SECURE MOBILE FINANCIAL TRANSACTION SYSTEM AND METHODS

BACKGROUND

The rapid popularization of communication devices saw rapid growth of people possessing them. A communication device described herein is a device which is free to move within a service area formed by a mobile communication network and wirelessly connects to and communicates with a desired counter party whenever and wherever. Typically, it has an operating system (OS), and can run various types of application software, known as apps. Users interact with such apps through high-resolution touchscreens, while gaining access to high-speed data access via including, but not limited to Wi-Fi and mobile broadband. Other functions include but not limited to, having portable media players, digital cameras, pocket video cameras, GPS navigation units, and other peripheral modules. As such, communication devices are capable of combining with card reading devices to evolve into a new breed of mobile transaction terminal. A simple transaction server serves as a control gateway between these mobile transaction terminals and the Acquirer, typically a bank or a card scheme. However, transaction cards contain highly sensitive cardholder information that requires special transmission and storage. Known systems present certain security compliance drawbacks, where security is not focally designed to operate as an integrated system throughout the Cardholder Data Environment (CDE) ecosystem. Hence, this give opportunities for hackers and fraud syndicates to gain entry point into the network, stealing valuable customer information or inject spyware. Another drawbacks of existing systems is the accidental unauthorized storage of sensitive data in memory cache, demiliarized zone (DMZ) or exposed perimeter networking. Hence, many are not in compliant with the payment card industry standards such as PCI DSS.

OBJECTS OF THE INVENTION

An object of the present invention is to enhance security on the mobile financial transaction system that either uses the secured information of transaction cards, or highly sensitive details necessary for effecting a transaction. They system comprises of an apparatus, a communication protocol, and a gateway processor.

An object of the present invention is to provide methods for effecting a secure mobile financial transaction that uses either uses the secured information of transaction cards, or highly sensitive details necessary for effecting a transaction.

SUMMARY OF THE INVENTION

The disclosed invention addresses the drawbacks of existing systems and methods by offering system security compliance.

In an embodiment, through security algorithm set in the software application, un-identified transaction device will not couple with the communication device.

In an embodiment, an encryption module implemented at the transaction device for simultaneous encryption of card information upon reading.

In an embodiment, a communication protocol comprises of standardized interchange message format that exchange encrypted transaction information there between the apparatus and the gateway processor.

In an embodiment, the interchange message discloses information format necessary for effective communication there between the transaction device and the gateway processor, which comprises, but not limited to message functions, message classes, message origins, data elements and code values.

In one exemplary embodiment, a hardware security module (HSM), a software security module (SSM), a key management module, a cryptographic module, or any combination thereof, are implemented at the gateway processor to manage the transmission of encrypted and decrypted card information and transaction messages.
In an embodiment, a risk management module implemented at the gateway processor analyzes any unusual or suspicious activities at the apparatus, including but not limited to faulty card, technical fallback, manual entry of card information.

In an embodiment, system management module implemented at the gateway processor automatically updates the latest version of security protection for the system.

In an embodiment, the gateway processor stores a master key in its security module.

In an embodiment, the master key generates the primary key based on the transaction device's identification.

In an embodiment, the primary key further generates secondary keys. Such secondary keys are shared between the transaction device and the gateway processor.

In an embodiment, the secondary key further generates one-off keys.

In an embodiment, during the transmission of transaction message from the transaction device to the gateway processor, the said one-off key is used to encrypt the transaction message.

In an embodiment, the said transaction message and the transaction device identification are encapsulated, and sent through the communication protocol.

In an embodiment, the encapsulated message is decapsulated in the gateway processor. An one-off key is used to decrypt the said message.

In an exemplary embodiment of the present disclosure, through the use of global positioning system (GPS) already present in the communication device, the actual physical geolocation of the financial transaction which took place is reflected on the electronic receipt.

In another exemplary embodiment of the present disclosure, through the use of digital camera already present in the communication device, the image of the person associated with the financial transaction is captured and reflected on the electronic receipt.

In yet another further exemplary embodiment of the present disclosure, through the biometric identification already present in the communication device, the fingerprint of the person associated with the financial transaction is captured and reflected on the electronic receipt.

In a further another exemplary embodiment of the present disclosure, derived unique key per transaction is used for dynamic key encryption purpose.

In a further still exemplary embodiment of the present disclosure, electronic signature (eSignature) module is implemented for signature verification purpose.

