

A DONGLE DEVICE WITH COMMUNICATION MODULE FOR A SECURE ELECTRONIC TRANSACTION

CROSS REFERENCE TO RELATED APPLICATION

[0001] The present application claims the benefit of an Indian Provisional Patent Application entitled, "SYSTEM AND METHOD FOR SECURE ELECTRONIC TRANSACTION" with serial number 3415/CHE/2011, filed at Government of India Patent Office on October 3, 2011, the content of which is incorporated by reference herein.

BACKGROUND

Technical field

[0002] The embodiments herein generally relate to a field of electronic transaction. The embodiments herein particularly relate to a dongle device for an electronic transaction and more particularly relates to a dongle device with communication module for a secure electronic transaction.

Description of the Related Art

[0003] Currently, there are hundreds of magnetic stripe readers/swipers on the market and all of them are at least as long as the credit card itself. There exist different types of card readers/swipers. One type of a card reader is a traditional card swiper with a single rail, which allows a card to be held against a base of the reader by the user and moved across the read head of the reader. Another type of a card reader guides a card by the two sets of rails and a backstop. Once the user has inserted the card against the backstop, the card is read as it is removed from the swiper. The magnetic stripe cards having standard specifications can typically be

read by the point-of-sale devices at a merchant's location. When the card is swiped through an electronic card reader at the checkout counter at a merchant's store, the reader usually uses its built-in modem to dial the number of a company that handles the credit authentication requests. After the account is verified, an approval signal is sent back to the merchant to complete a transaction.

[0004] The conventional swipe device using the magnetic card readers for an electronic payment is bulky. Further the merchant has to produce the printed receipts for the customer, which is very cumbersome for the merchant handling the multiple customers. Still further, the merchant has to keep record of all the printed receipts, to avoid a dispute about the transactions. It is advantageous for an individual to make a payment to another individual or merchant by swiping his magnetic stripe card through a reader connected to a mobile device. The mobile device should include a communication medium such as GPRS, WiFi, Bluetooth, etc., to transmit the card data to the server. Further the mobile device should be carried everywhere.

[0005] As a result, there were huge developments in providing the card reader for a mobile device. In the currently available systems, a portable swipe machine for the mobile devices is provided and the card data is encrypted on the mobile device. Hence there is a chance of an insecure transaction over the mobile device. Further, the existing systems communicate a relevant data through the electrical signals, which are extremely slow compared to the electromagnetic signals. In the current scenario, the communication is always performed on IP

network, since IP networks are wide spread. Further the existing devices work only with the high end devices such as iPhone, iPad or any other smart phone, thereby making the system very costly for the prospective users. Further the currently used swipe machines are active devices, in which the machines need to be charged with an external power supply or through a connected device.

[0006] In view of the above facts, there is a need for a dongle device with a communication module to carry out a secure electronic transaction. There is also a need for a system and method for providing a secure electronic transaction in a cost effective manner. Further there is a need for a system and method to enable a fast, efficient and secure electronic transaction by using a dongle device. Yet there is a need for a system and method to utilize the fast and efficient IP communication, thereby reducing a need for the use of an electrical signal.

[0007] The above mentioned shortcomings, disadvantages and problems are addressed herein and which will be understood by reading and studying the following specification.

OBJECTS OF THE EMBODIMENTS

[0008] The primary object of the embodiments herein is to provide a dongle device for a secure electronic transaction.

[0009] Another object of the embodiments herein is to provide a dongle device with a communication module for a secure electronic transaction.

[0010] Yet another object of the embodiments herein is to provide a dongle device to connect directly to a server or a payment gateway to perform a secure electronic transaction.

5 [0011] Yet another object of the embodiments herein is to provide a method to transform a card data into a token data and to transmit the token data without sending the card data from a computing device to a server.

[0012] Yet another object of the embodiments herein is to provide a method for converting the card data into an audio data at supersonic frequencies.

10 [0013] Yet another object of the embodiments herein is to provide a method for converting the card data into the noise like signals i.e. spread spectrum signals.

[0014] Yet another object of the embodiments herein is to provide a method and a system for mutually authenticating a dongle device and a payment server.

15 [0015] These and other objects and advantages of the embodiments herein will become readily apparent from the following detailed description taken in conjunction with the accompanying drawings.

SUMMARY

20 [0016] The various embodiments herein provide a dongle device with a communication module for a secure electronic transaction. The dongle device comprises a housing provided with a slot for swiping a magnetic stripe card, a slot for inserting a contact type card, a communication module, a key pad, a connector, a

cover for safeguarding the connector, a stylus, a universal serial bus (USB) port, a processor and a display. The card is read and the card data are transmitted through supersonic frequencies to a payment gateway server. The connector is provided on the housing for connecting the communication module.

5 [0017] According to an embodiment herein, the communication module is any one of a Wireless module, a Bluetooth module, a mobile communication module, a zigbee module and an audio jack.

 [0018] According to an embodiment herein, the communication module is configured with any one of a Wireless module, a Bluetooth module, a mobile
10 communication module, a zigbee module and an audio jack by a user.

 [0019] According to an embodiment herein, the communication module is configured with any one of a Wireless module, a Bluetooth module, a mobile communication module, a zigbee module and an audio jack at a time manufacturing.

 [0020] According to an embodiment herein, the communication module
15 is a plug and play module. The plug and play module is connected through a propriety port or a standard port or the connector which is provided on the housing. The standard port includes a USB port and a serial port the USB port.

 [0021] According to an embodiment herein, the dongle device further comprises a magnetic card reader, a contact type card reader and a NFC reader.

20 [0022] According to an embodiment herein, a magnetic card reader or a contact type card reader or the NFC reader is activated accordingly when a magnetic card is swiped through the slot for swiping a magnetic stripe card or when a contact

type card is inserted through the slot for inserting a contact type card or when a NFC card is tapped.

5 [0023] According to an embodiment herein, the connector comprises a power module, a line detector module and a line for establishing a bi-directional data communication.

[0024] According to an embodiment herein, the connector provides a mechanical support.

[0025] According to an embodiment herein, the processor is provided with a software to convert the card data into an audio data at supersonic frequencies.

