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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 October 2019 (31.10.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/209435 A1

(51) International Patent Classification:
G06Q 20/40 (2012.01) *G06Q 20/20* (2012.01) *G06Q 20/38* (2012.01)

(21) International Application Number:
PCT/US2019/023506

(22) International Filing Date:
22 March 2019 (22.03.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201811015706 25 April 2018 (25.04.2018) IN

(71) Applicant: **MASTERCARD INTERNATIONAL INCORPORATED** [US/US]; 2000 Purchase Street, Purchase, NY 10577 (US).

(72) Inventor: **POL, Parag**; B 104 Rail Vihar Irwo Classic Appt., Near Boom Plaza, Sec 57, Gurgaon 122001 (IN).

(74) Agent: **DOBBYN, Colm, J.**; Mastercard International Incorporated, 2000 Purchase Street, Purchase, NY 10577 (US).

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

(54) **Title:** WEARABLE DEVICE FOR AUTHENTICATING PAYMENT TRANSACTIONS

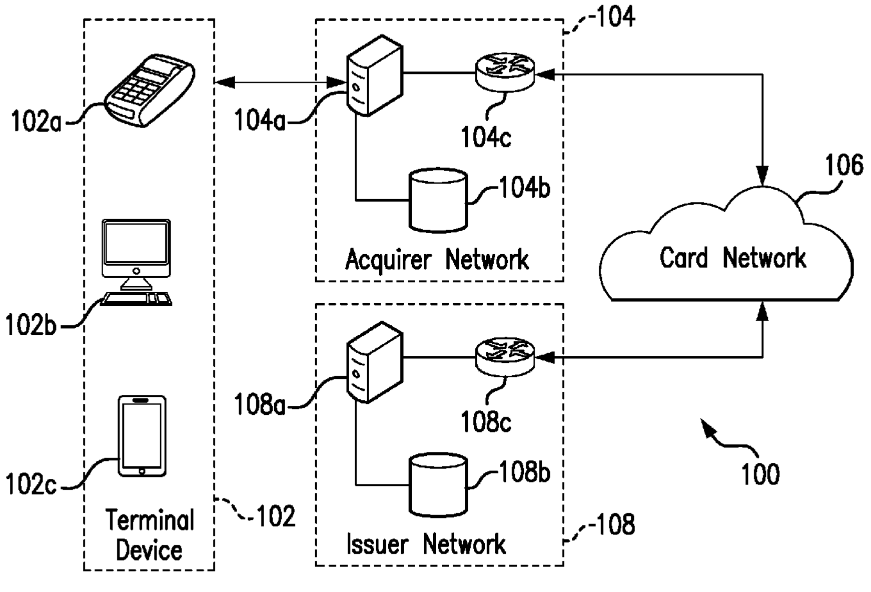

FIG. 1

(57) **Abstract:** The invention comprises a wearable device for enabling an electronic payment transaction through a payment account, at a point-of-sale (POS) terminal having wireless communication capability. The wearable device comprises a wirelesss transceiver, at least one fingerprint sensor, and a non-transient memory based data repository configured for storing one or more fingerprint based biometric templates and a unique device identifier corresponding to the wearable device. The wearable device additionally includes a processor configured to (i) generate one or more biometric templates based on fingerprint based biometric information received from the at least one fingerprint sensor, (ii) enroll the generated one or more biometric templates by storing said one or more biometric templates within non-transitory memory in the wearable device, and (iii) wirelessly transmit an electronic payment authorization to the POS terminal.

[Continued on next page]

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

Published:

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

WEARABLE DEVICE FOR AUTHENTICATING PAYMENT TRANSACTIONS

CROSS-REFERENCE TO RELATED APPLICATION

This application claims the benefit of, and priority to, Indian Patent Application No. 201811015706 filed on April 25, 2018. The entire disclosure of the above application is incorporated herein by reference.

FIELD OF THE INVENTION

The present invention relates to the field of electronic transactions, and more specifically to methods and systems for reducing user interventions necessary for authentication of transactions and improving the user experience.

BACKGROUND OF THE INVENTION

Electronic transactions and payments using payment cards or electronic payment accounts are increasingly common – with the number of electronic payment transactions and ubiquity of electronic transaction mechanisms and services growing steadily.

Prior art authentication mechanisms require identification of an electronic transaction account, payment card, or payment card account that is to be debited in connection with the proposed electronic transaction. Identification of an electronic transaction account and/or authentication of a person authorized to use such account, in some prior art systems, required users to present a device or token (such as a magnetic stripe card) that enabled a terminal device to read information identifying the concerned account. Possession of the device or token also served as an additional authentication mechanism – as it is presumed that the person presenting the device or token is the person authorized to hold/use such device or token. Such systems present difficulties in cases where the device or token are not in possession of the authorized user (for example, a customer forgets to carry his credit card or debit card). In other systems, an electronic transaction account, payment card or payment card account may be identified based on user input provided at a user input device, which user input typically comprises a numeric or alphanumeric ID corresponding to the electronic transaction account, payment card or payment card account.

Thereafter, existing solutions typically implement one or more authentication mechanisms to ensure that requested transactions are only permitted if received from an authorized individual/entity. Authentication mechanisms include several different approaches, including for example, single-factor authentication or multi-factor authentication. Authentication mechanisms can also vary depending on a required level of security – for example, low security transactions can rely on static password/passcode type authentication, while higher security transactions can require one or more of multi-factor authentication, dynamic password generation, biometric authentication, etc.

Such prior art mechanisms typically offer a poor user experience, particularly since the user may be required to memorize several different numeric or alphanumeric IDs for each of her/his accounts or payment cards, added to which extracting a payment card, swiping it at a terminal device and/or complying with one or more authentication requirements is often cumbersome and inconvenient.

There is accordingly a need for systems and methods that reduce active interventions required by a user for authentication purposes, while retaining appropriate levels of transaction security.

The present invention provides efficient and secure mechanisms to address the above requirements. Additionally, the invention enables these mechanisms to be implemented using terminal devices that are capable of wireless communication, including for example, point-of-sale (POS) terminals having wireless capabilities.

SUMMARY

The invention provides methods and systems for reducing user interventions necessary for authentication of transactions and improving the user experience.

The invention comprises a wearable device for enabling an electronic payment transaction through a payment account, at a point-of-sale (POS) terminal having wireless communication capability. The wearable device comprises a wirelesss transceiver, at least one fingerprint sensor, and a non-transient memory based data repository configured for storing one or more fingerprint based biometric templates and a unique device identifier corresponding to the wearable device. The wearable device additionally includes a processor configured to (i) generate one or more biometric templates based on fingerprint based biometric information received from the at least one fingerprint sensor, (ii) enroll the generated one or more biometric templates by storing said one or more biometric templates within non-transitory memory in the wearable device, and (iii) wirelessly transmit an electronic payment authorization to the POS terminal, wherein said electronic payment authorization is transmitted in response to (a) receipt of a payment transaction request at the POS terminal, (b) receiving fingerprint biometric information from the at least one fingerprint sensor, and (c) determining that the received fingerprint biometric information matches a biometric template stored within the data repository.

The electronic payment authorization transmitted by the processor to the POS terminal may comprise one or more of (i) user account information, payment card information or payment account information associated with the wearable device, (ii) the unique identifier corresponding to the wearable device and (iii) a transaction authentication signal.

In an embodiment, the electronic payment authorization transmitted by the processor to the POS terminal may additionally comprise both of (i) user account information, payment card information or payment account information associated with the wearable device, and (ii) the unique identifier corresponding to the wearable device.

The processor may be configured to (i) communicate with a remote authentication server through a data connection with a client terminal that is in network communication with the remote authentication server, and (ii) in response to commencement of a process for associating the wearable device with a user account, payment card or payment account, transmit the unique device identifier corresponding to the wearable device to the remote authentication server, wherein an association between the transmitted unique device identifier and the user account, payment card or payment account is thereafter recorded at the remote authentication server.

The processor may be configured to respond to a determination that the wearable device is not communicably coupled with the remote authentication server, by preventing storage of fingerprint biometric information in the data repository of the wearable device.

The processor may in an embodiment be configured to store within the data repository, data corresponding to any of a user account, payment card or payment account that has been associated with the unique device identifier corresponding to the wearable device at the remote authentication server.

In a particular embodiment, the wearable device is configured and sized as a finger ring.

In another embodiment of the wearable device, as claimed in claim 1, the processor is configured to (i) generate a plurality of biometric templates based on fingerprint based biometric information corresponding to a plurality of fingerprints simultaneously presented for fingerprint acquisition at the at least one fingerprint sensor, and (ii) enroll the generated plurality of biometric templates by storing said plurality of biometric templates within non-transitory memory in the wearable device.

Additionally, the electronic payment authorization may be transmitted in response to (i) receiving fingerprint biometric information corresponding to a plurality of fingerprints simultaneously presented for authentication at the at least one fingerprint sensor within the wearable device, and (ii) determining that the receiving fingerprint biometric information corresponding to a plurality of fingerprints simultaneously presented for authentication at the at least one fingerprint sensor within the wearable device matches the enrolled plurality of biometric templates stored within the non-transitory memory in the wearable device.

In an embodiment of the wearable device, the at least one fingerprint sensor comprises two or more fingerprint sensors. Said two or more fingerprint sensors may be located and sized to enable a user to simultaneously present a thumb and forefinger for fingerprint scanning at said fingerprint sensors.

