

METHOD AND SYSTEM FOR AUTHENTICATING USERS

FIELD

[0001] Various embodiments of the disclosure relate generally to methods and systems for authentication. More specifically, various embodiments of the disclosure relate to a method and a system for authenticating users for transactions.

BACKGROUND

[0002] Advancements in the field of technology have paved way for users to perform financial transactions electronically. Examples of terminal devices that facilitate such transactions include automated teller machines (ATMs), point-of-sale (POS) devices, or the like. One of the most commonly used mode for performing such transactions is the ATM. The ATM provides the users (e.g., banking customers) with the ability to withdraw funds, deposit funds, transfer funds, and access account information.

[0003] Prior to processing a financial transaction performed via an ATM (or any other terminal device), it is important to authenticate the user performing the transaction. A traditional approach of user authentication requires the user to provide a personal identification number (PIN) linked to a transaction card (such as a debit card, a credit card, or the like) of the user, while initiating the transaction. The reliance on the PIN and lack of human supervision creates the risk of a perpetrator compromising the security of the ATMs. For example, the perpetrator may acquire information encrypted in a magnetic stripe or an electronic chip of the transaction card and the PIN entered by the user, by way of skimming devices, keypad overlays, hidden cameras, or the like. The acquired information may subsequently be used to gain unauthorized access to user's funds, thus resulting in financial losses to the user as well as to the financial institution that maintains a user account of the user. Similar problems may arise for transactions performed via the POS devices.

[0004] In light of the foregoing, there exists a need for a solution that provides a secure user authentication mechanism that prevents an unauthorized user from gaining unauthorized access to the user's funds.

SUMMARY

[0005] In an embodiment of the disclosure, a method for authenticating a user for a transaction is provided. When the transaction is initiated by the user at a terminal device by

way of a payment mode, an input personal identification number (PIN) entered by the user, an input pattern drawn by the user on a touch screen of the terminal device, and input biometric information of the user while the input pattern is being drawn by the user is recorded by the terminal device. The transaction is executed by the terminal device based on an authentication of the user. The user is authenticated when the input PIN, the input pattern, and the input biometric information match a reference PIN, a reference pattern, and reference biometric information that are linked to the payment mode, respectively. Further, the reference biometric information is associated with the reference pattern.

[0006] In another embodiment of the disclosure, a terminal device is provided. The terminal device includes a numeric keypad, a touch screen, and a set of biometric sensors. The numeric keypad is configured to record an input PIN entered by a user for initiating a transaction at the terminal device. The touch screen is configured to display a first plurality of objects. The touch screen is further configured to record an input pattern that is drawn by the user by connecting a second plurality of objects of the first plurality of objects. Further, the set of biometric sensors is configured to record input biometric information of the user while the input pattern is being drawn by the user. The user is authenticated for the transaction when the input PIN, the input pattern, and the input biometric information match a reference PIN, a reference pattern, and reference biometric information that are linked to a payment mode utilized for initiating the transaction, respectively. Further, the reference biometric information is associated with the reference pattern.

[0007] In another embodiment of the disclosure, a system for authenticating a user for a transaction is provided. The system includes a terminal device that includes a numeric keypad, a touch screen, and a set of biometric sensors. The numeric keypad is configured to record an input PIN entered by the user for initiating the transaction at the terminal device. The touch screen is configured to display a first plurality of objects. The touch screen is further configured to record an input pattern that is drawn by the user by connecting a second plurality of objects of the first plurality of objects. The set of biometric sensors is configured to record input biometric information of the user while the input pattern is being drawn by the user. The system further includes a server that communicates with the terminal device. The server is configured to authenticate the user when the input PIN, the input pattern, and the input biometric information that are recorded by the terminal device match a reference PIN, a reference pattern, and reference biometric information that are linked to a payment mode

utilized for initiating the transaction, respectively. Further, the reference biometric information is associated with the reference pattern.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] The accompanying drawings illustrate the various embodiments of systems, methods, and other aspects of the disclosure. It will be apparent to a person skilled in the art that the illustrated element boundaries (e.g., boxes, groups of boxes, or other shapes) in the figures represent one example of the boundaries. In some examples, one element may be designed as multiple elements, or multiple elements may be designed as one element. In some examples, an element shown as an internal component of one element may be implemented as an external component in another, and vice versa.

[0009] Various embodiments of the disclosure are illustrated by way of example, and not limited by the appended figures, in which like references indicate similar elements:

[0010] FIG. 1 is a block diagram that illustrates an exemplary environment for authenticating users, in accordance with an exemplary embodiment of the disclosure;

[0011] FIG. 2A is a block diagram that illustrates a perspective view of an automated teller machine (ATM) of the environment of FIG. 1, in accordance with an exemplary embodiment of the disclosure;

[0012] FIG. 2B is a block diagram that illustrates various components of the ATM, in accordance with an exemplary embodiment of the disclosure;

[0013] FIGS. 3A-3D, collectively represent a process flow diagram that illustrates an exemplary scenario for registering reference information of a user with an issuer in the environment of FIG. 1, in accordance with an exemplary embodiment of the disclosure;

[0014] FIG. 4 represents an exemplary scenario that illustrates different reference patterns and corresponding reference fingerprints that the user registers with the issuer, in accordance with an exemplary embodiment of the disclosure;

[0015] FIG. 5 is a table that illustrates a tabular database maintained at an issuer server of the issuer, in accordance with an exemplary embodiment of the disclosure;

[0016] FIGS. 6A-6C, collectively represent a process flow diagram that illustrates an exemplary scenario for authenticating the user for a transaction in the environment of FIG. 1, in accordance with an exemplary embodiment of the disclosure;

[0017] FIG. 7 is a block diagram that illustrates a perspective view of a point-of-sale (POS) device of the environment of FIG. 1, in accordance with an exemplary embodiment of the disclosure;

[0018] FIG. 8 is a block diagram that illustrates various components of the issuer server, in accordance with an exemplary embodiment of the disclosure;

[0019] FIGS. 9A and 9B, collectively represent a flow chart that illustrates a method for facilitating registration of the reference information with the issuer, in accordance with an exemplary embodiment of the disclosure;

[0020] FIG. 9C is a flow chart that illustrates a method for executing the transaction initiated by the user, in accordance with an exemplary embodiment of the disclosure;

[0021] FIG. 10A is a flow chart that illustrates a method for registering the reference information with the issuer, in accordance with an exemplary embodiment of the disclosure;

[0022] FIGS. 10B and 10C, collectively represent a flow chart that illustrates a method for authorizing the transaction initiated by the user, in accordance with an exemplary embodiment of the disclosure;

[0023] FIG. 11 represents a high-level flow chart that illustrates a method for authenticating the user for the transaction, in accordance with an exemplary embodiment of the disclosure; and

[0024] FIG. 12 is a block diagram that illustrates system architecture of a computer system in the environment of FIG. 1, in accordance with an exemplary embodiment of the disclosure.

[0025] Further areas of applicability of the disclosure will become apparent from the detailed description provided hereinafter. It should be understood that the detailed description of exemplary embodiments is intended for illustration purposes only and is, therefore, not intended to necessarily limit the scope of the disclosure.

DETAILED DESCRIPTION

[0026] The disclosure is best understood with reference to the detailed figures and description set forth herein. Various embodiments are discussed below with reference to the figures. However, those skilled in the art will readily appreciate that the detailed descriptions given herein with respect to the figures are simply for explanatory purposes as the methods and systems may extend beyond the described embodiments. In one example, the teachings presented and the needs of a particular application may yield multiple alternate and suitable approaches to implement the functionality of any detail described herein. Therefore, any approach may extend beyond the particular implementation choices in the following embodiments that are described and shown.

[0027] References to “an embodiment”, “another embodiment”, “yet another embodiment”, “one example”, “another example”, “yet another example”, “for example”, and so on, indicate that the embodiment(s) or example(s) so described may include a particular feature, structure, characteristic, property, element, or limitation, but that not every embodiment or example necessarily includes that particular feature, structure, characteristic, property, element, or limitation. Furthermore, repeated use of the phrase “in an embodiment” does not necessarily refer to the same embodiment.

OVERVIEW

[0028] In current transaction systems, when a user initiates a transaction at a terminal device, the user provides a personal identification number (PIN) to the terminal device for authentication. The sole reliance on the PIN, however, creates the risk of a perpetrator acquiring, by fraudulent means on the terminal device, the PIN and details of a transaction card utilized for initiating the transaction. The acquired information may subsequently be used to gain unauthorized access to user’s funds. Thus, the sole reliance on the PIN for authenticating a user may not prevent the user from being defrauded.

[0029] Various embodiments of the disclosure provide a method and a system for authenticating a user to solve the abovementioned problems. When the user is issued a payment mode (e.g., a transaction card), the user is required to register reference information of the user with an entity that has issued the payment mode to the user (e.g., an issuer that maintains a user account of the user). The user may register the reference information with the issuer by way of a terminal device. To initiate the registration, the user enters a reference PIN for multiple times by way of a numeric keypad of the terminal device and draws a reference pattern for multiple times on a touch screen of the terminal device. The terminal

device records the reference PIN entered each time by the user and the reference pattern drawn each time by the user. The terminal device further records reference biometric information of the user while the reference pattern is being drawn each time by the user, reference time-durations taken by the user to draw the reference pattern each time, and reference pressure values corresponding to pressures applied by the user for drawing the reference pattern each time. An example of the reference biometric information may include a reference fingerprint of a finger used by the user for drawing the reference pattern multiple times. The reference PIN, the reference pattern, the reference biometric information, the reference time-durations, and the reference pressure values are collectively referred to as the reference information. A server associated with the issuer receives the reference information recorded by the terminal device. Based on the reference pressure values and reference time-durations, the server determines pressure and time ranges for authenticating the user, respectively. The server then links the reference PIN, the reference pattern, the reference biometric information, the time range, and the pressure range with the payment mode, thereby successfully registering the reference information of the user with the issuer.

[0030] Upon successful registration, the user may utilize the payment mode to perform transactions. For example, the user may utilize the payment mode for initiating a transaction at the terminal device, for example, an automated teller machine (ATM) or a point-of-sale (POS) device. Further, the user enters an input PIN by way of the numeric keypad and draws an input pattern on the touch screen. The terminal device records the input PIN entered by the user and the input pattern drawn by the user. The terminal device further records input biometric information of the user while the input pattern is being drawn by the user, an input time-duration taken by the user to draw the input pattern, and an input pressure value corresponding to a pressure applied by the user for drawing the input pattern. The input PIN, the input pattern, the input biometric information, the input time-duration, and the input pressure value are collectively referred to as authentication information of the user. The server receives the authentication information recorded by the terminal device and authenticates the user based on the authentication information and the reference information linked to the payment mode. For example, the server authenticates the user when the input PIN matches the reference PIN, the input pattern matches the reference pattern, the input biometric information matches the reference biometric information, the input time-duration is within the time range, and the input pressure value is within the pressure range. The terminal device executes the transaction when the user is successfully authenticated.

[0031] Thus, the user is authenticated based on a combination of the input PIN, the input pattern, the input biometric information, the input time-duration, and the input pressure value. The use of various factors such as the PIN, the pattern, the biometric information, the time-duration, and the pressure value to authenticate the user provides a more secure method for authenticating users as compared to the conventional PIN based user authentication methods implemented at the terminal device.

