June 2023

BIOMETRIC AUTHENTICATION FOR PAYMENT TRANSACTIONS

Manas Sharma
Visa

Pranutha Deep Vellanki
Visa

BIOMETRIC AUTHENTICATION FOR PAYMENT TRANSACTIONS

VISA

INVENTORS:

MANAS SHARMA

PRANUTHA DEEP VELLANKI

TECHNICAL FIELD

[0001] The present subject matter is, in general, related to authentication of online transactions, and in particular to, a system and method of providing biometric based authentication (or non-visual interaction-based authentication) for validating payment transactions.

BACKGROUND

[0002] Mobile application based online payments using smart devices have become a necessary part of our day-to-day life. Online payments include card-on-file payments, Unified Payments Interface (UPI), net banking, and the like. Online payments are authenticated using one or more issuer authentication techniques. To enhance security, at present, Two Factor of Authentication (2FA) or Additional Factor of Authentication (AFA) is used. For example, in 2FA online transactions are authenticated using One Time Password (OTP) which are delivered to consumer registered mobile phone or email or both.

[0003] Users having low vision use smartphones equipped with accessibility features such as screen readers and screen magnifiers. Online payment transactions may also be performed by such users. However, entering OTPs (e.g., for validating the payment transactions) while having those features turned on may expose the users to cyber-attacks. Also, there are possibilities that the OTPs may be seen by intruders while the users enter the OTPs. Moreover, it is difficult for visually impaired users to validate the payment transactions using OTPs. Hence, to overcome these and other associated problems, there exists a need for identifying secure authentication techniques for validating online payments and transactions.

[0004] The information disclosed in the background section of the disclosure is only for enhancement of understanding of the general background of the invention and should not be taken as an acknowledgement or any form of suggestion that this information forms the prior art already known to a person skilled in the art.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, explain the disclosed principles. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The same numbers are used throughout the figures to reference like features and components. Some embodiments of device or system and/or methods in accordance with embodiments of the present subject matter are now described, by way of example only, and with reference to the accompanying figures, in which:

[0006] **Figure. 1** shows an exemplary system **100** where the proposed technique of authenticating payment transactions may be implemented, in accordance with some embodiments of the present disclosure.

[0007] **Figure 2** shows an exemplary block diagram **200** of the system **100** as illustrated in **Figure 1**, in accordance with some embodiments of the present disclosure.

[0008] **Figure 3** illustrates a flow diagram representing an exemplary method **300** of performing online payment transactions, in accordance with some embodiments of the present disclosure.

[0009] **Figure 4** illustrates a flow diagram representing an exemplary method **400** of authenticating online payment transactions, in accordance with some embodiments of the present disclosure.

[0010] The figures depict embodiments of the disclosure for purposes of illustration only. One skilled in the art will readily recognize from the following description that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles of the disclosure described herein.

DESCRIPTION OF THE DISCLOSURE

[0011] In the present document, the word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment or implementation of the present subject matter described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments.

[0012] While the disclosure is susceptible to various modifications and alternative forms, specific embodiments thereof have been shown by way of example in the drawings and will be described in detail below. It should be understood, however that it is not intended to limit the disclosure to the particular forms disclosed, but on the contrary, the disclosure is to cover all modifications, equivalents, and alternative falling within the spirit and the scope of the disclosure.

[0013] The terms “comprises”, “comprising”, or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a setup, device, or method that comprises a list of components or steps does not include only those components or steps but may include other components or steps not expressly listed or inherent to such setup or device or method. In other words, one or more elements in a device or system or apparatus proceeded by “comprises… a” does not, without more constraints, preclude the existence of other elements or additional elements in the device or system or apparatus.

[0014] The terms "an embodiment", "embodiment", "embodiments", "the embodiment", "the embodiments", "one or more embodiments", "some embodiments", and "one embodiment" mean "one or more (but not all) embodiments of the invention(s)" unless expressly specified otherwise. The terms "including", "comprising", “having” and variations thereof mean "including but not limited to", unless expressly specified otherwise.

[0015] The present disclosure relates to a system and a method for authenticating online payment transactions. In an exemplary embodiment or aspect, the authentication is provided by self-authenticating the transaction by sending a push approval request to a mobile device of a user. In the present disclosure, a payment transaction may refer to an online transaction performed using a physical or virtual payment card and the physical or virtual payment card may comprise a debit card, a credit card, a prepaid card, a virtual card, and the like.