10 [0026] According to an embodiment herein, the communication module interacts with a payment gateway server for completing a transaction.

[0027] According to an embodiment herein, a payment transaction is made through a mobile phone or a cell phone connected to the audio jack of the dongle.

15 [0028] According to an embodiment herein, the audio jack supports a payment transaction during a listening of music by enabling a transmission at the audible and supersonic frequencies simultaneously.

[0029] According to an embodiment herein, the communication module links a transaction originated in a cloud computing server with a payment gateway server through a mobile device to complete a financial transaction.

20

[0030] According to an embodiment herein, the processor interacts with a central server through a mobile device or with the central server directly. The central server is the server of dongle manufacturer.

[0031] According to an embodiment herein, the processor interacts not only with the central server through a mobile device but also with the payment gateway server.

[0032] According to an embodiment herein, the audio jack supports both a data transmission and an audio transmission with the mobile device.

[0033] According to an embodiment herein, the audio jack supports a two way communication between a mobile phone and the dongle.

[0034] According to an embodiment herein, the audio jack is provided with a plurality of ports, and wherein the plurality of ports includes a microphone port and a speaker port.

[0035] According to an embodiment herein, the two way communication is established between a mobile phone and the dongle by using a microphone port and a speaker port, and wherein the microphone port is used for a communication from the dongle to the mobile phone, and wherein the speaker port is used for a communication from the mobile phone to the dongle.

[0036] According to an embodiment herein, the audio jack is provided with a plurality of ports, and wherein the plurality of ports includes a plurality of microphone ports and a plurality of speaker ports.

[0037] According to an embodiment herein, the plurality of microphone ports and the plurality of speaker ports are used for transmitting an additional signaling and data.

[0038] According to an embodiment herein, the audio jack supports a
5 two way encrypted link.

[0039] According to an embodiment herein, a communication over the audio jack is done through a noise like signal and wherein the noise like signal is spread spectrum signals and wherein the spread spectrum signals are generated using hardware and software.

10 [0040] According to an embodiment herein, the computing device is any one of a cell phone, smart phone, an Apple's iPhone, an iPod, an iPad, an iTouch, a Google's Android device and a general purpose computer.

[0041] The various embodiments herein provide a method for a secure electronic transaction using a dongle device. The method comprises the steps of
15 logging in by a merchant into a client application installed on a computing device, using a card in a dongle device, by swiping in case of a MSR card, inserting in case of an EMV card and tapping in case of a NFC card, tracking a status of a card used, reading a card data by a respective card readers such as MSR card reader in case of MSR card, a EMV card reader in case of EMV card and a NFC card reader in case
20 of NFC card, in the dongle device, extracting a public key burnt on a flash of the dongle, processing the card data by a processor for producing a cipher data, representing the cipher data and a PIN data as an audio signal, transmitting the

cipher data and the PIN data to a mobile device through an audio jack of the mobile device, and wherein the data communicated between the mobile device and the dongle device is in a form of acoustic signals in audible and supersonic frequencies or audio tones, collecting a transaction information through a graphical user interface (GUI) and wherein the GUI is provided by the client application, collecting a part of a card number from the merchant, constructing a hash value out of the cipher data by using a hash algorithm of a client application running on a computing device such as a mobile device and wherein the hash algorithm is exchanged and stored between the mobile device and the payment server for a first time, transmitting the hash value along with the transaction information to a production server through a first communication network, processing the cipher data and the PIN data in a payment server of the production server, sending a transaction request to a third party system to perform an electronic transaction, transmitting a transaction information to the third party system through a second communication network, performing the electronic transaction by the third party system and indicating a transaction status and wherein the transaction status is indicated by an audio tone or a colored light. The transaction status is one of a bad transaction and a good transaction.

[0042] According to an embodiment herein, the step of processing the swipe data by a microchip for producing a cipher data comprises generating a random number for avoiding a replay attack, decoding the swipe data by a comparator, converting the swipe data into a card data by a converter, tokenization

of the card data by a tokenizer by Xoring the card data with a dongle ID, encrypting the card data into a cipher data by an encryption engine using a RSA algorithm, and wherein a public key is used in RSA algorithm for encrypting the card data and modulating the cipher data by a modulation engine using Frequency Shift Keying (FSK). The dongle ID is a unique and secret ID related to the dongle.

[0043] According to an embodiment herein, the step of processing the cipher data in a payment server of the production server comprises decoding the hash value by a decoder of the payment server for producing the cipher data, decrypting the cipher data by a decryption engine of the payment server using a private key, retrieving a merchant information stored in a payment database of the production server, reproducing a complete card number by stitching a part of the card number entered by the merchant with a card data received from the dongle and authenticating the merchant.

[0044] According to an embodiment herein, the step of representing the cipher data as an audio signal comprises filtering the cipher data by a low pass filter and dividing a voltage of cipher data for producing amplitude for the audio signal.

[0045] According to an embodiment herein, the step of constructing the hash value out of the encrypted data by the hash function of the client application running on the mobile device is done by creating a date/time stamp.

[0046] According to an embodiment herein, the method further comprises sending an electronic receipt to the customer through a short message service (SMS) or an e-mail.

[0047] According to an embodiment herein, the method further comprises recording a transaction status by a counter of the microchip.

5 [0048] According to an embodiment herein, the method further comprises measuring a voltage level of a battery of the dongle by an analog-to-digital convertor (ADC) of the microprocessor, sending a measured voltage level along with the transaction data to the production server, collating a reading of the battery by the payment server, computing a remaining voltage level in the battery by the payment server and sending an information corresponding to the remaining voltage level in the battery to a user.

10 [0049] According to an embodiment herein, the transaction information includes an amount of the transaction, a unique PIN data of the card entered by the card holder, an additional data related to the transaction, and a signature of a card holder.

[0050] According to an embodiment herein, the unique PIN is data is
15 any one of a scrambled PIN data or a PIN block or a onetime password (OTP).

[0051] According to an embodiment herein, the method further comprises an updating of the public key, and wherein the updating of the public key comprises swiping a non financial card on a swipe machine, reading a swipe data by a reader head of the dongle, extracting a public key from the swipe data and
20 updating the public key associated with the dongle.