The invention alternatively comprises a system for enabling an electronic payment transaction through a payment account, at a point-of-sale (POS) terminal having wireless communication capability. The system comprises a remote authentication server, and a wearable device. The wearable device comprises a wirelesss transceiver, a fingerprint sensor, and a non-transient memory based data repository configured for storing one or more fingerprint based biometric templates and a unique device identifier corresponding to the wearable device. The wearable device additionally includes a processor configured to (i) generate one or more biometric templates based on fingerprint based biometric information received from the fingerprint sensor, and (ii) wirelessly transmit an electronic payment authorization to the POS terminal, wherein said electronic payment authorization is transmitted in response to (a) receipt of a payment transaction request at the POS terminal, (b) receiving fingerprint biometric information from the fingerprint sensor, and (c) determining that the received fingerprint biometric information matches a biometric template stored within the data repository.

In an embodiment of the system, the electronic payment authorization transmitted by the processor to the POS terminal comprises one or more of (i) user account information, payment card information or payment account information associated with the wearable device, (ii) the unique identifier corresponding to the wearable device and (iii) a transaction authentication signal.

The electronic payment authorization transmitted by the processor to the POS terminal may comprise both of (i) user account information, payment card information or payment account information associated with the wearable device, and (ii) the unique identifier corresponding to the wearable device.

The processor within said system may be configured to (i) communicate with the remote authentication server through a data connection with a client terminal that is in network communication with the remote authentication server, and (ii) in response to commencement of a process for associating the wearable device with a user account, payment card or payment account, transmit the unique device identifier corresponding to the wearable device to the remote authentication server. The remote authentication server is configured to record an association between the transmitted unique device identifier and the user account, payment card or payment account.

In a further embodiment the processor is configured to respond to a determination that the wearable device is not communicably coupled with the remote authentication server, by preventing storage of a fingerprint biometric information in the data repository of the wearable device.

The processor may in an embodiment be configured to store within the data repository, data corresponding to any of a user account, payment card or payment account that has been associated with the unique device identifier corresponding to the wearable device at the remote authentication server.

In another embodiment, the processor is configured to (i) generate a plurality of biometric templates based on fingerprint based biometric information corresponding to a plurality of fingerprints simultaneously presented for fingerprint acquisition at the at least one fingerprint sensor, and (ii) enroll the generated plurality of biometric templates by storing said plurality of biometric templates within non-transitory memory in the wearable device. In this embodiment, the electronic payment authorization is transmitted in response to (i) receiving fingerprint biometric information corresponding to a plurality of fingerprints simultaneously presented for authentication at the at least one fingerprint sensor within the wearable device, and (ii) determining that the receiving fingerprint biometric information corresponding to a plurality of fingerprints simultaneously presented for authentication at the at least one fingerprint sensor within the wearable device matches the enrolled plurality of biometric templates stored within the non-transitory memory in the wearable device.

In a particular embodiment of the system the at least one fingerprint sensor comprises two or more fingerprint sensors. Said two or more fingerprint sensors may be located and sized to enable a user to simultaneously present a thumb and forefinger for fingerprint scanning at said fingerprint sensors.

The invention further provides a method for enabling an electronic payment transaction through a payment account, at a point-of-sale (POS) terminal having wireless communication capability, the method comprising (i) generating one or more biometric templates based on fingerprint based biometric information received from a fingerprint sensor provided within a wearable device, (ii) storing the one or more fingerprint based biometric templates within a data repository within the wearable device, (iii) wirelessly transmitting an electronic payment authorization from the wearable device to the POS terminal, wherein said electronic payment authorization is transmitted in response to (a) receipt of a payment transaction request at the POS terminal, (b) receiving fingerprint biometric information from the fingerprint sensor, and (c) determining that the received fingerprint biometric information matches a biometric template stored within the data repository.

In a method embodiment, the electronic payment authorization transmitted by the processor to the POS terminal includes one or more of (i) a unique device identifier corresponding to the wearable device, (ii) user account information, payment card information or payment account information associated with the wearable device, and (iii) a transaction authentication signal.

The electronic payment authorization transmitted by the processor to the POS terminal may include both of (i) user account information, payment card information or payment account information associated with the wearable device, and (ii) the unique identifier corresponding to the wearable device.

The method may additionally include the steps of (i) initiating a process for associating the wearable device with a user account, payment card or payment account at a remote authentication server, (ii) transmitting the unique device identifier corresponding to the wearable device, from the wearable device to the remote authentication server through a data connection with a client terminal that is in network communication with the remote authentication server, and (iii) recording an association between the transmitted unique device identifier and the user account, payment card or payment account, at the remote authentication server.

In an embodiment, the method includes the step of responding to a determination that the wearable device is not communicably coupled with the remote authentication server, by preventing storage of a fingerprint biometric information in the data repository of the wearable device.

The method may additionally include the step of storing within the data repository, data corresponding to any of a user account, payment card or payment account that has been associated with the unique device identifier corresponding to the wearable device at the remote authentication server.

In a further embodiment, the method comprises (i) generating a plurality of biometric templates based on fingerprint based biometric information corresponding to a plurality of fingerprints simultaneously presented for fingerprint acquisition at the at least one fingerprint sensor, (ii) enrolling the generated plurality of biometric templates by storing said plurality of biometric templates within non-transitory memory in the wearable device, and (iii) transmitting the electronic payment authorization in response to (a) receiving fingerprint biometric information corresponding to a plurality of fingerprints simultaneously presented for authentication at the at least one fingerprint sensor within the wearable device, and (b) determining that the receiving fingerprint biometric information corresponding to a plurality of fingerprints simultaneously presented for authentication at the at least one fingerprint sensor within the wearable device matches the enrolled plurality of biometric templates stored within the non-transitory memory in the wearable device.

In a method embodiment, the at least one fingerprint sensor comprises two or more fingerprint sensors. Said two or more fingerprint sensors may be located and sized to enable a user to simultaneously present a thumb and forefinger for fingerprint scanning at said fingerprint sensors.

BRIEF DESCRIPTION OF THE ACCOMPANYING DRAWINGS

Figure 1 illustrates a system for authenticating and implementing electronic transactions through a payment card transaction system.

Figure 2 illustrates an exemplary POS terminal device of the type used to implement payment card based transactions.

Figure 3 illustrates an exemplary wearable device in accordance with the teachings of the present invention.

Figure 4 illustrates an exemplary wireless data exchange between a wearable authentication device and a POS terminal having wireless capability.

Figure 5 illustrates exemplary components within a wearable device in accordance with the teachings of the present invention.

Figure 6 illustates network communication between the wearable device and an authentication server.

Figures 7 and 8 illustrate method embodiments of the invention.

Figures 9A and 9B illustrate exemplary embodiments of the wearable device.

Figure 10 illustrates an exemplary computer system according to which various embodiments of the present invention may be implemented.

DETAILED DESCRIPTION

The present invention provides secure authentication mechanisms for electronic transactions while reducing user interventions necessary to effect such electronic transactions.

For the purposes of the present invention, the following terms shall be understood to have the corresponding meanings provided below:

“**Acquirer**” shall mean a business (e.g., a financial institution or a merchant bank) that contracts with a merchant to coordinate with the issuer network of a customers’ payment card.

“**Acquirer network**” shall refer to a communication network, including hardware, software and other equipment used by an acquirer to transmit and process card based transactions and information related to merchants, customers, payment cards and transactions.

"**Biometric template**" shall mean a digital reference or digital record of distinct biometric features or characteristics that have been extracted from a biometric sample.

"**Cardholder**" or "**Customer**" shall mean an authorized payment card user who is making a purchase or effecting an electronic transaction with a payment card.

"**Card network**" shall refer to the intermediary between the merchant's acquirer and the customer's issuer (for example, Mastercard® or Visa®). The card network primarily coordinates payment card transactions between acquirers and issuers, and additionally coordinates clearing and settlement services to transfer payments from issuers to merchants.

"**Device having wireless capability**" shall mean any device that is capable of wireless communication with other wireless communication enabled devices. Non-limiting embodiments of devices having wireless capability include any processor driven computing devices including desktops, laptops, tablets and personal digital assistants, and telecommunication devices, having any of 1G, 2G, 3G, 4G, LTE, GPRS, EDGE, GPS, cellular, satellite, wifi, Bluetooth, Bluetooth lite and RFID based communication capabilities, for communication other devices having corresponding wireless capabilities.

"**Issuer**" shall mean a financial institution that issues payment cards and maintains a contract with a customer or card holder for repayment or settlement of purchases made on the payment card.

"**Issuer network**" shall refer to a communication network, including hardware, software and other equipment used by an issuer to transmit and process payment card transactions and information related to customers, payment cards and transactions.

"**Merchant**" shall mean an authorized acceptor of payment cards for the payment of goods or services sold by the merchant.

"**Passive authentication**" shall mean one or both of electronic account identification or customer identity authentication, where a user does not have to affirmatively present a payment card, or affirmatively provide user input through a manual input mechanism for achieving said electronic account identification or user identity authentication.

"**Payment card**" shall mean a card or data associated with a payment account that may be provided to a merchant in order to fund a financial transaction via the associated payment account. Payment cards may include credit cards, debit cards, charge cards, stored-value cards, prepaid cards, fleet cards, virtual payment numbers, virtual card numbers, controlled payment numbers, etc. A payment card may be a physical card that may be provided to a merchant, or may be data representing the associated payment account (e.g., as stored in a communication device, such as a smart phone or computer). For example, in some instances, data including a payment account number may be considered a payment card for the processing of a transaction funded by the associated payment account. In some instances, a check may be considered a payment card where applicable.

"**Payment account**" shall mean any account that may be used for the purposes of effecting an electronic payment or electronic transaction, and shall include any electronic transaction account, payment card account, bank account or electronic wallet account.

