Title: METHODS AND SYSTEM FOR SECURE DATA PROCESSING USING MOBILE DEVICES

Abstract: The present invention provides methods and systems for data processing such as data collection, verification and transmission with enhanced security performed using mobile devices using a transaction application integrated with a mobile device. A transaction application is integrated with a user's mobile device. The system comprises a centralized transaction module which enables a user to perform various transactions. The transactions can be selected from a group comprising making payments for goods purchased, account to account transfer, ATM cash withdrawal, internet banking and the like.
BACKGROUND

The present invention relates to data processing performed using mobile devices. More specifically, the present invention relates to data collection, verification and transmission with enhanced security performed using mobile devices using a transaction application integrated with a mobile device.

Payments made for goods purchased using cards with magnetic identification strip and smart cards, direct on the merchants end or using internet have gained significant popularity and have reduced the hassles of cash-based transaction significantly. Additionally, electronic account to account transfer, have facilitated to make transactions with great ease and enhanced security. These processes require a lot of data processing which are confidential and thus needs to be secure.

Data processing and transmission are secured by various means such as through various levels of encryption. However, data which are confidential such as data related to card with magnetic identification strip and smart cards, financial accounts and the like are prone to various threats of misuse at the time of collection.

However, the above mentioned processes require the availability of various means such as cards with magnetic identification strips and/or internet to make various transactions. Further, the data collection, verification and transmission such as data related to a card with magnetic strip and identification number, have to be performed with
added security. Thus there is a need of a unitary solution to further ease the data processing and make them more secure.

SUMMARY

An object of the present invention is to enable secure data processing for various transactions through mobile devices.

Another object of the present invention is secure identification of an entity through mobile devices.

Yet another object of the present invention is to provide a method and system for enabling payments at merchant's outlet for goods and services purchased through mobile device.

Yet another object of the present invention is to enable electronic accounts to accounts transfer of money through mobile devices.

Yet another object of the present invention is to enable withdrawal of cash from Automated Teller Machines (ATM) though mobile devices.

Yet another object of the present invention is to enable internet transactions with the help of mobile devices to enhance security.

BRIEF DESCRIPTION OF THE DRAWINGS

The preferred embodiments of the invention will hereinafter be described in conjunction with the appended drawings provided to illustrate and not to limit the invention, wherein like designations denote like elements, and in which:
FIG. 1 is a block diagram illustrating an environment in which present invention can be implemented, in an embodiment of the present invention.

FIG. 2 is a block diagram illustrating a mobile device and an integrated virtual transaction application in accordance with an embodiment of the present invention.

FIG. 3 is a flow chart illustrating a method for performing transaction at a merchant's Point of Sale (POS) terminal in accordance with an embodiment of the present invention.

FIG. 4 is a flow chart illustrating a method for performing account to account transfer in accordance with an embodiment of the present invention.

FIG. 5 is a flow chart illustrating a method for withdrawing money using a mobile device at an Automated Teller Machine (ATM) in accordance with an embodiment of the present invention.

FIG. 6 is a flow chart illustrating a method for bill payment using a mobile device in accordance with an embodiment of the present invention.

DESCRIPTION OF PREFERRED EMBODIMENTS

While the preferred embodiments of the invention have been illustrated and described, it will be clear that the invention is not limited to these embodiments only. Numerous modifications, changes, variations, substitutions and equivalents will be apparent to those skilled in the art without departing from the spirit and scope of the invention as described in the claims.
The present invention relates to data processing such as data collection, verification and transmission with enhanced security performed using mobile devices using a virtual transaction application integrated with a mobile device. In accordance with one embodiment of the present invention, the data processing is related to cash less 5transactions made to purchase a good from a merchant. Several other embodiments exists using data processing through mobile devices without departing from the scope of invention. In accordance with an embodiment of the present invention, the mobile device is selected from a group comprising cellular phones, Personal Digital Assistant (PDA), pagers, palmtops and the like. The system of carrying out the data processing through mobile device comprises a virtual transaction application downloaded and installed in user’s mobile device, a scanning module, a data transfer module, a centralized transaction module, user’s financial institution, merchant's financial institution and a mobile operator.

