FORM 2
The Patents Act 1970
(39 of 1970)
&
The Patent Rules 2003
COMPLETE SPECIFICATION
(See Section 10 and rule 13)

TITLE OF THE INVENTION:
A DONGLE DEVICE WITH TAMPER PROOF CHARACTERISTICS FOR A SECURE ELECTRONIC TRANSACTION

APPLICANT:
Ezetap Mobile Solutions Private Limited
5th Floor, Beta Building, Sigma
Tech Park, Varthur Main Road,
Ramagondanahalli, Bangalore - 560066
Karnataka, India

PREAMBLE OF THE DESCRIPTION:

THE FOLLOWING SPECIFICATION PARTICULARLY DESCRIBES THE INVENTION AND THE METHOD IT IS BEING PERFORMED

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 dongle device with a tamper proof characteristic for a secure electronic transaction.

Description of the Related Art

[0003] Currently, there are hundreds of magnetic stripe readers/swipers on the market. All of them are at least as long as the credit card itself. There are different types of card readers/swipers exist in the market. One of the types is a traditional card swiper with a single rail, which allows a card to be held against a base of the reader by a user and moved across a read head of the reader. Another type of a card reader guides a card by a two sets of rails and a backstop. When 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 the standard specifications can typically be read by the point-of-sale devices at a merchant location. When the card is swiped through an electronic card reader at a checkout counter in a merchant store, the reader usually uses a built-in modem to dial a

number of a company that handles the credit authentication requests. After an 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. Also the merchant has to keep a 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] At present, there were huge developments in providing the card reader for a mobile device. In the currently available systems, a portable swipe machine is provided for mobile devices 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 the 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 an IP network, since the 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 swipe machines used presently are active devices, where 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 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 the need for the use of 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 tamper proof characteristics for a secure electronic transaction.

[0010] Yet another object of the embodiments herein is to provide a dongle device with a security mesh to prevent a drilling to avoid a tampering of key board.

[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 audio data at supersonic frequencies.

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

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

[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

[0016] The various embodiments herein provide a dongle device with tamper proof characteristics for a secure electronic transaction. The dongle device comprises a housing which includes a first half and a second half. A main circuit board is placed in the first half and a secondary circuit board placed is the second half. The housing further includes 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 processor continuously monitors a connection between the main circuit board and the secondary circuit board and detects a tampering of the compressible connector between the main circuit board and the secondary circuit board. The processor kills the dongle device when the processor detects a tampering of the compressible connector between the main circuit board and the secondary circuit board. The first half and the second half of the dongle device are ultrasonically sealed together. The main circuit board and the secondary circuit board are electrically and electronically connected through a compressible connector. The connector is an audio jack.

[0017] According to an embodiment herein, the processor kills the device by destroying all the keys used for encryption and making the dongle device non operative, when a tampering of the dongle device is detected.

[0018] According to an embodiment herein, the processor kills the device by destroying a public key used for generating all the keys employed for an encryption and making the dongle device non operative, when a tampering of the dongle device is detected.

[0019] According to an embodiment herein, the dongle device further comprises a tamper detection circuit connected to the processor to detect a tampering of the compressible connector between the main circuit board and the secondary circuit board.

[0020] According to an embodiment herein, the dongle device further comprises a battery to supply an electrical power to the tamper detection circuit, when an external power supply to the dongle device is disconnected.

[0021] According to an embodiment herein, the secondary board of the dongle device includes four layers. The four layers are a first layer, a second layer, a third layer and a fourth layer.

[0022] According to an embodiment herein, the first layer of the secondary board includes NFC antenna and LED.

[0023] According to an embodiment herein, the second layer of the dongle device includes a capsense electrode layer. The capsense electrode layer is formed right under the keypad. The capsense electrode layer is formed in a form of a mesh.

[0024] According to an embodiment herein, the third layer of the secondary board includes a security mesh to prevent a drilling to avoid a tampering of the key board.

[0025] According to an embodiment herein, the fourth layer of the secondary board includes a plurality of resistors to form a resistor ladder to detect a tampering of the security mesh.

[0026] According to an embodiment herein, the security mesh of the dongle device has a plurality of patterns.

[0027] According to an embodiment herein, the security mesh provided at each cap sense electrode has a different pattern.

[0028] According to an embodiment herein, the pattern of the security mesh provided at each cap sense electrode is randomly selected at a time of manufacture. The pattern of the security mesh is provided at each capsense electrode at the time of manufacture is not known to a manufacturer.

