FORM – 2

THE PATENTS ACT, 1970

(39 of 1970)

&

THE PATENTS RULES, 2003

COMPLETE SPECIFICATION

(See Section 10 and Rule 13)

A COMPUTER IMPLEMENTED SYSTEM AND METHOD FOR FACILITATING CARDLESS TRANSACTIONS

AGASHE, MANDAR

an Indian national,

of, “Chandrashekhar”, 242,

Shaniwar Peth, Pune- 411030,

Maharashtra, India.

The following specification particularly describes the invention and the manner in which it is to be performed

This application is a patent of addition to Indian Patent Application No. 57/MUM/2013 filed on January 8th, 2013, the entire contents of which are specifically incorporated herein by reference.

FIELD OF THE DISCLOSURE

The present disclosure generally relates internet commerce and, in particular, relates to systems and methods for performing financial transactions.

DEFINITIONS OF TERMS USED IN THE SPECIFICATION

The term ‘customer device’ used hereinafter in the specification refers to, but is not limited to, a mobile phone, a desktop, a laptop, a tablet, an iPad, a PDA, a notebook, a net book, a terminal including a wired or a wireless computing/communicating device.

The term ‘cash-dispensing-receiving machine’ used hereinafter in the specification refers to, but is not limited to, a cash dispenser, a cash machine, a cash depositor, an Automated-Teller-Machine (ATM), a ATM machine, a cashpoint, a chip and pin, and a cash terminal.

The term ‘communication network’ used hereinafter in the specification refers to, but is not limited to, a computer network, an Internet, an Intranet, a Wi-Fi network, Wi-Max network, online network, a Local Area Network (LAN), a Wide Area Network (WAN), a Metropolitan Area Network (MAN), a Near Field Communication (NFC), a Bluetooth network, a Bling network, a cellular network including a wired and a wireless network, and a combination thereof.

The above definitions are in addition to those expressed in the art.

BACKGROUND

Advancement in the computer technology has made life easy by facilitating e-transactions using payment cards such as credit cards, debit cards or various other redeemable cards. If a person is running out of cash, he or she can use a credit or a debit card to make transactions. This technological advancement has helped users to not to move with lot of cash all the time and also provided a portable access to the user's bank accounts whenever or wherever required.

With the growing and emerging new technologies, internet commerce took one more leap and introduced the concept of direct online payment or withdrawal of cash at any given point of time such as cash-dispensing-receiving machine station, net banking, PayPal and the like. Further to the aforementioned, an individual is now able to make online payments through their user devices and can also store their account details on their devices protected by a password.

However, in recent times a growing number of thefts and fraud activities are being noticed. A majority of the cases involve hacking of user online accounts or user devices, carrying out forging activities such as misuse of credit cards, debit cards or user account details and the like, particularly, from the place where money is deposited or withdrawn from a cash-dispensing-receiving machine station. It has been further observed, hackers are able to install a computer chip on the cash-dispensing-receiving machine which will automatically retrieve and store information pertaining to the card which is inserted into the cash-dispensing-receiving machine. This type of theft is called 'skimming' and involves installation of a hidden camera at the cash station to capture the punched passwords, typically four digit numbers, and a 'skimmer' attached to the cash-dispensing-receiving machine to read the card number. By matching the skimmed card number and the password, the card becomes vulnerable to unauthorized access and other malicious attacks.

In order to avoid such aforementioned malicious activities, there is a long felt need for a system that will enable users to carry out card transactions securely without compromising with the user's card details including card number and password or PIN (personal identification number).

OBJECTS

Some of the objects of the system of the present disclosure are to ameliorate one or more problems of the prior art or to at least provide a useful alternative are described herein below:

An object of the present disclosure is to provide a computer implemented system and a method for cardless transactions.

Another object of the present disclosure is to provide a system for facilitating cardless transactions between a customer device and a cash-dispensing-receiving machine.

Another object of the present disclosure is to provide a system to withdraw cash from a cash-dispensing-receiving machine securely without using a payment card, particularly a debit card.

Another object of the present disclosure is to provide a system to deposit cash into a cash-dispensing-receiving machine securely without using a payment card, particularly a debit card.

Another object of the present disclosure is to provide a system that does not require user signatures for performing transactions.

Another object of the present disclosure is to provide a system where the user does not have to disclose a secret personal identification number (PIN) associated with the payment card.

Another object of the present disclosure is to provide a system implemented with biometric features for performing high value transactions.

Other objects and advantages of the system of the present disclosure will be more apparent from the following description when read in conjunction with the accompanying figures, which are not intended to limit the scope of the present disclosure.

SUMMARY

The present disclosure envisages a computer implemented system and method for performing cardless transactions between a customer device and a cash-dispensing-receiving machine securely. The system provides a simple solution for performing a cardless transaction on an existing cash-dispensing-receiving machine. The system includes a customer interface which can be installed and accessed on the customer device and a cash machine interface installed and accessed on the cash-dispensing-receiving machine. The customer initiates the transaction by requesting for a One Time Password (OTP) via a communication network. A transaction server of the system receives the request from the customer device and generates the OTP for the transaction. Further, the transaction server communicates the generated OTP to the customer device via the communication network. The customer can communicate the OTP to the cash-dispensing-receiving machine via the communication network. The cash machine interface installed and executed on the cash-dispensing-receiving machine receives the customer communicated OTP and proceeds for the

validation of the OTP and completion of the customer initiated transaction either by dispensing cash to the customer or depositing cash for the customer.

BRIEF DESCRIPTION OF THE ACCOMPANYING DRAWINGS

The computer implemented system and method for facilitating cardless transactions on a cash machine will now be described with reference to the accompanying drawings, in which:

FIGURE 1 describes, a computer implemented system for facilitating cardless transactions between a customer device and a cash-dispensing-receiving machine, in accordance with the present disclosure; and

FIGURE 2(a) and 2(b) describes, a flow chart corresponding to the computer implemented method for facilitating cardless transactions between a customer device and a cash-dispensing-receiving machine, in accordance with the present disclosure.