[0052] According to an embodiment herein, the method further comprises mapping a merchant ID, a terminal ID, a user ID, IMEI number of

computing device, a serial number of the dongle with a dongle ID for executing a secure electronic transaction.

[0053] According to an embodiment herein, the method further comprises mapping a dongle ID, serial number of dongle with IMEI number of a mobile device for executing a secure electronic transaction.

[0054] According to an embodiment herein, the public key is burned into the dongle at a manufacture time.

[0055] According to an embodiment herein, the dongle generates a session key and a secret key at the beginning of the transaction. The secret key is used for authenticating the payment server. The session key and secret key are encrypted by the public key and sent to the payment server.

[0056] According to an embodiment herein, the payment server further comprises a private key, and wherein the private key decrypts the secret key sent by the dongle and sends back the decrypted secret key to the dongle for mutually authenticating the dongle and the payment server.

[0057] According to an embodiment herein, the dongle further comprises a NFC tag, and wherein the NFC tag of the dongle includes a unique ID and a physical unclonable function (PUF).

[0058] According to an embodiment herein, the merchant device comprises a NFC tag, and wherein the NFC tag of the merchant device authenticates the dongle by verifying the unique ID of the dongle NFC tag.

[0059] According to an embodiment herein, a swipe data alone is sent as an audio signal after tokenization and encryption.

[0060] These and other aspects of the embodiments herein will be better appreciated and understood when considered in conjunction with the following description and the accompanying drawings. It should be understood, however, that the following descriptions, while indicating preferred embodiments and numerous specific details thereof, are given by way of illustration and not of limitation. Many changes and modifications may be made within the scope of the embodiments herein without departing from the spirit thereof, and the embodiments herein include all such modifications.

BRIEF DESCRIPTION OF THE DRAWINGS

[0061] The other objects, features and advantages will occur to those skilled in the art from the following description of the preferred embodiment and the accompanying drawings in which:

[0062] FIG. 1 illustrates a top side perspective view of a dongle device with a cover, according to an embodiment herein.

[0063] FIG. 2 illustrates a front side view of a dongle device with a cover, according to an embodiment herein.

[0064] FIG. 3 illustrates a back side view of a dongle device, according to an embodiment herein.

[0065] FIG. 4 illustrates a left side view of a dongle device without a cover, according to an embodiment herein.

[0066] FIG. 5 illustrates a right side view of a dongle device without a cover, according to an embodiment herein.

[0067] FIG. 6 illustrates a block circuit diagram of a dongle device with a communication module for secure electronic transaction, according to an
5 embodiment herein.

[0068] FIG. 7 illustrates a flowchart indicating a method for secure electronic transaction, according to an embodiment herein.

[0069] Although the specific features of the embodiments herein are shown in some drawings and not in others. This is done for convenience only as
10 each feature may be combined with any or all of the other features in accordance with the embodiments herein.

DETAILED DESCRIPTION OF THE EMBODIMENTS HEREIN

[0070] In the following detailed description, a reference is made to the accompanying drawings that form a part hereof, and in which the specific
15 embodiments that may be practiced is shown by way of illustration. These embodiments are described in sufficient detail to enable those skilled in the art to practice the embodiments and it is to be understood that the logical, mechanical and other changes may be made without departing from the scope of the embodiments. The following detailed description is therefore not to be taken in a limiting sense.

[0071] The various embodiments herein provide a dongle device with a
20 communication module for a secure electronic transaction. The dongle device comprises a housing provided with a slot for swiping a magnetic stripe card, a slot

for inserting a contact type card, a communication module, a key pad, a connector, a cover for safeguarding the connector, a stylus, a universal serial bus (USB) port, a processor and a display. The card is read and the card data are transmitted through supersonic frequencies to a payment gateway server. The connector is provided on
5 the housing for connecting the communication module.

[0072] According to an embodiment herein, the communication module is any one of a Wireless module, a Bluetooth module, a mobile communication module, a zigbee module and an audio jack.

[0073] According to an embodiment herein, the communication module
10 is configured with any one of a Wireless module, a Bluetooth module, a mobile communication module, a zigbee module and an audio jack by a user.

[0074] According to an embodiment herein, the communication module is configured with any one of a Wireless module, a Bluetooth module, a mobile communication module, a zigbee module and an audio jack at a time manufacturing.

[0075] According to an embodiment herein, the communication module
15 is a plug and play module. The plug and play module is connected through the USB port. The plug and play module is connected through a propriety port or a standard port or the connector which is provided on the housing, and wherein the standard port includes a USB port and a serial port.

[0076] According to an embodiment herein, the dongle device further
20 comprises a magnetic card reader, a contact type card reader and a NFC reader.

[0077] According to an embodiment herein, a magnetic card reader or a contact type card reader or the NFC reader is activated accordingly when a magnetic card is swiped through the slot for swiping a magnetic stripe card or when a contact type card is inserted through the slot for inserting a contact type card or when a NFC card is tapped.

[0078] According to an embodiment herein, the connector comprises a power module, a line detector module and a line for establishing a bi-directional data communication.

[0079] According to an embodiment herein, the connector provides a mechanical support.

[0080] According to an embodiment herein, the processor is provided with a software to convert the card data into an audio data at supersonic frequencies.

[0081] According to an embodiment herein, the communication module interacts with a payment gateway server for completing a transaction.

[0082] According to an embodiment herein, a payment transaction is made through a mobile phone or a cell phone connected to the audio jack of the dongle.

[0083] According to an embodiment herein, the audio jack supports a payment transaction during a listening of music by enabling a transmission at the audible and supersonic frequencies simultaneously.

[0084] According to an embodiment herein, the communication module links a transaction originated in a cloud computing server with a payment gateway server through a mobile device to complete a financial transaction.

5 [0085] According to an embodiment herein, the processor interacts with a central server through a mobile device or with the central server directly. The central server is the server of dongle manufacturer.

[0086] According to an embodiment herein, the processor interacts not only with the central server through a mobile device but also with the payment gateway server.

10 [0087] According to an embodiment herein, the audio jack supports both a data transmission and an audio transmission with the mobile device.

[0088] According to an embodiment herein, the audio jack supports a two way communication between a mobile phone and the dongle.