"**Terminal device having wireless capability**" shall mean any device that is (i) capable of receiving information for identifying an electronic payment account, payment card, or card holder, authenticating a card holder, and transmitting payment account information, payment card information or customer information directly or indirectly to one or more of an acquirer network, card network or issuer network and (ii) that is capable of wireless communication with other wireless communication enabled devices. Non-limiting embodiments of terminal devices having wireless capability include POS terminals, computing devices including desktops, laptops, tablets and personal digital assistants, and telecommunication devices, having any of 1G, 2G, 3G, 4G, LTE, GPRS, EDGE, GPS, cellular, satellite, wifi, Bluetooth, Bluetooth lite and RFID based communication capabilities, for communication other devices having corresponding wireless capabilities.

Figure 1 illustrates a conventional system 100 that can be used for implementing electronic transactions based on a payment card or payment card information presented by a cardholder at a terminal device 102. In certain embodiments of the present invention, system 100 may be modified to implement the invention. System 100 includes terminal device 102, acquirer network 104, card network 106 and issuer network 108. While Figure 1 has been used to illustrate a payment card based network, it would be understood that similar principles and one or more entities having some or all of the same functions may be used to effect payments through any electronic transaction account.

Acquirer network 104 may be communicably coupled with terminal device 102, and comprises server 104a, acquirer network database 104b and interface gateway 104c. Server 104a may be configured to receive and process information relating to payment card transactions. In an embodiment, the acquirer network may receive or process transactions received only from merchants having a merchant account with the acquirer – which determination may be made based on information retrieved from acquirer network database 104b. Interface gateway 104c may include a hardware or software network gateway configured to enable acquirer network 104 to communicate with card network 106.

Card network 106 may be communicably coupled to both acquirer network 104 and issuer network 108.

Issuer network 108 comprises server 108a, issuer network database 108b and interface gateway 108c. Server 108a may be configured to receive and process information relating to payment card transactions. In an embodiment, the issuer network may only receive or process transactions received from merchants having a merchant account with the issuer – which determination may be made based on information retrieved from issuer network database 108b. Interface gateway 108c may include a hardware or software network gateway configured to enable issuer network 108 to communicate with card network 106.

It would be understood that in an embodiment, when system 100 is configured to implement the present invention, terminal device 102 may comprise any processor implemented user interface device having wireless capability, including without limitation a POS terminal device 102a, computing device 102b, or mobile phone or smartphone 102c.

According to various embodiments of the invention, a system or method may be provided to (i) identify a payment account and authenticate a requested electronic transaction, based on presentation or detection of one or more wearable devices having wireless capability that have been previously associated with an authorized user of the payment account, and which are capable of biometric authentication of a person seeking to complete a requested electronic transaction.

Figure 2 illustrates a conventional electronic payment system 200 comprising POS terminal 202 and payment card 204. In operation, an electronic transaction request (for example a request to charge USD 123 to a payment card) is input at POS terminal 202. Payment card 204 is thereafter presented / swiped at POS terminal 202. POS terminal 202 reads information recorded on a magnetic stripe of payment card 204, and uses the extracted information to identify a payment card / payment card account to which the amount is to be charged. The individual presenting the payment card may thereafter be called upon to satisfy one or more authentication requirements using the POS terminal, whereupon the authentication inputs provided by such individual are verified against one or more predefined authentication keys – and in case of a match, the requested electronic transaction is carried out.

The present invention additionally relies on fingerprint based biometric sensors for the purpose of payment authentication. Fingerprint based biometrics involve acquiring an image/impression of a user's finger – which image / impression may thereafter be analyzed and compared against a database of previously enrolled or registered fingerprints or fingerprint templates that record information corresponding to specific biometric features of user fingerprints. The biometric features, including ridges and valleys and their respective characteristics such as loops, whorls and arches (i.e. biometric features) of a user's fingerprint, are analyzed to determine whether the analyzed fingerprint matches a previously enrolled or registered fingerprint or fingerprint template. If the analyzed fingerprint matches an enrolled fingerprint or fingerprint template stored in a database of enrolled fingerprints or fingerprint templates, the user is authenticated with consequent access or permission to access a requested device or service.

Figure 3 illustrates a wearable device 300 of a type that may be used to implement the present invention. Wearable device 300 illustrated in Figure 3 comprises an annular ring 302 – which may, in an embodiment, be configured as a finger ring, or worn as jewelry, or carried on the person of the individual. An outer circumferential surface of annular ring 302 is provided with a fingerprint sensor 304. It would however be understood that fingerprint sensor 304 may be located on any surface of annular ring 302.

While the illustrated wearable device 300 in Figure 3 is a ring, it would be understood that any other type of wearable device may be used including a watch, wristband, band, necklace, belt, buckle, clip and / or any other wearable item, provided that the wearable includes a fingerprint sensor and the other one or more components described in more detail below.

Fingerprint sensor 304 may comprise any sensor capable of sensing, imaging or otherwise capturing the biometric patterns of an individual's fingerprint(s). In various embodiments, fingerprint sensor 304 may be implemented using any fingerprint technologies including any of capacitive, ultrasonic, thermal, pressure, resistive, infrared or optical sensors. The fingerprint sensor 304 may in certain embodiments include a fingerprint touch sensor or a fingerprint swipe sensor.

Figure 4 illustrates specific components that may be implemented within a wearable device 402 of the type that may be used to implement the present invention. In addition to fingerprint sensor 404, wearable device 402 comprises fingerprint template repository 406, device ID and / or payment account data repository 408, processor 410, wireless communication system 412 and power source 414.

Fingerprint template repository 406 comprises a non-transitory memory configured to store one or more fingerprints or fingerprint templates corresponding to one or more enrolled fingerprints. It would be understood that authentication of an individual by wearable device 402 may comprise the step of comparing biometric features extracted from fingerprint information acquired at fingerprint sensor 404 against biometric features of enrolled fingerprints or fingerprint templates stored within fingerprint template repository.

Repository 408 may comprise a non-transitory memory configured to store one or both of (i) a unique device ID corresponding to the wearable device and (ii) information or data identifying one or more user accounts / payment cards / payment accounts associated with an authorized user of the wearable device (e.g. associated with a user whose fingerprints have been enrolled with the wearable device). In a particular embodiment, repository 408 may include information associating a specific user account / payment card / payment account and a corresponding enrolled fingerprint or fingerprint template stored within fingerprint template repository 406.

Processor 410 may include any processing device implemented within wearable device 402 that is capable of being configured to implement one or more of the feature extraction, feature analysis and / or fingerprint matching steps necessary for enrollment or matching of fingerprints in accordance with any of the inventions embodiments. Processor 410 may in certain embodiments additionally be configured for pre-processing of fingerprint images prior to feature extraction, with a view to improve the feature extraction process and the accuracy of fingerprint recognition.

The wearable device 402 includes wireless communication system 412, which system may include one or more controllers and hardware interfaces for wireless communication and optionally for wired communication as well. Wireless communication system 412 may include any wireless transceiver or wireless communicator or any system having wireless communication capability, such as for example any of 1G, 2G, 3G, 4G, LTE, GPRS, EDGE, GPS, cellular, satellite, wifi, Bluetooth, Bluetooth lite, infra red, ultrasonic, or RFID based communication capabilities. Wireless communication system 412 may be configured to enable wireless communication between wearable device 402 and a corresponding POS terminal having wireless capability and at which a specific transaction is sought to be carried out. Wireless communication 412 may additionally be configured for wireless or wire based communication with a network based remote authentication server.

Wearable device 402 may also include power source 414 – to power any one or more of the other components within said wearable device. Exemplary power sources may include a flexible strip battery, a rechargeable battery, one or more charged capacitors, one or more solar cells, and any other type of active or passive power source that may be implemented in a wearable device.

Figure 5 illustrates an exemplary instance of wireless communication between a wearable device in the form of finger ring 506 and POS terminal 502, when the two devices are within wireless communication range of each other. It would be understood that in certain embodiments, communication between the two devices may be initiated by a user moving hand 504 on which the finger ring 506 is worn, into communication proximity (i.e. within wireless communication range) of POS terminal 502 – so that finger ring 506 may communicate with POS terminal 502 for the purposes of authenticating a transaction requested at POS terminal 502. The manner in which such authentication is carried out, is explained in more detail in connection with the methods of Figures 7 and 8 below.

Figure 7 illustrates a method of registering or enrolling a wearable device of the type discussed above, for executing electronic payment transactions. It would be understood that the process of registering or enrolling a wearable device requires a user to register the wearable device at an authentication server – which registration may be achieved through a processor implemented user interface device that is in network communication with a remote authentication server.

In an embodiment of the method of Figure 7, implementing the method may include communicably coupling the wearable device with a processor implemented user interface device through which the user is carrying out the enrollment process. The processor implemented user interface device may comprise any processor implemented device that is in network communication with an authentication server (and may include a personal computer, laptop, tablet, smart phone, personal digital assistant etc.) The wearable device may be communicably coupled with the processor implemented user interface device by any number of mechanisms, including through a wireless link, or alternately through one or more wired links – for example, using a USB or micro USB cable.

For the purpose of fully explaining the method steps of Figure 7, reference may be made to Figure 6 which illustrates an exemplary arrangement where wearable device 602 is communicably coupled to client terminal 604 (which client terminal 604 may comprise any processor implemented terminal capable of implementing a user interface). Client terminal 604 is in turn in network communication with remote authentication server 608 – which network communication may include communication through the internet or cloud 606. By coupling wearable device 602 to a processor implemented user interface device 604 (in the illustration, a personal computer), the arrangement of Figure 6 enables a user to provide the user input necessary for the enrollment / registration with the authentication server.

Step 702 of Figure 7 comprises creating a user account at an authentication server, or alternatively accessing an existing user account previously generated at the authentication server.