DETAILED DESCRIPTION

The computer implemented system and method for facilitating cardless transactions of the present disclosure will now be described with reference to an embodiment which does not limit the scope and ambit of the disclosure. The description provided is purely by way of example and illustration.

The embodiment herein and the various features and advantageous details thereof are explained with reference to the non-limiting embodiments in the following description. Descriptions of well-known components and processing techniques are omitted so as to not unnecessarily obscure the embodiments herein. The examples used herein are intended merely to facilitate an understanding of ways in which the embodiments herein may be practiced and

to further enable those of skill in the art to practice the embodiments herein. Accordingly, the examples should not be construed as limiting the scope of the embodiments herein.

The description hereinafter, of the specific embodiments 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 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. 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 embodiments as described herein.

In the present scenario, a customer goes to a cash-dispensing-receiving machine station for the purpose of initiating a monetary transaction. Visiting the cash -dispensing-receiving machine station obviates the need for visiting a financial institution each time for withdrawing or depositing a cash amount. Typically, the customer uses his or her debit card for initiating the transaction and then enters a secret personal identification number (pin) associated with the debit card inserted into the cash -dispensing-receiving machine. This completes the customer initiated transaction either by dispensing or depositing the transaction amount. Herein above, there is a risk that card data as well as the secret pin can be stolen.

To obviate the drawbacks of the existing arts, the present disclosure envisages a computer implemented system and method for performing cardless transactions on existing cash -dispensing-receiving machines, interchangeably referred to as Automated Teller Machines (ATMs) or a cash machine. The system is accessible via a communication network. The system includes two types of interfaces namely, a cash machine interface and a customer interface. A financial institution, such as a bank, can register with the system by accessing a web application of the system and can install a cash machine interface on a cash machine installed at a particular location. Additionally, the financial institution can be provided with an option to install the cash machine interface on a plurality of cash-dispensing-receiving machines configured at various geographical locations. In turn, the financial institution is required to register each and every cash-dispensing-receiving machine on which the cash machine interface is installed, with the aforementioned computer implemented system. The cash machine is registered with the system using a unique cash-dispensing-receiving machine identification indicia. The cash machine interfaces installed and executed on the various cash machines at different locations either directly or indirectly in communication with a cash machine application installed on a server of the financial institution through a third party application. Thereby, the existing cash machine application enables the cash machine interface to access an existing repository to retrieve transaction related information for the purpose of completing a customer initiated transaction.

Further, a customer or a user can also get registered with the system, for example, by accessing a web application of the system using a customer device, and can install the customer interface on the customer device. On completion of the registration process, the system may transmits a verification message to the registered user to confirm the authenticity of the user as a registered user using at least one communication channel accessible to the customer such as an email,

a voice mail, a phone call, an instant message, and the like, based on user details provided by the user at the time of registration. The verification message may include a username and a password for the customer to login into the customer interface. A verification message is also sent to each of the registered cash-dispensing-receiving machine corresponding to the registered financial institution. This is done to check whether the cash machine is functioning properly or not. In an embodiment, verification messages are sent to the registered cash-dispensing-receiving machine in regular interval to check whether they are functioning properly or not.

Once the verification process is complete, the transaction server transmits a second message entailing a download link of the customer interface to the customer device. The customer device is registered with the system using a customer device identification indicia. As the customer device is registered with the customer device indicia and the cash-dispensing-receiving machine is registered with the cash machine identification indicia, enables the system of the present disclosure to identify each party involved in a transaction separately.

The system and method of the present disclosure will now be described herein below with reference to FIGURES 1 to 2.

FIGURE 1 illustrates a computer implemented system **100** for facilitating cardless transactions between a customer device **10** and a cash-dispensing-receiving machine **20**, in accordance with the present disclosure. The system **100** includes a customer interface **110** installed and executed on the customer device **10** accessible to the customer, a cash machine interface **120** installed and executed on the cash-dispensing-receiving machine **20** registered with a financial institution and in communication with a transaction server **130** via a communication network. In an embodiment, the customer interface **110** includes

a first trans-receiver **112** and a biometric module **114**. The cash machine interface **120**, on the other hand, includes a second trans-receiver **122**, a dispensing module **124**, and a depositing module **126**. Further, the transaction server **130** includes a customer repository **132**, a financial institution repository **134**, a third trans-receiver **136**, a fourth trans-receiver **138**, a One Time Password (OTP) generator **140**, and a validation module **142**.

In an embodiment, the customer interface **110** is configured to be identified with corresponding customer device identification indicia. The cash machine interface **120** is configured to be identified with the corresponding cash machine identification indicia. The customer repository **132** of the transaction server **130** stores customer related information such as customer registration information, customer identification (ID), customer privacy settings, financial account details of the customer, registered customer device identification indicia, and transaction history of the customer. The financial institution repository **134** of the transaction server **130** stores cash-dispensing-receiving machine information corresponding to a particular financial institution along with unique cash machine identification indicia for identifying each of the cash machines.

A registered customer may initiate a transaction by accessing the customer interface **110** on his/her customer device **10** and transmitting a first request to the transaction server **130** for generating an OTP for carrying out the transaction through the first trans-receiver **112** over the communication network. The third trans-receiver **136** of the transaction server **130** communicates with the customer interface **110** via the communication network for exchange of information. The third trans-receiver **136** receives the first request for generating the OTP from the customer interface **110** and further communicates the first request to the OTP generator **140**. The first request transmitted to the transaction server **130** from the customer interface **110** can include information

pertinent to the customer and/or the intended transaction such as customer ID, customer device identification indicia, a customer financial account details, a transaction amount and a combination thereof.

The OTP generator **140** based on the information received in the first request generates the OTP for the customer and transmits the generated OTP to the customer device **10** through the third trans-receiver **136** via the communication network. Additionally, the OTP generator **140** stores the generated OTP into the customer repository **132** corresponding to the customer for future reference.