15 [0089] According to an embodiment herein, the audio jack is provided with a plurality of ports, and wherein the plurality of ports includes a microphone port and a speaker port.

[0090] According to an embodiment herein, the two way communication is established between a mobile phone and the dongle by using a microphone port and a speaker port, and wherein the microphone port is used for a communication
20 from the dongle to the mobile phone, and wherein the speaker port is used for a communication from the mobile phone to the dongle.

[0091] According to an embodiment herein, the audio jack is provided with a plurality of ports, and wherein the plurality of ports includes a plurality of microphone ports and a plurality of speaker ports.

5 [0092] According to an embodiment herein, the plurality of microphone ports and the plurality of speaker ports are used for transmitting an additional signaling and data.

[0093] According to an embodiment herein, the audio jack supports a two way encrypted link.

10 [0094] According to an embodiment herein, a communication over the audio jack is done through a noise like signal and wherein the noise like signal is spread spectrum signals and wherein the spread spectrum signals are generated using hardware and software.

[0095] According to an embodiment herein, the computing device is any one of a cell phone, smart phone, an Apple's iPhone, an iPod, an iPad, an iTouch, a
15 Google's Android device and a general purpose computer.

[0096] The various embodiments herein provide a method for a secure electronic transaction using a dongle device. The method comprises the steps of logging in by a merchant into a client application installed on a computing device, using a card in a dongle device, by swiping in case of a MSR card, inserting in case
20 of an EMV card and tapping in case of a NFC card, tracking a status of a card used, reading a card data by a respective card readers such as MSR card reader in case of MSR card, a EMV card reader in case of EMV card and a NFC card reader in case

of NFC card, in the dongle device, extracting a public key burnt on a flash of the dongle, processing the card data by a processor for producing a cipher data, representing the cipher data and a PIN data as an audio signal, transmitting the cipher data and the PIN data to a mobile device through an audio jack of the mobile device, and wherein the data communicated between the mobile device and the dongle device is in a form of acoustic signals in audible and supersonic frequencies or audio tones, collecting a transaction information through a graphical user interface (GUI) and wherein the GUI is provided by the client application, collecting a part of a card number from the merchant, constructing a hash value out of the cipher data by using a hash algorithm of a client application running on a computing device such as a mobile device and wherein the hash algorithm is exchanged and stored between the mobile device and the payment server for a first time, transmitting the hash value along with the transaction information to a production server through a first communication network, processing the cipher data and the PIN data in a payment server of the production server, sending a transaction request to a third party system to perform an electronic transaction, transmitting a transaction information to the third party system through a second communication network, performing the electronic transaction by the third party system and indicating a transaction status and wherein the transaction status is indicated by an audio tone or a colored light. The transaction status is one of a bad transaction and a good transaction.

[0097] According to an embodiment herein, the step of processing the swipe data by a microchip for producing a cipher data comprises generating a random number for avoiding a replay attack, decoding the swipe data by a comparator, converting the swipe data into a card data by a converter, tokenization
5 of the card data by a tokenizer by Xoring the card data with a dongle ID, encrypting the card data into a cipher data by an encryption engine using a RSA algorithm, and wherein a public key is used in RSA algorithm for encrypting the card data and modulating the cipher data by a modulation engine using Frequency Shift Keying (FSK). The dongle ID is a unique and secret ID related to the dongle.

10 [0098] According to an embodiment herein, the step of processing the cipher data in a payment server of the production server comprises decoding the hash value by a decoder of the payment server for producing the cipher data, decrypting the cipher data by a decryption engine of the payment server using a private key, retrieving a merchant information stored in a payment database of the
15 production server, reproducing a complete card number by stitching a part of the card number entered by the merchant with a card data received from the dongle and authenticating the merchant.

[0099] According to an embodiment herein, the step of representing the cipher data as an audio signal comprises filtering the cipher data by a low pass filter
20 and dividing a voltage of cipher data for producing amplitude for the audio signal.

[00100] According to an embodiment herein, the step of constructing the hash value out of the encrypted data by the hash function of the client application running on the mobile device is done by creating a date/time stamp.

[00101] According to an embodiment herein, the method further comprises sending an electronic receipt to the customer through a short message service (SMS) or an e-mail.

[00102] According to an embodiment herein, the method further comprises recording a transaction status by a counter of the microchip.

[00103] According to an embodiment herein, the method further comprises measuring a voltage level of a battery of the dongle by an analog-to-digital convertor (ADC) of the microprocessor, sending a measured voltage level along with the transaction data to the production server, collating a reading of the battery by the payment server, computing a remaining voltage level in the battery by the payment server and sending an information corresponding to the remaining voltage level in the battery to a user.

[00104] According to an embodiment herein, the transaction information includes an amount of the transaction, a unique PIN data of the card entered by the card holder, an additional data related to the transaction, and a signature of a card holder.

[00105] According to an embodiment herein, the unique PIN is data is any one of a scrambled PIN data or a PIN block or a onetime password (OTP).

[00106] According to an embodiment herein, the method further comprises an updating of the public key, and wherein the updating of the public key comprises swiping a non financial card on a swipe machine, reading a swipe data by a reader head of the dongle, extracting a public key from the swipe data and
5 updating the public key associated with the dongle.

[00107] According to an embodiment herein, the method further comprises mapping a merchant ID, a terminal ID, a user ID, an IMEI number of a computing device, a serial number of the dongle with a dongle ID for executing a secure electronic transaction.

10 [00108] According to an embodiment herein, the method further comprises mapping a dongle ID, a serial number of dongle with an IMEI number of a mobile device for executing a secure electronic transaction.

[00109] According to an embodiment herein, the public key is burned into the dongle at a manufacture time.

15 [00110] According to an embodiment herein, the dongle generates a session key and a secret key at the beginning of the transaction. The secret key is used for authenticating the payment server. The session key and secret key are encrypted by the public key and sent to the payment server.

20 [00111] According to an embodiment herein, the payment server further comprises a private key, and wherein the private key decrypts the secret key sent by the dongle and sends back the decrypted secret key to the dongle for mutually authenticating the dongle and the payment server.

[00112] According to an embodiment herein, the dongle further comprises a NFC tag, and wherein the NFC tag of the dongle includes a unique ID and a physical unclonable function (PUF).