At step 704, a payment card or payment account is registered or otherwise associated with the user account. In an embodiment, associating a payment card or payment account with the user account may include providing one or more of a unique identifier corresponding to the payment card / payment account, card or account details, cardholder or account holder details, and /or any authentication information, that is/are necessary to establish that the user seeking to associate the payment card or payment account with the user account is in fact an authorized user for that payment card or payment account.

Step 706 comprises capturing fingerprint biometric information of an individual authorized to execute electronic transactions through the wearable device. The fingerprint biometric information may be captured at a fingerprint sensor (for example, at the fingerprint sensor within the wearable device). Step 706 may thereafter include storing the captured biometric information or storing a biometric template derived from said captured biometric information at either or both of the authentication server and a non-transitory memory provided within the wearable device. In a preferred embodiment, the captured biometric information or biometric template may be stored at least within the non-transitory memory provided within the wearable device. In a particular embodiment of the invention, the processor, controller and / or other components of the wearable device may be configured to permit (i) storage of fingerprint biometric information or fingerprint based biometric templates (associated with an authorized user) within a non-transitory memory in the wearable device, and / or (ii) modification of biometric information or biometric templates stored within a non-transitory memory in the wearable device, or (iii) classification or storage of fingerprint biometric information as a biometric template for comparison against fingerprint based biometric information received from the fingerprint sensor – only when the wearable device is communicably coupled with the remote authentication server, or in response to receiving an authorization signal from the remote authentication server.

In a specific embodiment, the processor, controller and / or other components of the wearable device may be configured to prevent (i) storage of fingerprint biometric information or fingerprint based biometric templates (associated with an authorized user) within a non-transitory memory in the wearable device, and / or (ii) modification of biometric information or biometric templates stored within a non-transitory memory in the wearable device, or (iii) classification or storage of fingerprint biometric information as a biometric template for comparison against fingerprint based biometric information received from the fingerprint sensor – in response to a determination that the wearable device is not communicably coupled with the remote authentication server. It would be understood that by implementing a safety mechanism wherein biometric information can only be added to or modified within the wearable device in response to prior authorization from the authentication server, the invention prevents an unauthorized individual from gaining access to the wearable device and changing the biometric information stored therein.

Step 708 comprises associating or registering (at the authentication server) at least a unique device ID corresponding to the wearable device under enrollment, with the user account or payment account or payment card. In certain embodiments, in addition to the unique device ID, step 706 may also involve associating or registering other information corresponding to the wearable device, including for example, device name, device model information, information corresponding to communication protocols capable of being used by the device, and / or any intrinsic expiration dates associated with the wearable device. In a further embodiment, the enrollment process may additionally involve storing within non-transitory memory within the wearable device, data corresponding to any of a user account or payment card or payment account with which the wearable device has been associated at the authentication server.

It would be understood that the order of execution of steps 706 and 708 of the method may be interchangeable.

The method of Figure 7 may be used to (i) enroll and associate a single wearable device with multiple payment cards or payment accounts associated with a user account, or (ii) enroll and associate a plurality of wearable devices with a single payment card or payment account associated with a user account, or (iii) enroll and associate a first wearable device with a first set of payment cards or payment accounts that are associated with a user account, and a second wearable device with a second set of payment cards or payment accounts that are associated with the user account.

As an alternative to enrolling or registering the wearable device with a user account that is in turn associated with a payment card or payment account, the method of Figure 7 also enables an embodiment where the wearable device may be registered / enrolled / otherwise associated directly with a payment card or payment account.

By implementing method steps 702 to 708, a user may enroll a wearable device with a user account, and more specifically with payment accounts or payment cards associated with said user account – such that the wearable device may be used to carry out electronic payment transactions in accordance with the methods discussed hereinbelow.

Figure 8 illustrates a method of executing an electronic transaction at a terminal device (for example, at a POS terminal), through a wearable device that has been enrolled or registered in accordance with the method discussed in connection with Figure 7 hereinabove.

Step 802 comprises receiving a transaction request at a terminal device. The terminal device may comprise any terminal device having wireless capability, and which has been used to initiate an electronic transaction request. Exemplary embodiments of such terminal devices may include a POS terminal being operated by a merchant, or an internet enabled processor implemented user interface device at which an online payment transaction has been initiated (for example, a network or internet enabled computer, smartphone, tablet or mobile device).

Step 804 comprises the step of initiating a wireless handshake between the terminal device and a wearable device. In an embodiment, the wireless handshake may be initiated by bringing the two devices within wireless communication range of each other, and optionally by providing an input or instruction to trigger the wireless handshake.

Step 806 comprises capturing fingerprint biometric information of a user at the fingerprint sensor disposed within the wearable device. Said capture may be achieved by the person seeking to execute the payment transaction bringing her/his fingerprint into contact with or within fingerprint capture range of the fingerprint sensor. In an embodiment the wearable device or the terminal device may prompt the user to submit her/his fingerprint for capture through one or more of audio, visual, tactile or other haptic feedback.

Step 808 comprises matching the captured fingerprint biometric information (or one or more biometric features or a biometric template derived from the captured fingerprint biometric information) against biometric template information corresponding to an authorized / enrolled user that is stored within the wearable device (for example, in a non-transitory memory within the wearable device). It would be understood that matching of fingerprint biometric information may be achieved in accordance with any one or more fingerprint biometric matching techniques. Additionally, in an embodiment, said matching may be executed at the processor within the wearable device.

Step 810 comprises responding to determination of a match between the captured biometric information and biometric template information stored in the wearable device – by transmitting from the wearable device to the terminal device, one or more of (i) user account information / payment card information / payment account information corresponding to the wearable device, (ii) unique ID information corresponding to the wearable device and (iii) a transaction authentication signal.

Step 812 comprises initiating a transaction execution request at the terminal device, wherein the transaction execution request is initiated based on the information received from the wearable device at step 810. In one embodiment, initiating the transaction instruction may comprise the terminal device forwarding an electronic transaction request to a user account, payment account, payment card account that has been identified based on the information received from the wearable device at step 810. In another embodiment, initiating the transaction execution request may additionally comprise forwarding the unique device ID corresponding to the wearable device along with the received user account / payment account / payment card account information to an authentication server – whereinafter, the authentication server may determine whether to authenticate the transaction based on first ascertaining whether the received unique ID associated with the wearable device matches a corresponding device ID that has been enrolled with the identified user account / payment account / payment card at the authentication server.

It would additionally be understood that the authentication server's response to the transaction execution request received from the terminal device may be based on one or more predefined transaction authentication rules or policies.

Subject to approval of the transaction request by the authentication server, the requested transaction may be approved and completed – and in an embodiment, confirmation of completion of the transaction may be communicated to the terminal device. In a particular embodiment, the terminal device may wirelessly communicate a transaction completion signal to the wearable authenticaton device, which may respond by providing the user with audio, visual, tactile or other haptic feedback in response to receiving the transaction completion signal.

In a specific embodiment of the invention more generally described above, the method of registering or enrolling a wearable device for executing electronic payment transactions (for example the method discussed in connection with Figure 7) which may at step 706 comprise enrolling two or more different fingerprints of a user, generating and storing biometric templates corresponding to each of the different user fingerprints. Thereafter, the wearable device may be configured to implement a specific embodiment of the transaction execution method discussed in connection with Figure 8 – wherein (i) step 806 comprises capturing fingerprint biometric information corresponding to a plurality of simultaneously presented fingerprints of a user at the fingerprint sensor disposed within the wearable device, (ii) step 808 comprises matching the captured fingerprint biometric information corresponding to the plurality of simultaneously presented user fingerprints that has been captured at step 806 against the plurality of fingerprint biometric templates generated and stored at step 706 and which have been associated with the wearable device and (iii) step 810 comprising requiring determination of a match between two or more of the captured or scanned simultaneously presented fingerprints (from step 806) and two or more enrolled fingerprint biometric templates (from step 706) that have been stored within the wearable device memory as a precondition to transmitting from the wearable device to the terminal device, one or more of (i) user account information / payment card information / payment account information corresponding to the wearable device, (ii) unique ID information corresponding to the wearable device and (iii) a transaction authentication signal.

It would be understood that the steps of (i) configuring the wearable device to enroll a plurality of user fingerprints corresponding to an authorized user, (ii) requiring a user (who is seeking authorization to initiate a transaction request through the wearable device) to simultaneously present a plurality of fingerprints for matching, and (iii) thereafter initiating a transaction request responsive to the plurality of fingerprints that are simultaneously presented by the user, being found to match a corresponding plurality of fingerprint biometric templates that have already been enrolled, stored and associated with an authorized user of the wearable device – serves to enhance the security of the wearable device by increasing the number of biometric authentication factors required for transaction authorization – which makes it harder for an unauthorized user to fake or spoof enrolled fingerprint biometrics of an authorized user.

In certain embodiments of the invention, the wearable device may be specifically configured to enable or facilitate simultaneous capture of fingerprint information corresponding to a plurality of a subject's fingerprints.

In one embodiment of the type illustrated in Figure 9A, the wearable device 900A may comprise a surface 902A having a single fingerprint sensor 904A disposed thereon, wherein said fingerprint sensor is sized and positioned so as to enable a subject to simultatneously bring two or more of the subject's fingerprints simultaneously into contact with said fingerprint sensor 904A.