The first trans-receiver **112** of the customer interface **110** executed on the customer device **10** receives the OTP from the transaction server **130**. Alternatively, the customer is facilitated to also use an IVR facility to connect with the transaction server **130** via a telecommunication network to create the OTP. The generated OTP can be combination of numbers, alphabets (including upper case or lower case) and special characters.

In accordance with the present disclosure, the customer communicates the received OTP from the transaction server **130** to the cash-dispensing-receiving machine **20** through a communication channel such as an email, an instant message, a voice call, a phone call via the communication network. In an embodiment, the communication network can be a wired or a wireless network or a combination of both. In another embodiment, the customer is enabled to communicate the OTP to the cash machine interface **120** manually by entering the OTP via a keypad (not shown in the figures) provided on the cash-dispensing-receiving machine **20**.

The second trans-receiver **122** of the cash machine interface **120** receives the OTP from the customer device **10**. To proceed with the transaction initiated by

the customer, the cash machine interface **120** transmits a second request via the second trans-receiver **122** to the transaction server **130** over the communication network for the completion of the transaction. The forth trans-receiver **138** of the transaction server **130** communicates with the cash machine interface **120** via the communication network and receives the second request. The second request transmitted to the transaction server **130** from the cash machine interface **120** may include, among other information, such as cash machine identification indicia, customer communicated OTP, transaction amount, financial institution associated with the customer and financial account details of the customer. The forth trans-receiver **138** of the transaction server **130** receives the second request and communicates the second request to the validation module **142**. The validation module **142** validates the information received, in particular the OTP, by comparing the customer communicated OTP with the OTP generated by the OTP generator **140** for the corresponding customer and stored into the customer repository **132**. In addition, the validation module **142** further validates the customer financial account associated with the customer ID, customer device **10** identification indicia, cash machine identification indicia, financial intuition associated with the customer, financial institution associated with the cash machine and the time limit of the OTP received from the cash machine interface **120**. In addition, the validation module **142** is further configured to check the limit of the financial balance of the customer's financial account in case the transaction type is to dispense the requested transaction amount to the customer. Subsequently, based on positive validation, the validation module **142** transmits a confirmation message to a third party payment gateway to proceed with the customer initiated transaction. The validation module **142** may also transmits a transaction confirmation message to both the customer device **10** received on the customer interface **110** and the cash-dispensing-receiving machine **20** received on the cash machine interface **120**.

In accordance with the present disclosure, the second trans-receiver **122** of the cash machine interface **120** receives the confirmation message from the transaction server **130**. Based on the positive validation and confirmation received from the transaction server **130**, the dispensing module **124** of the cash machine interface **120** is configured to dispense the transaction amount in the form of cash to the customer as requested. Likewise, based on the positive validation and confirmation received from the transaction server **130**, the depositing module **126** of the cash machine interface **120** is configured to deposit the transaction amount from the customer in the form such as cash, cheques, bills and the like, into the customer financial account. The dispensing module **124** and the depositing module **126** of the cash machine interface **120** individually mark completion of the customer initiated transaction and further record the transaction history.

In an embodiment, the OTP generated by the OTP generator **140** can be used for a single instance only. In case the customer attempts to use the OTP more than once, the transaction server **130** is enabled to generate an error message and report to customer user and the corresponding financial institution associated with the cash-dispensing-receiving machine **20**. After the expiry of the time period of the OTP, the OTP cannot be used for a transaction. The OTP is provided with a time limit, after the expiry of which, the OTP becomes invalid.

In accordance with the present disclosure, the customer interface **110** installed and executed on the customer device **10** can be further protected with a biometric password as per the requirement of the customer. For the purpose, the customer interface **110** further includes a biometric module **114** which enables the customer to create a biometric password and also store the biometric password into the customer repository **132** of the transaction server **130**. In an embodiment, for performing high valued transactions, the transaction server **130**

is enabled to ask the customer to provide the biometric password which can be a finger print, a voice recognition pattern, a face recognition pattern, a palm recognition pattern, an finger geometry recognition pattern, a signature recognition pattern, an eyes-iris recognition pattern, an eyes-retina recognition pattern, and a DNA recognition pattern. In one aspect of the present embodiment, the biometric password is requested before completing the customer initiated transaction such as before fulfilling the dispensing or depositing the transaction amount as requested by the customer. This feature further strengthens the security and safety of an innocent customer making a transaction.

In an embodiment of the system of the present disclosure, all the transaction steps are controlled by the customer. For example, even if the customer device **10** is stolen along with the user account details, financial transactions cannot be performed as the system **100** is provided with the functionality for receiving and authenticating username and password and/or a photograph of the customer each time the customer transmits the first request to the transaction server **130** for initiating the transaction.

In an embodiment of the present disclosure, the customer is provided with a physical card. This can be a dummy card configured to activate the existing cash-dispensing-receiving machines **20**. This card is provided to the customers to comply with the needs of the existing cash-dispensing-receiving machines **20**. Once the cash-dispensing-receiving machine **20** is activated with the help of the physical card provided to the customer, the cash machine interface **120** requests the customer to provide the OTP through a manually entry or via a communication network.

