(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 January 2015 (15.01.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/004677 A1

(51) International Patent Classification:
G06Q 20/00 (2012.01) *H04L 9/32* (2006.01)
G06F 21/31 (2013.01)

(21) International Application Number:
PCT/IN2014/000437

(22) International Filing Date:
1 July 2014 (01.07.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2212/MUM/2013 1 July 2013 (01.07.2013) IN

(72) Inventor; and
(71) Applicant : **AGASHE, Mandar** [IN/IN]; "Chandrashekhar", 242, Shaniwar Peth, Pune 411030, Maharashtra (IN).

(74) Agent: **MOHAN, Dewan**; R. K. Dewan & Company, Trade Mark & Patent Attorneys, Podar Chambers, S.A.Brelvi Road, Fort, Mumbai 400001, Maharashtra (IN).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

— *of inventorship (Rule 4.17(iv))*

[Continued on next page]

(54) Title: A COMPUTER IMPLEMENTED SYSTEM AND METHOD FOR PERFORMING CASHLESS TRANSACTIONS

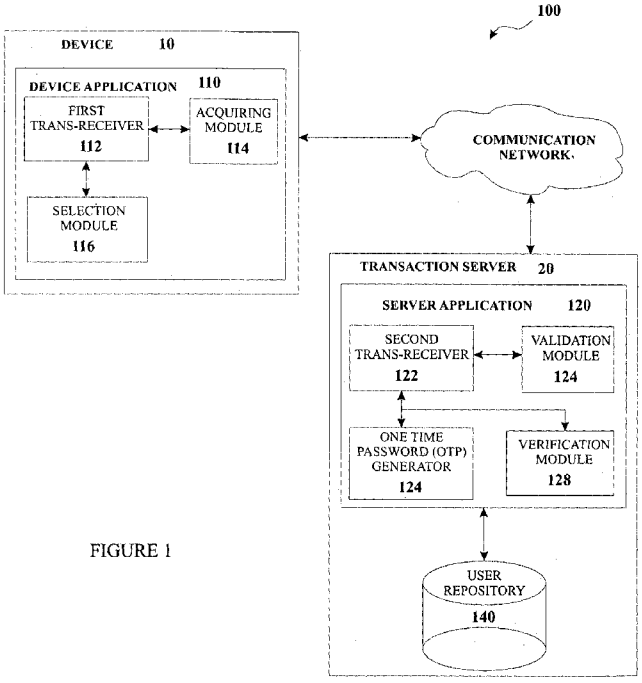

FIGURE 1

(57) Abstract: The present disclosure envisages a computer implemented system and method for performing cashless transactions. The system includes a device application can be installed and executed on a device accessible to a user and a server application configured in a transaction server. The user can register and download the device application on his/her device. A transaction is initiated by the user selecting the appropriate card (i.e. financial account detail related to the user) along with the transaction amount on the device application displayed on his/her device and further transmitting a request for a One Time Password (OTP) to the transaction server via a communication network. The server application is capable of generating a One Time Password (OTP) for the user initiated transaction. The OTP received by the user on his/her device can be utilized by the user for completing the monetary transaction.

WO 2015/004677 A1

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

A COMPUTER IMPLEMENTED SYSTEM AND METHOD FOR PERFORMING CASHLESS TRANSACTIONS

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 INVENTION

The present disclosure relates to a system and method for performing transactions over the World Wide Web.

DEFINITIONS OF TERMS USED IN THE SPECIFICATION

The expression 'device' used hereinafter in the specification refers to but is not limited to a mobile phones, a desktop, laptops, tablets, iPads, PDAs, notebooks, net books, terminals including wired or wireless computing/communicating devices.

The expression 'financial account' used hereinafter in the specification refers to but is not limited to a bank account, a financial repository account, a vault account, a credit union account, an investment firm account, a repository account, a PayPal account, and a Authorize.net account.

The expression 'authorizing interface' used hereinafter in the specification refers to but is not limited to a payment network, a VisaNet, a bank, a network, and a third party interface.

BACKGROUND OF INVENTION

Cash has been used as one of the most preferable modes of carrying out financial transactions, since decades. However, using cash as a mode of

transaction gets cumbersome when a large amount of money is required to be exchanged. Carrying a large amount of money, safeguarding the same against theft/robbery attempts involves a significant amount of overhead on the part of the people involved in said transaction.

Financial experts, have in the past attempted to reduce the dependency on hard cash and have introduced ways by which a transaction can be carried out without the exchange of hard cash. One of the ways of carrying out a transaction without using hard cash is by the way of cheque. Cheques were to a certain extent successful in reducing the dependency on hard cash. A cheque is typically available in paper-format. A cheque is exchanged between a payee and a payer. The payer presents the payee with a cheque and the payee is required to submit said cheque at his/her bank and wait for the transaction to be completed. A transaction, performed via a cheque requires at least three days for completion. Few of the drawbacks associated with cheque based transactions is that a cheque based transaction entails longer processing delays and cheque based transactions are prone to human errors.