[00113] According to an embodiment herein, the merchant device
5 comprises a NFC tag, and wherein the NFC tag of the merchant device authenticates the dongle by verifying the unique ID of the dongle NFC tag.

[00114] According to an embodiment herein, a swipe data alone is sent as an audio signal after tokenization and encryption.

[00115] FIG. 1 illustrates a top perspective view of a dongle with a cover,
10 according to an embodiment herein. The dongle device 100 comprises a slot for swiping a magnetic stripe card 101, a slot for inserting a contact type card 102, a communication module, a key pad, a connector, a cover 104 for safeguarding the connector, an indicator 103, a stylus 105, a universal serial bus (USB) port, a processor and a display. The contact type card is a europay mastercard and visa
15 (EMV) card. The dongle device 100 also comprises a near field communication (NFC) card reader (not shown in FIG. 1) for reading the NFC when tapped across the dongle device 100. The user uses his/her card for initiating the electronic transaction by swiping the MSR card or inserting the EMV card or tapping the NFC card in the dongle device 100 and corresponding card reader module is activated for
20 reading the card data. The activation of the card module is shown by illuminating the indicator 104. The stylus 105 is a writing utensil, or a small tool for some other form of marking or shaping or signing. The stylus 105 is also used for navigating or

providing more precision when used in a touch screen mobile device connected to the dongle device 100 for the electronic transaction.

[00116] According to an embodiment herein, the dongle device is connected to the computing device such as a mobile device, for transmitting a card data to the server. The card data comprises transaction information such as an amount of the transaction, a unique PIN of the card entered by the card holder, an additional data related to the transaction and a signature of a card holder.

[00117] The processor stores a dongle ID, a serial number of the dongle device 100 and a public key. The dongle ID and the serial number of the dongle device 100 are paired at a time of manufacturing the dongle device 100. The dongle ID is a unique and secret ID associated with the dongle device 100. The public key is used in RSA algorithm for encrypting the card data.

[00118] FIG. 2 illustrates a front view of a dongle with a cover, according to an embodiment herein. The dongle device 100 comprises a slot for swiping a magnetic stripe card 101, a magnetic stripe reader (MSR), a europay mastercard and visa (EMV) card reader, a near field communication (NFC) card reader, an indicator 103, a cover 104 and a lanyard 106. The lanyard 106 is worn around the neck or wrist to carry the dongle device 100.

[00119] The user uses his/her card for initiating the electronic transaction by swiping the MSR card or inserting the EMV card or tapping the NFC card in the dongle device 100 and corresponding card reader module is activated for reading the

card data. The activation of the card module is shown by illuminating the indicator 104.

[00120] FIG. 3 illustrates a back view of a dongle, according to an embodiment herein. The dongle device 100 comprises a USB socket 107, a keypad 108, a LED display 109, a stylus 105, a lanyard 106 and a rechargeable battery. The USB socket 107 is used for charging the rechargeable battery of the dongle device 100. The rechargeable battery supplies electrical power for the dongle device 100, when the dongle device is used independently without connecting to the mobile device. The dongle device 100 further comprises communication modules for sending the transaction information directly to the server or the payment gateway. The communication modules are a pluggable module to the dongle device 100 through the USB port or in-built in the dongle device 100 at the manufacture time. The dongle device 100 with the in-built communication modules are configured at manufacture time.

[00121] The dongle device 100 further comprises a method for composing a PG message (ISO 8583 or equivalent) and sending it directly through a WLAN or GPRS modem on the dongle device 100. The composed payment gateway message is sent to the mobile device and the mobile device sends it directly to the corresponding payment gateway and also the mobile device sends a parallel message to ezetap server.

[00122] FIG. 4 illustrates a right side view of a dongle without a cover, according to an embodiment herein. The dongle device 100 comprises a magnetic

stripe reader (MSR) provided in a slot for swiping a magnetic stripe card 101, a europay mastercard and visa (EMV) card reader in a slot for inserting a contact type card 102, a connector 110, a stylus 105, a lanyard 106 and a fastening means 401 for fastening the cover. The card is read and the card data are transmitted through the
5 supersonic frequencies to a payment gateway server. The card data are transmitted to a mobile device by connecting the dongle device 100 to the mobile device by the connector 110. The connector of the dongle device is connected to an audio jack of the mobile device. The card data is in the form of analog signals and is a unique data for each of the card.

10 [00123] FIG. 5 illustrates a left side view of a dongle without a cover, according to an embodiment herein. The dongle comprises a magnetic stripe reader (MSR) provided in a slot for swiping a magnetic stripe card 101, a USB socket 107, a connector 110, a lanyard 106 and fastening means 401. The USB socket 107 is used for charging the rechargeable battery of the dongle device 100. The
15 rechargeable battery supplies an electrical power for the dongle device 100, when the dongle device is used independently without connecting to the mobile device. The dongle device 100 further comprises communication modules for sending the transaction information directly to the server or the payment gateway. The communication modules are a pluggable module to the dongle device 100 through
20 the connector 110 or in-built in the dongle device 100 at the manufacture time. The dongle device 100 with the in-built communication modules are configured at manufacture time. The communication module is any of an Audio module (audio

interface), a Wireless module (WiFi interface), a Bluetooth module, a mobile communication module (GPRS interface) and a zigbee module.

5 [00124] According to an embodiment herein, the connector 110 comprises a power module, a line detector module and a line for establishing a bi-directional data communication. Further the connector 110 also provides a mechanical support for the communication modules connected to the dongle device 100.

10 [00125] According to an embodiment herein, the processor of the dongle device 100 is provided with software to convert the card data into audio data at supersonic frequencies.

[00126] According to an embodiment herein, the communication module connected to the dongle device 100 through the connector 110 interacts with a payment gateway server for completing a transaction.

15 [00127] According to an embodiment herein, the dongle device 100 is connected to the mobile device and a payment transaction is made through a mobile device connected to the dongle device through the audio jack. Further the audio jack supports a payment transaction during a listening of music by enabling transmission at audible and supersonic frequencies simultaneously. The communication module links a transaction originated in a cloud computing server with a payment gateway server through a mobile device to complete a financial transaction.