[0016] Referring now to **Figure 1**, which illustrates an exemplary system **100** where the proposed techniques of authenticating payment transactions may be implemented, in accordance with some embodiments of the present disclosure. The system **100** may include a mobile device **110** and a digital payment system **120** communicatively connected over a network. The mobile device **110** may include a mobile phone, a tablet, a laptop, or any other device that may support online payment transactions. In some implementations, a user may register the mobile device **110** with the digital payment system **120** for performing online payments. The user may perform the online payment using one or more applications installed in the mobile device **110**. For example, the applications may be any application that supports online payments such as an e-commerce application, a digital wallet application, a payment application, and the like.

[0017] In one non-limiting embodiment, the mobile device may need to be registered with the digital payment system **120** before performing any payment transaction. To perform registration of the mobile device **110** with the digital payment system **120**, the mobile device **110** may send a registration request to the digital payment system **120**. The registration request may comprise unique device identity among other information. In response to receiving the device registration request, the digital payment system **120** may send a registration response to the mobile device **110** indicating successful registration of the mobile device. In one non-limiting embodiment, during the registration process, the digital payment system **120** may acquire biometric data (e.g., fingerprints, iris scans, facial images, and the like) of the user through the mobile device **110**. In one non-limiting embodiment, the digital payment system **120** may store the unique device identity for verifying payment transactions initiated from the mobile device **120**.

[0018] In various embodiments, while making any payment transaction using the mobile device **120** (particularly, using any mobile application installed in the mobile device **120**), the mobile device **110** may generate a payment transaction request and the application installed in the mobile device **110** may initiate the payment transaction by sending the generated payment transaction request to the digital payment system **120**. In response to the payment transaction request from the mobile device **110**, the digital payment system **120** may transmit a biometric authentication request to the mobile device **110**. In response to the biometric authentication request from the digital payment system **120**, the mobile device may prompt the user to provide biometric data (e.g., fingerprints, iris scans, facial images, and the like). Upon receiving the biometric data from the user, the mobile device **110** may send the received biometric data to the digital payment system **120** for authentication. The digital payment system **120** upon receiving the biometric data of the user, may match the user's biometric data with biometric data of the user stored in a database. Upon successful match, the digital payment system **120** approves the transaction and sends a notification to the mobile device **110**, informing the success of the transaction. When the received biometric data of the user does not match with the stored biometric data, the digital payment system **120** declines the transaction and sends a notification to the mobile device **110**, informing the failure of the transaction.

[0019] Referring now to **Figure 2** that shows an exemplary block diagram **200** of the system **100** as illustrated in **Figure 1**. As shown in **Figure 2**, the mobile device **110** may include a memory **212**, a transceiver **216**, and a processor **214**. The transceiver **216** is configured to facilitate exchange of data between the mobile device **110** and the digital payment system **120**. The memory **212** is configured to store necessary commands needed from user end for initiating a payment transaction and for performing subsequent steps required for completing a payment transaction. The processor **214** is communicatively coupled to the memory **212** and to the transceiver **216**. The processor **214** processes or performs various operations of the system **100**. In an exemplary embodiment, the processor **214** may execute the instructions to run mobile applications and initiate a payment transaction request. The processor **214**, may also respond to the requests received from the digital payment system **120**.

[0020] The mobile device may communicate with the digital payment system **120** via a network **210**. The network **210** may comprise a data network such as, but not restricted to, the Internet, Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN), etc. In certain embodiments, the network **210** may include a wireless network, such as, but not restricted to, a cellular network and may employ various technologies including Enhanced Data rates for Global Evolution (EDGE), General Packet Radio Service (GPRS), Global System for Mobile Communications (GSM), Internet protocol Multimedia Subsystem (IMS), Universal Mobile Telecommunications System (UMTS) etc. In one embodiment, the network **210** may include or otherwise cover networks or subnetworks, each of which may include, for example, a wired or wireless data pathway.

[0021] As illustrated in **Figure 2**, the digital payment system **120** may include a processor **224** and a memory **222** storing instructions executable by at least the processor **224**. The processor **224** may execute user-generated or system-generated requests. In an exemplary embodiment, the processor **224** may receive the payment transaction request from the mobile device **110** and in response may transmit a biometric authentication request to the mobile device **110**. Further, the processor **224** may receive the biometric data of the user from the mobile device **110** for authenticating the transaction. The memory **222** may be communicatively coupled to the processor **224**. In some non-limiting embodiments, the data stored in the memory **222** may include registration data including biometric data, device information including unique identification of the mobile device **110**, merchant information, payment cards information, but not limited thereto. Further, the digital payment system **120** may includes a transceiver **228** configured to receive at least the device registration request, the payment transaction request from the user device **110**. The transceiver **228** is configured to send the device registration response and the response of the payment transaction request to the user device **110**.