To eliminate the disadvantages associated with cheque based transactions, internet commerce (e-commerce) was introduced. E-commerce or internet based transactions enable a person to use his/her credit/debit card to carry out a monetary transaction. Internet based transactions provide a person with remote access to his/her financial account and enable a person to carry out a transaction without walking into a bank and without using paper-based transaction methods. However, the drawbacks associated with internet based transactions are that they also suffer from processing delays and that they are prone to hacker attacks. The major drawback associated with internet based transactions is that the confidential information including the credit card number, the CVV (Card Verification Value) number and the card expiry date are transmitted through

public internet networks. Such transmissions are often prone to various types of hacker attacks and the confidentiality of the credit/debit card information is liable to be compromised.

Therefore, in order to overcome the drawbacks of the prior art systems, the present disclosure envisages a computer implemented system and method which enables a user to securely carry out his/ her transactions. The present disclosure envisages a system and a method which ensures that a user's confidential information remains secured and that it is not exposed to any sort of hacker attacks.

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 that provides complete security for the transactions performed by a user on the World Wide Web.

Another object of the present disclosure is to provide a system that offers a user a convenient, yet safe way of performing transactions.

Another object of the present disclosure is to provide a system that enables a user to perform transactions without making physical use of credit/debit cards.

Another object of the present disclosure is to provide a system that is cost-effective and compatible with existing hardware infrastructure.

Another object of the present disclosure is to provide a system that prevents the occurrence of fraudulent transactions.

SUMMARY

In an aspect of the present disclosure envisages a computer implemented system and method for performing cashless transactions. The system includes a two types computer applications a) a device application and b) a server application. The user can register with the system by accessing a web application of the system and receive a link to download and execute the device application on his/her registered device. The server application is configured in a transaction server for facilitating and managing the transactions performed by the user. The server application and the device application being accessible to each other via secure communication network. The server application is capable of generating a One Time Password (OTP) for the user initiated transaction by enabling the user to select the appropriate card (i.e. financial account detail related to the user) along with the transaction amount on the device application displayed on his/her device. The OTP received by the user on his/her device can be utilized by the user for completing the monetary transaction by entering on a commercial web page for purchasing any commodities or goods.

BRIEF DESCRIPTION OF THE ACCOMPANYING DRAWINGS

The computer implemented system and method for performing cashless transaction will now be described with reference to the accompanying drawings, in which:

FIGURE 1 describes, by the way of example, a computer implemented system for performing cashless transactions; and

FIGURE 2(a), 2(b) and **2(c)** describes, by the way of example, a flow chart corresponding to the computer implemented method for performing cashless transactions.

DETAILED DESCRIPTION

The computer implemented system and method for cashless transactions of the present disclosure will now be described with reference to the accompanying drawings which do not limit the scope and ambit of the disclosure. The description provided is purely by way of example and illustration.

The embodiments 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.

The present disclosure envisages a system and method for performing cashless transactions. Referring to the accompanying drawings, **FIGURE 1** illustrates a system **100** which includes a device application **110** installed and configured in a device **10** accessible to a user and a server application **120** configured in a transaction server **20.** The system **100** further includes a web application accessible through a web browser installed on the device **10** such as Internet Explorer of the Windows operating system. The device application **110** and the server application **120** are accessible to each other via a communication network. The communication network is selected from the group consisting of a computer network, an Internet, an Intranet, a Wi-Fi network, a Wi-Max network, an 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 cellular network including a wired and a wireless network, and a combination thereof.

In accordance with the present disclosure, the device application **110** includes a first trans-receiver **112**, an acquiring module **114** and a selection module **116.** The server application **120** includes a second trans-receiver **122**, a validation module **124**, a One Time Password (OTP) generator **126**, and a verification module **128.** In addition, the transaction server **20** includes a user repository **140** accessible by the server application **120.** The second trans-receiver **122** of the server application **120** is capable of communicating with the user repository **140** for the purpose storing and retrieving user related data.

The user can register with the system **100** by accessing the web application of the system **100** and can install the device application **110** on the device **10.** On completion of the registration process on the web application, the transaction server **20** of the system **100** stores the user related information into a user repository **140.** This user related information includes user registration

information, user login credentials, contact details, information related to user's financial accounts, unique device identification provided to the device **10** registered corresponding to the user. The user repository **140** is accessible by the server application **120** configured in the transaction server **20**. The transaction server **20** transmits a registration confirmation message to the registered user's contact details in a format such as an email format, an instant message format, a short messages service (SMS) format, a text message format and a combination thereof on successful completion of the registration process. The registration confirmation message is sent to the device **10** accessible to the user to confirm the authenticity of the registered user. The registration confirmation message includes a welcome note along with a link to download the device application **110** on the device **10** accessible to the user. The user can download the device application **110** on his/her device **10** and install the device application **110** for performing cashless transactions. In addition, a unique device identification is provided to the device **10** registered with the user. The details provided by the user, viz., the credit card details/debit card details/net banking account details are securely stored in a user repository **140** which is housed at a transaction server **20**.

In accordance with the present disclosure, whenever a user, registered with the system **100** decides to perform a transaction using his device **10** i.e., monetary transaction involving buying of commodities/goods, over the World Wide Web, he/she is required to click on the device **10** accessible to him/her. On the device application **110**, the user is provided with a window that asks the user to provide his/her login credentials. The acquiring module **114** acquires user login credentials from the user for initiating a transaction. Once the user provides his/her login credentials, the same are transmitted over a secured network connection to the transaction server **20** through the first trans-receiver **112**. The acquired login credentials are transmitted to the transaction server **20** for the

purpose of authentication. At the transaction server **20**, the second trans-receiver **122** of the server application **120** receives the acquired user login credentials. The second trans-receiver **122** in communicates the user login credential received from the device **10** to the validation module **124**. The validation module **124** validates the received user login credentials with the user credentials stored into the user repository **140**. Subsequent to successful validation of the log-in credentials, the second trans-receiver **122** of the server application **120** transmits a validation confirmation message to the corresponding device **10**.