FIG. 1 is a block diagram illustrating a system 100 in which present invention can be implemented, in an embodiment of the present invention. System 100 consists of a mobile device 102. Mobile device 102 consists of a virtual transaction application 104. Mobile device 102 is communicated with a transaction server module 106. The communication takes place through a secure channel. Transaction server module is connected to a financial institution 110 to complete the transaction with an account associated with financial institution 110. The system further comprises a merchant's Point of Sale (POS) terminal or an Automated Teller Machine 108, where the transaction has to be carried out.

FIG. 2 is a block diagram illustrating a mobile device and an integrated virtual transaction application in accordance with an embodiment of the present invention.
Virtual transaction application 104 is downloaded and installed in the user's mobile device 102. Virtual transaction application 104 is password protected, and can be operated only when the correct password has been entered into virtual transaction application 104. The password can be selected from a group comprising alphabetical passwords, alphanumeric passwords and numeric passwords. Means for changing the password has been provided in virtual transaction application 104. In case the password is forgotten, it can be retrieved or reset using various means such as through customer care representatives. Virtual transaction application 104-in a user’s mobile device 102 is registered to the user's financial institution such as bank through the centralized transaction server module 106. Further, virtual transaction application 104 is registered with mobile device 102 to enhance security. Virtual transaction application 104 registered with mobile device 102 does not function in any other device in case a copy of virtual transaction application 104 is downloaded from a mobile device to another mobile device.

FIG. 3 is a flow chart illustrating a method for performing transaction at a merchant's Point of Sale (POS) terminal in accordance with an embodiment of the present invention. In accordance with an embodiment of the present invention, the method of data secure data processing for making transactions using mobile device comprises making payments for the goods purchased.

At step 302, a user enters a password to login and open virtual transaction application 104. At step 304, a user selects an option for payment of goods purchased through a merchant's POS. At step 306 a dynamic number is generated in virtual transaction application 104. At step 308 a visual identifier is generated in virtual transaction application 104 in the user's mobile device. In accordance with an
embodiment of the present invention, the visual identifier stores information such as user's name, address and account number. In accordance with various embodiments of the present invention the visual identifier is associated with the dynamic number generated at step 306. A different dynamic number and an associated visual identifier are generated after every successful login.

In accordance with an embodiment of the present invention, the visual identifier is selected from a group comprising linear barcodes, stacked barcodes, 2D barcodes, datamatrix and the like.

In accordance with one embodiment of the present invention, the visual identifier in virtual transaction application 104 stores information related to card with magnetic identification strips and facilitates card transaction through the user's mobile device. In accordance with an embodiment of the present invention the card with magnetic identification strip is a credit card, a debit card and the like. The card information stored in the visual identifier may comprise user's name, user's card number, card expiry date, card verification value code (CVV) and other related information.

In accordance with another embodiment of the present invention, the visual identifier in virtual transaction application 104 contains information related to a card with magnetic identification strip that requires a Personal Identification Number (PIN) for further transactions, and facilitates data processing for the card transaction through the user's mobile device. The card information stored in the visual identifier comprises user's name, user's card number and card expiry date. In accordance with yet another embodiment of the present invention, the visual identifier in virtual transaction application 104 contains information related to card along with the Personal Identification Number (PIN) of the card.
and facilitates card transaction through the user's mobile device. The stored PIN facilitates
the user to carry out card transaction without entering the PIN in the merchant's POS 108.

In accordance with yet another embodiment of the present invention one or more financial accounts can be integrated with virtual transaction application 104 in the user's mobile device. One or more financial accounts comprise one or more card accounts and the like.

In accordance to various embodiments of the present invention the visual identifier may store various data considering the security and practicality required. In accordance with an embodiment of the present invention, the visual identifier is generated dynamically to virtual transaction application 104 in the user's mobile device at every successful login to enhance security.