Referring FIGURE 2(a) and 2(b), illustrates a flow chart corresponding to a method for implementing for a computer implemented system for facilitating

cardless transactions between a customer device and a cash-dispensing-receiving machine. The computer implemented method includes the following steps:

- storing, in a customer repository of a transaction server, a customer registration information, customer privacy settings, financial account details of the customer, registered customer device identification indicia and transaction history of the customer **202**;
- storing, in a financial institution repository of the transaction server, at least one cash-dispensing-receiving machine information corresponding to a financial institution including a cash-dispensing-receiving machine identification indicia **204**;
- transmitting, via a communication network, from a customer interface accessible on a customer device, a first request for generating an One Time Password (OTP) for initiating a transaction to the transaction server, wherein the customer interface configured to be identified with a corresponding customer device identification indicia **206**;
- receiving, at the transaction server, the first request for generating the OTP from the customer device and identifying the customer device identification indicia stored in the customer repository **208**;
- generating, at the transaction server, the OTP and transmitting the generated OTP to the customer device via the communication network **210**;
- receiving, at the customer interface accessible on the customer device, the generated OTP and further communicating the received OTP to the cash-dispensing-receiving machine **212**;
- receiving, at a cash machine interface accessible on the cash-dispensing-receiving machine, the OTP received from the customer **214**;

- transmitting via the communication network, from the cash-dispensing-receiving machine to the transaction server, a second request to process the customer initiated transaction **216**; and
- validating, at the transaction server, the received OTP by comparing it with the OTP generated by the OTP generator for the corresponding customer, further transmitting a confirmation transaction confirmation to the customer device and the cash-dispensing-receiving machine on positive validation **218**.

In accordance with the present disclosure, the step of communicating the OTP to the cash machine interface further includes the step of submitting the OTP manually by entering the OTP via a keypad provided on the cash-dispensing-receiving machine.

In accordance with the present disclosure, the step of communicating the OTP to the cash machine interface further includes the step of communicating the OTP to the cash machine interface via a wired or a wireless communication.

In accordance with the present disclosure, the step of validating, at the transaction server, further includes the step of transmitting a confirmation message to a third party payment gateway to proceed with the customer initiated transaction.

In accordance with the present disclosure, the step of validating, at the transaction server, further includes the step of requesting and receiving a biometric password from the customer device for high valued transactions.

TECHNICAL ADVANCEMENTS AND ECONOMIC SIGNIFICANCE

The system for card transaction, in accordance with the present disclosure described herein above has several technical advantages including but not limited to the realization of:

- a computer implemented system and method for cardless transactions;
- a system for facilitating cardless transactions between a customer device and a cash-dispensing-receiving machine;
- a system to withdraw cash from a cash-dispensing-receiving machine securely without a financial card, particularly a debit card;
- a system to deposit cash into a cash-dispensing-receiving machine securely without a financial card, particularly a debit card;
- a secure system where the transaction PIN is a one-time-password and cannot be reused;
- a system that does not require user signatures for performing the transactions;
- a system where the user does not have to disclose his/her secret personal-identification-number (PIN) associated with the financial card.; and
- a system implemented with biometric feature for performing high value transactions.

Throughout this specification the word “comprise”, or variations such as “comprises” or “comprising”, will be understood to imply the inclusion of a stated

element, integer or step, or group of elements, integers or steps, but not the exclusion of any other element, integer or step, or group of elements, integers or steps.

The use of the expression “at least” or “at least one” suggests the use of one or more elements or ingredients or quantities, as the use may be in the embodiment of the disclosure to achieve one or more of the desired objects or results.

The numerical values mentioned for the various physical parameters, dimensions or quantities are only approximations and it is envisaged that the values higher/lower than the numerical values assigned to the parameters, dimensions or quantities fall within the scope of the disclosure, unless there is a statement in the specification specific to the contrary.

I CLAIM:

1. A computer implemented system for cardless transactions between a customer device and a cash-dispensing-receiving machine over a communication network, said system comprising:
    - said customer device comprising a first processor and a first memory to store and install a customer interface;
        - a first trans-receiver configured to transmit a first request for generating a One Time Password (OTP) for initiating a transaction and receiving the OTP from a transaction server, wherein said customer interface is identifiable by corresponding customer device identification indicia;
    - said cash-dispensing-receiving machine comprising a second processor and a second memory to store and install cash machine interface;
        - a second trans-receiver configured to receive the OTP submitted by the customer and further configured to transmit a second request to said transaction server to process the customer initiated transaction;
    - said transaction server comprising:
        - a customer repository configured to store customer registration information, customer identification (ID), customer privacy settings, financial account details of the customer, registered customer device identification indicia and transaction history of the customer;
        - a financial institution repository configured to store at least one cash-dispensing-receiving machine information corresponding to a financial institution;
        - a third trans-receiver in communication with said customer device, said third trans-receiver configured to transmit and

receive transaction related information from said customer device;

- a fourth trans-receiver in communication with said cash-dispensing-receiving machine, said fourth trans-receiver configured to transmit and receive transaction related information from said cash-dispensing-receiving machine;
- an OTP generator in communication with said third trans-receiver, said OTP generator configured to receive the first request for generating a OTP from said customer device, said OTP generator configured to identify the customer device identification indicia stored in said customer repository and generate a OTP for the corresponding customer, said OTP generator configured to transmit the OTP to the corresponding customer device via said third trans-receiver; and
- a validation module in communication with said fourth trans-receiver and said customer repository, said validation module configured to receive the OTP and a cash-dispensing-receiving machine identification indicia, said validation module configured to validate the received OTP by comparing it with the OTP generated by said OTP generator for the corresponding customer.

2. The system as claimed in claim 1, wherein the first request transmitted to said transaction server from said customer interface device includes information selected from the group consisting of a customer ID, a customer device identification indicia, a customer financial account details, a transaction amount and a combination thereof.
3. The system as claimed in claim 1, wherein the OTP generated includes information selected from the group consisting of a customer ID, a customer

device identification indicia, a customer financial account details, a transaction amount and a combination thereof.

4. The system as claimed in claim 1, wherein the second request includes information selected from the group consisting of a cash-dispensing-receiving machine identification indicia, the customer submitted OTP, transaction amount and customer financial account information.
5. The system as claimed in claim 1, wherein said validation module configured to validate a customer financial account associated with the customer ID, customer device identification indicia, cash-dispensing-receiving machine identification indicia and the time limit of the OTP received from said cash machine interface, subsequently based on positive validation of the OTP said validation module further configured to transmit a confirmation message to a third party payment gateway to proceed with the customer initiated transaction and further transmit a transaction confirmation message to said customer interface and said cash machine interface.
6. The system as claimed in claim 5, wherein based on positive validation of the OTP, said cash machine interface configured to complete the customer initiated transaction by performing an action selected from the group consisting of dispensing of cash and depositing of cash.
7. The system as claimed in claim 1, wherein the cash-dispensing-receiving machine information includes cash-dispensing-receiving machine identification indicia, location, and transaction history.