The first trans-receiver **112** of the device application **110** receives the validation confirmation message from the transaction server **20** and further prompts the user on the device application **110** a list of credit cards/debit cards/net banking accounts that he/she had previously registered with the system **100**. The selection module **116** of the device application **110** receives a user selected financial account detail for the transaction. Subsequent to the user selecting a particular registered card and a particular amount for the transaction, the selection module **116** in communication with the first trans-receiver **112** and transmits the user selected financial account detail and the transaction amount to the transaction server **20** over a secured communication network. At the server application **120** of the transaction server **20**, the second trans-receiver **122** receives the user selected financial account detail and the transaction amount and triggers the One Time Password (OTP) generator **126**. The OTP generator **126** generates an OTP for the corresponding user initiated transaction. Subsequently, the OTP generated for a particular user is mapped on to the credit card/debit card/net banking account details corresponding to the to the credit card/debit card/net banking account selected by the user for performing the transaction. The OTP generated by the OTP generator **126** can consist of numerals or alphabets or a combination thereof. Further, the OTP generated has

time limit and therefore the user required to use the OTP for the transaction with the time limit of the OTP otherwise validity of the OTP will expire. In addition, the OTP generator **126** includes an OTP-database **126A** to store the generated OTP for the corresponding user. The OTP-database **126A** housed within the OTP generator **126** stores the OTP temporarily.

The OTP generated by the OTP generator **126** is communicated to the device **10** accessible to the user, by the way of an email or SMS (Short Message Service) or via an interactive voice recorder. The OTP generator **126** communicates the OTP to the second trans-receiver **122** which in turn transmits the OTP to the device **10** via a secured communication network.

In accordance with the present disclosure, the user accessing a third party commercial websites on the World Wide Web for purchasing commodities or goods online can enter the received OTP on a window provided on the web page on which he/she want to perform the transaction. The user, typically types out the OTP received on his/her device **10** on a window provided at the web page on which he/she performed the transaction. Once the user enters the received OTP on a window provided at the web page, the OTP entered by the user is transmitted to the transaction server **20** over a secured communication link. This is done by an authorizing interface interfaced with the third party commercial websites and the transaction server **20** through the communication network.

In accordance with the present disclosure, when the server application **120** of the transaction server **20** receives the OTP entered by the user, the second trans-receiver **122** triggers a verification module **128** which in turn verifies the OTP entered by the user with the entries (corresponding to OTPs) stored into the OTP-database **126A** corresponding to the user. The verification module **128**

also verifies whether the time limit of the OTP has expired. The verification module **128** runs a comparison on the OTPs stored in the OTP-database **126A** and the OTP input by the user, and if the OTP entered by the user matches with any of the OTP entries stored in the OTP-database **126A**, the transaction performed by the user is authenticated. Subsequent to the authentication of the OTP, the details corresponding to the credit card/debit card/net banking account are retrieved based on the mapping between the OTP and said details, and the transaction initiated by the user is further processed. Any of the well-known methods can be utilized for processing and clearing the transaction. Such a well-known method of processing a transaction is not discussed for the sake of brevity. The entries stored in the OTP-database **126A** are dynamically updated as soon as the OTPs are sent to the user at the first instance.

In accordance with the present disclosure, the OTP generated by the transaction server **30** can be utilized by the user to purchase goods/commodities from any normal store or a tele shopping network or an IVR (Interactive Voice Response) based shopping network. In one embodiment, if the user is visiting a normal store, the user is required to type out the OTP received on his/her device **10**, into a POS terminal located at the store. The OTP acts as a substitute for swiping the credit/debit card. Subsequently, the OTP is transferred from the POS terminal to the transaction server **20** via a communication network. The transaction server **20** subsequently triggers a verification module **128** which in turn, verifies the OTP entered by the user with the entries (corresponding to OTPs) stored in the OTP-database **126A**, and derives the card details from the OTP if the OTP entered by the user is appropriate.

In another embodiment, if the user is visiting an online tele shopping network or an IVR based shopping network, the user is required to enter the OTP received by him/her on the device **10**. The OTP is required to be entered by the user

through a device (preferably device **10**) that he/she uses to connect to the tele shopping network/IVR based shopping network. In case of an IVR based shopping network, the user can read out the OTP delivered to him/her. Subsequently, the OTP is transferred to the transaction server **20** via a communication network. The server application **120** of the transaction server **20** subsequently triggers the verification module **128** which in turn, verifies the OTP entered by the user with the entries (corresponding to OTPs) stored in the OTP-database **126A,** and derives the card details from the OTP if the OTP entered by the user is appropriate.