Merchant's POS terminal 108 is deployed at the merchant's end. A scanning module and a data transfer module are integrated with merchant's POS terminal 108. The scanning module facilitates in scanning the visual identifier generated in mobile device 15102. At step 308, the scanning module scans the visual identifier generated at virtual transaction application 104. At step 310, merchant's POS terminal 108 communicates with transaction server module 106 to complete the transaction for the goods purchased. The scanned visual identifier data is encrypted and sent to transaction server module 106. The data encryption in accordance to an embodiment of the present invention is done using an encryption algorithm selected from a group comprising PKI, RSA, Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple-DES, Skipjack and the like. Other encryption algorithms may also be used to enhance security and practicality in accordance with various embodiments of the present invention. Transaction server
module 106 authenticates merchant's POS terminal 108 and visual identifier data sent. Transaction server module 106 communicates with various financial institutions involved to complete the transaction.

Transaction server module 106 is a centralized server to enable secure data processing for transactions with various entities. In accordance with one embodiment of the present invention, the entities involved are a plurality of user's mobile device, merchant's point of sale module, user's financial institution and merchant's financial institution. Transaction server module 106 facilitates downloading and registration of virtual transaction application 104 on mobile device 102.

Virtual transaction application 104 is downloaded and registered on the user's mobile device. Merchant's point of sale module is registered to enable the transaction. User enters a password to unlock virtual transaction application 104 on user's mobile device. A visual identifier is generated in virtual transaction application 104 of the user's mobile device. The visual identifier is created dynamically at every login in virtual transaction application 104. After every successful login a different visual identifier is generated in the user's mobile device. The visual identifier stores information necessary to carry out the transactions. In accordance with an embodiment of the present invention, the visual identifier is selected from a group comprising linear barcodes, stacked barcodes, 2D barcodes, datamatrix and the like.

After the purchase of goods at a merchant's outlet is made, the user provides the visual identifier generated in the user's mobile device. The visual identifier is read by the merchant's point of sale module and the visual identifier data is sent to Transaction server module 106 for authorization. Transaction server module 106 authorizes the merchant's
point of sale module and the visual identifier data. The merchant's point of sale module transfers the invoice details to Transaction server module 106 and requests for completion of the transaction. Transaction server module 106 transfers the merchant's request to the user's financial institution. The user's financial institution serves or rejects the request based on the parameters set by the user's financial institution. In accordance with one embodiment of the present invention, the parameter set may be availability of cash in the user's account with the user's financial institution.

In case the user's financial institution authenticates and serves the request to enable the transaction, Transaction server module 106 sends a confirmation to merchant and the user's mobile device. The transaction is completed when the transfer between the user's account with the user's financial institution and the merchant's account with the merchant's financial institution is carried out.

In accordance with another embodiment of the present invention, the method of data processing for making transactions comprises fast, reliable and secure mode of transactions between a plurality of accounts through mobile devices. FIG. 4 is a flow chart illustrating a method for performing account to account transfer in accordance with an embodiment of the present invention. The plurality of account can be two accounts, one of sending user and another of receiving user. Sending user unlocks virtual transaction application 104 installed in sending user's mobile device by entering a valid password. Sending user selects an option for making account-to-account transfer from various options displayed in virtual transaction application 104 of the user's mobile device. Selecting the option for making account-to-account transfer opens up a form requiring various information to be filled up to enable account-to-account transfer using mobile
In accordance with an embodiment of the present invention, the information required to be filled up in the form is the receiving user's account number, where the money has to be transferred and amount. Other information can be required to be filled in the form without departing from the scope and spirit of the present invention in accordance with various embodiments of the present invention. Once the form is filled with required information, the user submits the request to Transaction server module 106 for authorization and to enable the account-to-account transfer. Transaction server module 106 then checks and authorizes the user's transaction application. Transaction server module 106 further checks the account number of the receiving user and available balance in the first user's account. Transaction server module 106 sends request for confirmation to receiving user's mobile device. In case the receiving user sends the confirmation, the accounts of sending and receiving users are updated. Transaction server module 106 sends the details related to the transaction query to the financial institutes of both sending and receiving users. The financial institute updates the accounts of both the user's with them and confirmation is send to both sending and receiving users.