8. A method for implementing a computer implemented system for facilitating cardless transactions between a customer device and a cash-dispensing-receiving machine over a communication network, , said method comprising:
    - storing, in a customer repository of a transaction server, a customer registration information, customer privacy settings, financial account

details of the customer, registered customer device identification indicia and transaction history of the customer;

- storing, in a financial institution repository of said transaction server, at least one cash-dispensing-receiving machine information corresponding to a financial institution along with a cash-dispensing-receiving machine identification indicia;
- transmitting via a communication network, from a customer interface accessible on a customer device, a first request for generating an One Time Password (OTP) for initiating a transaction to said transaction server, wherein said customer interface configured to be identified with a corresponding customer device identification indicia;
- receiving, at said transaction server, the first request for generating the OTP from said customer device and identifying the customer device identification indicia stored in said customer repository;
- generating, at said transaction server, the OTP and transmitting the generated OTP to said customer device via the communication network;
- receiving, at said customer interface accessible on said customer device, the generated OTP and further communicating the received OTP to said cash-dispensing-receiving machine;
- receiving, at a cash machine interface accessible on said cash-dispensing-receiving machine, the OTP received from the customer;
- transmitting via the communication network, from said cash-dispensing-receiving machine to said transaction server, a second request to process the customer initiated transaction; and
- validating, at said transaction server, the received OTP by comparing it with the OTP generated by said OTP generator for the corresponding customer, further transmitting a confirmation

transaction confirmation to said customer device and said cash-dispensing-receiving machine on positive validation.

9. The method as claimed in claim 8, wherein the step of communicating the OTP to said cash machine interface further includes the step of submitting the OTP manually by entering the OTP via a keypad provided on said cash-dispensing-receiving machine.
10. The method as claimed in claim 8, wherein the step of communicating the OTP to said cash machine interface further includes the step of communicating the OTP to the cash machine interface via a wired or a wireless communication.
11. The method as claimed in claim 8, wherein the step of validating, at said transaction server, further includes the step of transmitting a confirmation message to a third party payment gateway to proceed with the customer initiated transaction.
12. The method as claimed in claim 8, wherein the step of validating, at the transaction server, further includes the step of requesting and receiving a biometric password from the customer device for high valued transactions.

Dated this 27th day of August 2014

MOHAN DEWAN
OF R. K. DEWAN & CO.
APPLICANT'S PATENT ATTORNEY

ABSTRACT

The present disclosure envisages a computer implemented system and method for facilitating cardless transactions between a customer device and a cash-dispensing-receiving machine. The system is accessible via a communication network and there are provided two types of interfaces namely, a cash machine interface and a customer interface. The cash-dispensing-receiving machines are registered with the system with respect to it's association with a financial institution. The cash machine interface is installed and executed on the cash-dispensing-receiving machine and the customer interface is installed and executed on the customer device. The customer initiates the transaction by requesting for a One Time Password (OTP) via a communication network. A transaction server of the system receives the request from the customer device and generates the OTP for the transaction. The customer transmits the OTP received from the transaction server to the cash-dispensing-receiving machine for the purpose of completing the initiated transaction.