Referring to **FIGURE 2(a)**, **2(b)**, and **2(c)**, there is shown a flow chart corresponding to the method for implementing a system **100** of FIGURE 1 for performing cashless transactions. The system **100** includes a device application **110** and a server application **120**. The device application **110** is installed and executed on a device **10** accessible to the user and the server application **120** is configured on a transaction server **20**. The device application **110** and the server application **120** being accessible to each other via a communication network. The method, in accordance with the present disclosure includes the following steps:

- STEP 202 - enabling a user to access the device application **110** displayed on the device **10**;
- STEP 204 - prompting the user to enter his/her login credentials and transmitting the acquired user credential to the transaction server **20**;
- STEP 206 – verifying at the server application **120** of the transaction server **20**, the login credentials entered by the user and transmitting a verification confirmation message to the corresponding device **10** accessible to the user;
- STEP 208 – receiving at the device application **110**, the verification confirmation message from the transaction server **20** and prompting the

user to enter the details corresponding to his credit cards/debit cards and net banking account details, further transmitting the acquired user's credit cards/debit cards and net banking account details to the transaction server **20** through a secured communication network;

- STEP 210 – receiving and storing at the transaction server **20**, the details corresponding to the credit cards/debit cards/net banking accounts received from the device **10**, in a user repository **140** housed on the transaction server **20** and accessible to the server application **120**;
- STEP 212 - redirecting the user to the device application **110** in the event that the user wish performs a monetary transaction on a web page displayed on World Wide Web, in order to initiate the transaction;
- STEP 214 - prompting the user to enter his/her login credentials and further prompting the user after successful validation to select a particular card and corresponding transaction amount for completing the transaction, additionally, transmitting the acquired user selected card detail to the transaction server **20**;
- STEP 216 - receiving at the server application **120** the acquired user selected card detail and generating an OTP corresponding to the transaction, further associating a time limit to the generated OTP;
- STEP 218 - mapping the generated OTP to the credit card/debit card/net banking account details corresponding to the to the credit card/debit card/net banking account selected by the user for performing the transaction;
- STEP 220 - transmitting the OTP to the device **10** accessible to the user via a secured communication link;
- STEP 222 - receiving the device application **110**, the received OTP generated by the transaction server **20** for completing the user initiated transaction;

- STEP 224 - prompting the user to enter the received OTP on the web page displayed on World Wide Web for completing the user desired transaction;
- STEP 226 - transmitting the user entered OTP n the web page displayed on World Wide Web to the transaction server **20**;
- STEP 228 - comparing at the server application **120**, the OTP entered by the user with a list of OTPs stored in a OTP-database;
- STEP 230 - determining if the OTP entered by the user matches with any of the OTP entries stored in the OTP-database and further checking whether the time limit of the OTP has expired; and
- STEP 232 - retrieving the details corresponding to the credit card/debit card/net banking account chosen by the user, based on the mapping between the OTP and said details, and processing the transaction.

In accordance with the present disclosure, the method further includes the following steps:

- registering the user and the device **10** accessible to the user on the web interface and storing the user credentials into the user repository accessible by the server application **120** of the transaction server **20**; and
- receiving at the device application **110**, a unique device identification post user registration.

TECHNICAL ADVANCEMENTS

The technical advantages of the system and method envisaged by the present disclosure include the following:

- providing a system that ensures the transactions performed by a user on the World Wide Web are secure;
- providing a system that offers a user a convenient, yet safe way of

performing transactions;

- providing a system that enables a user to perform transactions without making physical use of credit/debit cards;
- providing a system that is reliable and tamper-proof;
- providing a system that is cost-effective and compatible with existing hardware infrastructure;
- providing a system that is user-friendly; and
- providing a system that prevents the occurrence of fraudulent transactions.

While considerable emphasis has been placed herein on the particular features of this invention, it will be appreciated that various modifications can be made, and that many changes can be made in the preferred embodiment without departing from the principles of the invention. These and other modifications in the nature of the invention or the preferred embodiments will be apparent to those skilled in the art from the disclosure herein, whereby it is to be distinctly understood that the foregoing descriptive matter is to be interpreted merely as illustrative of the invention and not as a limitation.

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 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.

The foregoing description 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.

CLAIMS:

1) A computer implemented system for cashless transaction comprising a device application installed and configured on a device accessible to a user and a server application configured on a transaction server, said device application and said server application being accessible to each other via a communication network, said system comprising:

- an acquiring module configured in said device application, said acquiring module configured to acquire at least a user credential to initiate a transaction, said acquiring module further configured to transmit the acquired user credential to said server application via a first trans-receiver;
- a validation module configured in said server application, said validation module configured receive the acquired user credential from said device application via a second trans-receiver, said validation module configured to validate the received user credential with the user credential stored into a user repository; wherein said user repository is accessible to said server application;
- a selection module configured in said device application, said selection module configured to prompt the user to user to select a financial account from a list of financial account details stored into said user repository, said selection module configured to transmit the acquired user's selection to said server application via the first trans-receiver; wherein said selection module prompts the user to select the financial account based on the successful validation of the user credential;
- an One Time Password (OTP) generator configured in said server application, said OTP generator configured to receive the acquired user selection from said device application via the second trans-receiver, said OTP generator configured to generate an OTP for the user who has

initiated the transaction, said OTP generator further configured to transmit the OTP to said device application via the second trans-receiver; and

- a verification module configured in said server application, said verification module configured to receive a user submitted OTP on a web interface via the second trans-receiver, said verification module configured verify the user submitted OTP with the OTP generated by said OTP generator.