[0029] According to an embodiment herein, the tamper detection circuit of the dongle device includes an input resistor and an output resistor connected at the two ends of each cap sense electrode.

[0030] According to an embodiment herein, the tamper detection circuit of the dongle device compares a voltage across the input resistor and a voltage across the output resistor to detect a tampering of the cap sense electrode.

[0031] According to an embodiment herein, a value of the input resistor and a value of the output resistor are set at the time of manufacture and the value of the input resistor and a value of the output resistor are not known for a manufacturer.

[0032] According to an embodiment herein, the value of the input resistor and a value of the output resistor are calibrated during a first use.

[0033] According to an embodiment herein, the dongle device comprises a magnetic card reader, a contact type card reader and a NFC reader.

[0034] 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 inserted through the slot for inserting 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.

[0035] According to an embodiment herein, the connector of the dongle device comprises a power module, a line detector module and a line for establishing a bi-directional data communication.

[0036] According to an embodiment herein, a card is read and the card data are transmitted through supersonic frequencies to a payment gateway server.

[0037] 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, inserting a card onto a dongle device, tracking a status of a card inserted, reading a card data on the dongle device, extracting a public key burnt on a flash of the dongle device, 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, collecting a transaction information through a graphical user interface (GUI), collecting a part of a card number from the

merchant, constructing a hash value out of the cipher data, 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.

[0038] According to an embodiment herein, the data communicated between the mobile device and the dongle is in a form of acoustic signals or audio tones.

[0039] According to an embodiment herein, the transaction information collected through the graphical user interface GUI is provided by the client application.

[0040] According to an embodiment herein, the hash value is collected out of the cipher data by using a hash algorithm. The hash algorithm is provided in the client application which is run on a mobile device. The hash algorithm is exchanged and stored between the mobile device and the payment server for a first time.

[0041] According to an embodiment herein, 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 processing the card data by a processor 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).

[0043] According to an embodiment herein, the dongle ID is a unique and secret ID related to the dongle.

[0044] 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.

[0045] 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 an amplitude for the audio signal.

[0046] 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 phone involves creating a date/time stamp.

[0047] According to an embodiment herein, the method for a secure electronic transaction using a dongle device further comprises sending an electronic receipt to the customer through a short message service (SMS) or an e-mail.

[0048] According to an embodiment herein, the method for a secure electronic transaction using a dongle device further comprises recording a transaction status by a counter of the microchip.

[0049] According to an embodiment herein, the method for a secure electronic transaction using a dongle device 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.

[0050] 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.

[0051] According to an embodiment herein, the unique PIN data is any one of a scrambled PIN data or a PIN block or a one time password (OTP).

[0052] According to an embodiment herein, the method for a secure electronic transaction using a dongle device further comprises an updating of the public key by inserting a non financial card on the dongle device, reading a swipe data by a reader head of the dongle device, extracting a public key from the card data and updating the public key associated with the dongle device.

[0053] According to an embodiment herein, the method for a secure electronic transaction using a dongle device further comprises mapping a merchant ID, a

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

[0054] According to an embodiment herein, the method for a secure electronic transaction using a dongle device further comprises mapping a dongle ID, a serial number of the dongle with IMEI number of a mobile phone for executing a secure electronic transaction.

[0055] According to an embodiment herein, the public key is burned into the dongle at a manufacturing time.

[0056] According to an embodiment herein, the dongle device 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 the secret key are encrypted by the public key and sent to the payment server.

[0057] According to an embodiment herein, the payment server further comprises a private key. The private key decrypts the secret key sent by the dongle device and sends back the decrypted secret key to the dongle for mutually authenticating the dongle device and the payment server.

[0058] According to an embodiment herein, the dongle device further comprises a NFC tag. The NFC tag of the dongle device includes a unique ID and a physical unclonable function (PUF).

[0059] According to an embodiment herein, the merchant device comprises a NFC tag. The NFC tag of the merchant device authenticates the dongle device by verifying the unique ID of the dongle NFC tag.

[0060] According to an embodiment herein, a card data is sent alone as an audio signal after tokenization and encryption.

[0061] 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

[0062] 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:

[0063] FIG. 1 illustrates a top perspective view of a dongle device with a cover, according to an embodiment herein.

[0064] FIG. 2 illustrates a front view of a dongle device with a cover, according to an embodiment herein.

[0065] FIG. 3 illustrates a back view of a dongle device, according to an embodiment herein.