TERMS DESCRIPTION (in addition to plain and dictionary meaning)

[0032] Transaction is an exchange of funds between two or more parties. For example, the transaction may include dispensing cash, at an ATM, equivalent to a transaction amount debited from a user account of a user. In another example, the transaction may include transferring a transaction amount from the user to a merchant, when the user makes a purchase from the merchant.

[0033] Terminal device is a computing device affiliated with a financial institution, (such as an acquirer). The terminal device enables users to perform various electronic transactions, such as cash withdrawals, cash deposits, purchase payments, funds transfer, or the like. Further, the terminal device facilitates registration of reference information of the users with corresponding issuers. Examples of the terminal device may include a POS device, a point-of-purchase (POP) device, a point-of-interaction (POI) device, an ATM, a bunch note acceptor (BNA), a currency recycler, or the like.

[0034] Payment mode is means of payment, such as a transaction card, a digital wallet, and/or like, that is linked to a user account. Examples of the transaction card may include, but are not limited to, a debit card, a credit card, a prepaid card, a gift card, a promotional card, and a contactless card. The payment mode may be utilized to perform transactions, such as cash withdrawals, cash deposits, purchase payments, funds transfer, or the like, from the user account to which it is linked. The payment mode may be a physical payment mode or a virtual payment mode that is electronically stored in a user device.

[0035] Pattern is drawn by connecting various objects displayed on a touch screen of a terminal device. A user may draw the pattern by utilizing at least one finger. The drawn pattern is utilized to authenticate the user for a transaction initiated by the user. When the pattern is being drawn by the user, a fingerprint of the finger utilized by the user to draw the pattern, a time-duration taken by the user to draw the pattern, and a pressure applied by the

user for drawing the pattern are recorded at the terminal device for authenticating the user for the transaction.

[0036] Time range corresponds to a range of time-durations that a genuine user may take to draw a registered pattern. The time range is determined during registration of reference information of the user with an issuer. Additionally, the time range may be updated after each successful authentication of the user. The time range is typically defined in seconds.

[0037] Pressure value corresponds to an amount of pressure applied by a user for drawing a pattern on a touch screen of a terminal device. In one example, the user may apply a constant pressure for drawing the pattern. In such a scenario, the pressure value is equal to the amount of the constant pressure. In another example, the pressure applied by the user may vary while the pattern is being drawn by the user. In such a scenario, the pressure value may correspond to any one of a mean, a median, a mode, a highest, a lowest, or a total of the varying pressure amounts. The pressure value is typically measured in Pascals.

[0038] Pressure range corresponds to a range of pressure values corresponding to pressures that a genuine user may apply for drawing a registered pattern. The pressure range is determined during registration of reference information of the user with an issuer. Additionally, the pressure range may be updated after each successful authentication of the user. The pressure range is typically defined in Pascals.

[0039] Reference information of a user includes a reference PIN entered by the user for multiple times, a reference pattern drawn by the user for multiple times, reference biometric information of the user recorded while the reference pattern is being drawn by the user for multiple times. The reference information further includes reference time-durations taken by the user to draw the reference pattern for multiple times, and reference pressure values corresponding to pressures applied by the user to draw the reference pattern for multiple times. The reference information of the user is registered with an issuer that maintains a user account of the user. The reference information is registered to enable an authentication of the user when the user performs transactions by utilizing a transaction card issued by the issuer.

[0040] Authentication information of a user is recorded by a terminal device when the user initiates a transaction at the terminal device by way of a payment mode. The

authentication information includes an input PIN entered by the user, an input pattern drawn at the terminal device by the user, input biometric information of the user recorded while the input pattern is being drawn by the user. The authentication information further includes an input time-duration taken by the user to draw the input pattern, and an input pressure value corresponding to a pressure applied by the user to draw the input pattern. The user is authenticated for the transaction based on the authentication information of the user and reference information of the user registered with an issuer that maintains a user account of the user.

[0041] Numeric keypad is installed in a terminal device and is utilized by users to enter PINs of the users. The numeric keypad may be a physical keypad or a virtual keypad that is integrated into a touch screen of the terminal device or any other screen of the terminal device.

[0042] FIG. 1 is a block diagram that illustrates an exemplary environment 100 for authenticating users, in accordance with an exemplary embodiment of the disclosure. The environment 100 includes a user 102, a payment mode 104 of the user 102, first and second terminal devices 106a and 106b, an acquirer server 108, a payment network server 110, and an issuer server 112. The first and second terminal devices 106a and 106b, the acquirer server 108, the payment network server 110, and the issuer server 112 communicate with each other by way of a communication network 114 or through separate communication networks established therebetween.

[0043] The user 102 is an individual who is to be authenticated. In one embodiment, the user 102 may be an account holder of a user account maintained at a financial institution, such as an issuer. For the sake of ongoing discussion and without limiting the scope of the disclosure, it is assumed that the payment mode 104 is a transaction card, and the issuer has issued the payment mode 104 to the user 102 for performing transactions from the user account. Hereinafter, the payment mode 104 is referred to and designated as the “transaction card 104”. The user 102 may utilize the transaction card 104 to perform the transactions at various terminal devices (for example, the first and second terminal devices 106a and 106b). Examples of the transactions performed at the terminal devices may include cash withdrawals, cash deposits, purchase payments, funds transfer, and the like. Prior to utilizing the transaction card 104 for performing the transactions, the user 102 is required to register reference information of the user 102 with the issuer that has issued the transaction card 104

to the user 102. The reference information is utilized by the issuer to authenticate the user 102, when a transaction is performed by the user 102 at a terminal device by utilizing the transaction card 104.

[0044] The transaction card 104 is linked to the user account and stores account information of the user account. The account information may include an account number, a name of an account holder (*i.e.*, the user 102), or the like. Further, the transaction card 104 may have a unique card number, an expiry date, and a card security code. The account information of the user account, the unique card number, the expiry date, and the card security code are collectively referred to as details of the transaction card 104. In one embodiment, the transaction card 104 is a physical card. In another embodiment, the transaction card 104 is a virtual card stored in a memory (not shown) of a user device (not shown) of the user 102. Examples of the transaction card 104 may include a credit card, a debit card, a membership card, a promotional card, a charge card, a prepaid card, a gift card, a contactless card, or the like.

[0045] The first and second terminal devices 106a and 106b include suitable logic, circuitry, interfaces, and/or code, executed by the circuitry, to allow users (such as the user 102) to perform the transactions from corresponding user accounts. Each of the first and second terminal devices 106a and 106b may be associated with a financial institution, such as an acquirer. Examples of the first and second terminal devices 106a and 106b may include an ATM, a bunch note acceptor (BNA), a currency recycler, a point-of-purchase (POP) device, a point-of-interaction (POI) device, a POS device, or the like. For the sake of brevity, it is assumed that the first terminal device 106a is an ATM, and the second terminal device 106b is a POS device. Further, the first terminal device 106a is hereinafter referred to and designated as the “ATM 106a”, and the second terminal device 106b is hereinafter referred to and designated as the “POS device 106b”.

[0046] The ATM 106a facilitates the registration of the reference information with the issuer that maintains the user account and has issued the transaction card 104 to the user 102. The reference information is registered to enable an authentication of the user 102 when the user 102 performs the transactions by utilizing the transaction card 104. When the user 102 initiates the registration at the ATM 106a, the ATM 106a prompts the user 102 to enter a reference PIN and draw a reference pattern for multiple times. Based on the reference PIN entered each time and the reference pattern drawn each time, the ATM 106a records the

reference information of the user 102. The reference information includes the reference PIN entered each time by the user 102, the reference pattern drawn each time by the user 102, and reference biometric information of the user 102 that is recorded while the reference pattern is being drawn each time (e.g., a reference fingerprint of a finger utilized by the user 102 to draw the reference pattern each time). The reference information may further include reference time-durations taken by the user 102 to draw the reference pattern each time and reference pressure values corresponding to pressures applied by the user 102 for drawing the reference pattern each time. The ATM 106a provides the reference information to the issuer.

[0047] The ATM 106a may further allow the user 102 to perform transactions and process the transactions performed by the user 102. When a transaction is initiated by the user 102 at the ATM 106a by way of the transaction card 104, the ATM 106a records the details of the transaction card 104 and authentication information of the user 102. The authentication information is recorded by the ATM 106a based on an input PIN entered and an input pattern drawn by the user 102 while initiating the transaction. The authentication information includes the input PIN, the input pattern, and input biometric information of the user 102 that is recorded while the input pattern was being drawn (e.g., an input fingerprint of a finger utilized by the user 102 to draw the input pattern). The authentication information further includes an input time-duration taken by the user 102 to draw the input pattern and an input pressure value corresponding to a pressure applied by the user 102 for drawing the input pattern. Additionally, the ATM 106a records transaction details of the transaction. The transaction details include a type of transaction (such as a cash withdrawal), a transaction amount, and/or the like. The ATM 106a provides the authentication information to the issuer for authenticating the user 102 for the transaction. The ATM 106a may execute the transaction based on the authentication of the user 102. For example, if the transaction is a cash withdrawal transaction, the ATM 106a may dispense cash equivalent to the transaction amount when the user 102 is authenticated.

[0048] The POS device 106b is functionally similar to the ATM 106a. For example, the POS device 106b may allow the user 102 to register the reference information with the issuer and perform transactions by using the transaction card 104 or any other payment mode, for example, a digital wallet.

[0049] The acquirer server 108 is a computing server that is operated by the acquirer and includes suitable logic, circuitry, interfaces, and/or code, executed by the circuitry, for

processing the transactions. The acquirer server 108 communicates with the ATM 106a and the POS device 106b for receiving the reference and authentication information. The acquirer server 108 further communicates with the payment network server 110 for processing various transactions performed at the ATM 106a and the POS device 106b.

[0050] The payment network server 110 is a computing server that is operated by a payment network and includes suitable logic, circuitry, interfaces, and/or code, executed by the circuitry, for processing the transactions. The payment network server 110 represents an intermediate entity between the acquirer server 108 and the issuer server 112 for processing the transactions.

[0051] The issuer server 112 is a computing server that is operated by the issuer and includes suitable logic, circuitry, interfaces, and/or code, executed by the circuitry, for authorizing transactions performed by way of the transaction card 104 or any other payment mode issued by the issuer. The issuer is a financial institution that manages accounts of multiple users, such as the user 102. Account details of the user accounts established with the issuer are stored as account profiles in a memory (shown later in FIG. 8) of the issuer server 112, in an external database associated with the issuer server 112, or on a cloud server associated with the issuer server 112. The account details may include details of the account holders, account numbers of the user accounts, account balances of the user accounts, details of the issued transaction cards, or the like. The details of the account holders include name, age, gender, registered contact number, registered e-mail ID, or the like.

[0052] When the registration of the reference information is initiated by the user 102, the issuer server 112 receives the details of the transaction card 104 and the reference information from the ATM 106a or the POS device 106b, by way of the acquirer server 108 and the payment network server 110. The issuer server 112 links the reference information with the transaction card 104 and stores the information pertaining to the link in the memory of the issuer server 112. In one example, the issuer server 112 may create a tabular database (shown later in FIG. 5) having various rows and columns for storing the information pertaining to various links, such as the link between the reference information and the transaction card 104. Each row of the tabular database corresponds to a unique link. For example, each row may store a user name, an account number of a user account, a unique card number associated with a transaction card, reference information linked to the transaction card, or the like.