In an embodiment of the type illustrated in Figure 9B, the wearable device 900B may comprise a surface 902B having a plurality of fingerprint sensors 904B, 904B' disposed thereon, wherein each of said fingerprint sensors 904B, 904B' is sized and positioned so as to enable a subject to simultaneously bring two or more of the subject's fingerprints simultaneously into contact with said fingerprint sensors 904B, 904B'. In an embodiment of the invention, wearable device 900B may comprise at least two separate fingerprint sensors disposed thereon, wherein the at least two fingerprint sensors 904B, 904B' are positioned and sized to enable ergonomic positioning of at least two of a subject's fingerprints simultaneously on said at least two separate fingerprint sensors. In a preferred embodiment, the at least two fingerprint sensors 904B, 904B' may be located and configured to enable a user to simultaneously present a thumbprint and a print of a forefinger / index finger for fingerprint acquisition purposes. In one embodiment, the wearable device 900B may comprise a ring, and each of the at least two fingerprint sensors 904B, 904B' may be located on an outer annular surface of said ring. In a more specific embodiment, the wearable device 9000B may include two fingerprint sensors positioned on an outer annular surface of said finger ring, and further may be located on substantially opposite sides of the ring. In another embodiment the wearable device 9000B may include two fingerprint sensors positioned on an outer annular surface of said ring, wherein the centres of each of said two fingerprint sensors are separated from each other by an angle of between at least 15 degrees and 180 degrees, and more preferably by an angle of between 30 degrees and 180 degrees.

In another specific embodiment, the wearable device may include at least two fingerprint sensors, wherein each of the at least two fingerprint sensors are located on different surfaces of the wearable device. In an exemplary embodiment, where the wearable device is an annular ring, one fingerprint sensor may be located on an outer annular surface of the ring, while another fingerprint sensor may be positioned on an inner annular surface of said ring. In another embodiment, where the wearable device has at least a front surface and a rear surface (for example, a pendant or ear-ring having a front surface and a rear surface), and one fingerprint sensor may be located on the front surface while the other fingerprint sensor may be located on the rear surface.

Figure 10 illustrates an exemplary computer system 1002 for implementing the present invention.

The illustrated system comprises computer system 1002 which in turn comprises one or more processors 1004 and at least one memory 1006. Processor 1004 is configured to execute program instructions - and may be a real processor or a virtual processor. It will be understood that computer system 1002 does not suggest any limitation as to scope of use or functionality of described embodiments. The computer system 1002 may include, but is not be limited to, one or more of a general-purpose computer, a programmed microprocessor, a micro-controller, an integrated circuit, and other devices or arrangements of devices that are capable of implementing the steps that constitute the method of the present invention. Exemplary embodiments of a computer system 1002 in accordance with the present invention may include one or more servers, desktops, laptops, tablets, smart phones, mobile phones, mobile communication devices, tablets, phablets and personal digital assistants. In an embodiment of the present invention, the memory 1006 may store software for implementing various embodiments of the present invention. The computer system 1002 may have additional components. For example, the computer system 1002 may include one or more communication channels 1008, one or more input devices 1010, one or more output devices 1012, and storage 1014. An interconnection mechanism (not shown) such as a bus, controller, or network, interconnects the components of the computer system 1002. In various embodiments of the present invention, operating system software (not shown) provides an operating environment for various softwares executing in the computer system 1002 using a processor 1004, and manages different functionalities of the components of the computer system 1002.

The communication channel(s) 1008 allow communication over a communication medium to various other computing entities. The communication medium provides information such as program instructions, or other data in a communication media. The communication media includes, but is not limited to, wired or wireless methodologies implemented with an electrical, optical, RF, infrared, acoustic, microwave, Bluetooth or other transmission media.

The input device(s) 1010 may include, but is not limited to, a touch screen, a keyboard, mouse, pen, joystick, trackball, a voice device, a scanning device, or any another device that is capable of providing input to the computer system 1002. In an embodiment of the present invention, the input device(s) 1010 may be a sound card or similar device that accepts audio input in analog or digital form. The output device(s) 1012 may include, but not be limited to, a user interface on CRT, LCD, LED display, or any other display associated with any of servers, desktops, laptops, tablets, smart phones, mobile phones, mobile communication devices, tablets, phablets and personal digital assistants, printer, speaker, CD/DVD writer, or any other device that provides output from the computer system 1002.

The storage 1014 may include, but not be limited to, magnetic disks, magnetic tapes, CD-ROMs, CD-RWs, DVDs, any types of computer memory, magnetic stripes, smart cards, printed barcodes or any other transitory or non-transitory medium which can be used to store information and can be accessed by the computer system 1002. In various embodiments of the present invention, the storage 1014 may contain program instructions for implementing any of the described embodiments.

In an embodiment of the present invention, the computer system 1002 is part of a distributed network or a part of a set of available cloud resources.

The present invention may be implemented in numerous ways including as a system, a method, or a computer program product such as a computer readable storage medium or a computer network wherein programming instructions are communicated from a remote location.

The present invention may suitably be embodied as a computer program product for use with the computer system 1002. The method described herein is typically implemented as a computer program product, comprising a set of program instructions that is executed by the computer system 1002 or any other similar device. The set of program instructions may be a series of computer readable codes stored on a tangible medium, such as a computer readable storage medium (storage 1014), for example, diskette, CD-ROM, ROM, flash drives or hard disk, or transmittable to the computer system 1002, via a modem or other interface device, over either a tangible medium, including but not limited to optical or analogue communications channel(s) 1008. The implementation of the invention as a computer program product may be in an intangible form using wireless techniques, including but not limited to microwave, infrared, Bluetooth or other transmission techniques. These instructions can be preloaded into a system or recorded on a storage medium such as a CD-ROM, or made available for downloading over a network such as the Internet or a mobile telephone network. The series of computer readable instructions may embody all or part of the functionality previously described herein.

Based on the above, it would be apparent that the present invention offers significant advantages - including convenient and secure ways for facilitating secure authentication of a user in connection with electronic or payment card based transactions. One immediate benefit is the significant improvement in customer experience due to the fact that the degree of effort or active intervention on the part of the user for commencing and/or carrying out an electronic or payment card based transaction is reduced, while maintaining and improving on security standards.

While the exemplary embodiments of the present invention are described and illustrated herein, it will be appreciated that they are merely illustrative. It will be understood by those skilled in the art that various modifications in form and detail may be made therein without departing from or offending the spirit and scope of the invention as defined by the appended claims. Additionally, the invention illustratively disclose herein suitably may be practiced in the absence of any element which is not specifically disclosed herein – and in a particular embodiment that is specifically contemplated, the invention is intended to be practiced in the absence of any one or more element which are not specifically disclosed herein.

WE CLAIM:

1. A wearable device for enabling an electronic payment transaction through a payment account, at a point-of-sale (POS) terminal having wireless communication capability, comprising:

a wirelesss transceiver;

at least one fingerprint sensor;

a non-transient memory based data repository configured for storing:

one or more fingerprint based biometric templates; and

a unique device identifier corresponding to the wearable device;

a processor configured to:

generate one or more biometric templates based on fingerprint based biometric information received from the at least one fingerprint sensor;

enroll the generated one or more biometric templates by storing said one or more biometric templates within non-transitory memory in the wearable device; and

wirelessly transmit an electronic payment authorization to the POS terminal, wherein said electronic payment authorization is transmitted in response to:

receipt of a payment transaction request at the POS terminal;

receiving fingerprint biometric information from the at least one fingerprint sensor; and

determining that the received fingerprint biometric information matches a biometric template stored within the data repository.

2. The wearable device as claimed in claim 1, wherein the electronic payment authorization transmitted by the processor to the POS terminal comprises one or more of (i) user account information, payment card information or payment account information associated with the wearable device, (ii) the unique identifier corresponding to the wearable device and (iii) a transaction authentication signal.

3. The wearable device as claimed in claim 2, wherein the electronic payment authorization transmitted by the processor to the POS terminal comprises both of (i) user account information, payment card information or payment account information associated with the wearable device, and (ii) the unique identifier corresponding to the wearable device.

4. The wearable device as claimed in claim 1, wherein the processor is configured to:

communicate with a remote authentication server through a data connection with a client terminal that is in network communication with the remote authentication server; and

in response to commencement of a process for associating the wearable device with a user account, payment card or payment account, transmit the unique device identifier corresponding to the wearable device to the remote authentication server, wherein an association between the transmitted unique device identifier and the user account, payment card or payment account is thereafter recorded at the remote authentication server.

5. The wearable device as claimed in claim 4, wherein the processor is configured to respond to a determination that the wearable device is not communicably coupled with the remote authentication server, by preventing storage of fingerprint biometric information in the data repository of the wearable device.

6. The wearable device as claimed in claim 4, wherein the processor is configured to store within the data repository, data corresponding to any of a user account, payment card or payment account that has been associated with the unique device identifier corresponding to the wearable device at the remote authentication server.

7. The wearable device as claimed in claim 1, wherein said wearable device is configured and sized as a finger ring.

8. The wearable device as claimed in claim 1, wherein the processor is configured to:

generate a plurality of biometric templates based on fingerprint based biometric information corresponding to a plurality of fingerprints simultaneously presented for fingerprint acquisition at the at least one fingerprint sensor; and

enroll the generated plurality of biometric templates by storing said plurality of biometric templates within non-transitory memory in the wearable device;

and wherein the electronic payment authorization is transmitted in response to:

receiving fingerprint biometric information corresponding to a plurality of fingerprints simultaneously presented for authentication at the at least one fingerprint sensor within the wearable device; and

determining that the receiving fingerprint biometric information corresponding to a plurality of fingerprints simultaneously presented for authentication at the at least one fingerprint sensor within the wearable device matches the enrolled plurality of biometric templates stored within the non-transitory memory in the wearable device.

9. The wearable device as claimed in claim 8, wherein the at least one fingerprint sensor comprises two or more fingerprint sensors.

10. The wearable device as claimed in claim 9, wherein said two or more fingerprint sensors are located and sized to enable a user to simultaneously present a thumb and forefinger for fingerprint scanning at said fingerprint sensors.