[0066] FIG. 4 illustrates a left side view of a dongle device without a cover, according to an embodiment herein.

[0067] FIG. 5 illustrates a right side view of a dongle device without a cover, according to an embodiment herein.

[0068] FIG. 6 illustrates a first layer of the secondary circuit board placed inside the second half of the housing of the dongle device, according to an embodiment herein.

[0069] FIG. 7 illustrates a second layer of the secondary circuit board placed inside the second half of the housing of the dongle device, according to an embodiment herein.

[0070] FIG. 8 illustrates a third layer of the secondary circuit board placed inside the second half of the housing of the dongle device, according to an embodiment herein.

[0071] FIG. 9 illustrates a fourth layer of the secondary circuit board placed inside the second half of the housing of the dongle device, according to an embodiment herein.

[0072] FIG. 10 illustrates a tamper detection circuit of the dongle device, according to an embodiment herein.

[0073] FIG. 11 illustrates a circuit diagram of the second layer of the secondary circuit board indicating the capsense electrodes, according to an embodiment herein.

[0074] Although the specific features of the embodiments herein are shown in some drawings and not in others. This is done for convenience only as 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

[0075] In the following detailed description, a reference is made to the accompanying drawings that form a part hereof, and in which the specific 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.

[0076] The various embodiments herein provide a dongle device with tamper proof characteristics for a secure electronic transaction. The dongle device comprises a housing which includes a first half and a second half. A main circuit board is placed in the first half and a secondary circuit board placed is the second half. The housing further includes 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 processor continuously monitors a connection between the main circuit board and the secondary circuit board and detects a tampering of the compressible connector between the main circuit board and the secondary circuit board. The processor kills the dongle device when the processor detects a tampering of the compressible connector between the main circuit board and the secondary circuit board. The first half and the second half of the dongle device are ultrasonically sealed together. The main circuit board and the secondary circuit board are electrically and electronically connected through a compressible connector. The connector is an audio jack.

[0077] According to an embodiment herein, the processor kills the device by destroying all the keys used for encryption and making the dongle device non operative, when a tampering of the dongle device is detected.

[0078] According to an embodiment herein, the processor kills the device by destroying a public key used for generating all the keys employed for an encryption and making the dongle device non operative, when a tampering of the dongle device is detected.

[0079] According to an embodiment herein, the dongle device further comprises a tamper detection circuit connected to the processor to detect a tampering of the compressible connector between the main circuit board and the secondary circuit board.

[0080] According to an embodiment herein, the dongle device further comprises a battery to supply an electrical power to the tamper detection circuit, when an external power supply to the dongle device is disconnected.

[0081] According to an embodiment herein, the secondary board of the dongle device includes four layers. The four layers are a first layer, a second layer, a third layer and a fourth layer.

[0082] According to an embodiment herein, the first layer of the secondary board includes NFC antenna and LED.

[0083] According to an embodiment herein, the second layer of the dongle device includes a capsense electrode layer. The capsense electrode layer is formed right under the keypad. The capsense electrode layer is formed in a form of a mesh.

[0084] According to an embodiment herein, the third layer of the secondary board includes a security mesh to prevent a drilling to avoid a tampering of the key board.

[0085] According to an embodiment herein, the fourth layer of the secondary board includes a plurality of resistors to form a resistor ladder to detect a tampering of the security mesh.

[0086] According to an embodiment herein, the security mesh of the dongle device has a plurality of patterns.

[0087] According to an embodiment herein, the security mesh provided at each cap sense electrode has a different pattern.

[0088] According to an embodiment herein, the pattern of the security mesh provided at each cap sense electrode is randomly selected at a time of manufacture. The pattern of the security mesh is provided at each capsense electrode at the time of manufacture is not known to a manufacturer.

[0089] According to an embodiment herein, the tamper detection circuit of the dongle device includes an input resistor and an output resistor connected at the two ends of each cap sense electrode.

[0090] According to an embodiment herein, the tamper detection circuit of the dongle device compares a voltage across the input resistor and a voltage across the output resistor to detect a tampering of the cap sense electrode.

[0091] According to an embodiment herein, a value of the input resistor and a value of the output resistor are set at the time of manufacture and the value of the input resistor and a value of the output resistor are not known for a manufacturer.

[0092] According to an embodiment herein, the value of the input resistor and a value of the output resistor are calibrated during a first use.