2) The system as claimed in claim 1, wherein said device application executed on the device accessible to the user is provided with a unique device identification post user registration.

3) The system as claimed in claim 1, wherein said OTP generator configured to map the contents of the OTP with the selected user's financial account.

4) The system as claimed in claim 1, wherein the second trans-receiver of said server application configured to transmit the OTP to said device application in a format selected from the group consisting of an email format, a Short Message Service (SMS) format, an interactive voice formation and a combination thereof.

5) The system as claimed in claim 1, wherein said OTP generator includes a OTP-database to store the generated OTP corresponding to the user and the unique device identification.

6) The system as claimed in claim 1, wherein said OTP generator configured to generate a time bound OTP.

7) The system as claimed in claim 1, wherein said verification module configured to validating the time limit of the user submitted OTP, said verification module further configured to authenticate the user initiated transaction either positive or negative.

8) The system as claimed in claim 1, wherein said OTP generator generates the OTP in format selected from the group consisting of a text format, a voice format, an image format and a combination thereof.

9) The system as claimed in claim 1, wherein the user submitted OTP on the web interface wherein the user submission OTP format includes a text format, a voice format, an image format and a combination thereof.

10) A computer implemented method for implementing a system for performing cashless transaction comprising a device application installed and configured on a device accessible to the user and a server application configured on a transaction server, said device application and said server application being accessible to each other via a communication network, said method comprising:

- acquiring at said device application, at least a user credential to initiate a transaction and transmitting the acquired user credential to said server application;
- receiving and validating at said server application, the received user credential acquired at said device application with the user credential stored into a user repository, wherein said user repository is accessible to said server application;
- prompting the user at said device application on successful validation of the user credential at said server application and enabling the user to

select a financial account from a list of financial account details stored into said user repository;

- transmitting the acquired user's selection of the financial account detail to said server application;
- receiving at said server application, the user selected financial account detail;
- generating an One Time Password (OTP) for the user who has initiated the transaction and further transmitting the generated OTP to said device application; and
- receiving at said server application, a user submitted OTP on a web interface and verifying the user submitted OTP with the generated OTP.

11) The method as claimed in claim 10, wherein said method further includes the following steps:

- registering the user and the device accessible to the user on said web interface and storing the user credentials into said user repository accessible by said server application; and
- receiving at said device application, a unique device identification post user registration.

12) The method as claimed in claim 10, wherein the step of generating the OTP at said server application includes the following steps:

- mapping the OTP with the user selected financial account detail;
- associating a time limit to the generated OTP; and
- storing the OTP into a OTP-database corresponding to the user and the unique device identification.

13) The method as claimed in claim 10, wherein the step of verifying the user submitted OTP with the generated OTP at the server application further includes the followings steps:

- validating the time limit of the user submitted OTP; and
- authenticating the user initiated transaction either positive or negative.

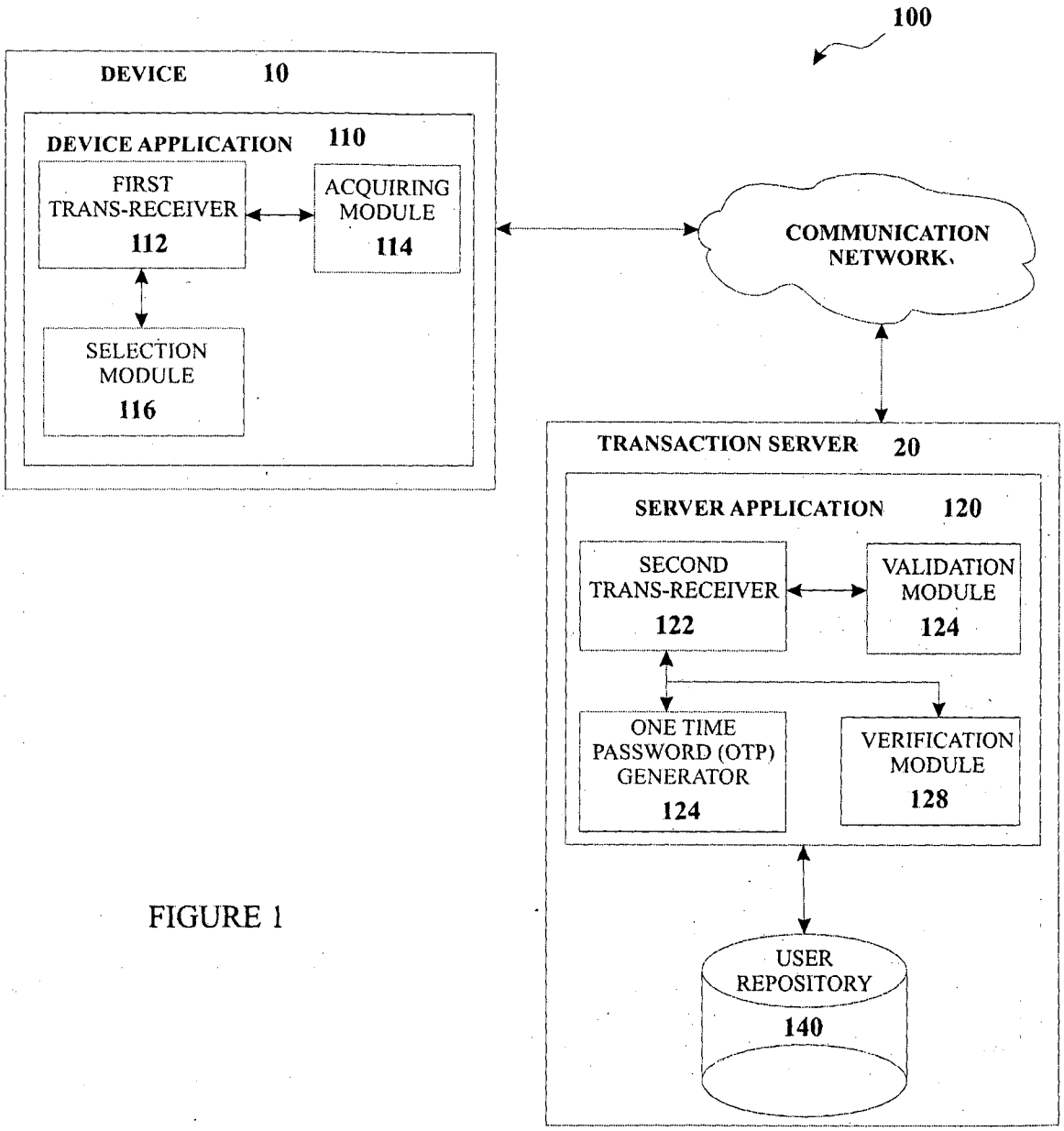
100
DEVICE 10
DEVICE APPLICATION 110
FIRST TRANS-RECEIVER 112
ACQUIRING MODULE 114
SELECTION MODULE 116
COMMUNICATION NETWORK
TRANSACTION SERVER 20
SERVER APPLICATION 120
SECOND TRANS-RECEIVER 122
VALIDATION MODULE 124
ONE TIME PASSWORD (OTP) GENERATOR 124
VERIFICATION MODULE 128
USER REPOSITORY 140