In accordance with yet another embodiment of the present invention, the method of data processing for making transactions comprises withdrawing money from Automated Teller machines (ATM) associated with a financial institution using mobile device. FIG. 5 is a flow chart illustrating a method for withdrawing money using a mobile device at an Automated Teller Machine (ATM) in accordance with an embodiment of the present invention.

The ATM comprises a reading module and a data transfer module. User enters a password to unlock virtual transaction application 104 on user's mobile device. A visual
identifier is generated in the user's mobile device. In accordance with an embodiment of the present invention, the visual identifier is selected from a group comprising linear barcodes, stacked barcodes, 2D barcodes, datamatrix and the like. The visual identifier generated is dynamic and a new visual identifier is generated after every successful login in virtual transaction application 104 in the user's mobile device. The visual identifier stores information necessary to carry out transactions. The visual identifier is read by the reading module integrated in the ATM and the visual identifier data is sent to Transaction server module 106 for authorization. Transaction server module 106 authorizes the ATM and the visual identifier data. In accordance with one embodiment of the present invention, Transaction server module 106 sends the request to the financial institutions to process the cash withdrawal. Financial institution then serves or rejects the request based on the parameters set by the financial institution. In accordance with one embodiment of the present invention, the parameter set may be availability of cash in the user's account with the financial institution. In accordance with another embodiment of the present invention, Transaction server module 106 authorizes the ATM and the visual identifier data and transfers the user's details back to the ATM to carry out the cash withdrawal process. The ATM associated with a financial institution then serves or rejects the request based on the parameters set by the financial institution. In accordance with one embodiment of the present invention, the parameter set may be availability of cash in the user's account with the financial institution.

In accordance with yet another embodiment of the present invention, the method of data processing for making transactions comprises secure transaction through internet with the help of a mobile device. While making a transaction through internet, an account identifier code needs to be filled in the form displayed by a website enabling transactions.
User enters a password to unlock virtual transaction application 104 on user's mobile device. User selects an option for making transaction through Internet from various options displayed in virtual transaction application 104 of the user's mobile device. An account identifier code is generated in virtual transaction application 104 of the user's mobile device. The account identifier code is created dynamically and a different account identifier code is generated in the user's mobile device every time user selects the option for making transaction through Internet. After the account identifier is filled in, it is transferred to centralized transaction module from website. A confirmation is sent to the user's mobile device to proceed for the transaction. The transaction is made after the user agrees for the transaction.

In accordance with yet another embodiment of the present invention, the method of making transactions comprises purchase of tickets related to movies and other events, travel reservation and the like. Various options are displayed in virtual transaction application 104 integrated to user's mobile device enabling various transactions. The transaction comprises purchase of tickets for movies, events and the like. It further comprises reservations made for travel such as train, bus, airway reservations and the like. FIG. 6 is a flow chart illustrating a method for bill payment using a mobile device in accordance with an embodiment of the present invention.

In accordance with various embodiments of the present invention, the communication established to transfer data among various entities is carried out though a means selected from the group comprising Short Messaging Service (SMS), Multimedia Messaging Service (MMS) and General Packet Radio Service (GPRS). Other means to
transfer the data comprising Bluetooth, Infrared and like may be implemented in accordance with other embodiments of the present invention.
What is claimed is:

1. A system for performing transactions via a mobile device, the system comprising:
   a. a virtual transaction application integrated with the mobile device, the virtual transaction application providing an interface for generating a visual identifier, the visual identifier associated with a number, the number being generated dynamically at every transaction, the visual identifier being used to authorize transactions; and
   b. a transaction server module connecting the virtual transaction application to a financial institution through a secure channel, the transaction server module enabling the transaction by validating the visual identifier and the associated dynamic number.