11. A system for enabling an electronic payment transaction through a payment account, at a point-of-sale (POS) terminal having wireless communication capability, the system comprising:

a remote authentication server; and

a wearable device comprising:

a wirelesss transceiver;

a fingerprint sensor;

a non-transient memory based data repository configured for storing:

one or more fingerprint based biometric templates; and a unique device identifier corresponding to the wearable device; a processor configured to:

generate one or more biometric templates based on fingerprint based biometric information received from the fingerprint sensor; and

wirelessly transmit an electronic payment authorization to the POS terminal, wherein said electronic payment authorization is transmitted in response to:

receipt of a payment transaction request at the POS terminal;

receiving fingerprint biometric information from the fingerprint sensor; and

determining that the received fingerprint biometric information matches a biometric template stored within the data repository.

12. The system as claimed in claim 11, wherein the electronic payment authorization transmitted by the processor to the POS terminal comprises one or more of (i) user account information, payment card information or payment account information associated with the wearable device, (ii) the unique identifier corresponding to the wearable device and (iii) a transaction authentication signal.

13. The system as claimed in claim 12, wherein the electronic payment authorization transmitted by the processor to the POS terminal comprises both of (i) user account information, payment card information or payment account information associated with the wearable device, and (ii) the unique identifier corresponding to the wearable device.

14. The system as claimed in claim 10, wherein:

the processor is configured to:

communicate with the remote authentication server through a data connection with a client terminal that is in network communication with the remote authentication server; and

in response to commencement of a process for associating the wearable device with a user account, payment card or payment account, transmit the unique device identifier corresponding to the wearable device to the remote authentication server;

and wherein the remote authentication server is configured to record an association between the transmitted unique device identifier and the user account, payment card or payment account.

15. The system as claimed in claim 14, wherein the processor is configured to respond to a determination that the wearable device is not communicably coupled with the remote authentication server, by preventing storage of a fingerprint biometric information in the data repository of the wearable device.

16. The system as claimed in claim 14, wherein the processor is configured to store within the data repository, data corresponding to any of a user account, payment card or payment account that has been associated with the unique device identifier corresponding to the wearable device at the remote authentication server.

17. The system as claimed in claim 11, wherein the processor is configured to:

generate a plurality of biometric templates based on fingerprint based biometric information corresponding to a plurality of fingerprints simultaneously presented for fingerprint acquisition at the at least one fingerprint sensor;

enroll the generated plurality of biometric templates by storing said plurality of biometric templates within non-transitory memory in the wearable device;

and wherein the electronic payment authorization is transmitted in response to:

receiving fingerprint biometric information corresponding to a plurality of fingerprints simultaneously presented for authentication at the at least one fingerprint sensor within the wearable device; and

determining that the receiving fingerprint biometric information corresponding to a plurality of fingerprints simultaneously presented for authentication at the at least one fingerprint sensor within the wearable device matches the enrolled plurality of biometric templates stored within the non-transitory memory in the wearable device.

18. The system as claimed in claim 17, wherein the at least one fingerprint sensor comprises two or more fingerprint sensors.

19. The system as claimed in claim 18, wherein said two or more fingerprint sensors are located and sized to enable a user to simultaneously present a thumb and forefinger for fingerprint scanning at said fingerprint sensors.

20. A method for enabling an electronic payment transaction through a payment account, at a point-of-sale (POS) terminal having wireless communication capability, the method comprising:

generating one or more biometric templates based on fingerprint based biometric information received from a fingerprint sensor provided within a wearable device;

storing the one or more fingerprint based biometric templates within a data repository within the wearable device;

wirelessly transmitting an electronic payment authorization from the wearable device to the POS terminal, wherein said electronic payment authorization is transmitted in response to:

receipt of a payment transaction request at the POS terminal;

receiving fingerprint biometric information from the fingerprint sensor; and

determining that the received fingerprint biometric information matches a biometric template stored within the data repository.

21. The method as claimed in claim 20, wherein the electronic payment authorization transmitted by the processor to the POS terminal includes one or more of (i) a unique device identifier corresponding to the wearable device, (ii) user account information, payment card information or payment account information associated with the wearable device, and (iii) a transaction authentication signal.

22. The method as claimed in claim 18, wherein the electronic payment authorization transmitted by the processor to the POS terminal includes both of (i) user account information, payment card information or payment account

information associated with the wearable device, and (ii) the unique identifier corresponding to the wearable device.

23. The method as claimed in claim 20, comprising the steps of:

initiating a process for associating the wearable device with a user account, payment card or payment account at a remote authentication server;

transmitting the unique device identifier corresponding to the wearable device, from the wearable device to the remote authentication server through a data connection with a client terminal that is in network communication with the remote authentication server; and

recording an association between the transmitted unique device identifier and the user account, payment card or payment account, at the remote authentication server.

24. The method as claimed in claim 23, comprising responding to a determination that the wearable device is not communicably coupled with the remote authentication server, by preventing storage of a fingerprint biometric information in the data repository of the wearable device.

25. The method as claimed in claim 20, comprising storing within the data repository, data corresponding to any of a user account, payment card or payment account that has been associated with the unique device identifier corresponding to the wearable device at the remote authentication server.

26. The method as claimed in claim 20, comprising

generating a plurality of biometric templates based on fingerprint based biometric information corresponding to a plurality of fingerprints simultaneously presented for fingerprint acquisition at the at least one fingerprint sensor;

enrolling the generated plurality of biometric templates by storing said plurality of biometric templates within non-transitory memory in the wearable device;

and transmitting the electronic payment authorization in response to:

receiving fingerprint biometric information corresponding to a plurality of fingerprints simultaneously presented for authentication at the at least one fingerprint sensor within the wearable device; and

determining that the receiving fingerprint biometric information corresponding to a plurality of fingerprints simultaneously presented for authentication at the at least one fingerprint sensor within the wearable device matches the enrolled plurality of biometric templates stored within the non-transitory memory in the wearable device.

27. The method as claimed in claim 26, wherein the at least one fingerprint sensor comprises two or more fingerprint sensors.

28. The method as claimed in claim 27, wherein said two or more fingerprint sensors are located and sized to enable a user to simultaneously present a thumb and forefinger for fingerprint scanning at said fingerprint sensors.

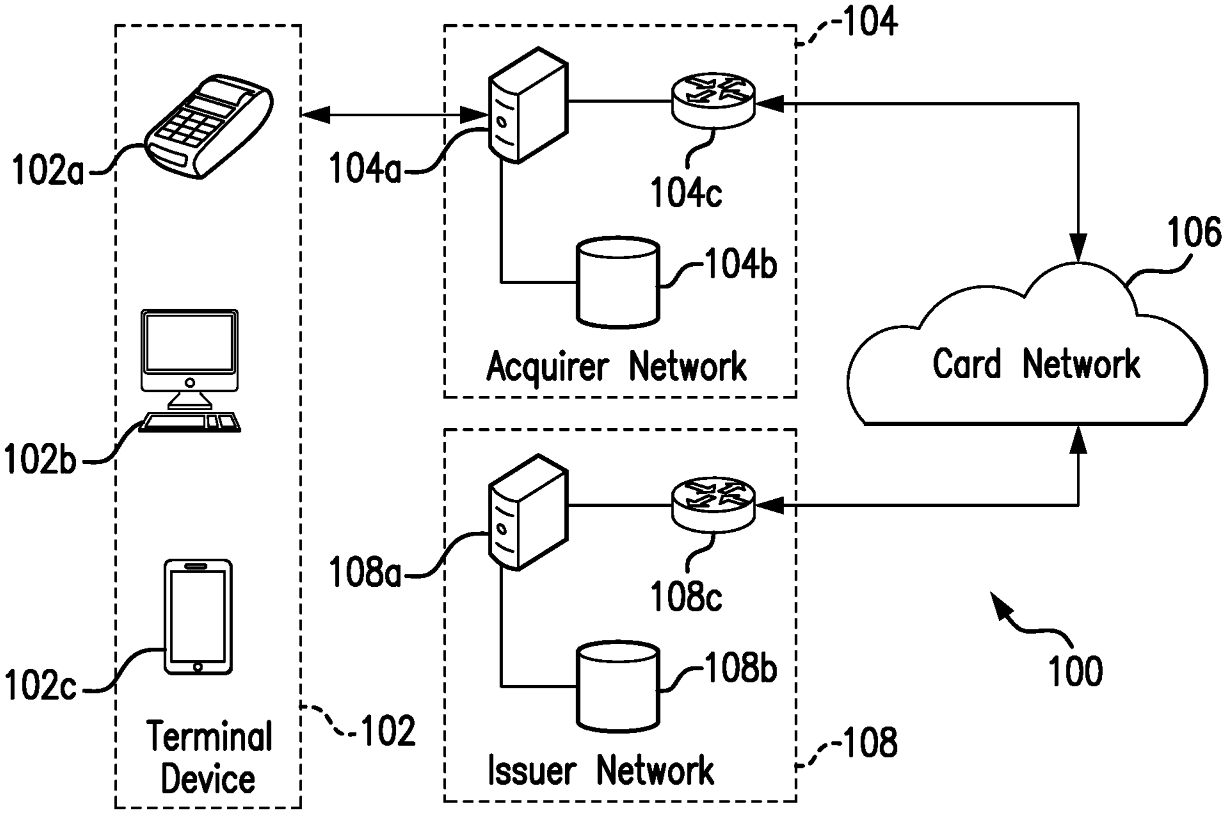
104
102a
104a
104c
106
104b
Acquirer Network
Card Network
102b
108a
108c
100
102c
108b
Terminal Device
102
Issuer Network
108