NAME : AGASHE MANDAR
NO : 2789/MUM/2013

NO. OF SHEETS: 03
SHEET N0:01

COMPLETE SPECIFICATION

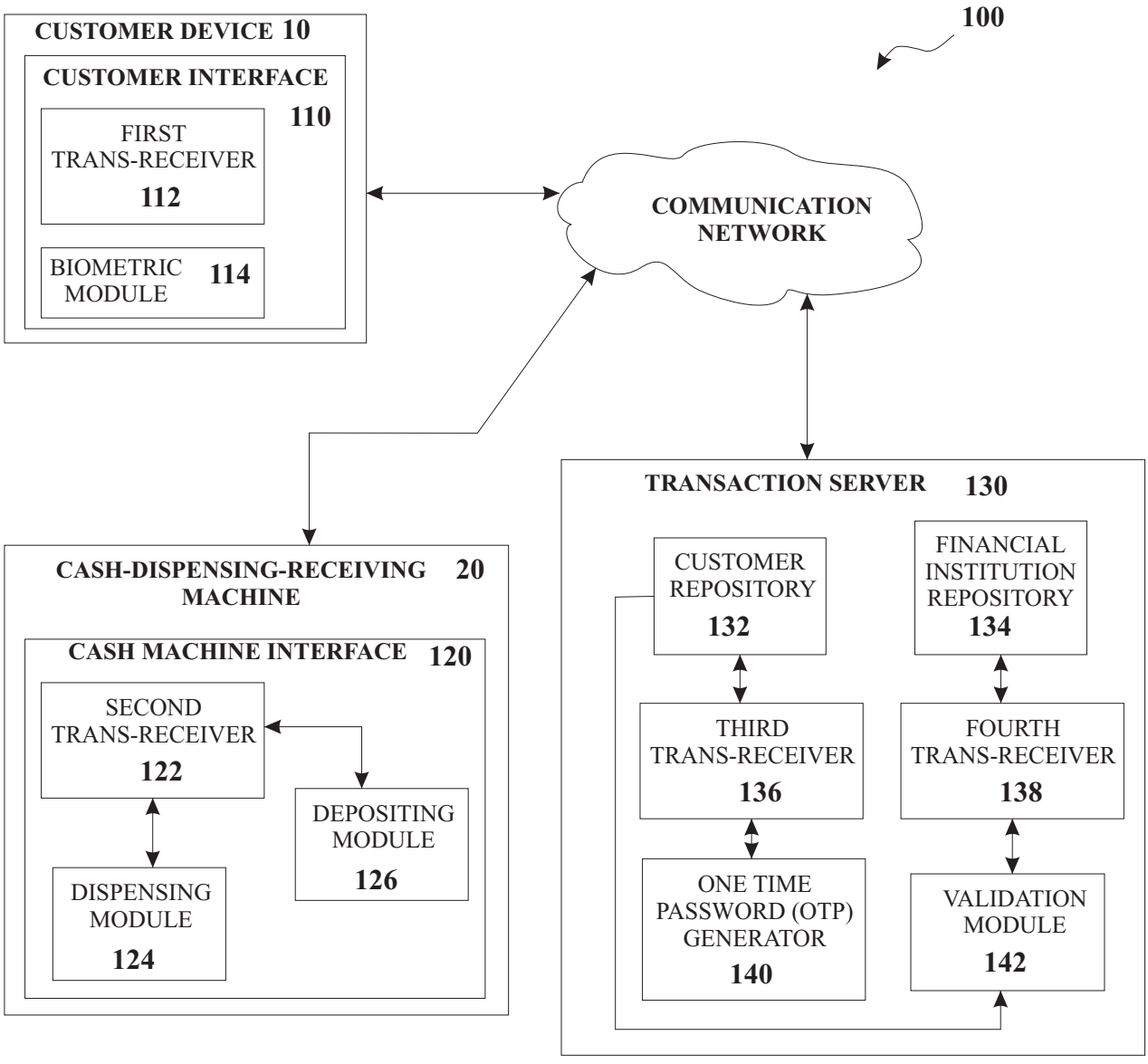

FIGURE 1

MOHAN DEWAN
of R.K. DEWAN & Co.
APPLICANTS' PATENT ATTORNEY

COMPLETE SPECIFICATION

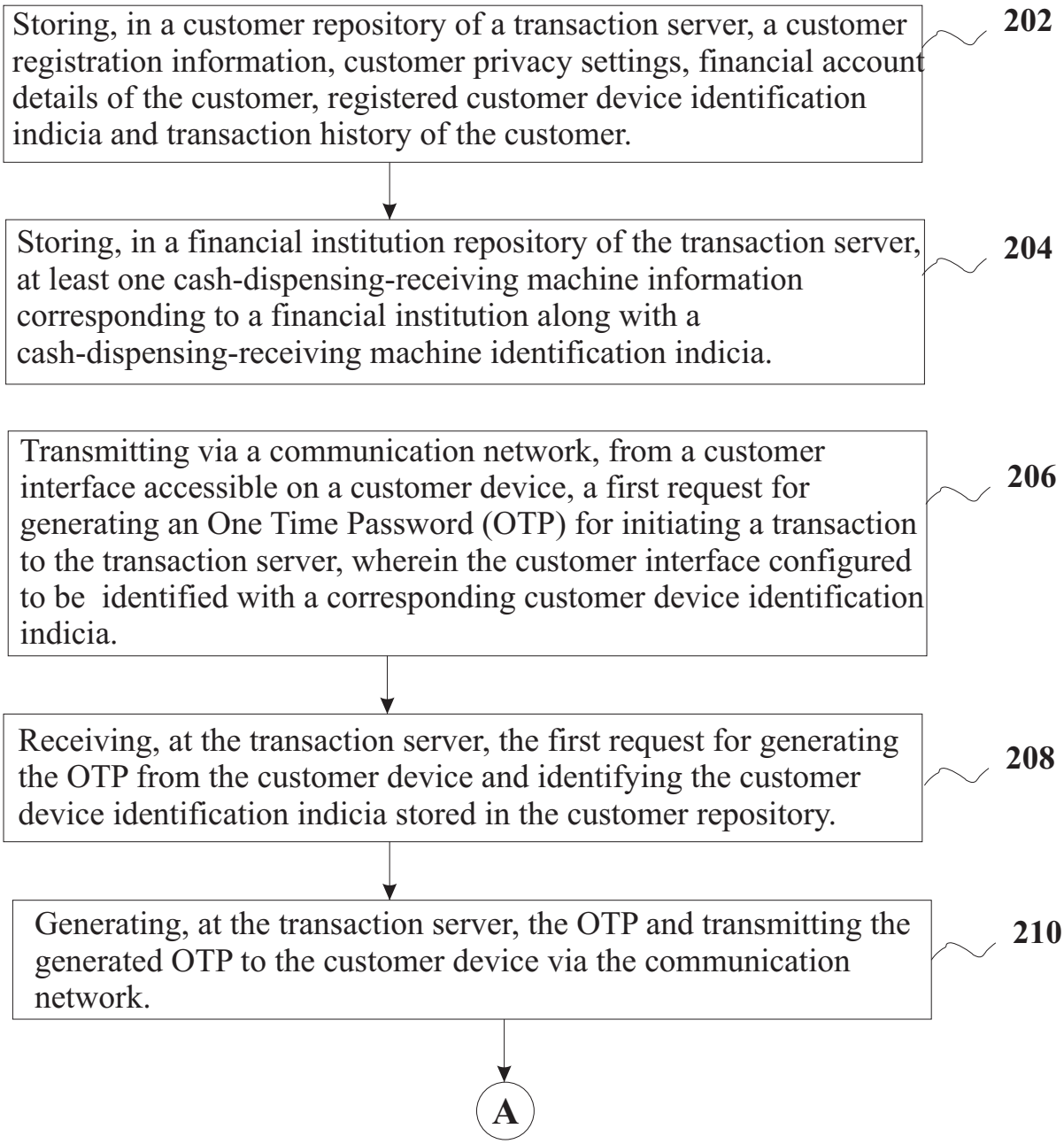

FIGURE 2(a)