[0022] The memory **212**, **222** may include a Random-Access Memory (RAM) unit and/or a non-volatile memory unit such as a Read Only Memory (ROM), optical disc drive, magnetic disc drive, flash memory, Electrically Erasable Read Only Memory (EEPROM), a memory space on a server or cloud and so forth. For the sake of illustration, it is assumed here that the memory is a non-volatile memory. Examples of the processor may include, but not restricted to, a general-purpose processor, a Field Programmable Gate Array (FPGA), an Application Specific Integrated Circuit (ASIC), a Digital Signal Processor (DSP), microprocessors, microcomputers, micro-controllers, digital signal processors, central processing units, state machines, logic circuitries, and/or any devices that manipulate signals based on operational instructions.

[0023] Referring now to **Figure 3** that depicts a flowchart illustrating a method **300** of performing a payment transaction, in accordance with some embodiments of the present disclosure. The various operations of the method **300** are performed by the mobile device **110** and in particular, by the processor **214** of the mobile device **110**. The method comprises, at block **302,** initiating a payment transaction for any purchase/transaction and transmitting a payment transaction request to the digital payment system **120**. Further, at block **304,** the mobile device **110** receives a biometric authentication request from the digital payment system **120.** At block **306,** in response to receiving the biometric authentication request from the digital payment system **120**, the mobile device **110** prompts the user to provide the biometric data which is then transmitted to the digital payment system **120** for authentication. At block **308**, the mobile device **110** receives a notification indicating the status of the transaction.

[0024] Referring now to **Figure 4** that depicts a flowchart illustrating a method **400** of authenticating online payment transactions, in accordance with some embodiments of the present disclosure. The method is performed by the digital payment system **120**, and in particular, by the processor **224** of the digital payment system **120**. The method comprises, at block **402,** receiving a payment transaction request from the mobile device **110.** At block **404,** upon receiving the payment transaction request, the digital payment system **120** sends a request for user's biometric data for performing biometric authentication. At block **406,** the digital payment system **120** receives the user's biometric data from the mobile device **110** and compares the received biometric data with the user’s biometric data stored in the memory **222**. At block **408**, if the biometric data matches, the digital payment system **120** approves the transaction and sends a notification informing the status of the transaction to the mobile device **110**.

<u>Advantages of the proposed disclosure</u>

[0025] The proposed techniques may help visually impaired users to authenticate payment transactions using the biometric means. By authenticating using biometric means the visually impaired users may not need any external support to carry out the transactions. Further, the proposed techniques also help to reduce fraudulent transactions as there is no OTP generated and the transaction verification is done by biometric means.

[0026] The illustrated steps are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments. It must also be noted that as used herein, the singular forms “a,” “an,” and “the” include plural references unless the context clearly dictates otherwise.

[0027] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, the computer readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term “computer readable medium” should be understood to include tangible items and exclude carrier waves and transient signals, i.e., are non-transitory. Examples include Random Access

Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, CD ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[0028] Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. Accordingly, the disclosure of the embodiments of the disclosure is intended to be illustrative, but not limiting, of the scope of the disclosure.

[0029] With respect to the use of substantially any plural and/or singular terms herein, those having skill in the art can translate from the plural to the singular and/or from the singular to the plural as is appropriate to the context and/or application. The various singular/plural permutations may be expressly set forth herein for sake of clarity.

BIOMETRIC AUTHENTICATION FOR PAYMENT TRANSACTIONS

ABSTRACT

The present disclosure relates to system and method of authenticating online payment transactions. The method includes receiving a payment transaction request from a mobile device **110.** Upon receiving the payment transaction request, a digital payment system **120** transmits a request for user's biometric data for performing biometric authentication. Upon receiving the user's biometric data from the mobile device **110,** the digital payment system **120** compares the received biometric data with the user's biometric data stored in a memory. If the biometric data matches, the digital payment system **120** approves the transaction and a notification is sent to the mobile device. The proposed method may help visually impaired users to authenticate payment transactions using the biometric means. Further, the proposed method also helps to reduce fraudulent transactions.