2. The system of claim 1 wherein the virtual transaction application comprises:
   a. means for opening the virtual transaction application using a password;
   b. means for allowing a user to select an account from a plurality of accounts, registered with the virtual transaction application, using which the user performs the transaction.

3. The system of claim 2 wherein the virtual transaction application further comprises means for allowing the user to view the transaction history of the user.
4. A method of performing transaction using one or more mobile device, the
transaction being performed on a merchant's Point of Sale (POS) terminal, the
mobile device being used by a user, the mobile device comprising a virtual
transaction application integrated with the mobile device, the method comprising:

a. opening the virtual transaction application by entering a password

b. selecting an option for POS transaction in the virtual transaction application;

c. selecting an account from a plurality of accounts registered with the virtual
   transaction application, to perform the transaction;

d. generating a dynamic number, the dynamic number being generated at the
   virtual transaction application;

e. generating a visual identifier associated with the dynamic number, the visual
   identifier being generated at the virtual transaction application;

f. scanning the generated visual identifier, the visual identifier being scanned
   at the merchant's POS terminal;

g. sending the information related to the visual identifier and transaction
   request to a transaction server module, the information being sent by
   merchant's POS terminal;
h. verifying the information related to the visual identifier, the verification being done by the transaction server module;

i. sending the transaction request and the information related to the account to a financial institution;

if the transaction is authorized by the financial institute,

j. sending the successful transaction receipt to the merchant's POS terminal;

else,

k. sending the failure transaction information to the merchant's POS terminal;

5. The method of claim 4 wherein the visual identifier is a barcode.

6. The method of claim 4 wherein the visual identifier is a 2D matrix.

7. The method of claim 4 wherein the communication among the virtual transaction application, transaction server module, merchant's POS terminal and the financial institution is done through a secure channel.

8. The method of claim 4 wherein a different dynamic number is generated for every transaction.

9. A method of performing transaction using one or more mobile device, the transaction being performed to transfer money from a first account to a second account, the mobile device being used by a user, the mobile device comprising a
virtual transaction application integrated with the mobile device, the method comprising:

a. opening the virtual transaction application by entering a password

b. selecting an option for Peer-to-Peer (P2P) transaction in the virtual transaction application;

c. selecting the first account from a plurality of accounts registered with the virtual transaction application, to perform the transaction;

d. generating a dynamic number, the dynamic number being generated at the virtual transaction application;

e. entering details of a second account and an amount to be transferred to the second account;

f. sending the information related to the dynamic number and transaction request to a transaction server module, the information being sent by the virtual transaction application;

g. verifying the information related to the visual identifier, the verification being done by the transaction server module;

h. sending the transaction request and the information related to the account to a financial institution;
if the transaction is authorized by the financial institute,

i. sending the successful transaction receipt to the virtual transaction application;

else,

j. sending the failure transaction information to the virtual transaction application;

10. The method of claim 9 wherein the communication among the virtual transaction application, transaction server module and the financial institution is done through a secure channel.

11. The method of claim 9 wherein a different dynamic number is generated for every transaction.

12. A method of performing transaction using one or more mobile device, the transaction being performed to withdraw money from a first account, the money being withdrawn from an Automated Teller Machine (ATM), the mobile device being used by a user, the mobile device comprising a virtual transaction application integrated with the mobile device, the method comprising:

a. opening the virtual transaction application by entering a password

b. selecting an option for ATM transaction in the virtual transaction application;
c. selecting the first account from a plurality of accounts registered with the
virtual transaction application, to perform the transaction;

d. generating a dynamic number, the dynamic number being generated at the
virtual transaction application;

e. generating a visual identifier associated with the dynamic number, the visual
identifier being generated at the virtual transaction application;

f. scanning the generated visual identifier, the visual identifier being scanned
at the ATM;

g. sending the information related to the visual identifier and transaction
request to a transaction server module, the information being sent by ATM;

h. verifying the information related to the visual identifier, the verification being
done by the transaction server module;

i. sending the transaction request and the information related to the account to
a financial institution;

if the transaction is authorized by the financial institute,

j. sending the successful transaction receipt to the ATM;

else,

k. sending the failure transaction information to the ATM;
13. The method of claim 12 wherein the visual identifier is a barcode.