[0053] When the transaction is initiated by the user 102, the issuer server 112 receives the details of the transaction card 104, the authentication information, and the transaction details from the payment network server 110. The issuer server 112 authenticates the user 102 and authorizes the transactions, based on the details of the transaction card 104, the authentication information, the transaction details, and the link between the reference information and the transaction card 104.

[0054] The communication network 114 is a medium through which content and messages are transmitted between the ATM 106a, the POS device 106b, the acquirer server 108, the payment network server 110, the issuer server 112, or other entities that are pursuant to one or more standards for the interchange of transaction messages, such as the ISO8583 standard. Examples of the communication network 114 may include, but are not limited to, a Wi-Fi network, a light fidelity (Li-Fi) network, a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN), a satellite network, the Internet, a fiber optic network, a coaxial cable network, an infrared (IR) network, a radio frequency (RF) network, and combinations thereof. Various entities in the environment 100 may connect to the communication network 114 in accordance with various wired and wireless communication protocols, such as Transmission Control Protocol and Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Long Term Evolution (LTE) communication protocols, or any combination thereof.

[0055] Although the disclosure describes that the transaction card 104 is utilized by the user 102 for initiating the registration of the reference information with the issuer and for initiating the transaction, the scope of the disclosure is not limited to it. In various other embodiments, the user 102 may have a digital wallet and may register the reference information with a digital wallet service provider of the digital wallet, without deviating from the scope of the disclosure. Upon the registration, the user 102 may utilize the digital wallet for initiating the transaction. In such a scenario, the operations performed by the issuer server 112 may be performed by a server associated with the digital wallet service provider.

[0056] FIG. 2A is a block diagram that illustrates a perspective view of the ATM 106a, in accordance with an exemplary embodiment of the disclosure. The ATM 106a includes a card reader 202 having a card slot 204. The card reader 202 is configured to record details of transaction cards (e.g., the transaction card 104) that are utilized at the ATM 106a. The ATM 106a further includes a numeric keypad 206 and a touch screen 208. The numeric

keypad 206 and the touch screen 208 are utilized by users (such as the user 102) for entering PINs and for drawing patterns, respectively. The numeric keypad 206 is configured to record the PINs entered by the users, and the touch screen 208 is configured to record the patterns drawn by the users. The ATM 106a further includes biometric sensors 210 that are configured to record biometric information of the users while the users draw the patterns on the touch screen 208. Examples of the biometric sensors 210 may include fingerprint sensors, iris sensors, or the like. For the sake of ongoing discussion and without limiting the scope of the disclosure, it is assumed that the biometric sensors 210 are fingerprint sensors that record fingerprints of the users while the patterns are being drawn by the users. Hereinafter, the biometric sensors 210 are referred to and designated as the “fingerprint sensors 210”.

[0057] The ATM 106a further includes pressure sensors 212 that are configured to record pressure values while the users draw the patterns on the touch screen 208. In one embodiment, the fingerprint sensors 210 and the pressure sensors 212 may be located beneath the touch screen 208. The ATM 106a further includes a timer 214 that is configured to record time-durations taken by the users to draw the patterns on the touch screen 208. Further, the ATM 106a is equipped with a display screen 216 and a cash dispenser 218. The display screen 216 displays various messages related to the success and failure of the registration and transactions to the users. The cash dispenser 218 dispenses cash when the transactions initiated at the ATM 106a are cash withdrawals. However, when the transactions initiated at the ATM 106a are cash deposits, the cash dispenser 218 may serve as a cash deposit machine.

[0058] Although the touch screen 208 and the display screen 216 are realized as separate components in FIG. 2A, the scope of the disclosure is not limited to it. In various other embodiments, the touch screen 208 may be integrated into the display screen 216, without deviating from the scope of the disclosure. In such a scenario, the fingerprint sensors 210 and the pressure sensors 212 may be located behind the display screen 216.

[0059] FIG. 2B is a block diagram that illustrates various components of the ATM 106a, in accordance with an exemplary embodiment of the disclosure. As illustrated in FIG. 2A, the ATM 106a includes the card reader 202, the numeric keypad 206, the touch screen 208, the fingerprint sensors 210 (*i.e.*, the biometric sensors 210), the pressure sensors 212, and the timer 214. The ATM 106a further includes a first processing circuitry 220, a first memory 222, and a first transceiver 224. The card reader 202, the numeric keypad 206, the touch screen 208, the fingerprint sensors 210, the pressure sensors 212, the timer 214, the

first processing circuitry 220, the first memory 222, and the first transceiver 224 communicate with each other by way of a first communication bus 226.

[0060] The card reader 202 includes suitable logic, circuitry, interfaces, and/or code, executable by the circuitry, to record details of transaction cards (such as the transaction card 104) that are utilized at the ATM 106a. The card reader 202 may be a magnetic stripe or electronic chip card reader equipped with the card slot 204 into which the transaction cards may be inserted or swiped. In one embodiment, the card reader 202 records the details of the transaction cards that are inserted in or swiped across the card slot 204. The card reader 202 may be further enabled with Near Field Communication (NFC) capabilities, such that the details of the transaction cards may be recorded when the transaction cards are tapped on the card slot 204 or are presented within an NFC range of the ATM 106a.

[0061] The numeric keypad 206 includes suitable logic, circuitry, interfaces, and/or code, executable by the circuitry, to record PINs and transaction details of the transactions initiated by the users (such as the user 102) at the ATM 106a. The numeric keypad 206 includes various buttons (or keys) that are utilized by the users for entering the PIN and/or the transaction details. The buttons may display numbers (such as '0' to '9'), functions (such as 'Enter', 'Clear', or 'Cancel'), or the like. In one embodiment, the numeric keypad 206 is a physical keypad. In another embodiment, the numeric keypad is a virtual keypad integrated into the touch screen 208, the display screen 216, or a separate screen (not shown) of the ATM 106a.

[0062] The touch screen 208 includes suitable logic, circuitry, interfaces, and/or code, executable by the circuitry, to record the patterns drawn by the users. The touch screen 208 is configured to display various objects (e.g., dots, circles, squares, triangles, rectangles, or any other geometric or non-geometric shapes) to the users, and the users are prompted to draw patterns by connecting two or more of the displayed objects. When the users touch or press an object on the touch screen 208 with a finger, and drag the finger over other objects to draw a pattern, the touch screen 208 is configured to record the touch positions and the drawn pattern (*i.e.*, a sequential combination of the touch positions). In one embodiment, the pattern drawn on the touch screen 208 is visible, *i.e.*, lines connecting the two or more objects in the pattern are visible. In another embodiment, the pattern drawn on the touch screen 208 is invisible, *i.e.*, lines connecting the two or more objects in the pattern are invisible. Examples of the touch screen 208 may include, but are not limited to, a resistive touch screen, a

capacitive touch screen, a surface acoustic wave (SAW) touch screen, and an optical touch screen.

[0063] The fingerprint sensors 210 include suitable logic, circuitry, interfaces, and/or code, executable by the circuitry, to record fingerprints of the users while the patterns are being drawn by the users on the touch screen 208. The fingerprint sensors 210 may be an array of sensors that are arranged beneath the touch screen 208, or more specifically, beneath an area covering the various objects displayed on the touch screen 208. In one example, a fingerprint sensor is located beneath each object. In one embodiment, the fingerprint sensors 210 are in physical contact with the touch screen 208. In another embodiment, the fingerprint sensors 210 are physically disconnected from the touch screen 208. When a user (such as the user 102) draws a pattern by utilizing a finger, the fingerprint sensors 210 are configured to record a fingerprint of the finger. In one example, the fingerprint sensors 210 may record a digital image of the fingerprint. Examples of the fingerprint sensors 210 may include, but are not limited to, optical fingerprint sensors, capacitive fingerprint sensors, ultrasonic fingerprint sensors, and thermal fingerprint sensors.

[0064] The pressure sensors 212 include suitable logic, circuitry, interfaces, and/or code, executable by the circuitry, to record the amount of pressures applied by the users on the touch screen 208 for drawing the patterns. The pressure sensors 212 may be an array of sensors that are arranged beneath the touch screen 208, or more specifically, beneath the area covering the various objects displayed on the touch screen 208. In one example, a pressure sensor is located beneath each object displayed on the touch screen 208. In one embodiment, the pressure sensors 212 are in physical contact with the touch screen 208. In another embodiment, the pressure sensors 212 are physically disconnected from the touch screen 208.

[0065] When a user (such as the user 102) draws a pattern by utilizing a finger, the pressure sensors 212 are configured to record a pressure value corresponding to an amount of pressure applied by the user for drawing the pattern. In an example, the pressure applied by the user may be constant. In such a scenario, the pressure value may correspond to the amount of constant pressure applied by the user. In another example, the pressure applied by the user may vary while the pattern is being drawn by the user. In such a scenario, the pressure value may correspond to one of a mean, a median, a mode, a highest, a lowest, or a total of the varying pressures applied by the user. Examples of the pressure sensors 212 may include, but are not limited to, resistive pressure sensors, capacitive pressure sensors, optical

pressure sensors, ultrasonic pressure sensors, magnetic pressure sensors, piezoresistive pressure sensors, and piezoelectric pressure sensors.

[0066] The timer 214 includes suitable logic, circuitry, interfaces, and/or code, executable by the circuitry, to record time-durations taken by the users to draw the patterns. The timer 214 is activated when a first touch is recorded on the touch screen 208 (*i.e.*, when the finger is placed on the touch screen 208), and is deactivated when the last touch is recorded on the touch screen 208 (*i.e.*, when the finger is lifted off the touch screen 208).

[0067] The first processing circuitry 220 includes suitable logic, circuitry, interfaces, and/or code, executable by the circuitry, to facilitate registration of reference information of the users with issuers that maintain user accounts of the users. The first processing circuitry 220 further facilitates authentication of the users and executes transactions initiated by the users at the ATM 106a. The first processing circuitry 220 facilitates the registration and authentication by way of the card reader 202, the numeric keypad 206, the touch screen 208, the fingerprint sensors 210, the pressure sensors 212, and the timer 214. The operations performed by the first processing circuitry 220 are explained in detail in conjunction with FIGS. 3A-3D, 6A-6C, and 9A-9C. Examples of the first processing circuitry 220 may include an application specific integrated circuit (ASIC) processor, a reduced instruction set computer (RISC) processor, a complex instruction set computer (CISC) processor, a field programmable gate array (FPGA), or the like.

[0068] The first memory 222 includes suitable logic, circuitry, interfaces, and/or code, executable by the circuitry, to facilitate the registration of the reference information with the issuer and processing the transactions initiated at the ATM 106a. The first memory 222 may temporarily store the PINs, the patterns, the fingerprints, the pressure values, and the time-durations recorded by the ATM 106a in an encrypted format. Examples of the first memory 222 may include a random access memory (RAM), a read-only memory (ROM), a removable storage drive, a hard-disk drive (HDD), a flash memory, a solid-state memory, or the like. It will be apparent to a person skilled in the art that the scope of the disclosure is not limited to realizing the first memory 222 in the ATM 106a, as described herein. In another embodiment, the first memory 222 may be realized in the form of a database server or a cloud storage working in conjunction with the ATM 106a, without departing from the scope of the disclosure.