[0093] According to an embodiment herein, the dongle device comprises a magnetic card reader, a contact type card reader and a NFC reader.

[0094] 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 inserted through the slot for inserting 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.

[0095] According to an embodiment herein, the connector of the dongle device comprises a power module, a line detector module and a line for establishing a bi-directional data communication.

[0096] According to an embodiment herein, a card is read and the card data are transmitted through supersonic frequencies to a payment gateway server.

[0097] 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, inserting a card onto a dongle device, tracking a status of a card inserted, reading a card data on the dongle device, extracting a public key burnt on a flash of the dongle device, 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, collecting a transaction information through a graphical user interface (GUI), collecting a part of a card number from the

merchant, constructing a hash value out of the cipher data, 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.

[0098] According to an embodiment herein, the data communicated between the mobile device and the dongle is in a form of acoustic signals or audio tones.

[0099] According to an embodiment herein, the transaction information collected through the graphical user interface GUI is provided by the client application.

[00100] According to an embodiment herein, the hash value is collected out of the cipher data by using a hash algorithm. The hash algorithm is provided in the client application which is run on a mobile device. The hash algorithm is exchanged and stored between the mobile device and the payment server for a first time.

[00101] According to an embodiment herein, 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.

[00102] According to an embodiment herein, the step processing the card data by a processor 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).

[00103] According to an embodiment herein, the dongle ID is a unique and secret ID related to the dongle.

[00104] 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.

[00105] 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 an amplitude for the audio signal.

[00106] 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 phone involves creating a date/time stamp.

[00107] According to an embodiment herein, the method for a secure electronic transaction using a dongle device further comprises sending an electronic receipt to the customer through a short message service (SMS) or an e-mail.

[00108] According to an embodiment herein, the method for a secure electronic transaction using a dongle device further comprises recording a transaction status by a counter of the microchip.

[00109] According to an embodiment herein, the method for a secure electronic transaction using a dongle device 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.

[00110] 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.

[00111] According to an embodiment herein, the unique PIN data is any one of a scrambled PIN data or a PIN block or a one time password (OTP).

[00112] According to an embodiment herein, the method for a secure electronic transaction using a dongle device further comprises an updating of the public key by inserting a non financial card on the dongle device, reading a swipe data by a reader head of the dongle device, extracting a public key from the card data and updating the public key associated with the dongle device.

[00113] According to an embodiment herein, the method for a secure electronic transaction using a dongle device further comprises mapping a merchant ID, a

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

[00114] According to an embodiment herein, the method for a secure electronic transaction using a dongle device further comprises mapping a dongle ID, a serial number of the dongle with IMEI number of a mobile phone for executing a secure electronic transaction.

[00115] According to an embodiment herein, the public key is burned into the dongle at a manufacturing time.

[00116] According to an embodiment herein, the dongle device 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 the secret key are encrypted by the public key and sent to the payment server.

[00117] According to an embodiment herein, the payment server further comprises a private key. The private key decrypts the secret key sent by the dongle device and sends back the decrypted secret key to the dongle for mutually authenticating the dongle device and the payment server.

[00118] According to an embodiment herein, the dongle device further comprises a NFC tag. The NFC tag of the dongle device includes a unique ID and a physical unclonable function (PUF).

[00119] According to an embodiment herein, the merchant device comprises a NFC tag. The NFC tag of the merchant device authenticates the dongle device by verifying the unique ID of the dongle NFC tag.

[00120] According to an embodiment herein, a card data is sent alone as an audio signal after tokenization and encryption.

[00121] FIG. 1 illustrates a top perspective 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 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 (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 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.

[00122] According to an embodiment herein, the dongle device is connected to the computing device (i.e. 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.

[00123] 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.

[00124] FIG. 2 illustrates a front view of a dongle with 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 (not shown in FIG. 2), a near field communication (NFC) card reader (not shown in FIG. 2), 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.

[00125] 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 showcased by illuminating the indicator 104.

[00126] 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 (not shown in FIG. 3). The USB socket 107 is used for charging the rechargeable battery of the dongle device 100. The rechargeable battery supplies power for the dongle device 100, when 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.

[00127] 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.

[00128] 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 fastening means 401 for fastening the cover. The card is read and the card data are transmitted through 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.

[00129] 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) 101, a USB socket 107, a connector110, a lanyard 106 and fastening means 401. The USB socket 107 is used for charging the rechargeable battery of the dongle device 100. The rechargeable battery supplies power for the dongle device 100, when 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 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.