14. The method of claim 12 wherein the visual identifier is a 2D matrix.

15. The method of claim 12 wherein the communication among the virtual transaction application, transaction server module, merchant's POS terminal and the financial institution is done through a secure channel.

16. The method of claim 12 wherein a different dynamic number is generated for every transaction.

17. A method of performing transaction using one or more mobile device, the transaction being performed for a bill payment, the mobile device being used by a user, the mobile device comprising a virtual transaction application integrated with the mobile device, the method comprising:

   a. opening the virtual transaction application by entering a password

   b. selecting an option for bill payment in the virtual transaction application;

   c. selecting the first account from a plurality of accounts registered with the virtual transaction application, to perform the transaction;

   d. generating a dynamic number, the dynamic number being generated at the virtual transaction application;
e. selecting a biller from a plurality of billers registered with the virtual transaction application;

f. entering details of bill amount to be paid;

g. sending the information related to the dynamic number and transaction request to a transaction server module, the information being sent by the virtual transaction application;

h. verifying the information related to the visual identifier, the verification being done by the transaction server module;

i. sending the transaction request and the information related to the account to a financial institution;

if the transaction is authorized by the financial institute,

j. sending the successful transaction receipt to the virtual transaction application and the biller;

else,

k. sending the failure transaction information to the virtual transaction application;
18. The method of claim 17 wherein the communication among the virtual transaction application, transaction server module and the financial institution is done through a secure channel.

19. The method of claim 17 wherein a different dynamic number is generated for every transaction.
Enter password and open virtual transaction application

Select an option for POS in the virtual transaction application and choose account for transaction

Generate dynamic number and an associated visual identifier

Scanner scans the visual identifier at merchant's POS

Merchant's POS sends the scanned information to transaction server module

Transaction server module verifies the information related to the visual identifier

Is scanned information valid?

Send failure notice to merchant's POS

Transaction module forwards the transaction request to financial institute

Financial institution verifies the request and settle down the transaction

Is transaction authorized?

Successful transaction receipt sends to the merchant machine

Failure transaction information sends to the merchant machine
Enter password and open virtual transaction application

Select an option for P2P in the transaction application and choose account for transaction

Generate dynamic number

Enter details of beneficiary account

Virtual Transaction Application sends the scanned information to transaction server module

Transaction server module verifies the information related to the visual identifier

Is scanned information valid?

Transaction server module forwards the transaction request to financial institute

Financial institution verifies the request and settle down the transaction

Is transaction authorized?

Send failure notice to virtual transaction application

Failure transaction information sends to virtual transaction application

Successful transaction receipt sends to virtual transaction application

Fig. 4.
Enter password and open virtual transaction application

Select an option for ATM in the virtual transaction application and choose account for transaction

Generate dynamic number and an associated visual identifier

Scanner scans the visual identifier at ATM

ATM sends the scanned information to transaction server module

Transaction server module verifies the information related to the visual identifier

Is scanned information valid?

Send failure notice to ATM

Transaction module forwards the transaction request to financial institute

Financial institution verifies the request and settle down the transaction

Is transaction authorized?

Failure transaction information sends to the ATM

Successful transaction receipt sends to the ATM

Fig. 5.
Enter password and open virtual transaction application

Select an option for bill payment in the transaction application and choose account for transaction

Generate dynamic number

Select a biller from the list of registered billers

Enter amount to be paid

Virtual Transaction Application sends the transaction information to transaction server module

Transaction server module verifies the information

Is scanned information valid?

Send failure notice to virtual transaction application

Transaction server module forwards the transaction request to financial institute

Financial institution verifies the request and settle down the transaction

Is transaction authorized?

Failure transaction information send to virtual transaction application

Successful transaction receipt sends to virtual transaction application