Figure. 4

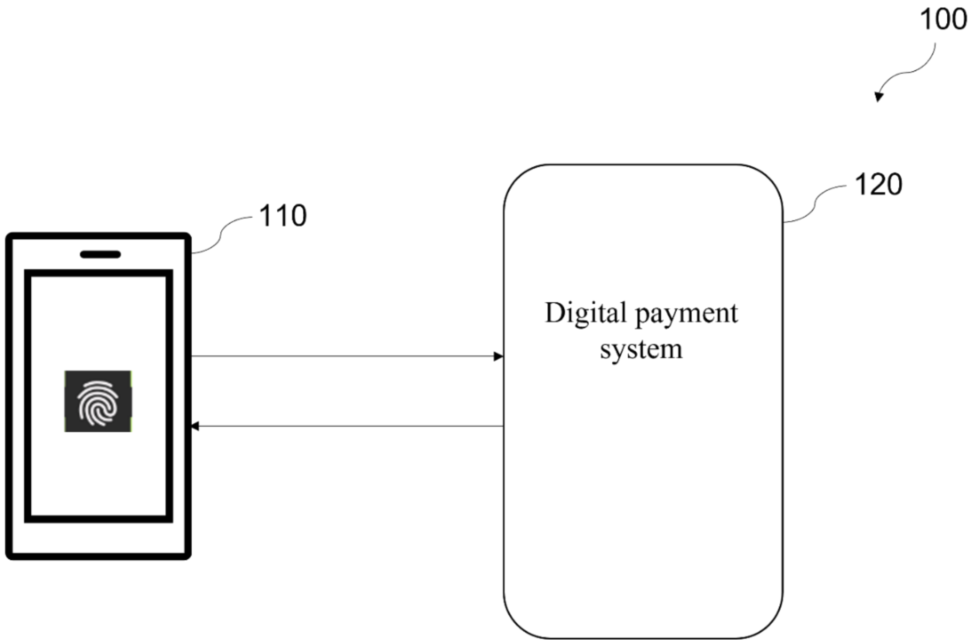

Figure 1

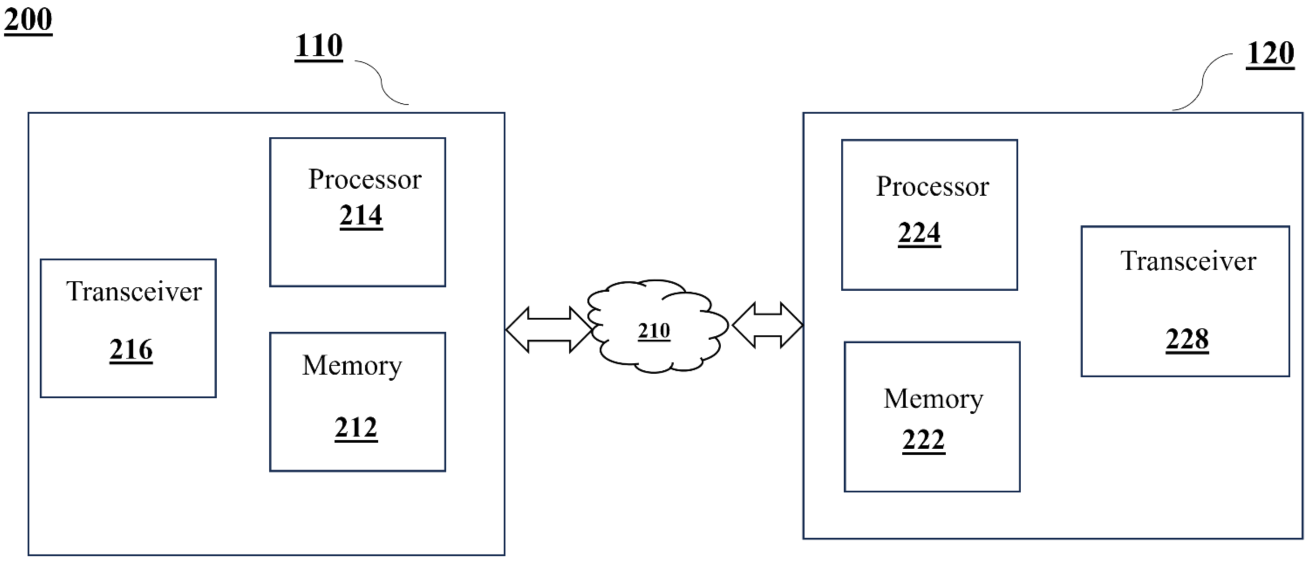

Figure 2

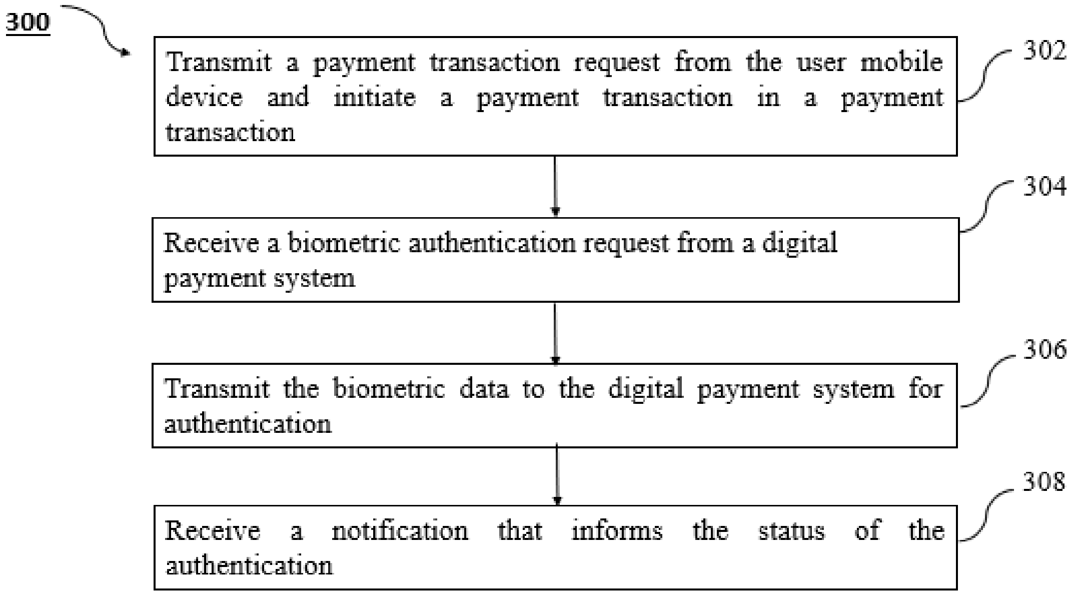
300
Transmit a payment transaction request from the user mobile device and initiate a payment transaction in a payment transaction
302
Receive a biometric authentication request from a digital payment system
304
Transmit the biometric data to the digital payment system for authentication
306
Receive a notification that informs the status of the authentication