In yet another exemplary embodiment of the present disclosure, electronic signature captured for display on the electronic receipt is masked for security purpose.

In yet another exemplary embodiment of the present disclosure, electronic signature is digitally deconstructed and stored in the gateway processor. The deconstructed data is reconstructed to form into an original receipt format, serving purposes such as, but not limited to chargeback disputes.

Advantageously, with the present invention disclosures, transaction security is greatly enhanced since

any payment card fraud cases can be easily traced.

In an embodiment, the presence of dynamic currency converter (DCC) supports real-time conversion of foreign currency into local one.

In another exemplary embodiment of the present disclosure, a method is provided to reduce the probability of erraneous bid and ask price entry by user.

In an embodiment, a method is provided for re-writing transaction card information for the purpose of adding monetary value in the store-value card.

In an embodiment, the PED present in the transaction device satisfies transaction requirements that may use static PIN for authentication

In an embodiment, the PED present in the transaction device satisfies transaction requirements that may use dynamic PIN for authentication

In an embodiment, the PED present in the transaction device satisfies transaction requirements that may use online PIN for authentication

In an embodiment, the PED present in the transaction device satisfies transaction requirements that may use offline PIN for authentication

In one exemplary embodiment of the present disclosure, a system is provided to allow user gain access to periodical bill payments through the software application.

In accordance to yet still another embodiment of this invention, the transaction device provides the functionality that can operate with existing NFC contactless magswipe transaction card.

In accordance to yet still another embodiment of this invention, the transaction device provides the functionality that can operate with existing NFC contactless EMV transaction card.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates a flow diagram showing a system communication in accordance with an non-restrictive illustrative embodiment of the present invention there between the apparatus and gateway processor via communication protocol.

FIG. 2 illustrates a flow diagram of the connectivity link between the transaction device and the communication device.

FIG. 3 illustrates a flow diagram of the security protocol from the apparatus to the gateway processor in accordance with an non-restrictive illustrative embodiment of the present invention.

FIG. 4 illustrates a flow diagram of the security protocol from the gateway processor to the apparatus in accordance with an non-restrictive illustrative embodiment of the present invention.

FIG. 5 illustrates a flow diagram of the risk assessment on the financial transactions effected in the system in accordance with an non-restrictive illustrative embodiment of the present invention.

FIG. 6a illustrates the perspective back view of a transaction device linked to a communication device.

FIG. 6b illustrates the perspective view of a transaction device linked to a communication device.

FIG. 7a illustrates the perspective back view of a transaction device linked to a communication device in one housing.

FIG. 7b illustrates the perspective view of a transaction device linked to a communication device in one housing.

FIG. 8 illustrates a flow chart of bill payment process in accordance with an non-restrictive illustrative embodiment of the present invention.

FIG. 9 illustrates a flow chart of monetary value-adding to a store-value card process with an non-restrictive illustrative embodiment of the present invention .

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

Generally stated and in accordance with an embodiment of the invention, there is provided a system and methods for performing secured financial transactions with mobility function using a transaction card, with an apparatus through a gateway processor via a communication protocol.

FIG. 1 shows a transaction network 100 including a transaction apparatus 10, a communication protocol 20 and a gateway processor 30. The apparatus 10 comprises of the coupling of transaction device 12 and communication device 14, of which the said coupling is controlled by software

application 16. The communication protocol 20 functions as a message standard exchange there between the apparatus 10 and the gateway processor 30

FIG. 2 shows the connectivity 200 between the transaction device 202 and the communication device 206 in the apparatus 10. The connectivity link 204 is selected from the group consisting of cable, a wireless connection, an analog channel, a hands-free interface, a tethering interface, a Blue-tooth, a USB, a Wifi, radio frequency communication, microwave communication and infrared communication and any combination thereof

FIG. 3 shows a security protocol 300, where encrypted message 322 is transmitted from the apparatus 10 to the gateway processor 30. The gateway processor 30 holds a master key 302 that it stored. This master key 302 will generate primary key 204, after which the primary key 304 is discarded. Prior to the discard, a secondary key 306 is generated, from which one-off key 308 are further generated. The secondary key 306 is shared between the apparatus 10 and the gateway processor 30, of which the secondary key 306 in apparatus 10 is used to generate one-off key 308 for encryption purpose, while an identical secondary key 306 in gateway server 30 is used to generate one-off key 308 for decryption purpose. Read data 320 captured is encrypted with one-off key 308 to become encrypted message 322. Encrypted message 322 is further encapsulated through transaction device ID 324 to become encapsulated message 326, which is transmitted to the gateway processor 30. When encapsulated message 326 reached gateway processor 30, it is decapsulated through the authentication of the same transaction device ID 324 to obtain encrypted message 322. Read data 320 is thus obtained by using the one-off key 308 to decrypt the encrypted message 322.