[00130] 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.

[00131] 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.

[00132] 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.

[00133] 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.

[00134] According to an embodiment herein, the processor of the dongle device 100 interacts with a ezetap server through a mobile device or with the ezetap server directly. The processor interacts not only with the ezetap server through a mobile device but also with the payment gate way server.

[00135] According to an embodiment herein, the audio jack supports both a data transmission and an audio transmission with the mobile device.

[00136] According to an embodiment herein, a communication over the audio jack is done through the 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.

[00137] FIG. 6 illustrates a first layer of the secondary circuit board placed inside the second half of the housing of the dongle device, according to an embodiment herein. The dongle device comprises a housing. The housing includes a first half and a second half. The first half and the second half are ultrasonically sealed together. The main circuit board is placed in the first half and similarly the secondary circuit board is placed is the second half. The main circuit board and the secondary circuit board are electrically and electronically connected through a compressible connector. Further the processor is adopted for continuously monitoring a connection between the main circuit board and the secondary circuit board. If the connection between the main circuit board and the secondary circuit board is broken or tampered, the processor kills the dongle device. The secondary circuit board includes four layers. The four layers are a first layer,

a second layer, a third layer and a fourth layer. The first layer 600 comprises a NFC antenna 602 and a LED circuitry 601 as shown in FIG. 6. When the NFC card is tapped across the dongle device, the NFC antenna 602 reads a NFC tag in the NFC card and enables the dongle device to do a secure electronic transaction. The LED circuitry 601 process the input data provided by using the keypad on the dongle device and displays the input information on the LED display.

[00138] FIG. 7 illustrates a second layer of the secondary circuit board placed inside the second half of the housing of the dongle device, according to an embodiment herein. The second layer 700 includes capsense electrodes 701. The capsense electrodes 701 are formed right under the keypad of the dongle device. The capsense electrode 701 is formed in a form of a mesh as shown in FIG. 7.the pattern of mesh formed under each cap sense electrode is different to one another. The mesh pattern formed under each capsense electrode is randomly selected from a plurality of patterns and is formed during a manufacturing time and is not even known to a manufacturer.

[00139] FIG. 8 illustrates a third layer of the secondary circuit board placed inside the second half of the housing of the dongle device, according to an embodiment herein. The third layer 800 of the secondary circuit board of the dongle device includes a security mesh 801. The security mesh 801 prevents drilling, to avoid a tampering of the circuit board. The security mesh 801 includes a plurality of patterns. The security meshes 801 provided at each cap sense electrode has a different pattern. The patterns of the security mesh 801 provided at each cap sense electrode is randomly selected at a time of the manufacture of the dongle device. The patterns of the security mesh 801 are provided at each cap sense electrode at the time of manufacture is not known to a manufacturer.

[00140] FIG. 9 illustrates a fourth layer of the secondary circuit board placed inside the second half of the housing of the dongle device, according to an embodiment herein. The fourth layer 900 of the secondary circuit board includes a plurality of resistors as shown in FIG. 9 to form a resistor ladder to detect a tampering of the security mesh.

[00141] FIG. 10 illustrates a tamper detection circuit of the dongle device, according to an embodiment herein. The tamper detection circuit 1000 includes an input resistor and an output resistor connected at the two ends of each of the cap sense electrodes. The tamper detection circuit compares a voltage across the input resistor and a voltage across the output resistor to detect a tampering of the cap sense electrodes. The value of the input resistor and the value of the output resistor are set at the time of manufacture and the value of the input resistor and a value of the output resistor are not known for a manufacturer.

[00142] According to an embodiment herein, the value of the input resistor and a value of the output resistor are calibrated during a first use.

[00143] FIG. 11 is a circuit diagram of the second layer of the secondary circuit board illustrating the capsense electrodes, according to an embodiment herein. The second layer includes capsense electrodes. The capsense electrodes are formed right under the keypad of the dongle device. The capsense electrode is formed in a form of a mesh.

[00144] 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.

[00145] 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.

[00146] 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.