FIG. 1

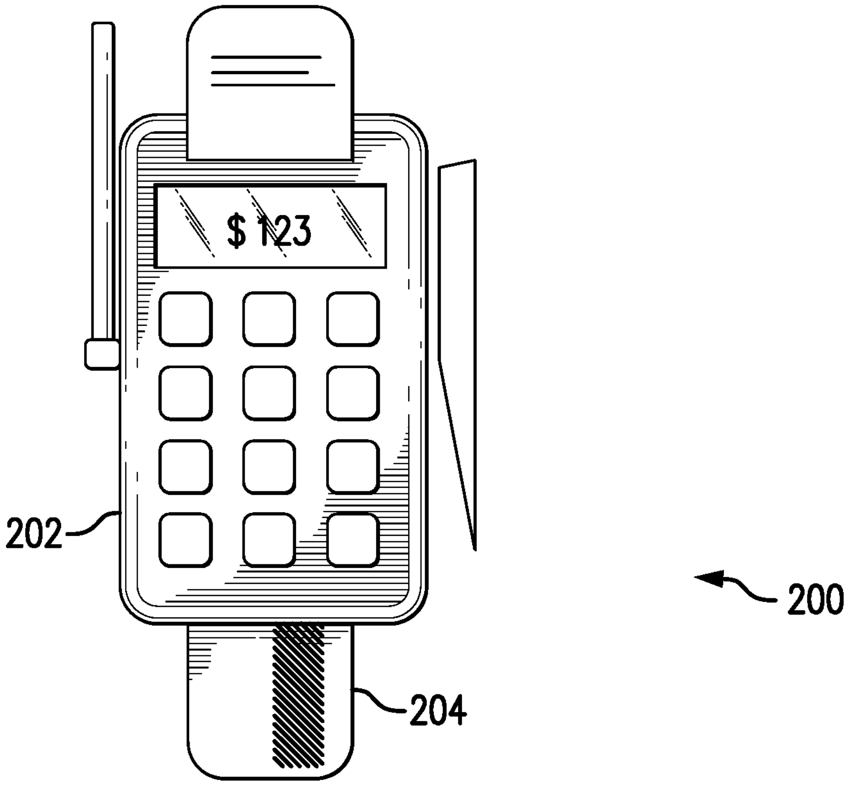

FIG. 2

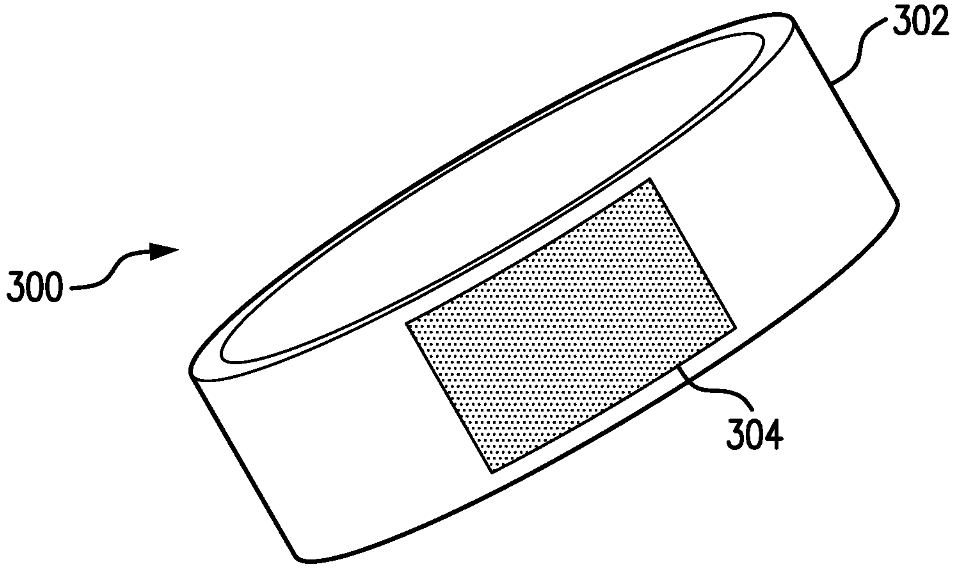

FIG. 3

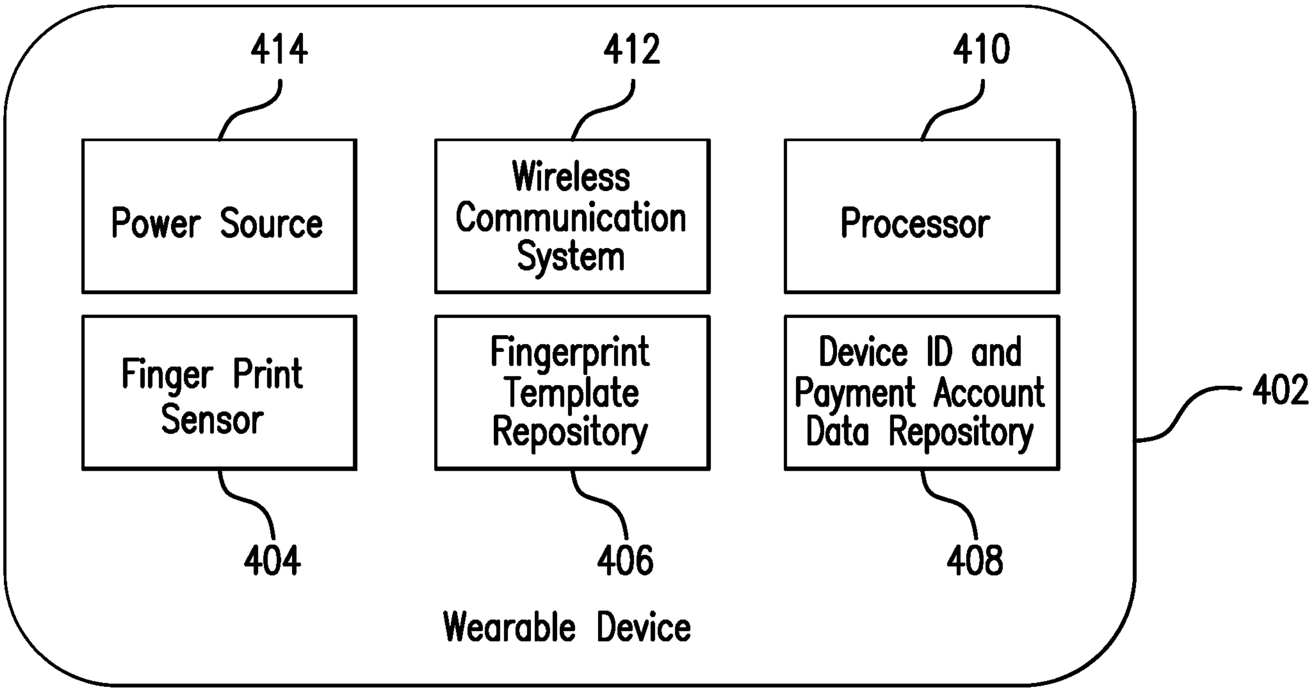
414
412
410
Power Source
Wireless Communication System
Processor
Finger Print Sensor
Fingerprint Template Repository
Device ID and Payment Account Data Repository
402
404
406
408
Wearable Device