MOHAN DEWAN
of R.K. DEWAN & Co.
APPLICANTS' PATENT ATTORNEY

COMPLETE SPECIFICATION

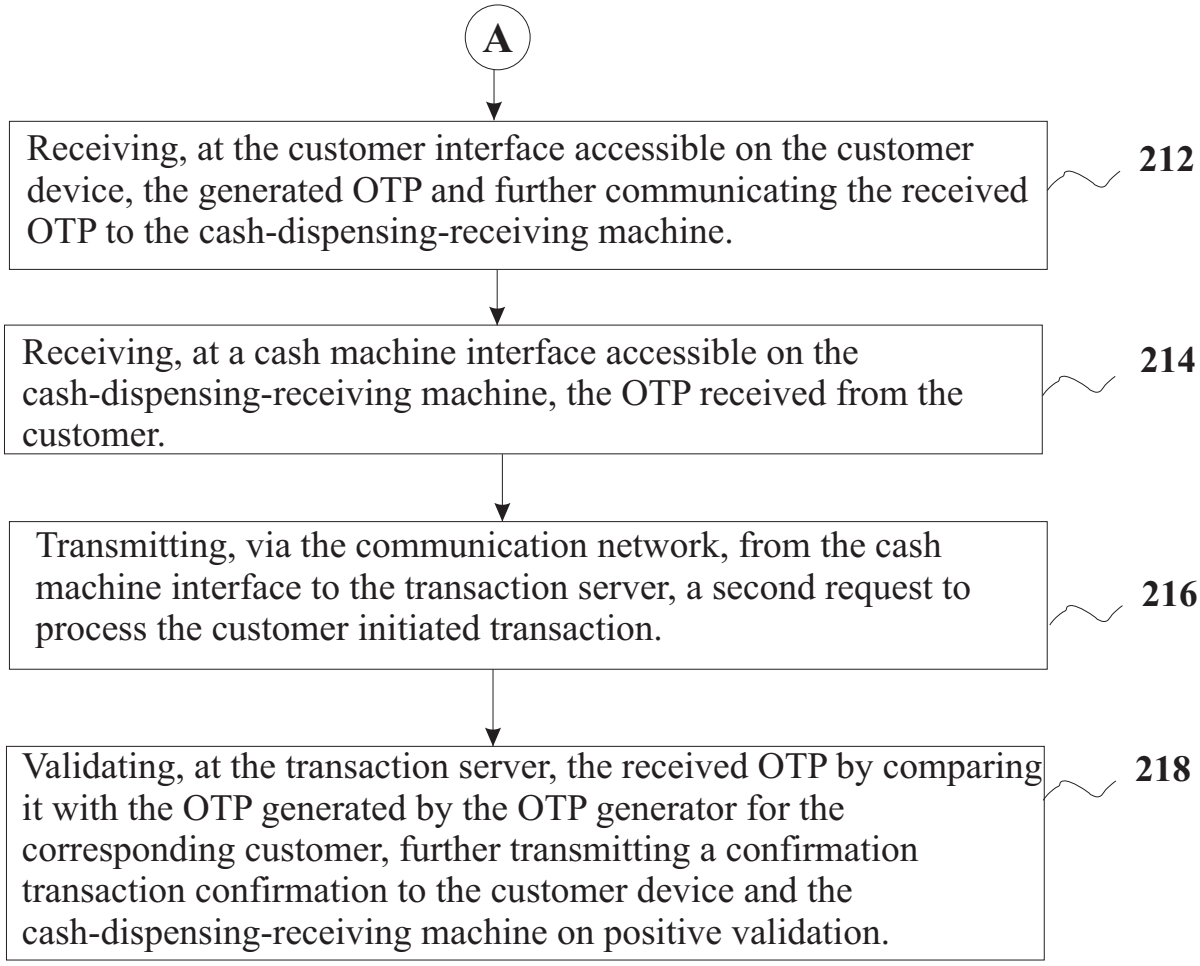

FIGURE 2(b)

MOHAN DEWAN
of R.K. DEWAN & Co.
APPLICANTS' PATENT ATTORNEY

FIELD OF THE DISCLOSURE

The present disclosure generally relates internet commerce and, in particular relates to system for performing financial transactions for making payments and withdrawal of cash using a card, particularly a debit or a credit card.

DEFINITIONS OF TERMS USED IN THE SPECIFICATION

The expression 'user' used hereinafter in the specification refers to but is not limited to a customer, payer, merchant, and payee.

The expression 'handheld device'/ landlines phone used hereinafter in the specification refers to but is not limited to mobile phones, laptops, tablets, desktops, iPads, PDAs, notebooks, net books and the like, including wired or wireless computing devices.

The above definitions are in addition to those expressed in the art.

BACKGROUND

E-commerce has made life easy by introducing the concept of e-transactions of finances through cards such as credit cards, debit cards or various other redeemable cards. If a person is running out of cash he can use his credit or debit card to make transactions. This concept helped users to not to move with lot of cash all the time and also provides a portable access to the user's bank accounts whenever or wherever required.

One individual (the payer) may wish to pay money to another individual (the payee) for variety of reasons. With the growing and emerging new technologies internet commerce took one more leap and introduced the concept of direct online payment such as net banking, PayPal and the like. Further to the aforementioned, an individual is able to make online payments through

handheld devices and can also store their account details on their handheld devices protected by password.

However, in recent times a growing number of thefts and fraud activities are registered in police FIRs. A majority of the registered cases involves hacking of user online accounts or user handheld devices, carrying out forging activities such as misuse of credit cards, debit cards or user account details and the like. Particularly where money is withdrawn from an ATM booth or machine a new type of card theft has been prevalent. This theft called 'skimming' involves installing a hidden camera in the ATM station in which the passwords, typically four numbers are keyed in are captured and a 'skimmer' attached to the ATM instrument reads the card number and by matching the skimmed card number and the password the card becomes vulnerable to attack.

Further, to avoid the aforementioned malicious activities, there is a long felt need for a system that will enable users to carry out card transactions securely without compromising the user's card and pin.

OBJECTS

Some of the objects of the system of the present disclosure, which at least one embodiment herein satisfies, are as follows:

An object of the present disclosure is to provide a system for secured card transactions.

An object of the present disclosure to provide a secure system where user ID (here user is a customer) is not made public.