FIG. 4 shows a security protocol 400, where encrypted message 408 is transmitted from the gateway processor 30 to the apparatus 10. A secondary key 402 is generated, from which one-off key 404 is further generated. The secondary key 402 is shared between the gateway server 30 and the apparatis 10, of which the secondary key 402 in gateway server 30 is used to generate one-off key 404 for encryption purpose, while an identical secondary key 402 in apparatus 10 is used to generate one-off key 408 for decryption purpose. Data 406 is encrypted with one-off key 404 to become encrypted message 408. Encrypted message 408 is further encapsulated through transaction device ID 410 to become encapsulated message 412, which is transmitted to the apparatus 10. When encapsulated message 412 reached apparatus 10, it is decapsulated through the authentication of the same transaction device ID 410 to obtain encrypted message 408. Data 406 is thus obtained by using the one-off key 404 to decrypt the encrypted message 408.

FIG. 5 shows the risk assessment 500 on the financial transactions effected in the system. Transaction activities will trigger the module 502 to start taking effect, where data will be analyzed primarily at

504. When the behavior triggered suspicion, the data will be further analyzed by risk assessment unit 506. Should the analyzed result be tolerable, the transaction will be tagged as low-risk, thus allowing for the transaction to continue. However, should the analyzed result be intolerable, the transaction will be terminated at 512.

With reference to FIG. 6A, an embodiment 600 of a perspective back view of a transaction device 606 linked to a communication device 608 is shown. The transaction device 606 has a slot 604 that runs along the length or a with of the transaction device 606, allowing a magnetic stripe of a transaction card to be read. The transaction device 606 has another slot 602, allowing a IC chip of a transaction card to be inserted and read. The communication device 608 has a interactive touchscreen 610, allowing a user to interact with the software application present in the communication device.

With further reference now to FIG. 6b, an embodiment 600 of a perspective view of a transaction device 606 linked to a communication device 608 is shown. The transaction device 606 has a physical alphanumeric keypad 612, allowing a user to key in PIN deemed necessary for effecting a financial transaction.

With particular reference now to FIG. 7A, an embodiment of a perspective back view of a transaction device linked to a communication device in one housing 700 is shown. The housing 706 is shared between the transaction device and the communication device. The housing 706 has a slot 704 that runs along a length or a width of the housing, allowing a magnetic stripe of a transaction card to be read. The housing 706 has another slot 702, allowing a IC chip of a transaction card to be inserted and read. The housing 706 has an interactive touchscreen 708, allowing a user to interact with the software application present in the apparatus.

With further reference now to FIG. 7B, an embodiment of a perspective view of a transaction device linked to a communication device in one housing 700 is shown. The housing 706 has a physical alphanumeric keypad 710, allowing a user to key in PIN deemed necessary for effecting a financial transaction.

In summary, an archetypical working adult with commitments have a whole range of periodical expenses, such as that but not limted to credit card bills, utility bills, refuse collection bills, car loans, housing loans, ticket fines, insurance premiums, children's tuition fees and goodwill donations. One existing method to settle these bill payments maybe be going to each individual creditor organization's website to pay accordingly, or through an bill aggregator website, while repeatedly going through the process such as typing in credit or debit card number and other necessary information. While another existing method is paying through a physical payment kiosk.

FIG. 8 illustrates a flowchart diagram of a method for bill payment 800. The method 800 begins operation at the initialization of software application request 802, where the user will then select bill 804 and be prompted if there is another bill 806 to add to the current process. If there is another bill 506 to add, it will return to select bill 804. Else, user will proceed to checkout 808, where the read card 810 action will take place. User will also be required to enter PIN entry 812. An electronic receipt will be sent to user's email 814, and user be promted to logout 816. If not, user will go back to select bill 804. Else, bill payment process is completed on 818.

Store-value cards are used extensively such as transit system farecards, telephone prepaid calling cards or for micropayments in shops or vending machines. However, the existing method for doing a value-add to the said store-value cards are almost limited to stationary places such as vending machines and ATMs. This method of value-adding the store-value cards with mobility creates the flexibility for users, eliminating process such as transportation and waiting, thus, saving time and money.