20

[00128] According to an embodiment herein, the processor of the dongle device 100 interacts with a central server or ezetap server through a mobile device

or with the central server or ezetap server directly. The processor interacts not only with the central server or the ezetap server through a mobile device but also with the payment gate way server.

[00129] According to an embodiment herein, the audio jack supports both
5 a data transmission and an audio transmission with the mobile device.

[00130] According to an embodiment herein, a communication over the audio jack is done through a noise like signals and wherein the noise like signals is spread spectrum signals and wherein the spread spectrum signals are generated using hardware and software.

10 [00131] FIG. 6 illustrates a block circuit diagram of a dongle device with a communication module for secure electronic transaction, according to an embodiment herein. The dongle device comprises a MSR card reader 601, a EMV card reader 602 and a NFC card reader 603 for reading the card data when used with the dongle device. The dongle device further comprises a microprocessor 604 for
15 processing the card data, read by the corresponding card readers (601 or 602 or 603) and for enabling a secure payment transaction with the payment gateway, an interface circuitry 605 connected to a connector 606 and communication modules 607. The connector 606 enables the external communication modules 607 to be connected to the dongle device for transmitting the card data to the server or
20 payment gateway directly. The communication modules 607 is any of an Audio module (audio interface) 607a, a Bluetooth module 607b, a mobile communication

module (GPRS interface) 607c, a Wireless module (WiFi interface) 607d and a zigbee module.

[00132] According to an embodiment herein, the communication modules 607 are in-built in the dongle device at the manufacture time. The dongle device with the in-built communication modules 607 is configured at the manufacture time.

[00133] FIG. 7 illustrates a flowchart indicating a method for secure electronic transaction, according to an embodiment herein. The user uses his/her card for initiating the electronic transaction by swiping the MSR card or inserting the EMV card or tapping the NFC card in the dongle device and corresponding card reader module is activated for reading the card data. The activation of the card module is showcased by illuminating the indicator. The card data is read to collect and transmit the card data to the server (701). The method further comprises generating a carrier wave (signal) beyond the audio range by using a Frequency-shift keying (FSK) frequency modulation technique (702) and the card data is transmitted through discrete frequency changes of FSK signal, conditioning the FSK signal for transmitting through on audio port with respect to a voltage amplitude etc., (703) and transmitting the conditioned FSK signal through the audio port (704).

[00134] According to an embodiment herein, the method for mutually authenticating the dongle and the payment server to enable a secure electronic transaction comprises the steps of logging in by a merchant into a client application installed on a computing device, using a card in a dongle device such as swiping in case of MSR card, inserting in case of EMV card and tapping in case of NFC card,

tracking a status of a card used, reading a card data by a respective card readers such as MSR card reader in case of MSR card, EMV card reader in case of EMV card and NFC card reader in case of NFC card) of the dongle device, extracting a public key burnt on a flash of the dongle, processing the card data by a processor for producing a cipher data, representing the cipher data and a PIN data as an audio signal, transmitting the cipher data and the PIN data to a mobile device through an audio jack of the mobile device, and wherein the data communicated between the mobile device and the dongle device is in a form of acoustic signals or audio tones, collecting a transaction information through a graphical user interface (GUI) and wherein the GUI is provided by the client application, collecting a part of a card number from the merchant, constructing a hash value out of the cipher data by using a hash algorithm of a client application running on a computing device (mobile device) and wherein the hash algorithm is exchanged and stored between the mobile device and the payment server for a first time, transmitting the hash value along with the transaction information to a production server through a first communication network, processing the cipher data and the PIN data in a payment server of the production server, sending a transaction request to a third party system to perform an electronic transaction, transmitting a transaction information to the third party system through a second communication network, performing the electronic transaction by the third party system and indicating a transaction status and wherein the transaction status is indicated by an audio tone or a colored light. The transaction status is one of a bad transaction and a good transaction.

[00135] According to an embodiment herein, the step of processing the card data by a processor for producing a cipher data comprises generating a random number for avoiding a replay attack, decoding the card data by a comparator, tokenization of the card data by a tokenizer by Xoring the card data with a dongle ID, encrypting the card data into a cipher data by an encryption engine using a RSA algorithm, and wherein a public key is used in RSA algorithm for encrypting the card data and modulating the cipher data by a modulation engine using Frequency Shift Keying (FSK). The dongle ID is a unique and secret ID related to the dongle device.

[00136] According to an embodiment herein, the step of processing the cipher data in a payment server of the production server comprises decoding the hash value by a decoder of the payment server for producing the cipher data, decrypting the cipher data by a decryption engine of the payment server using a private key, retrieving a merchant information stored in a payment database of the production server, reproducing a complete card number by stitching a part of the card number entered by the merchant with a card data received from the dongle and authenticating the merchant.

[00137] According to an embodiment herein, the step of representing the cipher data as an audio signal comprises filtering the cipher data by a low pass filter and dividing a voltage of cipher data for producing amplitude for the audio signal.

[00138] According to an embodiment herein, the step of constructing the hash value out of the encrypted data by the hash function of the client application running on the mobile device is done by creating a date/time stamp.

5 [00139] According to an embodiment herein, the method further comprises sending an electronic receipt to the customer through a short message service (SMS) or an e-mail.

[00140] According to an embodiment herein, the method further comprises recording a transaction status by a counter of the processor.

10 [00141] According to an embodiment herein, the method further comprises measuring a voltage level of a rechargeable battery of the dongle device by an analog-to-digital convertor (ADC) of the processor, sending a measured voltage level along with the transaction data to the production server, collating a reading of the rechargeable battery by the payment server, computing a remaining voltage level in the rechargeable battery by the payment server and sending an
15 information corresponding to the remaining voltage level in the rechargeable battery to a user.

[00142] According to an embodiment herein, the transaction information includes an amount of the transaction, a unique PIN data of the card entered by the card holder, an additional data related to the transaction, and a signature of a card
20 holder.

[00143] According to an embodiment herein, the unique PIN is data is any one of a scrambled PIN data or a PIN block or a onetime password (OTP).