[0069] The first transceiver 224 includes suitable logic, circuitry, interfaces and/or code, executable by the circuitry, to transmit and receive data over the communication network 114 using one or more communication protocols. The first transceiver 224 transmits various requests and messages, related to registration of the reference information and authorization of the transaction, to the acquirer server 108. The first transceiver 224 receives various requests and messages related to registration of the reference information and authorization of the transaction, from the acquirer server 108. Examples of the first transceiver 224 may include, but are not limited to, an antenna, a radio frequency transceiver, a wireless transceiver, a Bluetooth transceiver, an Ethernet port, a universal serial bus (USB) port, or any other device configured to transmit and receive data.

[0070] FIGS. 3A-3D, collectively represent a process flow diagram 300 that illustrates an exemplary scenario for registering the reference information with the issuer, in accordance with an exemplary embodiment of the disclosure. The user 102 is required to register the reference information for the transaction card 104 with the issuer prior to utilizing the transaction card 104 for performing the transactions. The user 102 may register the reference information with the issuer by way of an ATM (such as the ATM 106a) or a POS device (such as the POS device 106b). For the sake of brevity, it is assumed that the user 102 initiates the registration of the reference information at the ATM 106a.

[0071] The transaction card 104 is utilized by the user 102 at the ATM 106a for initiating the registration (as shown by arrow 302). In one example, the user 102 inserts the transaction card 104 in the card slot 204. In another example, the user 102 swipes the transaction card 104 across the card slot 204. In another example, the user 102 taps the transaction card 104 on the card slot 204. In another example, the user 102 presents the transaction card 104 in the vicinity of the card slot 204.

[0072] The card reader 202 records the details of the transaction card 104 (as shown by arrow 304). The ATM 106a, by way of the display screen 216, prompts the user 102 to enter a PIN for a first time (as shown by arrow 306). The user 102 enters a PIN for the first time (hereinafter referred to as a “first reference PIN”) by using the numeric keypad 206 (as shown by arrow 308). The numeric keypad 206 records the first reference PIN (as shown by arrow 310). The ATM 106a prompts the user 102 to enter the same PIN for a second time (as shown by arrow 312). The user 102 enters the PIN for the second time (hereinafter referred to as a “second reference PIN”) by using the numeric keypad 206 (as shown by arrow 314). The

numeric keypad 206 records the second reference PIN (as shown by arrow 316). The first processing circuitry 220 determines if the first and second reference PINs are same (as shown by arrow 318). The first processing circuitry 220 determines if the first and second reference PINs are same by utilizing known-in-the-art PIN comparison methods. In one exemplary scenario, the first and second reference PINs may be different. In such a scenario, the first processing circuitry 220 displays a “Registration Unsuccessful” message to the user 102 on the display screen 216 and may prompt the user 102 to re-initiate the registration. For the sake of brevity, it is assumed that the first and second reference PINs are same.

[0073] When the first and second reference PINs are same, various objects are displayed on the touch screen 208 and the ATM 106a prompts the user 102 to draw a pattern for a first time (as shown by arrow 320). The user 102 draws a pattern for the first time (hereinafter referred to as a “first reference pattern”) by connecting two or more objects of the various objects displayed on the touch screen 208 (as shown by arrow 322). The touch screen 208 records the first reference pattern (as shown by arrow 324). The fingerprint sensors 210 record a fingerprint of a finger utilized by the user 102 to draw the first reference pattern (hereinafter referred to as a “first reference fingerprint”). The pressure sensors 212 record a pressure value corresponding to a pressure applied by the user 102 for drawing the first reference pattern (hereinafter referred to as a “first reference pressure value”). Further, the timer 214 records a time-duration taken by the user 102 to draw the first reference pattern (hereinafter referred to as a “first reference time-duration”). Thus, the ATM 106a records the first reference fingerprint, the first reference pressure value, and the first reference time-duration (as shown by arrow 326).

[0074] The ATM 106a prompts the user 102 to draw the same pattern for a second time by utilizing the same finger (as shown by arrow 328). The user 102 draws the pattern for the second time (hereinafter referred to as a “second reference pattern”) on the touch screen 208 (as shown by arrow 330). The touch screen 208 records the second reference pattern (as shown by arrow 332). The fingerprint sensors 210 record a fingerprint of a finger utilized by the user 102 to draw the second reference pattern (hereinafter referred to as a “second reference fingerprint”). The pressure sensors 212 record a pressure value corresponding to a pressure applied by the user 102 for drawing the second reference pattern (hereinafter referred to as a “second reference pressure value”). Further, the timer 214 records a time-duration taken by the user 102 to draw the second reference pattern (hereinafter referred to as a “second reference time-duration”). Thus, the ATM 106a records the second reference

fingerprint, the second reference pressure value, and the second reference time-duration (as shown by arrow 334).

[0075] The ATM 106a further prompts the user 102 to draw the same pattern for the third time by utilizing the same finger (as shown by arrow 336). The user 102 draws the pattern for the third time (hereinafter referred to as a “third reference pattern”) on the touch screen 208 (as shown by arrow 338). The touch screen 208 records the third reference pattern (as shown by arrow 340). The fingerprint sensors 210 record a fingerprint of a finger utilized by the user 102 to draw the third reference pattern (hereinafter referred to as a “third reference fingerprint”). The pressure sensors 212 record a pressure value corresponding to a pressure applied by the user 102 for drawing the third reference pattern (hereinafter referred to as a “third reference pressure value”). Further, the timer 214 records a time-duration taken by the user 102 to draw the third reference pattern (hereinafter referred to as a “third reference time-duration”). Thus, the ATM 106a records the third reference fingerprint, the third reference pressure value, and the third reference time-duration (as shown by arrow 342).

[0076] The first processing circuitry 220 determines if the first through third reference patterns are same (as shown by arrow 344) by utilizing known-in-the-art pattern comparison methods. In one exemplary scenario, the first through third reference patterns may not match with each other. In such a scenario, the first processing circuitry 220 displays the “Registration Unsuccessful” message to the user 102 on the display screen 216 and may prompt the user 102 to re-initiate the registration. For the sake of brevity, it is assumed that the first through third reference patterns match with each other, *i.e.*, the first through third reference patterns are same. The first processing circuitry 220 further determines if the first through third reference fingerprints are same (as shown by arrow 346) by utilizing known-in-the-art fingerprint comparison methods. In one exemplary scenario, the first through third reference fingerprints may not match with each other. In such a scenario, the first processing circuitry 220 displays the “Registration Unsuccessful” message to the user 102 on the display screen 216 and may prompt the user 102 to re-initiate the registration. For the sake of brevity, it is assumed that the first through third reference fingerprints match with each other, *i.e.*, the first through third reference fingerprints are same.

[0077] When the first through third reference patterns are same and the first through third reference fingerprints are same, the first processing circuitry 220 generates a registration request for registering the reference information (*i.e.*, the first reference PIN, the first

reference pattern, the first reference fingerprint, the first through third reference pressure values, and the first through third reference time-durations) with the issuer (as shown by arrow 348). The registration request is pursuant to one or more standards for the interchange of transaction messages (such as the ISO8583 standard), and includes various fields (such as data elements) for storing various details. The registration request includes the details of the transaction card 104 and the reference information. In an embodiment, the first reference fingerprint included in the registration request corresponds to a digital image of the first reference fingerprint. In another embodiment, the first reference fingerprint included in the registration request corresponds to an encrypted fingerprint template of the digital image of the first reference fingerprint. The encrypted fingerprint template may be generated by the first processing circuitry 220 based on the digital image of the first reference fingerprint.

[0078] The first processing circuitry 220 communicates the registration request to the acquirer server 108 (as shown by arrow 350). The acquirer server 108 receives the registration request from the ATM 106a and identifies a payment network associated with the transaction card 104, as known by those skilled in the art. The acquirer server 108 communicates the registration request to the payment network server 110 of the identified payment network (as shown by arrow 352). The payment network server 110 receives the registration request and identifies the issuer that corresponds to the transaction card 104, as known by those skilled in the art. Once the issuer is identified, the payment network server 110 communicates the registration request to the issuer server 112 of the identified issuer (as shown by arrow 354).

[0079] Upon reception of the registration request, the issuer server 112 determines, based on the first through third reference pressure values, the pressure range for authenticating the user 102 (as shown by arrow 356). The pressure range may define a range of pressure values corresponding to pressures that may be applied by a genuine user (*i.e.*, the user 102) for drawing the first reference pattern. In an example, an upper bound of the pressure range may be equal to a highest value of one of the first through third reference pressure values, and a lower bound of the pressure range may be equal to a lowest value of one of the first through third reference pressure values. Further, the issuer server 112 determines, based on the first through third reference time-durations, the time range for authenticating the user 102 (as shown by arrow 358). The time range may define a range of time-durations that may be taken by the user 102 to draw the first reference pattern. In an example, an upper bound of the time range may be equal to a highest value of one of the first

through third reference time-durations, and a lower bound of the time range may be equal to a lowest value of one of the first through third reference time-durations.

[0080] The issuer server 112 links the first reference PIN, the first reference pattern, the first reference fingerprint, the pressure range, and the time range to the transaction card 104 (as shown by arrow 360), thereby registering the reference information of the user 102 with the issuer. The issuer server 112 stores, in the memory of the issuer server 112, the information pertaining to the link between the transaction card 104 and the first reference PIN, the first reference pattern, the first reference fingerprint, the pressure range, and the time range (as shown by arrow 362). In one example, the issuer server 112 adds a row to the tabular database such that the added row includes the name of the user 102, the account number of the user account of the user 102, the unique card number of the transaction card 104, the first reference PIN, the first reference pattern, the first reference fingerprint, the pressure range, and the time range.

[0081] The issuer server 112 generates the registration response indicating that the registration of the transaction card 104 is successful (as shown by arrow 364). The registration response is transmitted to the ATM 106a by the issuer server 112 by way of the payment network server 110 and the acquirer server 108 (as shown by arrows 366, 368, and 370). The first processing circuitry 220 displays a “Registration Successful” message to the user 102 (as shown by arrow 372) on the display screen 216.

[0082] The user 102 may further choose to register additional reference information with the issuer. While registering the additional reference information, the user 102 may draw the same reference pattern by utilizing a different finger, a different reference pattern by utilizing the same finger, or a different reference pattern by utilizing a different finger. Further, upon successful registration, the issuer server 112 may add, to the tabular database, another row including the additional reference information. The user 102 may thus be authenticated based on any one of the reference information or the additional reference information.

[0083] In another embodiment, instead of the ATM 106a, the issuer server 112 may determine if the first and second reference PINs are same, if the first through third reference patterns are same, and if the first through third reference fingerprints are same, without deviating from the scope of the disclosure. The scope of the disclosure is further not limited to the registration of the reference information upon issuance of the transaction card 104. In

various other embodiments, the registration of the reference information may correspond to updating existing reference information registered with the issuer, without deviating from the scope of the disclosure.