FIGURE 1

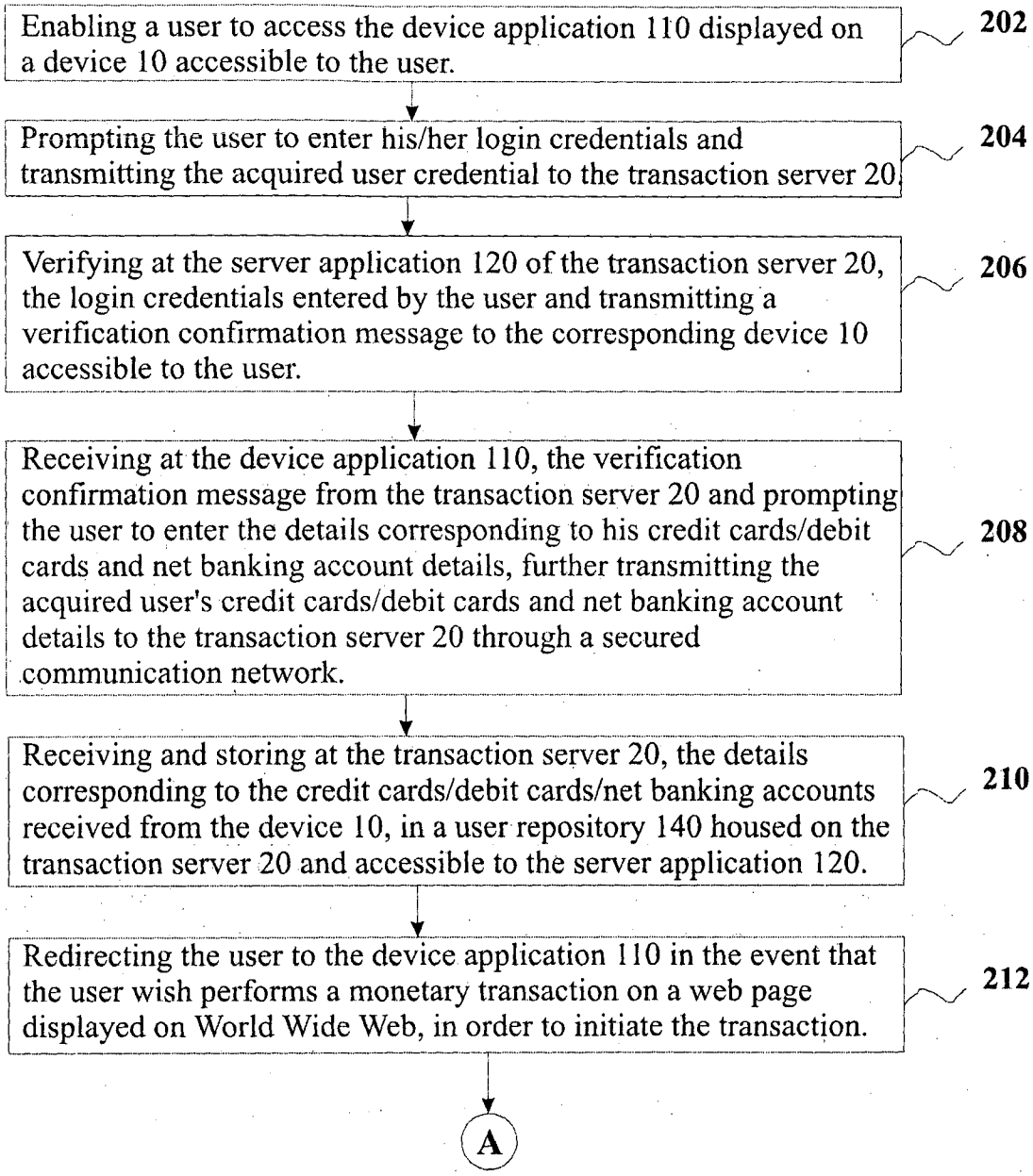
Enabling a user to access the device application 110 displayed on a device 10 accessible to the user.
202
Prompting the user to enter his/her login credentials and transmitting the acquired user credential to the transaction server 20.
204
Verifying at the server application 120 of the transaction server 20, the login credentials entered by the user and transmitting a verification confirmation message to the corresponding device 10 accessible to the user.
206
Receiving at the device application 110, the verification confirmation message from the transaction server 20 and prompting the user to enter the details corresponding to his credit cards/debit cards and net banking account details, further transmitting the acquired user's credit cards/debit cards and net banking account details to the transaction server 20 through a secured communication network.
208
Receiving and storing at the transaction server 20, the details corresponding to the credit cards/debit cards/net banking accounts received from the device 10, in a user repository 140 housed on the transaction server 20 and accessible to the server application 120.
210
Redirecting the user to the device application 110 in the event that the user wish performs a monetary transaction on a web page displayed on World Wide Web, in order to initiate the transaction.
212
A