[00144] According to an embodiment herein, the method further comprises mapping a merchant ID, a terminal ID, a user ID, an IMEI number of a computing device, a serial number of the dongle with a dongle ID for executing a secure electronic transaction.

5 [00145] According to an embodiment herein, the method further comprises mapping a dongle ID, a serial number of dongle with the IMEI number of a mobile device for executing a secure electronic transaction.

[00146] According to an embodiment herein, the public key is burned in to the dongle at a manufacture time.

10 [00147] According to an embodiment herein, the dongle generates a session key and a secret key at the beginning of the transaction. The secret key is used for authenticating the payment server. The session key and secret key are encrypted by the public key and sent to the payment server.

[00148] According to an embodiment herein, the payment server further
15 comprises a private key. The private key decrypts the secret key sent by the dongle and sends back the decrypted secret key to the dongle for mutually authenticating the dongle and the payment server.

[00149] According to an embodiment herein, the dongle further
comprises a NFC tag, and wherein the NFC tag of the dongle includes a unique ID
20 and a physical unclonable function (PUF).

[00150] According to an embodiment herein, the merchant device comprises a NFC tag, and wherein the NFC tag of the merchant device authenticates the dongle by verifying the unique ID of the dongle NFC tag.

5 [00151] According to an embodiment herein, a swipe data alone is sent as an audio signal after tokenization and encryption.

[00152] The embodiments herein provide a dongle device for a secure electronic transaction. The dongle device provides a fast, efficient, cost effective and secure electronic transaction.

10 [00153] The embodiments herein provide a dongle device which can connect directly to a server or a payment gateway to perform a secure electronic transaction. The method of the embodiments herein provides a secure electronic transaction by transforming card data into a token data and transmitting the token data without sending the card data from a computing device to a server. The dongle device of the embodiments herein converts the card data into audio data at
15 supersonic frequencies. The dongle device of the embodiments herein converts the card data into noise like signals i.e. spread spectrum signals.

[00154] The dongle device provides a method for mutually authenticating the dongle device and the payment server.

20 [00155] Although the embodiments herein are described with various specific embodiments, it will be obvious for a person skilled in the art to practice the embodiments herein with modifications.

[00156] The foregoing description of the specific embodiments herein will so fully reveal the general nature of the embodiments herein that others can, by applying current knowledge, readily modify and/or adapt for various applications such specific embodiments herein without departing from the generic concept, and, therefore, such adaptations and modifications should and are intended to be comprehended within the meaning and range of equivalents of the disclosed embodiments. It is to be understood that the phraseology or terminology employed herein is for the purpose of description and not of limitation.

[00157] Therefore, while the embodiments herein have been described in terms of preferred embodiments, those skilled in the art will recognize that the embodiments herein can be practiced with modification within the spirit and scope of the appended claims.

[00158] Although the embodiments herein are described with various specific embodiments, it will be obvious for a person skilled in the art to practice the invention with modifications. However, all such modifications are deemed to be within the scope of the claims.

[00159] It is also to be understood that the following claims are intended to cover all of the generic and specific features of the embodiments described herein and all the statements of the scope of the embodiments which as a matter of language might be said to fall there between.

CLAIMS

What is claimed is:

1. A dongle device with communication module for a secure electronic transaction comprising:

5 a housing;
a slot for swiping a magnetic stripe card;
a slot for inserting a contact type card;
a communication module;
a key pad;
10 a connector provided on the housing for connecting the communication module;
a cover for safeguarding the connector;
a stylus;
a universal serial bus (USB) port;
a processor;
15 a display; and
wherein a card is read and a card data are transmitted through supersonic frequencies to a payment gateway server.

2. The dongle device according to claim 1, wherein the communication module is
20 any one of a Wireless module, a Bluetooth module, a mobile communication module, a zigbee module and an audio jack.

3. The dongle device according to claim 1, wherein the communication module is configured with any one of a Wireless module, a Bluetooth module, a mobile communication module, a zigbee module and an audio jack by a user.

5

4. The dongle device according to claim 1, wherein the communication module is configured with any one of a Wireless module, a Bluetooth module, a mobile communication module, a zigbee module and an audio jack at a time manufacturing.

10

5. The dongle device according to claim 1, wherein the communication module is a plug and play module.

15

6. The dongle device according to claim 1, wherein the plug and play module is connected through a propriety port or a standard port or the connector which is provided on the housing, and wherein the standard port includes a USB port and a serial port.

20

7. The dongle device according to claim 1 further comprises a magnetic card reader, a contact type card reader and a NFC reader.

8. The dongle device according to claim 1, wherein a magnetic card reader or a contact type card reader or the NFC reader is activated accordingly when a magnetic card is swiped through the slot for swiping a magnetic stripe card or when a contact type card is inserted through the slot for inserting a contact type card or when a NFC card is tapped.

9. The dongle device according to claim 1, wherein the connector comprises a power module, a line detector module and a line for establishing a bi-directional data communication.

10. The dongle device according to claim 1, wherein the connector provides a mechanical support.

11. The dongle device according to claim 1, wherein the processor is provided with software to convert the card data into an audio data at supersonic frequencies.

12. The dongle device according to claim 1, wherein the communication module interacts with a payment gateway server for completing a transaction.

13. The dongle device according to claim 1, wherein a payment transaction is made through a mobile phone connected to the audio jack of the dongle device.

14. The dongle device according to claim 1, wherein the audio jack supports a payment transaction during a listening of music by enabling a transmission at audible and supersonic frequencies simultaneously.

5 15. The dongle device according to claim 1, wherein the communication module links a transaction originated in a cloud computing server with a payment gateway server through a mobile phone to complete a financial transaction.

10 16. The dongle device according to claim 1, wherein the processor interacts with a central server through a mobile phone or with the central server directly.

17. The dongle device according to claim 1, wherein the processor interacts not only with the central server through a mobile phone but also with the payment gateway server.

15 18. . The dongle device according to claim 1, wherein the audio jack supports both a data transmission and an audio transmission with the mobile phone.

20 19. The dongle device according to claim 1, wherein the audio jack supports a two way communication between a mobile phone and a dongle.

20. The dongle device according to claim 1, wherein the audio jack is provided with a plurality of ports, and wherein the plurality of ports includes a microphone port and a speaker port.

