem banks, Ethernet cards, universal serial bus (USB) interface cards, serial interfaces, token ring cards, fibre distributed data interface (FDDI) cards, wireless local area system (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 system devices. These system connectivity or network devices 1012 may enable the processor 1002 to communicate with the Internet or one or more intranets. With such a system connection, it is contemplated that the processor 1002 might receive information from the system, or might output information to the system 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 1002, may be received from and outputted to the system, for example, in the form of a computer data signal embodied in a carrier wave.

[0091] The processor 1002 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 1004), flash drive, ROM 1006, RAM 1008, or the system connectivity or network devices 1012. While only one processor 1002 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.

[0092] 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 to provide the functionality of a number of servers that is not directly bound to the number of computers in the technical architecture. In an embodiment, the functionality disclosed above may be provided by executing an application and/or applications in a cloud computing environment. Cloud computing may comprise providing computing services via a system 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.

[0093] It is understood that by programming and/or loading executable instructions onto the technical architecture, at least one of the CPU 1002, the ROM 1006, and the RAM 1008 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.

[0094] Whilst the foregoing description has described exemplary embodiments, it will be understood by those skilled in the art that many variations of the embodiments can be made within the scope of the present invention as defined by the claims. Moreover, features of one or more embodiments may be mixed and matched with features of one or more other embodiments.

Claims

1. A WiFi router for processing a payment transaction between a merchant and a user using a merchant WiFi network connected to the router, the router comprising a computer processor and a data storage device, the data storage device storing instructions operable to cause the processor to:

receive, from a user electronic device, a connection request for connecting the user electronic device to the merchant WiFi network for paying the payment transaction, the connection request comprising a user device identifier associated with the user electronic device;

determine, using a merchant database, that the user electronic device is enrolled with the merchant for making payment using the merchant WiFi network based on a pairing between the user device identifier and a router identifier associated with the router;

transmit, to the user electronic device, a connection response indicating that the user electronic device is connected to the router for paying the payment transaction, the connection response comprising details of the payment transaction;

receive, from the user electronic device, a confirmation response for the merchant to proceed with the payment transaction;

retrieve, from the merchant database, payment instrument data associated with a user payment instrument in response to the confirmation response to proceed with the payment transaction, the payment instrument data comprises a payment account identifier; and

communicate, to a payment network server, a payment transaction request for processing the payment transaction, the payment transaction request comprising the payment transaction details and the payment instrument data.

2. The router of claim 1, wherein the payment transaction details comprise a payment amount associated with the payment transaction.

3. The router of claim 1 or claim 2, wherein the data storage device further comprises instructions operative by the processor to: transmit, to the user electronic device, a payment approval response indicating whether the payment transaction is approved or refused.

4. The router of any one of claims 1 to 3, wherein the data storage device further comprises instructions operative by the processor to perform an enrolment procedure, the enrolment procedure comprising:

transmitting, to the user electronic device, a pairing request for pairing a user device identifier with the router identifier;

receiving, from the user electronic device, a pairing response indicating the user's approval of said pairing; and

storing details of said pairing in the merchant database.

5. The router of claim 4, wherein the enrolment procedure further comprises:

transmitting, to the user electronic device, a payment instrument request in response to the user's approval of said pairing;

receiving, from the user electronic device, a payment instrument response comprising details of the user payment instrument;

transmitting, to the payment network server, the details of the user payment instrument for tokenization of the user payment instrument;

receiving, from the payment network server, a payment token associated with the user payment instrument; and

storing, on the merchant database, the payment token against the user device identifier.

6. The router of claim 5, wherein the enrolment procedure further comprises:

transmitting, to the user electronic device, a password input request comprising a request for the user to retrieve a password from a merchant payment terminal;

receiving, from the user electronic device, a password input response comprising a password input; and

verifying that the password input matches the password, the payment instrument request is transmitted to the user electronic device if the password input is verified.