[0084] Although in FIGS. 3A-3D, the user 102 is prompted to enter the reference PIN two times and draw the reference pattern three times, it will be apparent to a person skilled in the art that the scope of the disclosure is not limited to it. In various other embodiments, the user 102 may be prompted to enter the reference PIN and draw the reference pattern any number of times, without deviating from the scope of the disclosure. In another embodiment, the reference PIN may already be registered with the issuer when the issuer issues the transaction card 104 to the user 102. In such a scenario, the user 102 may be required to enter the reference PIN only once during registration of the reference information with the issuer.

[0085] FIG. 4 represents an exemplary scenario 400 that illustrates different reference patterns and corresponding reference fingerprints that the user 102 registers with the issuer, in accordance with an exemplary embodiment of the disclosure. The user 102 may choose a different reference pattern for each finger to register with the issuer. When the user 102 initiates the registration of the reference information at the ATM 106a, the user 102 is prompted to draw a pattern on the touch screen 208 that displays first through ninth objects 402a-402i. The user 102 may draw a reference pattern 404a by connecting the first through ninth objects 402a-402i using a thumb 406a. In the pattern 404a, the third object 402c is the first selection and the seventh object 402g is the final selection. Thus, a reference fingerprint 408a of the thumb 406a is linked to the reference pattern 404a, and the reference pattern 404a and the reference fingerprint 408a are registered with the issuer as the reference information of the user 102.

[0086] Likewise, the user 102 may draw other reference patterns 404b-404e by connecting objects that are similar to the first through ninth objects 402a-402i. The user 102 may draw the reference patterns 404b-404e by utilizing an index finger 406b, a middle finger 406c, a ring finger 406d, and a little finger 406e, respectively. Thus, fingerprints 408b-408e of the index finger 406b, the middle finger 406c, the ring finger 406d, and the little finger 406e are linked to the reference patterns 404b-404e, respectively. Further, the patterns 404b-404e that are linked with the reference fingerprints 408b-408e are registered with the issuer as the additional reference information of the user 102. Thus, any one of the reference

patterns 404a-404e and the corresponding reference fingerprints 408a-408e may be utilized to authenticate the user 102 for transactions.

[0087] It will be apparent to a person skilled in the art that the scope of the disclosure is not limited to displaying nine objects (*i.e.*, the first through ninth objects 402a-402i) on the touch screen 208. In various other embodiments, different number of objects (e.g., 16 objects) may be displayed on the touch screen 208, without deviating from the scope of the disclosure. In another embodiment, the user 102 may choose to register a same reference pattern for two or more fingers. In another embodiment, a reference pattern may be drawn by the user 102 by utilizing two or more fingers simultaneously. In such a scenario, two or more reference fingerprints are linked with one reference pattern. For example, the user 102 may draw a reference pattern 404f by simultaneously utilizing the index finger 406b and the middle finger 406c. Thus, the reference fingerprints 408b and 408c are linked with the reference pattern 404f, and registered with the issuer as additional reference information of the user 102.

[0088] FIG. 5 is a table that illustrates the tabular database 500 maintained at the issuer server 112, in accordance with an exemplary embodiment of the disclosure. The tabular database 500 is stored in the memory of the issuer server 112, in the external database associated with the issuer server 112, or on the cloud server associated with the issuer server 112. The tabular database 500 is created by the issuer server 112 when various users register corresponding reference information with the issuer.

[0089] The tabular database 500 includes rows 502a-502c and columns 504a-504h. The columns 504a-504h represent names of the various users, account numbers of user accounts of the various users, unique card numbers of transaction cards issued to the various users, reference PINs registered with the issuer for authenticating the various users, reference patterns registered with the issuer for authenticating the various users, reference fingerprints registered with the issuer for authenticating the various users, pressure ranges (in Pascals) registered with the issuer for authenticating the various users, and time ranges (in seconds) registered with the issuer for authenticating the various users, respectively.

[0090] The rows 502a-502c represent links between transaction cards and reference information of the various users registered with the issuer. The row 502a represents a link between a transaction card of a user A and reference information of the user A, whereas the row 502b represents a link between the transaction card of the user A and additional

reference information of the user A. In an example, the user A corresponds to the user 102. Further, the row 502c represents a link between a transaction card of a user B and reference information of the user B.

[0091] The row 502a is added by the issuer server 112 when the user A registers reference information of the user A with the issuer. The row 502a includes an account number of a user account of the user A (say, 100100) and a unique card number of the transaction card of the user A (say, 4000400). The row 502a further includes a reference PIN (say, 5475) and a reference pattern (say, the reference pattern 404a) registered with the issuer. The row 502a further includes a reference fingerprint (say, the reference fingerprint 408a) of the thumb 406a utilized by the user A for drawing the reference pattern 404a. The row 502a further includes a pressure range (say, 0.29 to 0.31 Pascals) and a time range (say, 1.60 to 1.80 seconds) that are associated with the reference pattern 404a and the reference fingerprint 408a for authenticating the user A.

[0092] The row 502b is added by the issuer server 112 when the user A registers the additional reference information with the issuer. The row 502b includes the account number of the user account of the user A (say, 100100) and the unique card number of the transaction card of the user A (say, 4000400). The row 502b further includes the reference PIN (say, 5475) and another reference pattern (say, the reference pattern 404e) registered with the issuer for authenticating the user A. The row 502b further includes a reference fingerprint (*i.e.*, the reference fingerprint 408e) of the little finger 406e utilized by the user A for drawing the reference pattern 404e. The row 502b further includes a pressure range (say, 0.25 to 0.27 Pascals) and a time range (say, 1.32 to 1.54 seconds) that are associated with the reference pattern 404e and the reference fingerprint 408e for authenticating the user A.

[0093] The row 502c is added by the issuer server 112 when the user B registers reference information with the issuer. The row 502c includes an account number of a user account of the user B (say, 200200) and a unique card number of a transaction card of the user B (say, 5000500). The row 502c further includes a reference PIN (say, 1201) and a reference pattern (say, a reference pattern 506) registered with the issuer for authenticating the user B. The row 502c further includes a reference fingerprint (*i.e.*, a reference fingerprint 508) of a finger utilized by the user B for drawing the reference pattern 506. The row 502c further includes a pressure range (say, 0.28 to 0.30 Pascals) and a time range (say, 1.05 to

1.30 seconds) that are associated with the reference pattern 506 and the reference fingerprint 508 for authenticating the user B.

[0094] It will be apparent to a person skilled in the art that the data stored in the tabular database 500 may be stored in an encrypted format. It will further be apparent to a person skilled in the art that the pressure and time ranges disclosed in the tabular database 500 are exemplary values. Thus, in another embodiment, the pressure and time ranges may vary, without deviating from the scope of the disclosure.

[0095] FIGS. 6A-6C, collectively represent a process flow diagram 600 that illustrates an exemplary scenario for authenticating the user 102 for a transaction, in accordance with an exemplary embodiment of the disclosure. The issuer issues the transaction card 104 to the user 102 for performing transactions from the user account of the user 102. Prior to utilizing the transaction card 104 for performing the transactions, the user 102 is required to register user's reference information with the issuer. The user 102 may register multiple reference information with the issuer, such as five reference information (*i.e.*, five reference pattern-fingerprint pairs) as illustrated in FIG. 4. For the sake of brevity, it is assumed that the user 102 has registered only one reference information (*i.e.*, the reference information of the user 102) with the issuer. However, it will be apparent to a person skilled in the art that when multiple reference information of the user 102 is registered with the issuer, each reference information may be utilized for authenticating the user 102 in a similar manner as described below. Further, in one embodiment, the user 102 may not be allowed to use the same reference information for conducting two consecutive transactions.

[0096] The transaction card 104 may be utilized by the user 102 for performing various transactions at an ATM (such as the ATM 106a) or a POS device (such as the POS device 106b). For the sake of brevity, it is assumed that the user 102 initiates the transaction (*e.g.*, a cash withdrawal) at the ATM 106a by utilizing the transaction card 104 (as shown by arrow 602). The card reader 202 records the details of the transaction card 104 (as shown by arrow 604).

[0097] The ATM 106a, by way of the display screen 216, prompts the user 102 to enter a PIN (as shown by arrow 606). The user 102 enters a PIN, *i.e.*, an "input PIN", by way of the numeric keypad 206 (as shown by arrow 608). The numeric keypad 206 records the input PIN (as shown by arrow 610). The ATM 106a prompts the user 102 to draw a pattern (as shown by arrow 612). The user 102 draws a pattern, *i.e.*, an "input pattern", on the touch

screen 208 (as shown by arrow 614). The touch screen 208 records the input pattern (as shown by arrow 616). Further, the fingerprint sensors 210 record a fingerprint of a finger utilized by the user 102 to draw the input pattern (hereinafter referred to as an “input fingerprint”). The pressure sensors 212 record a pressure value corresponding to a pressure applied by the user 102 for drawing the input pattern (hereinafter referred to as an “input pressure value”). Additionally, the timer 214 records a time-duration taken by the user 102 to draw the input pattern (hereinafter referred to as an “input time-duration”). Thus, the ATM 106a records the input fingerprint, the input pressure value, and the input time-duration (as shown by arrow 618). The input PIN, the input pattern, the input fingerprint, the input pressure value, and the input time-duration are collectively referred to as the authentication information of the user 102.

[0098] The ATM 106a further prompts the user 102 to enter the transaction details of the transaction (as shown by arrow 620). The user 102 enters the transaction details (as shown by arrow 622). In an example, the user 102 enters the transaction details by way of the numeric keypad 206. Further, the ATM 106a (e.g., the numeric keypad 206) records the transaction details of the transaction initiated by the user 102 (as shown by arrow 624). The first processing circuitry 220 generates an authorization request for authorizing the transaction (as shown by arrow 626). The authorization request is pursuant to one or more standards for the interchange of transaction messages (such as the ISO8583 standard), and includes various fields (such as data elements) for storing various details. The authorization request includes the details of the transaction card 104, the authentication information, and the transaction details. In an example, the input fingerprint included in the authorization request corresponds to a digital image of the input fingerprint. In another example, the input fingerprint included in the authorization request corresponds to an encrypted fingerprint template of the digital image of the input fingerprint. The encrypted fingerprint template may be generated by the first processing circuitry 220 based on the digital image of the input fingerprint.

[0099] The first processing circuitry 220 communicates the authorization request to the acquirer server 108 (as shown by arrow 628). The acquirer server 108 communicates the authorization request to the payment network server 110 of the payment network associated with the transaction card 104 (as shown by arrow 630). The payment network server 110 receives the authorization request and communicates the authorization request to the issuer server 112 of the issuer associated with the transaction card 104 (as shown by arrow 632).

[0100] Based on the details of the transaction card 104, the issuer server 112 retrieves the first reference PIN, the first reference pattern, the first reference fingerprint, the pressure range, and the time range that are linked to transaction card 104 (as shown by arrow 634). For example, the issuer server 112 may refer to the tabular database 500 stored in the memory of the issuer server 112 and retrieve the first reference PIN, the first reference pattern, the first reference fingerprint, the time range, and the pressure range that are linked to transaction card 104.