FIGURE 2(a)

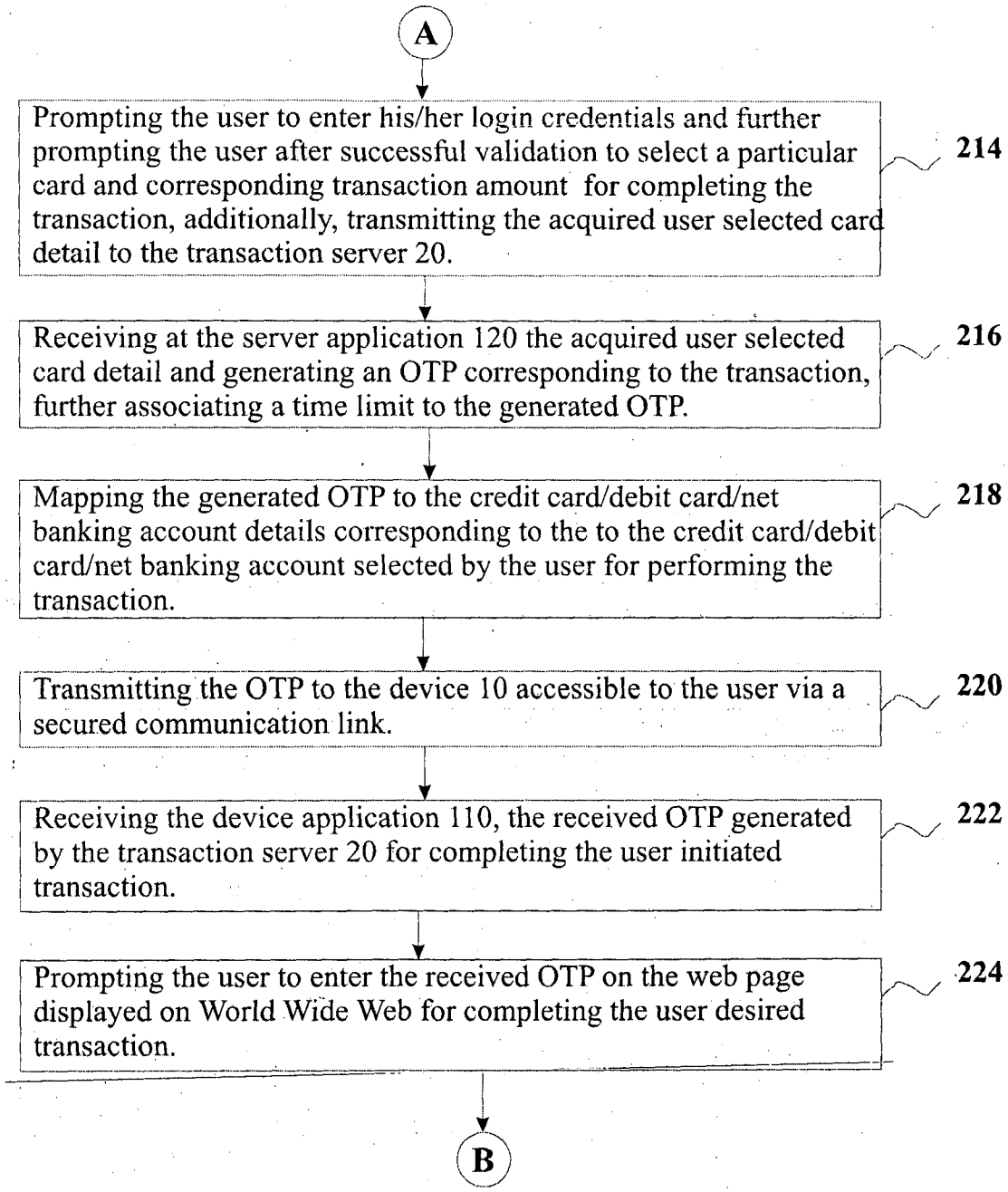
A
Prompting the user to enter his/her login credentials and further prompting the user after successful validation to select a particular card and corresponding transaction amount for completing the transaction, additionally, transmitting the acquired user selected card detail to the transaction server 20.
214
Receiving at the server application 120 the acquired user selected card detail and generating an OTP corresponding to the transaction, further associating a time limit to the generated OTP.
216
Mapping the generated OTP to the credit card/debit card/net banking account details corresponding to the to the credit card/debit card/net banking account selected by the user for performing the transaction.
218
Transmitting the OTP to the device 10 accessible to the user via a secured communication link.
220
Receiving the device application 110, the received OTP generated by the transaction server 20 for completing the user initiated transaction.
222
Prompting the user to enter the received OTP on the web page displayed on World Wide Web for completing the user desired transaction.
224
B