Another object of the present disclosure is to provide a system to withdraw cash from an ATM machine securely with a card, particularly a debit card.

Another object of the present disclosure is to provide a system to deposit cash into an ATM machine securely with a card, particularly a debit card.

Still another object of the present disclosure is to provide system that does not require user signatures for performing transactions.

Further an object of the present disclosure is to provide a system implemented with biometric features for performing high value transactions.

Other objects and advantages of the system of the present disclosure will be more apparent from the following description when read in conjunction with the accompanying figures, which are not intended to limit the scope of the present disclosure.

DETAILED DESCRIPTION OF AN EMBODIMENT OF THE DISCLOSURE.

The system and method for card transaction of the present disclosure will now be described with reference to an embodiment which does not limit the scope and ambit of the disclosure. The description provided is purely by way of example and illustration.

The embodiment herein and the various features and advantageous details thereof are explained with reference to the non-limiting embodiments in the following description. Descriptions of well-known components and processing techniques are omitted so as to not unnecessarily obscure the embodiments herein. The examples used herein are intended merely to facilitate an

understanding of ways in which the embodiments herein may be practiced and to further enable those of skill in the art to practice the embodiments herein. Accordingly, the examples should not be construed as limiting the scope of the embodiments herein.

The description hereinafter, of the specific embodiments 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 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. 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 embodiments as described herein.

An individual willing to utilize the system of the present disclosure for carrying out his/ her financial transactions is required to register at least of one handheld device with the system along with I-PIN number of the handheld device.

On successful registration with the system an individual becomes a user or a member of the system. If a user of the system is a customer, the system as envisaged by the present disclosure provides a secure and unique code known as customer authentication code.

Current system

A person goes to a merchant or an ATM , he uses his debit card , he then enters his PIN and then the transaction gets completed. Here there is a risk that card data as well as pin can be stolen.

In accordance with the system according to this disclosure the use approaches the service provider, for example an ATM with his/her mobile device which has an application loaded thereon which links the mobile device directly with the service provider say for example the debit card provider . The mobile app is used to generate a random new Pin by the customer which can then be used instead of his regular Pin - Since this is one time use Pin it cannot be reused even if the card is stolen and also it becomes unusable after a time limit if not used. The mobile app is password protected by the customer and therefore even if the card and the mobile phone are both stolen at the same time the thief will still not be able to carry out an unauthorized transaction.

Thus the steps for carrying out the transactions are as follows. The customer generates a onetime Pin on his own hand held device to be used with his credit or debit card using a secure mobile app. This pin gets automatically notified to the card company at the back end.

This pin can be used on web or actual merchant or atm for one time use within a specified time limit.

Thus the pin is generated when the Customer logs into a Pin app or an app provided by his or her bank.

The customer uses this secure Pin or a Biometric Pin and logs into the app on his mobile.

The customer generates a one time pin or the customer can also select a random Pin and send it via the Pin app to get logged onto the back end system for one transaction

Alternatively, the customer can also send an sms to the backend server using the customer's registered mobile number or use an IVR system to create a single transaction Pin.

The app generates a onetime pin which has to be used within a certain time for the customer's debit card

The customer uses a regular debit card on the merchant POS device or on an ATM and enters the single transaction Pin.

The transaction will travel like a regular transaction to the bank switch where it will get authenticated using a Pin server provided to the bank

Similarly if the customer goes to an ATM the customer will enter this transaction Pin instead of the regular pin and do the transaction

The generated Pin can be combination of numbers, alphabets (including upper case or lower case) and special characters.

The aforementioned steps disclosed here and above for withdrawal of cash from an ATM machine can also be used for depositing cash into a user's financial institution account.

Typically, the message/s sent by the user as customer to the system either through the network provider or through the system via sms, mms, email, mobile application, IVR, audio and the like.

The time bound One Time Pin generated by the system can be used for a single instance only, if used more than once, the system will generate an error message and report to customer user and merchant user. After the expiry of the time period of the Pin, the Pin cannot be used for a transaction.

The time bound Pin generated can be used within a limited time period. After the expiry of the time period , it becomes invalid.

The system validation process of the user's account involves checking the limit of the withdrawal in case of a debit card, checking the available balance in case of debit card and the like.

Further, an embodiment of the present disclosure could also include a secure system incorporated with a biometric feature on the hand held device. For performing high value transactions the system will ask the user to provide a biometric parameter such as a thumb impression, a voice recognition pattern, a face recognition pattern, a palm recognition pattern and the like before releasing money from the user's account finally. This feature eliminates occurrence of any an unauthorized transaction.

In an embodiment of the system of the present disclosure, all the transaction steps are controlled by a user as customer for making payments. For example, even if the user handheld device is stolen along with the user account details, monetary transactions cannot be performed as the system is provided with a

means for receiving and authenticating user ID proof or photograph to perform transaction.

TECHNICAL ADVANCEMENTS AND ECONOMIC SIGNIFICANCE

The system for card transaction, in accordance with the present disclosure described herein above has several technical advantages including but not limited to the realization of:

- a system for card transactions;
- a secure system where the transaction Pin is a one time pin and cannot be reused ;
- a system that does not require user signatures for performing the transactions; and
- a system implemented with biometric feature for performing high value transactions.

Throughout this specification the word "comprise", or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated element, integer or step, or group of elements, integers or steps, but not the exclusion of any other element, integer or step, or group of elements, integers or steps.

The use of the expression "at least" or "at least one" suggests the use of one or more elements or ingredients or quantities, as the use may be in the embodiment of the disclosure to achieve one or more of the desired objects or results.

The numerical values mentioned for the various physical parameters, dimensions or quantities are only approximations and it is envisaged that the values higher/lower than the numerical values assigned to the parameters, dimensions or quantities fall within the scope of the disclosure, unless there is a statement in the specification specific to the contrary.

Dated this 27th day of August 2013.

MOHAN DEWAN
OF R. K. DEWAN & CO.
APPLICANT'S PATENT ATTORNEY