FIG. 9 illustrates a flowchart diagram of a method for adding monetary value to store-value card 900. The method 900 begins operation at the initialization of software application request 902. Upon reading the transaction card 904, the user will be prompted to enter PIN 906. Upon the authorization 908 by the transaction card issuer, user will be prompted to enter value-add monetary amount 910. User will then be prompted to remove the existing transaction card from the transaction device and replace it with the store-value card for reading 914. Upon reading the store-value card 914, the card data will be sent to the store-value card issuer 916 for authorization. Authorization data will be sent back to allow the new data value to be written on the store-value card 918. The software application will end 920 upon the completion of the transaction.

CLAIMS

1. The present invention provides a system and methods for performing secure mobile financial transactions between an apparatus through a gateway processor via a communication protocol, using a transaction card.

2. An apparatus according to claim 1, wherein comprises of a transaction device, a communication device and a software application.

3. An apparatus according to claim 2, wherein the said transaction device comprises of a device selected from the group consisting of: a secure controller, an analog signal reader, a digital signal reader, a bar code reader, a magnetic stripe reader, an integrated circuit reader, a smartcard reader and writer, an EMV reader and writer, a (Near-Field Communication) NFC controller, pin entry device (PED), an optical scanner, an alphanumeric keypad, a crytopgraphic module and any combination thereof.

4. An apparatus according to claim 2, wherein the said transaction device comprises of an integrated EMV kernel with an operating system (OS), and a firmware.

5. An apparatus according to claim 2, wherein the said transaction card is selected from the group consisting of but not limited to: a debit card, a credit card, a cash card, smart card, a stored value card, an ATM card and any combination thereof.

6. An apparatus according to claim 2, wherein the said communication device communicates with the transaction device through a connectivity link.

7. An apparatus according to claim 6, wherein the said connectivity link is selected from the group consisting of cable, a wireless connection, an analog channel, a hands-free interface, a tethering interface, a Blue-tooth, a USB, a Wifi, radio frequency communication, microwave communication and infrared communication and any combination thereof.

8. An apparatus according to claim 3, wherein the said transaction device and the communication device is combined to share one housing.

9. An apparatus according to claim 2, wherein the said communication device receives data from the transaction device;

10. An apparatus according to claim 2, wherein the said communication device transmits data to the transaction device;

11. An apparatus according to claim 2, wherein the communication device transmits data to gateway processor;

12. An apparatus according to claim 2, wherein the communication device receives data from gateway processor;

13. An apparatus according to claim 2, wherein the said software application allows interaction between user and the system.

14. A system according to claim 1, wherein the communication protocol comprises of, but not limited to standardized interchange message format and ISO message format that exchange transactions information.

15. A system according to claim 11, wherein the standardized interchange message comprises of a message consisting: messages, data elements and code values, application, registration procedures codes, maintenance procedures for messages, data elements and code values and any combination thereof.

16. A system according to claim 1, wherein the said communication protocol may be sent wirelessly through, but not limited to Internet, GPRS, GSM, Wifi, radio frequency communication, microwave communication and infrared communication.

17. A system according to claim 1, wherein the said gateway processor comprises of a crytographic module, a master key cryptographic module, hardware security (HS) module, a dynamic currency converter (DCC) module, a risk management module, terminal management module, and any combination thereof.

18. A system according to claim 1, wherein all cryptographic keys used must reside within the transaction device.

19. A system according to claim 1, wherein the transaction device stores all cryptographic keys within the internal Flash of the processor, or in the internal SRAM of the process during operation: Once loaded, functions to read the key from the device will be removed in the supplied source code.

20. A system according to claim 1, wherein all cryptographic keys used by the transaction device must be unique per reader, with the exception of public keys which must be signed by a commercially recognized Certificate Authority.

21. A system according to claim 1, wherein all account data read from either the analog signal reader, or a digital signal reader, or a bar code reader, or a magnetic stripe reader, or an integrated circuit reader, or a smartcard reader and writer, or an EMV reader and writer, or a (Near-Field Communication) NFC controller, or a pin entry device (PED), or an optical scanner, or an alphanumeric keypad, or a crytopgraphic module or any combination thereof of the transaction device is encrypted immediately upon entry into the transaction device and processed within the secure controller of the transaction device.

22. A system according to claim 1, wherein data is output encrypted under approved encryption algorithms, such as but not limited to ANSI X9 and ISO algorithm.