FIGURE 2(b)

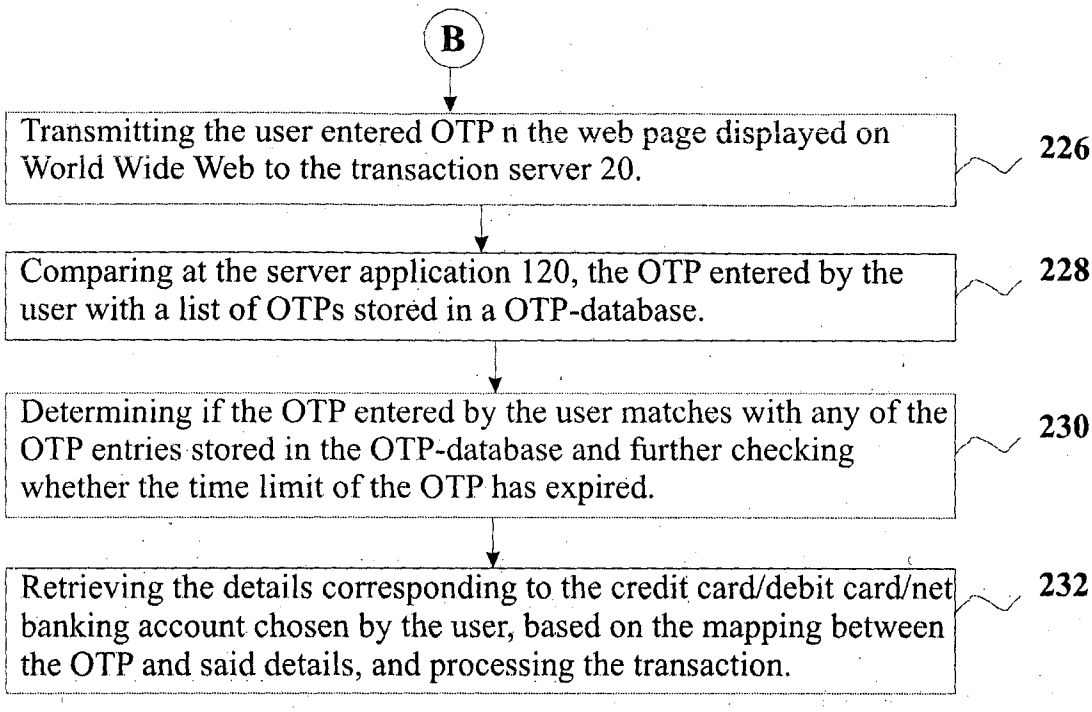
B
Transmitting the user entered OTP n the web page displayed on World Wide Web to the transaction server 20.
226
Comparing at the server application 120, the OTP entered by the user with a list of OTPs stored in a OTP-database.
228
Determining if the OTP entered by the user matches with any of the OTP entries stored in the OTP-database and further checking whether the time limit of the OTP has expired.
230
Retrieving the details corresponding to the credit card/debit card/net banking account chosen by the user, based on the mapping between the OTP and said details, and processing the transaction.
232

FIGURE 2(c)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IN2014/000437

A. CLASSIFICATION OF SUBJECT MATTER
G06Q20/00,G06F21/31,H04L9/32 Version=2014.01

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q,G06F,H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Databases: Questel,IPO internal database,Google patent search
Search terms: Cashless Transaction, One Time Password Generator

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012011066 A1 (TODD N. TELLE ET AL) 12 January 2012 Whole document	Claims 1-13
X	EP 2608486 A1 (PRASANNA BIDARE) 26 June 2013 Paragraphs [0057]-[0059], [0077] and Claim 8	Claims 1-13
A	IN 1354/MUM/2004(AGASHE MANDAR DNYANESHWAR)21 Aug 2007 Whole document	Claims 1-13

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24-11-2014	24-11-2014
Name and mailing address of the ISA/ Indian Patent Office Plot No.32, Sector 14,Dwarka,New Delhi-110075 Facsimile No.	Authorized officer Anjali Telephone No. +91-1125300200

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IN2014/000437

Citation	Pub.Date	Family	Pub.Date
US 2012011066 A1	12-01-2012	WO 2012009248 A1	19-01-2012
		EP 2593914 A1	22-05-2013
EP 2608486 A1	26-06-2013	US 2013179954 A1	11-07-2013