[0101] The issuer server 112 determines if the input PIN matches the first reference PIN (as shown by arrow 636). The issuer server 112 determines if the input PIN matches the first reference PIN by utilizing known-in-the-art PIN comparison methods. In one exemplary scenario, the input PIN and the first reference PIN match. The issuer server 112 then determines if the input pattern matches the first reference pattern (as shown by arrow 638). The issuer server 112 determines if the input pattern matches the first reference pattern by utilizing known-in-the-art pattern comparison methods. In one exemplary scenario, the first reference pattern and the input pattern match. The issuer server 112 then determines if the input fingerprint matches the first reference fingerprint (as shown by arrow 640). The issuer server 112 determines if the input fingerprint matches the first reference fingerprint by utilizing known-in-the-art fingerprint comparison methods. In one exemplary scenario, the first reference fingerprint and the input fingerprint match. The issuer server 112 then determines if the input pressure value is within the pressure range (as shown by arrow 642). In one exemplary scenario, the input pressure value is within the pressure range. The issuer server 112 then determines if the input time-duration is within the time range (as shown by arrow 644). In one exemplary scenario, the input time-duration is within the time range. The issuer server 112 then successfully authenticates the user 102 (as shown by arrow 646). As the user 102 is successfully authenticated, the issuer server 112 updates the pressure range and the time range based on the input pressure value and the input time-duration, respectively (as shown by arrow 648).

[0102] The issuer server 112 authorizes the transaction based on the transaction amount and the account balance of the user account (as shown by arrow 650). In an example, the issuer server 112 determines if the transaction amount is less than or equal to the account balance. If the transaction amount is less than or equal to the account balance, the issuer server 112 authorizes the transaction. If the transaction amount is more than the account balance, the issuer server 112 declines the transaction. For the sake of brevity, it is assumed

that the issuer server 112 authorizes the transaction. The issuer server 112 generates the authorization response indicating that the transaction is authorized (as shown by arrow 652), and communicates the authorization response to the ATM 106a by way of the payment network server 110 and the acquirer server 108 (as shown by arrows 654, 656, and 658). Upon reception of the authorization response, the first processing circuitry 220 displays a “Transaction Successful” message to the user 102 by way of the display screen 216 (as shown by arrow 660). Further, the first processing circuitry 220 executes the transaction. In other words, the cash equivalent to the transaction amount is dispensed to the user 102, by way of the cash dispenser 218 (as shown by arrow 662).

[0103] It will be apparent to a person skilled in the art that if the issuer determines that the input PIN does not match the first reference PIN, the input pattern does not match the first reference pattern, the input fingerprint does not match the first reference fingerprint, the input pressure value is not within the pressure range, or the input time-duration is not within the time range, the issuer server 112 communicates a “Transaction Unsuccessful” message to the user 102 by way of the authorization response. It will further be apparent to a person skilled in the art that other types of transactions (such as cash deposit, funds transfer, and the like) may be processed in a manner similar to the process flow diagram 600.

[0104] Although the disclosure describes that fingerprints that are recorded while patterns are drawn by users are utilized for authenticating the users, the scope of the disclosure is not limited to it. In various other embodiments, other biometric information of the users (such as iris) may also be utilized for authenticating the users, without deviating from the scope of the disclosure.

[0105] Although the disclosure describes that the acquirer and the issuer are different financial institutions (*i.e.*, the acquirer server 108 and the issuer server 112 are shown as separate entities), the scope of the disclosure is not limited to it. In various other embodiments, the acquirer and the issuer may be the same financial institution, without deviating from the scope of the disclosure. Consequently, the acquirer server 108 and the issuer server 112 may correspond to a single entity. In such a scenario, the ATM 106a and the POS device 106b may communicate the registration and authorization requests directly to the issuer server 112.

[0106] The scope of the disclosure is not limited to the authentication of the user 102 for a transaction. In various other embodiments, the user 102 may be authenticated by way of

the above-described user authentication method, prior to accessing an account (e.g., a social media account, an electronic commerce account, an electronic mail account, or the like), entering an establishment, and the like, without deviating from the scope of the disclosure.

[0107] FIG. 7 is a block diagram that illustrates a perspective view of the POS device 106b, in accordance with an exemplary embodiment of the disclosure. The POS device 106b includes a card reader 702 having a card slot 704. The POS device 106b further includes a numeric keypad 706 and a touch screen 708. Further, the POS device 106b includes fingerprint sensors 710 and pressure sensors 712 that are located beneath the touch screen 708. The POS device 106b further includes a timer 714. Further, the POS device 106b is equipped with a display screen 716. The card reader 702, the numeric keypad 706, the touch screen 708, the fingerprint sensors 710, the pressure sensors 712, the timer 714, and the display screen 716 are functionally similar to the card reader 202, the numeric keypad 206, the touch screen 208, the fingerprint sensors 210, the pressure sensors 212, the timer 214, and the display screen 216 of the ATM 106a, respectively. The POS device 106b may further include a processing circuitry (not shown), a memory (not shown), and a transceiver (not shown) that are functionally similar to the first processing circuitry 220, the first memory 222, and the first transceiver 224 of the ATM 106a, respectively.

[0108] It will be apparent to a person skilled in the art that when the registration of the reference information with the issuer is initiated at the POS device 106b, the operations performed by the POS device 106b for registering the reference information with the issuer are similar to the operations performed by the ATM 106a in the process flow diagram 300. Similarly, when the transaction (e.g., a purchase from a merchant associated with the POS device 106b) is initiated at the POS device 106b, the operations performed by the POS device 106b for executing the transaction is similar to the operations performed by the ATM 106a in the process flow diagram 600.

[0109] FIG. 8 is a block diagram that illustrates various components of the issuer server 112, in accordance with an exemplary embodiment of the disclosure. The issuer server 112 includes a second processing circuitry 802, the memory of the issuer server 112 (hereinafter referred to and designated as a “second memory 804”), and a second transceiver 806. The second processing circuitry 802, the second memory 804, and the second transceiver 806 communicate with each other by way of a second communication bus 808.

[0110] The second processing circuitry 802 facilitates registration of reference information of users (such as the user 102) with the issuer and authorizes transactions initiated at the ATM 106a or the POS device 106b. The second processing circuitry 802 includes a registration manager 810 and an authorization manager 812.

[0111] The registration manager 810 includes suitable logic, circuitry, interfaces, and/or code, executable by the circuitry for facilitating the registration of reference information of the users with the issuer. When the registration of the reference information of the user 102 with the issuer is initiated at the ATM 106a or the POS device 106b, the registration manager 810 receives, by way of the second transceiver 806, the registration request generated by the ATM 106a or the POS device 106b, respectively. The registration manager 810 determines the pressure range and the time range based on the first through third reference pressure values and the first through third reference time-durations, respectively. Further, the registration manager 810 links the first reference PIN, the first reference pattern, the first reference fingerprint, the pressure range, and the time range to the transaction card 104, and stores the information pertaining to the link in the second memory 804. The registration manager 810 generates the registration response indicating that the registration is successful. Examples of the registration manager 810 may include an ASIC processor, a RISC processor, a CISC processor, an FPGA, or the like.

[0112] The authorization manager 812 includes suitable logic, circuitry, interfaces, and/or code, executable by the circuitry for authenticating users and authorizing the transactions. When a transaction is initiated by the user 102 at the ATM 106a or the POS device 106b, the authorization manager 812 receives, by way of the second transceiver 806, the authorization request generated by the ATM 106a or the POS device 106b, respectively. The authorization manager 812 retrieves, based on the details of the transaction card 104, the first reference PIN, the first reference pattern, the first reference fingerprint, the pressure range, and the time range that are linked to the transaction card 104. Further, the authorization manager 812 determines if the first reference PIN and the input PIN match, if the first reference pattern and the input pattern match, if the first reference fingerprint and the input fingerprint match, if the input pressure value is within the pressure range, and if the input time-duration is within the time range. Based on the determination, the authorization manager 812 authenticates the user 102. The authorization manager 812 further authorizes the transaction based on the transaction amount of the transaction and the account balance, and generates the authorization response indicating whether the transaction is authorized or

declined. Examples of the authorization manager 812 may include an ASIC processor, a RISC processor, a CISC processor, an FPGA, or the like.

[0113] The second memory 804 includes suitable logic, circuitry, interfaces, and/or code, executable by the circuitry, for storing the account profiles of various user accounts that are maintained at the issuer. The second memory 804 further stores the tabular database 500. Further, the second memory 804 may store the registration and authorization requests. Examples of the second memory 804 may include a RAM, a ROM, a removable storage drive, an HDD, a flash memory, a solid-state memory, or the like. It will be apparent to a person skilled in the art that the scope of the disclosure is not limited to realizing the second memory 804 in the issuer server 112, as described herein. In another embodiment, the second memory 804 may be realized in form of a database server or a cloud storage working in conjunction with the issuer server 112, without departing from the scope of the disclosure.

[0114] The second transceiver 806 includes suitable logic, circuitry, interfaces and/or code, executable by the circuitry, for transmitting and receiving data over the communication network 114 using one or more communication protocols. The second transceiver 806 receives various requests and messages from the payment network server 110. For example, the second transceiver 806 receives the registration and authorization requests from the payment network server 110. The second transceiver 806 transmits various requests and messages to the payment network server 110. For example, the second transceiver 806 transmits the registration and authorization responses to the payment network server 110. Examples of the second transceiver 806 may include, but are not limited to, an antenna, a radio frequency transceiver, a wireless transceiver, an Ethernet port, a USB port, or any other device configured to transmit and receive data.

[0115] FIGS. 9A and 9B, collectively represent a flow chart 900A that illustrates a method for facilitating registration of the reference information with the issuer, in accordance with an exemplary embodiment of the disclosure. The user 102 may initiate the registration of the reference information with the issuer at an ATM (such as the ATM 106a) or a POS device (such as the POS device 106b). For the sake of brevity, it is assumed that the user 102 initiates the registration of the reference information with the issuer at the ATM 106a.

[0116] The user 102 may utilize the transaction card 104 at the ATM 106a to initiate the registration. Referring now to FIG. 9A, at step 902, the card reader 202 records the details of the transaction card 104. The ATM 106a prompts the user 102 to enter a PIN for the first

time. The user 102 enters the first reference PIN by way of the numeric keypad 206. At step 904, the numeric keypad 206 records the first reference PIN. The ATM 106a prompts the user 102 to enter the same PIN for the second time. The user 102 enters the second reference PIN by way of the numeric keypad 206. At step 906, the numeric keypad 206 records the second reference PIN. At step 908, the first processing circuitry 220 determines if the first and second reference PINs are same. If at step 908, the first processing circuitry 220 determines that the first and second reference PINs are same, step 910 is performed.

[0117] The ATM 106a prompts the user 102 to draw a pattern for the first time. The user 102 draws the first reference pattern on the touch screen 208. At step 910, the touch screen 208 records the first reference pattern. At step 912, the fingerprint sensors 210, the pressure sensors 212, and the timer 214 record the first reference fingerprint, the first reference pressure value, and the first reference time-duration that are associated with the first reference pattern, respectively.

[0118] The ATM 106a then prompts the user 102 to draw the same pattern for the second time by utilizing the same finger. The user 102 draws the second reference pattern on the touch screen 208. At step 914, the touch screen 208 records the second reference pattern. At step 916, the fingerprint sensors 210, the pressure sensors 212, and the timer 214 record the second reference fingerprint, the second reference pressure value, and the second reference time-duration that are associated with the second reference pattern, respectively.