308

Figure 3

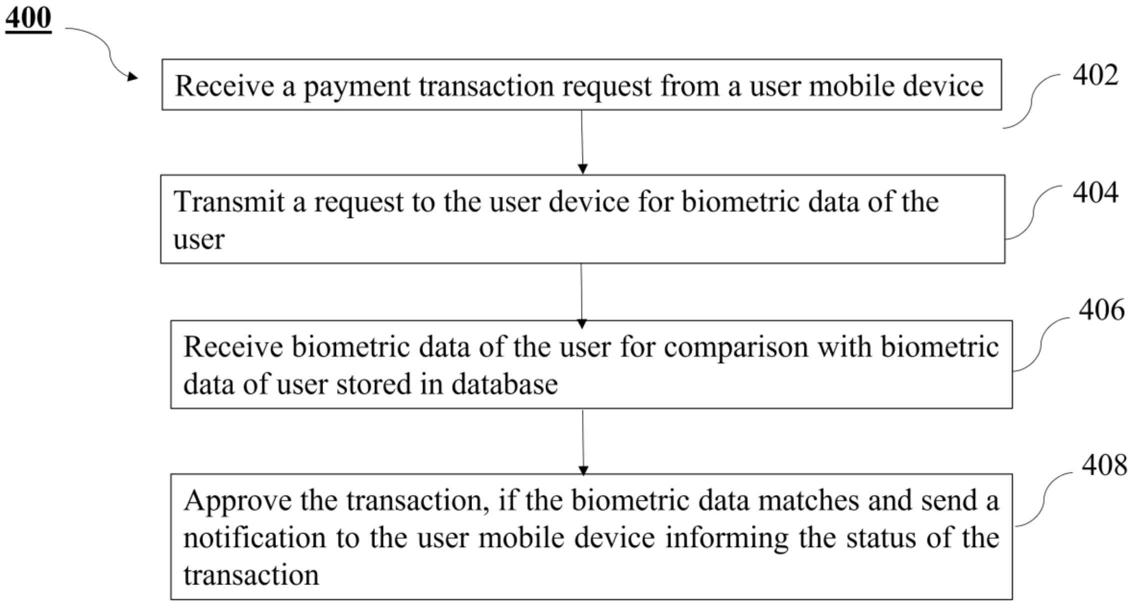
400
Receive a payment transaction request from a user mobile device
402
Transmit a request to the user device for biometric data of the user
404
Receive biometric data of the user for comparison with biometric data of user stored in database
406
Approve the transaction, if the biometric data matches and send a notification to the user mobile device informing the status of the transaction
408

Figure 4