[00147] 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 tamper proof characteristics for a secure electronic transaction comprising:

a housing, and wherein the housing has a first half and a second half, and wherein the first half and the second half are ultrasonically sealed together;

a main circuit board placed in the first half;

a secondary circuit board is placed is the second half, and wherein the main circuit board and the secondary circuit board are electrically and electronically connected through a compressible connector;

a slot for swiping a magnetic stripe card;

a slot for inserting a contact type card;

a communication module;

a key pad;

a connector, wherein the connector is an audio jack;

a cover for safeguarding the connector;

a stylus:

a universal serial bus (USB) port;

a processor, wherein the processor continuously monitors a connection between the main circuit board and the secondary circuit board and wherein the processor detects a tampering of the compressible connector between the main circuit

board and the secondary circuit board, when the connection between the main circuit board and the secondary circuit board is broken or tampered, and wherein the processor kills the dongle device when the processor detects a tampering of the compressible connector between the main circuit board and the secondary circuit board; and

a display.

2. The dongle device according to claim 1, further comprises a tamper detection circuit connected to the processor to detect a tampering of the compressible connector between the main circuit board and the secondary circuit board.

3. The dongle device according to claim 1 further comprises a battery to supply an electrical power to the tamper detection circuit, when an external power supply to the dongle device is disconnected.

4. The dongle device according to claim 1, wherein the secondary board has four layers, and wherein the four layers are a first layer, a second layer, a third layer and a fourth layer.

5. The dongle device according to claim 1, wherein the first layer has NFC antenna and LED.

6. The dongle device according to claim 1, wherein the second layer has a capsense electrode layer, and wherein the capsense electrode layer is formed right under the keypad, and wherein the capsense electrode layer is formed in a form a mesh.

7. The dongle device according to claim 1, wherein the third layer has a security mesh to prevent a drilling to avoid a tampering of key board.

8. The dongle device according to claim 1, wherein the fourth layer has a plurality of resistors to form a resistor ladder to detect a tampering of the security mesh.

9. The dongle device according to claim 1, wherein the security mesh has a plurality of patterns.

10. The dongle device according to claim 1, wherein a security mesh provided at each cap sense electrode has a different pattern.

11. The dongle device according to claim 1, wherein a pattern of the security mesh provided at each cap sense electrode is randomly selected at a time of manufacture, and wherein the pattern of the security mesh is provided at each cap sense electrode at the time of manufacture is not known to a manufacturer.

12. The dongle device according to claim 1, wherein the tamper detection circuit has an input resistor and an output resistor connected at the two ends of each cap sense electrode.

13. The dongle device according to claim 1, wherein the tamper detection circuit compares a voltage across the input resistor and a voltage across the output resistor to detect a tampering of the cap sense electrode.

14. The dongle device according to claim 1, wherein a value of the input resistor and a value of the output resistor are set at the time of manufacture and the value of the input resistor and a value of the output resistor are not known for a manufacturer.

15. The dongle device according to claim 1, wherein the value of the input resistor and a value of the output resistor are calibrated during a first use.

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

17. 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 inserting 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.

18. 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.

19. The dongle device according to claim 1, wherein a card is read and the card data are transmitted through supersonic frequencies to a payment gateway server.

20. 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;

swiping a card onto a dongle;

tracking a status of a swipe;

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

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

processing the swipe data by a microchip 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 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 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, and wherein the transaction status is one of a bad transaction and a good transaction.

21. The method of claim 20, wherein the step 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);

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

22. The method of claim 20, 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;

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.

23. The method of claim 20, 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.

24. The method of claim 20, 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.

25. The method of claim 20, wherein the method further comprises sending an electronic receipt to the customer through a short message service (SMS) or an e-mail.

26. The method of claim 20, wherein the method further comprises recording a transaction status by a counter of the microchip.

27. The method of claim 20, 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,

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.

28. The method of claim 20, 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.

29. The method according to claim 20, wherein the unique PIN is data is any one of a scrambled PIN data or a PIN block or a one time password.

30. The method of claim 20, 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, extracting a public key from the swipe data and updating the public key associated with the dongle.

31. The method according to claim 20 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.

32. The method according to claim 20 further comprises mapping a dongle ID, serial number of dongle with IMEI number of a mobile phone for executing a secure electronic transaction.

33. The method according to claim 20, wherein the public key is burned inot the dongle at a manufacture time.

34. The method according to claim 20, wherein the dongle generates a session key and a secret key at the beginning of the transaction, and wherein the secret key is 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.

35. The method according to claim 20, wherein 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.

36. The method according to claim 20, wherein 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).

37. The method according to claim 20, 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.

38. The method according to claim 20, wherein a swipe data alone is sent as an audio signal after tokenization and encryption.



Date: 27 September 2012 **Rakesh Prabhu**

Place: Bangalore **Counsel for the Applicant**