[0119] The ATM 106a further prompts the user 102 to draw the same pattern for the third time by utilizing the same finger. The user 102 draws the third reference pattern on the touch screen 208. At step 918, the touch screen 208 records the third reference pattern. At step 920, the fingerprint sensors 210, the pressure sensors 212, and the timer 214 record the third reference fingerprint, the third reference pressure value, and the third reference time-duration that are associated with the third reference pattern, respectively.

[0120] Referring now to FIG. 9B, at step 922, the first processing circuitry 220 determines if the first through third reference patterns are same. If at step 922, the first processing circuitry 220 determines that the first through third reference patterns are same, step 924 is performed. At step 924, the first processing circuitry 220 determines if the first through third reference fingerprints are same. If at step 924, the first processing circuitry 220 determines that the first through third reference fingerprints are dissimilar, step 926 is performed. If at step 922, the first processing circuitry 220 determines that the first through

third reference patterns are dissimilar, step 926 is performed. Similarly, if at step 908, the first processing circuitry 220 determines that the first and second reference PINs are dissimilar, step 926 is performed. At step 926, the first processing circuitry 220 displays the “Registration Unsuccessful” message to the user 102 by way of the display screen 216, and may prompt the user 102 to re-initiate the registration.

[0121] If at step 924, the first processing circuitry 220 determines that the first through third reference fingerprints are same, step 928 is performed. At step 928, the first processing circuitry 220 generates the registration request for registering the reference information of the user 102 (*i.e.*, the first reference PIN, the first reference pattern, the first reference fingerprint, the first through third reference time-durations, and the first through third reference pressure values) with the issuer. At step 930, the first processing circuitry 220 communicates the registration request to the acquirer server 108. At step 932, the first processing circuitry 220 receives the registration response from the acquirer server 108 indicating that the registration is successful. At step 934, the first processing circuitry 220 displays the “Registration Successful” message to the user 102 by way of the display screen 216.

[0122] Although the disclosure describes that the user 102 may initiate the registration with the issuer by way of a terminal device (such as the ATM 106a or the POS device 106b), the scope of the disclosure is not limited to it. In various other embodiments, the user 102 may initiate the registration by way of the user device (e.g., a smartphone, a laptop, a tablet, or the like) of the user 102 or by visiting the issuer premise and utilizing a registration device (e.g., a touch screen enabled electronic device) at the issuer premise, without deviating from the scope of the disclosure.

[0123] FIG. 9C is a flow chart 900B that illustrates a method for executing a transaction initiated by the user 102, in accordance with an exemplary embodiment of the disclosure. The user 102 may initiate the transaction at an ATM (such as the ATM 106a) or a POS device (such as the POS device 106b). For the sake of brevity, it is assumed that the user 102 initiates the transaction at the ATM 106a.

[0124] The user 102 utilizes the transaction card 104 to initiate the transaction (e.g., a cash withdrawal). At step 936, the card reader 202 records the details of the transaction card 104. The ATM 106a prompts the user 102 to enter a PIN. The user 102 enters the input PIN by way of the numeric keypad 206. At step 938, the numeric keypad 206 records the input

PIN. The ATM 106a prompts the user 102 to draw a pattern. The user 102 draws the input pattern on the touch screen 208. At step 940, the touch screen 208 records the input pattern. At step 942, the fingerprint sensors 210, the pressure sensors 212, and the timer 214 record the input fingerprint, the input pressure value, and the input time-duration that are associated with the input pattern, respectively.

[0125] The ATM 106a prompts the user 102 to enter the transaction details of the transaction. In an example, the user 102 enters the transaction details by way of the numeric keypad 206. At step 944, the numeric keypad 206 records the transaction details of the transaction initiated by the user 102. At step 946, the first processing circuitry 220 generates the authorization request for authenticating the user 102 and authorizing the transaction.

[0126] At step 948, the first processing circuitry 220 communicates the authorization request to the acquirer server 108. At step 950, the first processing circuitry 220 receives the authorization response from the acquirer server 108. At step 952, the first processing circuitry 220 determines if the transaction is authorized. If at step 952, the first processing circuitry 220 determines that the transaction is authorized, step 954 is performed. At step 954, the first processing circuitry 220 displays the “Transaction Successful” message to the user 102 by way of the display screen 216. At step 956, the first processing circuitry 220 executes the transaction, *i.e.*, dispenses cash equivalent to the transaction amount to the user 102 by way of the cash dispenser 218. If at step 952, the first processing circuitry 220 determines that the transaction is declined, step 958 is performed. At step 958, the first processing circuitry 220 displays the “Transaction Unsuccessful” message to the user 102 by way of the display screen 216, and may prompt the user 102 to re-initiate the transaction.

[0127] Although the disclosure describes that the user 102 may initiate the transaction by way of a terminal device (such as the ATM 106a or the POS device 106b), the scope of the disclosure is not limited to it. In various other embodiments, the user 102 may initiate the transaction by way of the user device (e.g., a smartphone, a laptop, a tablet, or the like) of the user 102, without deviating from the scope of the disclosure.

[0128] FIG. 10A is a flow chart 1000A that illustrates a method for registering the reference information of the user 102 with the issuer, in accordance with an exemplary embodiment of the disclosure. The registration of the reference information of the user 102 with the issuer may be initiated by the user 102 at the ATM 106a or the POS device 106b.

[0129] At step 1002, the issuer server 112 receives the registration request from the payment network server 110 when the user 102 initiates the registration at the ATM 106a or the POS device 106b. At step 1004, the issuer server 112 determines, based on the first through third reference pressure values, the pressure range for authenticating the user 102. At step 1006, the issuer server 112 determines, based on the first through third reference time-durations, the time range for authenticating the user 102.

[0130] At step 1008, the issuer server 112 links the first reference PIN, the first reference pattern, the first reference fingerprint, the pressure range, and the time range to the transaction card 104, thereby registering the reference information of the user 102 with the issuer. At step 1010, the issuer server 112 stores information pertaining to the link between the transaction card 104 and the first reference PIN, the first reference pattern, the first reference fingerprint, the pressure range, and the time range in the second memory 804. At step 1012, the issuer server 112 generates the registration response indicating that the registration is successful. At step 1014, the issuer server 112 communicates the registration response to the payment network server 110.

[0131] FIGS. 10B and 10C, collectively represent a flow chart 1000B that illustrates a method for authorizing the transaction initiated by the user 102, in accordance with an exemplary embodiment of the disclosure. Upon successful registration, the user 102 may utilize the transaction card 104 for performing various transactions. Referring now to FIG. 10B, at step 1016, the issuer server 112 receives the authorization request from the payment network server 110 when the user 102 initiates the transaction at the ATM 106a or the POS device 106b. At step 1018, the issuer server 112 retrieves, based on the details of the transaction card 104, the first reference PIN, the first reference pattern, the first reference fingerprint, the pressure range, and the time range that are linked to the transaction card 104.

[0132] At step 1020, the issuer server 112 determines if the input PIN matches the first reference PIN. If at step 1020, the issuer server 112 determines that the input PIN matches the first reference PIN, step 1022 is performed. At step 1022, the issuer server 112 determines if the input pattern matches the first reference pattern. If at step 1022, the issuer server 112 determines that the input pattern matches the first reference pattern, step 1024 is performed. At step 1024, the issuer server 112 determines if the input fingerprint matches the first reference fingerprint. If at step 1024, the issuer server 112 determines the input fingerprint matches the first reference fingerprint, step 1026 is performed.

[0133] At step 1026, the issuer server 112 determines if the input pressure value is within the pressure range. If at step 1026, the issuer server 112 determines that the input pressure value is within the pressure range, step 1028 is performed. At step 1028, the issuer server 112 determines if the input time-duration is within the time range. If at step 1028, the issuer server 112 determines that the input time-duration is within the time range, step 1030 is performed. Referring now to FIG. 10C, at step 1030, the issuer server 112 successfully authenticates the user 102. At step 1032, the issuer server 112 updates the pressure range and the time range based on the input pressure value and the input time-duration, respectively.

[0134] At step 1034, the issuer server 112 determines if the transaction amount is less than or equal to the account balance. If at step 1034, the issuer server 112 determines that the transaction amount is less than or equal to the account balance, step 1036 is performed. At step 1036, the issuer server 112 authorizes the transaction. At step 1038, the issuer server 112 generates the authorization response indicating that the transaction is authorized.

[0135] If at step 1034, the issuer server 112 determines that the transaction amount is more than the account balance, step 1040 is performed. Similarly, if at steps 1020 and 1022, the issuer server 112 determines that the first reference PIN and the input PIN do not match and the first reference pattern and the input pattern do not match, respectively, step 1040 is performed. Further if at steps 1024, 1026, and 1028, the issuer server 112 determines that the first reference fingerprint and the input fingerprint do not match, the input pressure value is not within the pressure range, and the input time-duration is not within the time range, respectively, step 1040 is performed.

[0136] At step 1040, the issuer server 112 declines the transaction. At step 1042, the issuer server 112 generates the authorization response indicating that the transaction is declined. Additionally, the issuer server 112 may generate an alert message and communicate the alert message to the user device of the user 102. At step 1044, the issuer server 112 communicates the authorization response to the payment network server 110. Step 1044 is also performed after step 1038.

[0137] FIG. 11 represents a high-level flow chart 1100 that illustrates a method for authenticating the user 102 for a transaction, in accordance with an exemplary embodiment of the disclosure. At step 1102, a terminal device (such as the ATM 106a or the POS device 106b) records the input PIN entered by the user 102, the input pattern drawn by the user on a touch screen (such as the touch screen 208) of the terminal device, and input biometric

information (such as the input fingerprint) of the user 102 while the input pattern is being drawn by the user 102. The terminal device records the input PIN, the input pattern, and the input fingerprint when the transaction is initiated by the user 102 at the terminal device by way of a payment mode (such as the transaction card 104). At step 1104, the terminal device executes the transaction based on the authentication of the user 102. The user 102 is authenticated when the input PIN, the input pattern, and the input fingerprint match the first reference PIN, the first reference pattern, and reference biometric information (*i.e.*, the first reference fingerprint) that are linked to the payment mode, respectively. The reference biometric information is associated with the reference pattern.

[0138] FIG. 12 is a block diagram that illustrates system architecture of a computer system 1200, in accordance with an exemplary embodiment of the disclosure. An embodiment of disclosure, or portions thereof, may be implemented as computer readable code on the computer system 1200. In one example, the ATM 106a, the POS device 106b, the acquirer server 108, the payment network server 110, and the issuer server 112 may be implemented as the computer system 1200.

[0139] Hardware, software, or any combination thereof may embody modules and components used to implement methods of FIGS. 9A-9C, 10A-10C, and 11. The computer system 1200 includes a processor 1202 that may be a special-purpose or a general-purpose processing device. The processor 1202 may be a single processor, multiple processors, or combinations thereof. Further, the processor 1202 may be connected to a communication infrastructure 1204, such as a bus, message queue, multi-core message-passing scheme, and the like. The computer system 1200 may further include a main memory 1206 and a secondary memory 1208. Examples of the main memory 1206 may include RAM, ROM, and the like. The secondary memory 1208 may include an HDD or a removable storage drive, such as a floppy disk drive, a magnetic tape drive, a compact disc, an optical disk drive, a flash memory, and the like.