23. A system according to claim 1, wherein Plaintext sensitive card information is protected from being available to the communication device.

24. A system according to claim 1, wherein the gateway processor stores a master key.

25. A system according to claim 1, wherein the master key generates a primary key.

26. A system according to claim 1, wherein the primary key generates a secondary key.

27. A system according to claim 1, wherein the secure message transmission process from the apparatus to the gateway processor comprises of:

(a) the secondary key is shared between the gateway processor and the transaction device.
(b) the shared secondary key generates one-off keys.
(c) the transaction device ID is shared between the transaction device and gateway processor.
(d) the card data captured by the transaction device is encrypted by one-off key.
(e) the encrypted data is encapsulated with the transaction device ID to become an encapsulated message for transmission to gateway processor.
(f) the encapsulated message is decapsulated through the transaction device ID's authentication present in the gateway processor.
(g) the encrypted message is further decrypted with the one-off key generated by the shared secondary key, present in the gateway processor.

28. A system according to claim 1, wherein the secure message transmission process from the gateway processor to the apparatus comprises of:

(a) the secondary key is shared between the gateway processor and the transaction device.
(b) the shared secondary key generates one-off keys.
(c) the transaction device ID is shared between the transaction device and gateway processor.
(d) the data sent from bank is encrypted by one-off key.
(e) the encrypted data is encapsulated with the transaction device ID to become an encapsulated message for transmission to apparatus.
(f) the encapsulated message is decapsulated through the transaction device ID's authentication present in the apparatus.
(g) the encrypted message is further decrypted with the one-off key generated by the shared secondary key, present in the apparatus.

29. A system according to claim 16, wherein the said risk management module may check whether there is a decision to be made under transaction with special circumstances. Such circumstances may comprise, but not limited to transaction ceiling limit, a velocity check, a higher-than-normal frequency rate of faulty card fallback to magnetic swipe, and a check on unusual offline transaction.

30. A system according to claim 16, wherein the said system management module may periodically check for, and automatically install any security update for the system.

31. A system according to claim 16, wherein the said dynamic currency conversion (DCC) allows customers to see the exact amount their transaction card will be charged, expressed in their home currency.

32. A security system of claim 1, wherein the enhanced security features comprising: the capture of geolocation of payment transaction through GPS already present in the communication device, to be displayed on the electronic receipt;

33. A security system of claim 1, wherein the enhanced security features comprising: the capture of image on the person associated with the financial transaction through digital camera already present in commuincation device, to be displayed on the electronic receipt; and

34. A security system of claim 1, wherein the enhanced security features comprising: the capture of fingerprint through biometric identification already present in the communication device, to be displayed on the electronic receipt; and

35. A security system of claim 1, wherein the enhanced security features comprising: the identity morphing detection.

36. A method for re-writing a store-value card having data stored on a IC chip incorporated into the card, the method comprising the steps of:

(a) providing a transaction device comprising a reader, for capturing transaction card data;
(b) card data is encrypted by one-off key; providing a keypad for capturing PIN;
(c) entered PIN information is encrypted by one-off key;
(d) encrypted transaction message and PIN are encapsulated, together with transaction device identification for transmission;
(e) Encapsulated message is transmitted to the gateway processor via the communication protocol;
(f) gateway processor decapsulates the message;
(g) gateway processor decrypts the transaction message;
(h) gateway processor sends the decrypted message to bank for transaction authorization;
(i) gateway processor receives the authorized message from bank;
(j) gateway processor encrypts the message;
(k) gateway processor encapsulates the message for transmission via the communication protocol;
(l) software application decapsulates the message;
(m) software application decypts the message;
(n) user to enter top-up amount via the software application;
(o) providing a transaction device comprising a writer to rewrite the data stored in the IC chip incorporated into the store-value card;

37. The method of claim 29 further comprising the step of user swiping a magnetic swipe transaction card to allow transaction device to capture the card information.

38. The method of claim 29 further comprising the step of user chipping EMV or IC smart transaction card to allow transaction device to capture the card information.

39. The method of claim 29 further comprising the step of user tapping NFC transaction card to allow transaction device to capture the card information.

40. A method of using the mobile financial payment via the system in claim 1, relating to a plurality of selectable financial instruments for effecting the financial payment to a payee.

41. The method in claim 33, wherein user can make financial payment to the selected payee comprising: a recurring bill, a bill from a billing aggregator, a bill from an individual bill company, a "pay to anyone" payment.