5 21. The dongle device according to claim 1, wherein the two way communication is established between a mobile phone and the dongle by using a microphone port and a speaker port, and wherein the microphone port is used for a communication from the dongle to the mobile phone, and wherein the speaker port is used for a communication from the mobile phone to the dongle.

10 22. The dongle device according to claim 1, wherein the audio jack is provided with a plurality of ports, and wherein the plurality of ports includes a plurality of microphone ports and a plurality of speaker ports.

15 23. The dongle device according to claim 1, wherein the plurality of microphone ports and the plurality of speaker ports are used for transmitting an additional signaling and data.

20 24. The dongle device according to claim 1, wherein the audio jack supports a two way encrypted link.

25. The dongle device according to claim 1, wherein a communication over the audio jack is done through a noise like signal and wherein the noise like signal is spread spectrum signals and wherein the spread spectrum signals are generated using a hardware and a software.

5

26. A method for a secure electronic transaction using a dongle device comprising the steps of:

logging in by a merchant into a client application installed on a computing device;

10

swiping a card onto a dongle device;

tracking a status of a swipe;

reading a swipe data by a magnetic card reader of the dongle device;

extracting a public key burnt on a flash of the dongle device;

processing the swipe data by a microchip for producing a cipher data;

15

representing the cipher data and a PIN data as an audio signal;

transmitting the cipher data and the PIN data to a mobile device through an audio jack of the mobile device, and wherein the data communicated between the mobile phone and the dongle device is in a form of acoustic signals or audio tones;

20

collecting a transaction information through a graphical user interface (GUI) and wherein the GUI is provided by the client application ;

collecting a part of a card number from the merchant;

constructing a hash value out of the cipher data by using a hash algorithm of a client application running on a computing device and wherein the hash algorithm is exchanged and stored between the mobile device and the payment server for a first time;

5 transmitting the hash value along with the transaction information to a production server through a first communication network;

processing the cipher data and the PIN data in a payment server of the production server;

10 sending a transaction request to a third party system to perform an electronic transaction;

transmitting a transaction information to the third party system through a second communication network;

performing the electronic transaction by the third party system; and

15 indicating a transaction status and wherein the transaction status is indicated by an audio tone or a colored light, and wherein the transaction status is one of a bad transaction and a good transaction.

27. The method of claim 26, wherein the step processing the swipe data by a microchip for producing a cipher data comprises:

20 generating a random number for avoiding a replay attack;

decoding the swipe data by a comparator;

converting the swipe data into a card data by a converter;

tokenization of the card data by a tokenizer by Xoring the card data with a dongle ID;

encrypting the card data into a cipher data by an encryption engine using a RSA algorithm, and wherein a public key is used in RSA algorithm for encrypting the card data; and

modulating the cipher data by a modulation engine using Frequency Shift Keying (FSK);

wherein the dongle ID is a unique and secret ID related to the dongle device.

10 28. The method of claim 26, wherein the step of processing the cipher data in a payment server of the production server comprises:

decoding the hash value by a decoder of the payment server for producing the cipher data;

15 decrypting the cipher data by a decryption engine of the payment server using a private key;

retrieving a merchant information stored in a payment database of the production server;

reproducing a complete card number by stitching a part of the card number entered by the merchant with a card data received from the dongle device; and

20 authenticating the merchant.

29. The method of claim 26, wherein the step of representing the cipher data as an audio signal comprises:

filtering the cipher data by a low pass filter; and

dividing a voltage of cipher data for producing an amplitude for the audio signal.

5

30. The method of claim 26, wherein the step of constructing the hash value out of the encrypted data by the hash function of the client application running on the mobile phone is done by creating a date/time stamp.

10 31. The method of claim 26, wherein the method further comprises sending an electronic receipt to the customer through a short message service (SMS) or an e-mail.

15 32. The method of claim 26, wherein the method further comprises recording a transaction status by a counter of the microchip.

33. The method of claim 26, wherein the method further comprises:

measuring a voltage level of a battery of the dongle by an analog-to-digital convertor (ADC) of the microprocessor,

20 sending a measured voltage level along with the transaction data to the production server,

collating a reading of the battery by the payment server,

computing a remaining voltage level in the battery by the payment server, and sending an information corresponding to the remaining voltage level in the battery to a user.

5 34. The method of claim 26, wherein the transaction information includes an amount of the transaction, an unique PIN data of the card entered by the card holder, an additional data related to the transaction, and a signature of a card holder.

10 35. The method according to claim 26, wherein the unique PIN is data is any one of a scrambled PIN data or a PIN block or a onetime password (OTP).

15 36. The method of claim 26, wherein the method further comprises an updating of the public key, and wherein the updating of the public key comprises swiping a non financial card on a swipe machine, reading a swipe data by a reader head of the dongle device, extracting a public key from the swipe data and updating the public key associated with the dongle device.

20 37. The method according to claim 26 further comprises mapping a merchant ID, a terminal ID, a user ID, an IMEI number of a computing device, a serial number of the dongle with a dongle ID for executing a secure electronic transaction.

38. The method according to claim 26 further comprises mapping a dongle ID, a serial number of dongle with an IMEI number of a mobile phone for executing a secure electronic transaction.

5 39. The method according to claim 26, wherein the public key is burned to the dongle device at a manufacture time.

40. The method according to claim 26, wherein the dongle generates a session key and a secret key at a beginning of a transaction, and wherein the secret key is
10 used for authenticating the payment server, and wherein the session key and secret key are encrypted by the public key and sent to the payment server.

41. The method according to claim 26, wherein the payment server further comprises a private key, and wherein the private key decrypts the secret key sent
15 by the dongle and sends back the decrypted secret key to the dongle for mutually authenticating the dongle device and the payment server.

42. The method according to claim 26, wherein the dongle further comprises a NFC tag, and wherein the NFC tag of the dongle device includes a unique ID and a
20 physical unclonable function (PUF).

43. The method according to claim 26, wherein the merchant device comprises a NFC tag, and wherein the NFC tag of the merchant device authenticates the dongle by verifying the unique ID of the dongle NFC tag.

5 44. The method according to claim 26, wherein a swipe data alone is sent as an audio signal after tokenization and encryption.