[0140] The computer system 1200 further includes an input/output (I/O) interface 1210 and a communication interface 1212. The I/O interface 1210 includes various input and output devices that are configured to communicate with the processor 1202. Examples of the input devices may include a keyboard, a mouse, a joystick, a touchscreen, a microphone, and the like. Examples of the output devices may include a display screen, a speaker, headphones, and the like. The communication interface 1212 may be configured to allow data to be

transferred between the computer system 1200 and various devices that are communicatively coupled to the computer system 1200. Examples of the communication interface 1212 may include a modem, a network interface, *i.e.*, an Ethernet card, a communications port, and the like. Data transferred via the communication interface 1212 may correspond to signals, such as electronic, electromagnetic, optical, or other signals as will be apparent to a person skilled in the art.

[0141] A person of ordinary skill in the art will appreciate that embodiments of the disclosed subject matter can be practiced with various computer system configurations, including multi-core multiprocessor systems, minicomputers, mainframe computers, computers linked or clustered with distributed functions, as well as pervasive or miniature computers that may be embedded into virtually any device. Further, the operations may be described as a sequential process, however some of the operations may in fact be performed in parallel, concurrently, and/or in a distributed environment. In addition, in some embodiments the order of operations may be rearranged without departing from the spirit of the disclosed subject matter.

[0142] The user 102 is authenticated based on a combination of the input PIN, the input pattern, the input fingerprint, the input time-duration, and the input pressure value. The use of factors such as the input pattern and the input fingerprint in the authentication of the user 102 makes it difficult for a perpetrator to gain unauthorized access to the funds of the user 102. Further, a time-duration taken to draw a pattern and a pressure applied for drawing a pattern may be different for different individuals. Hence, the authentication of the user 102 based on a time-duration (*i.e.*, the input time-duration) taken to draw the input pattern and a pressure value (*i.e.*, the input pressure value) corresponding to a pressure applied while the input pattern is being drawn further makes it difficult for the perpetrator to access the user's funds. Thus, the multiple parameters utilized for authenticating the user 102 prevent the user 102 from being defrauded, especially in the event that the perpetrator feloniously acquires the PIN (*i.e.*, the input PIN), thereby preventing financial losses to the user 102 as well as a financial institution associated with the user 102. Hence, the user authentication method of the disclosure is a more secure method for authenticating users as compared to conventional user authentication methods that do not utilize patterns, fingerprints associated with the patterns, time-durations taken to draw the patterns, and pressures applied for drawing the patterns to authenticate users. Further, the user authentication method of the disclosure may also be implemented in existing terminal devices.

[0143] Techniques consistent with the disclosure provide, among other features, systems and methods for authenticating users (e.g., the user 102). While various exemplary embodiments of the disclosed system and method have been described above, it should be understood that they have been presented for purposes of example only, not limitations. It is not exhaustive and does not limit the disclosure to the precise form disclosed. Modifications and variations are possible in light of the above teachings or may be acquired from practicing of the disclosure, without departing from the breadth or scope.

[0144] In the claims, the words ‘comprising’, ‘including’ and ‘having’ do not exclude the presence of other elements or steps than those listed in a claim. The terms “a” or “an,” as used herein, are defined as one or more than one. Unless stated otherwise, terms such as “first” and “second” are used to arbitrarily distinguish between the elements such terms describe. Thus, these terms are not necessarily intended to indicate temporal or other prioritization of such elements. The fact that certain measures are recited in mutually different claims does not indicate that a combination of these measures cannot be used to advantage.

What is claimed is:

1. A method for authenticating a user for a transaction, the method comprising:

recording, by a terminal device when the transaction is initiated by the user at the terminal device by way of a payment mode, an input personal identification number (PIN) entered by the user, an input pattern drawn by the user on a touch screen of the terminal device, and input biometric information of the user while the input pattern is being drawn by the user; and

executing, by the terminal device, the transaction based on an authentication of the user, wherein the user is authenticated when the input PIN, the input pattern, and the input biometric information match a reference PIN, a reference pattern, and reference biometric information that are linked to the payment mode, respectively, and wherein the reference biometric information is associated with the reference pattern.

2. The method of claim 1, wherein the terminal device is at least one of an automated teller machine or a point-of-sale device.

3. The method of claim 1, wherein the input and reference biometric information correspond to input and reference fingerprints of fingers utilized by the user to draw the input and reference patterns, respectively.

4. The method of claim 1, further comprising recording, by the terminal device prior to the initiation of the transaction by the user, the reference pattern drawn by the user for a plurality of times, the reference biometric information while the reference pattern is being drawn by the user for the plurality of times, and a plurality of reference time-durations taken by the user to draw the reference pattern for the plurality of times, respectively, wherein:

the reference pattern and the reference biometric information are linked to the payment mode when the reference pattern is same for each of the plurality of times and the reference biometric information is same for each of the plurality of times, and

a time range for authenticating the user is determined based on the plurality of reference time-durations, and wherein the determined time range is linked to the payment mode.

5. The method of claim 4, further comprising recording, by the terminal device when the transaction is initiated by the user, an input time-duration taken by the user to draw the input pattern, wherein the user is authenticated when the input time-duration is within the

determined time range, and wherein when the user is authenticated, the determined time range is updated based on the input time-duration.

6. The method of claim 1, further comprising recording, by the terminal device prior to the initiation of the transaction by the user, the reference pattern drawn by the user for a plurality of times, the reference biometric information while the reference pattern is being drawn by the user for the plurality of times, and a plurality of reference pressure values corresponding to pressures applied by the user for drawing the reference pattern for the plurality of times, respectively, wherein:

the reference pattern and the reference biometric information are linked to the payment mode when the reference pattern is same for each of the plurality of times and the reference biometric information is same for each of the plurality of times, and

a pressure range for authenticating the user is determined based on the plurality of reference pressure values, and wherein the determined pressure range is linked to the payment mode.

7. The method of claim 6, further comprising recording, by the terminal device when the transaction is initiated by the user, an input pressure value corresponding to a pressure applied by the user for drawing the input pattern, wherein the user is authenticated when the input pressure value is within the determined pressure range, and wherein when the user is authenticated, the determined pressure range is updated based on the input pressure value.

8. A terminal device, comprising:

a numeric keypad configured to record an input PIN entered by a user for initiating a transaction at the terminal device;

a touch screen configured to display a first plurality of objects, and record an input pattern that is drawn by the user by connecting a second plurality of objects of the first plurality of objects; and

a set of biometric sensors configured to record input biometric information of the user while the input pattern is being drawn by the user, wherein the user is authenticated for the transaction when the input PIN, the input pattern, and the input biometric information match a reference PIN, a reference pattern, and reference biometric information that are linked to a payment mode utilized for initiating the transaction, respectively, and wherein the reference biometric information is associated with the reference pattern.

9. The terminal device of claim 8, wherein the terminal device is at least one of an automated teller machine or a point-of-sale device.
10. The terminal device of claim 8, wherein the input and reference biometric information correspond to input and reference fingerprints of fingers utilized by the user to draw the input and reference patterns, respectively.
11. The terminal device of claim 8, wherein prior to the initiation of the transaction by the user:
- the touch screen is further configured to record the reference pattern that is drawn by the user for a plurality of times; and
 - the set of biometric sensors is further configured to record the reference biometric information while the reference pattern is being drawn by the user for the plurality of times, wherein the reference pattern and the reference biometric information are linked to the payment mode when the reference pattern is same for each of the plurality of times and the reference biometric information is same for each of the plurality of times.
12. The terminal device of claim 11, further comprising:
- a timer configured to:
 - record a plurality of reference time-durations taken by the user to draw the reference pattern for the plurality of times, respectively; and
 - record an input time-duration taken by the user to draw the input pattern, wherein the user is authenticated when the input time-duration is within a time range linked to the payment mode, and wherein the time range is determined based on the plurality of reference time-durations; and
 - a set of pressure sensors configured to:
 - record a plurality of reference pressure values corresponding to pressures applied by the user for drawing the reference pattern for the plurality of times, respectively; and
 - record an input pressure value corresponding to a pressure applied by the user for drawing the input pattern, wherein the user is authenticated when the input pressure value is within a pressure range linked to the payment mode, and wherein the pressure range is determined based on the plurality of reference pressure values.
13. A system for authenticating a user for a transaction, the system comprising:

a terminal device, comprising:

a numeric keypad configured to record an input PIN entered by the user for initiating the transaction at the terminal device;

a touch screen configured to display a first plurality of objects, and record an input pattern that is drawn by the user by connecting a second plurality of objects of the first plurality of objects; and

a set of biometric sensors configured to record input biometric information of the user while the input pattern is being drawn by the user; and

a server that is communicatively coupled to the terminal device, and is configured to authenticate the user when the input PIN, the input pattern, and the input biometric information that are recorded by the terminal device match a reference PIN, a reference pattern, and reference biometric information that are linked to a payment mode utilized for initiating the transaction, respectively, wherein the reference biometric information is associated with the reference pattern.

14. The system of claim 13, wherein the terminal device is at least one of an automated teller machine or a point-of-sale device.

15. The system of claim 13, wherein the input and reference biometric information correspond to input and reference fingerprints of fingers utilized by the user to draw the input and reference patterns, respectively.

16. The system of claim 13, wherein prior to the initiation of the transaction by the user:

the touch screen is further configured to record the reference pattern that is drawn by the user for a plurality of times;

the set of biometric sensors is further configured to record the reference biometric information while the reference pattern is being drawn by the user for the plurality of times; and

the server is further configured to link the reference pattern and the reference biometric information to the payment mode when the reference pattern is same for each of the plurality of times and the reference biometric information is same for each of the plurality of times.

17. The system of claim 16, wherein the terminal device further comprises a timer, and wherein:

the timer is configured to record a plurality of reference time-durations taken by the user to draw the reference pattern for the plurality of times, respectively; and

the server is further configured to:

determine, based on the plurality of reference time-durations recorded by the terminal device, a time range for authenticating the user; and

link the time range to the payment mode.

18. The system of claim 17, wherein when the transaction is initiated by the user:

the timer is further configured to record an input time-duration taken by the user to draw the input pattern; and

the server is further configured to:

determine whether the input time-duration is within the time range linked to the payment mode, wherein the user is authenticated when the input time-duration is within the time range; and

update, when the user is authenticated, the time range based on the input time-duration.

19. The system of claim 16, wherein the terminal device further comprises a set of pressure sensors, and wherein:

the set of pressure sensors is configured to record a plurality of reference pressure values corresponding to pressures applied by the user for drawing the reference pattern for the plurality of times, respectively; and

the server is further configured to:

determine, based on the plurality of reference pressure values recorded by the terminal device, a pressure range for authenticating the user; and

link the pressure range to the payment mode.

20. The system of claim 19, wherein when the transaction is initiated by the user:

the set of pressure sensors is further configured to record an input pressure value corresponding to a pressure applied by the user for drawing the input pattern; and

the server is further configured to:

determine whether the input pressure value is within the pressure range linked to the payment mode, wherein the user is authenticated when the input pressure value is within the pressure range; and

update, when the user is authenticated, the pressure range based on the input pressure value.