7. The router of claim 5, wherein the enrolment procedure further comprises:

transmitting, to the user electronic device, a network password input request comprising a request for a network password;

receiving, from the user electronic device, a network password input response comprising a network password input; and

verifying that the network password input matches the network password, the payment instrument request is transmitted to the user electronic device if the network password input is verified.

8. The router of any one of claims 5 to 7, wherein the payment token is generated by the payment network server.

9. The router of any one of claims 5 to 8, wherein the payment token associated with the user payment instrument is associated with the user device identifier and the router identifier so that the payment token is valid only for payment transactions made through the user electronic device and the router.

10. The router of any one of claims 1 to 9, wherein the user device identifier and/or the router identifier comprises a media access control (MAC) address.

11. A computer implemented method for processing a payment transaction between a merchant and a user using a merchant WiFi network connected to a router, the method comprising:

receiving, from a user electronic device, a connection request for connecting the user electronic device to the merchant WiFi network for paying the payment transaction, the connection request comprising a user device identifier associated with the user electronic device;

determining, using a merchant database, that the user electronic device is enrolled with the merchant for making payment using the merchant WiFi network based on a pairing between the user device identifier and a router identifier associated with the router;

transmitting, to the user electronic device, a connection response indicating that the user electronic device is connected to the router for paying the payment transaction, the connection response comprising details of the payment transaction;

receiving, from the user electronic device, a confirmation response for the merchant to proceed with the payment transaction;

retrieving, from the merchant database, payment instrument data associated with a user payment instrument in response to the confirmation response to proceed with the payment transaction, the payment instrument data comprises a payment account identifier; and

communicating, to a payment network server, a payment transaction request for processing the payment transaction, the payment transaction request comprising the payment transaction details and the payment instrument data.

12. The method of claim 11, wherein the payment transaction details comprise a payment amount associated with the payment transaction.

13. The method of claim 11 or claim 12 further comprising:

transmitting, to the user electronic device, a payment approval response indicating whether the payment transaction is approved or refused.

14. The method of any one of claims 11 to 13 further comprising performing an enrolment procedure, the enrolment procedure comprising:

transmitting, to the user electronic device, a pairing request for pairing a user device identifier with the router identifier;

receiving, from the user electronic device, a pairing response indicating the user's approval of said pairing; and

storing details of said pairing in the merchant database.

15. The method of claim 14, wherein the enrolment procedure further comprises:

transmitting, to the user electronic device, a payment instrument request in response to the user's approval of said pairing;

receiving, from the user electronic device, a payment instrument response comprising details of the user payment instrument;

transmitting, to the payment network server, the details of the user payment instrument for tokenization of the user payment instrument;

receiving, from the payment network server, a payment token associated with the user payment instrument; and

storing, on the merchant database, the payment token against the user device identifier.

16. The method of claim 15, wherein the enrolment procedure further comprises:

transmitting, to the user electronic device, a password input request comprising a request for the user to retrieve a password from a merchant payment terminal;

receiving, from the user electronic device, a password input response comprising a password input; and

verifying that the password input matches the password, the payment instrument request is transmitted to the user electronic device if the password input is verified.

17. The method of claim 15, wherein the enrolment procedure further comprises:

transmitting, to the user electronic device, a network password input request comprising a request for a network password;

receiving, from the user electronic device, a network password input response comprising a network password input; and

verifying that the network password input matches the network password, the payment instrument request is transmitted to the user electronic device if the network password input is verified.

18. The method of any one of claims 15 to 17, wherein the enrolment procedure further comprises receiving, from the user electronic device, an authorization to use the payment token for processing the payment transaction.

19. The method of any one of claims 15 to 18, wherein the payment token is associated with the user device identifier and the router identifier so that the payment token is valid only for payment transactions made through the user electronic device and the router.

20. A non-transitory computer-readable medium having stored thereon program instructions for causing at least one processor to perform the method of claim 11.