FIG. 4

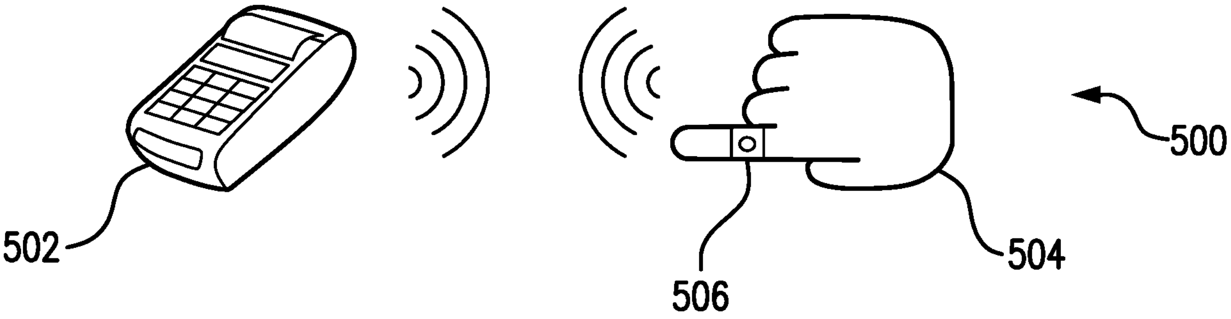

FIG. 5

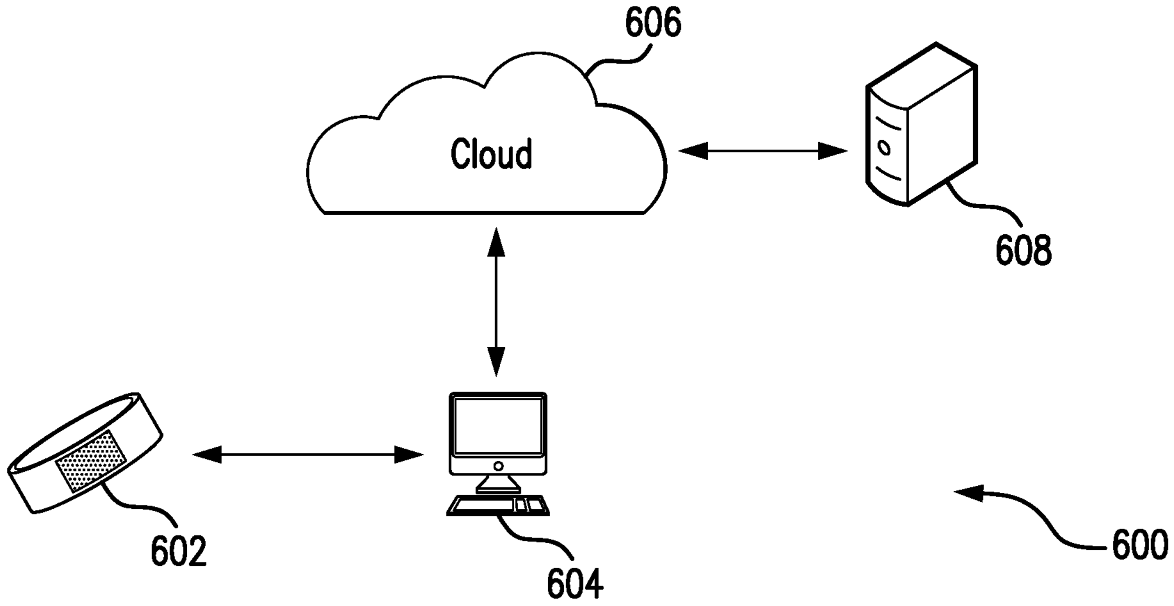

FIG. 6

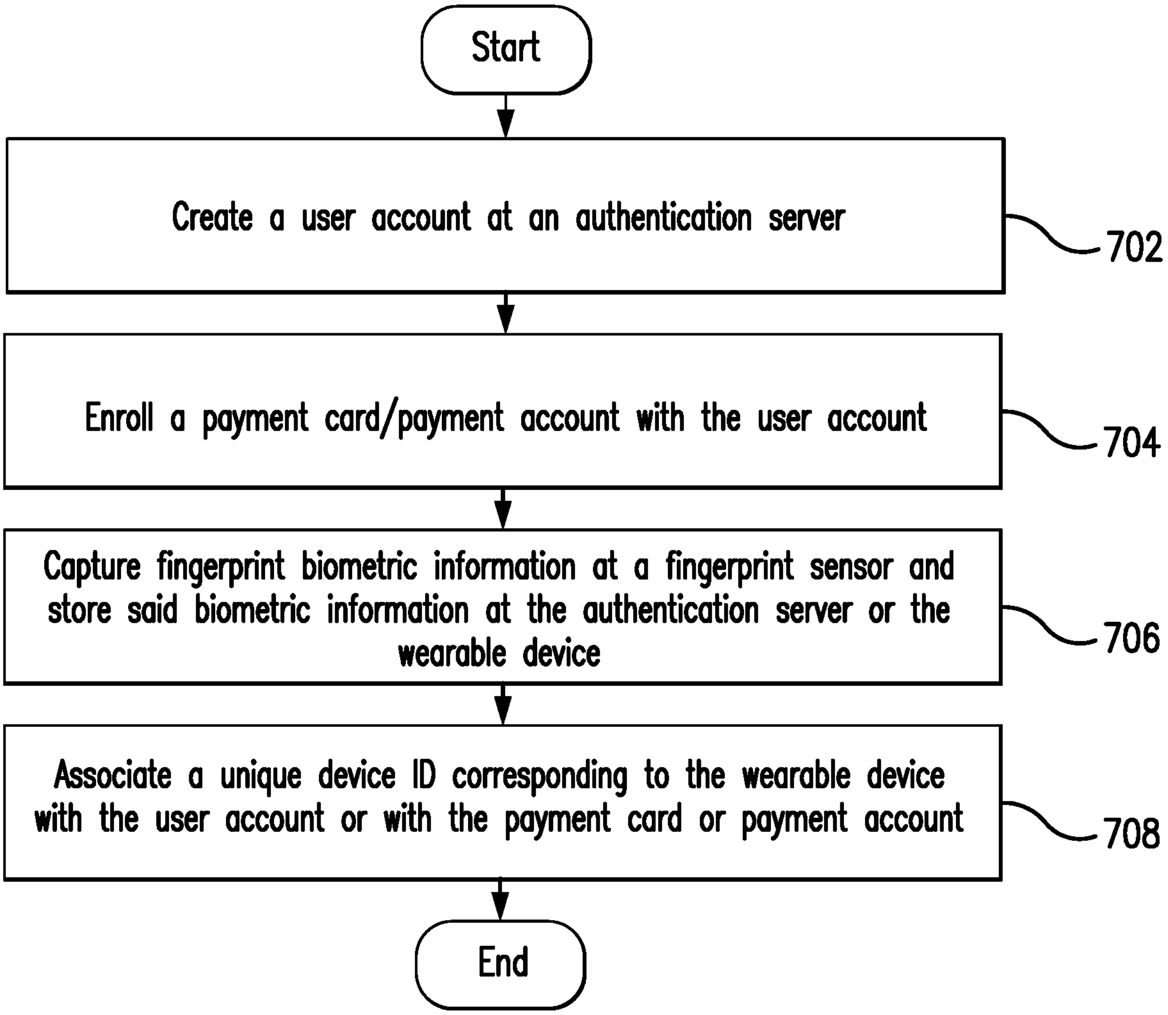
Start
Create a user account at an authentication server
702
Enroll a payment card/payment account with the user account
704
Capture fingerprint biometric information at a fingerprint sensor and store said biometric information at the authentication server or the wearable device
706
Associate a unique device ID corresponding to the wearable device with the user account or with the payment card or payment account
708
End

FIG. 7

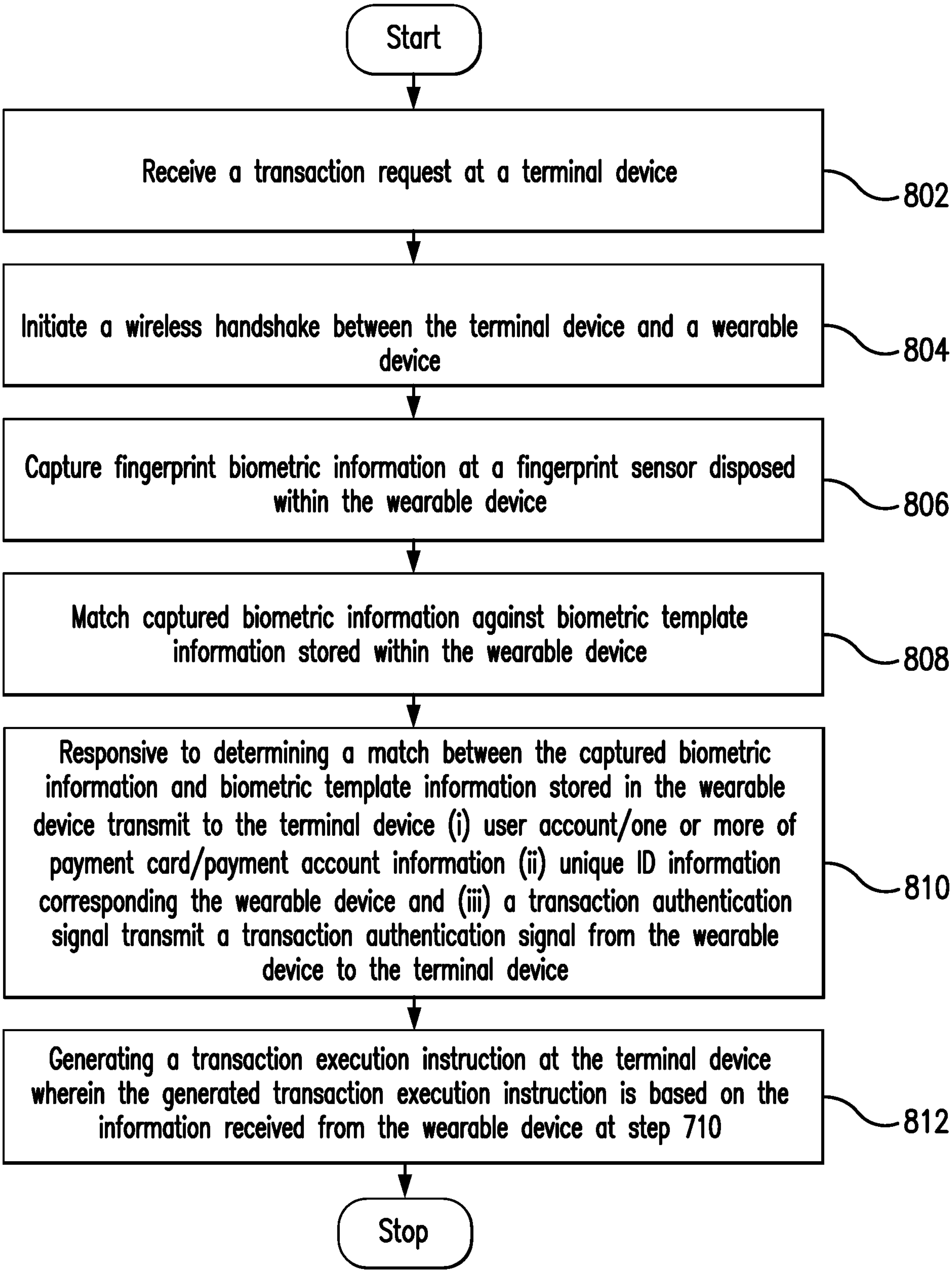
Start
Receive a transaction request at a terminal device
802
Initiate a wireless handshake between the terminal device and a wearable device
804
Capture fingerprint biometric information at a fingerprint sensor disposed within the wearable device
806
Match captured biometric information against biometric template information stored within the wearable device
808
Responsive to determining a match between the captured biometric information and biometric template information stored in the wearable device transmit to the terminal device (i) user account/one or more of payment card/payment account information (ii) unique ID information corresponding the wearable device and (iii) a transaction authentication signal transmit a transaction authentication signal from the wearable device to the terminal device
810
Generating a transaction execution instruction at the terminal device wherein the generated transaction execution instruction is based on the information received from the wearable device at step 710
812
Stop

FIG. 8

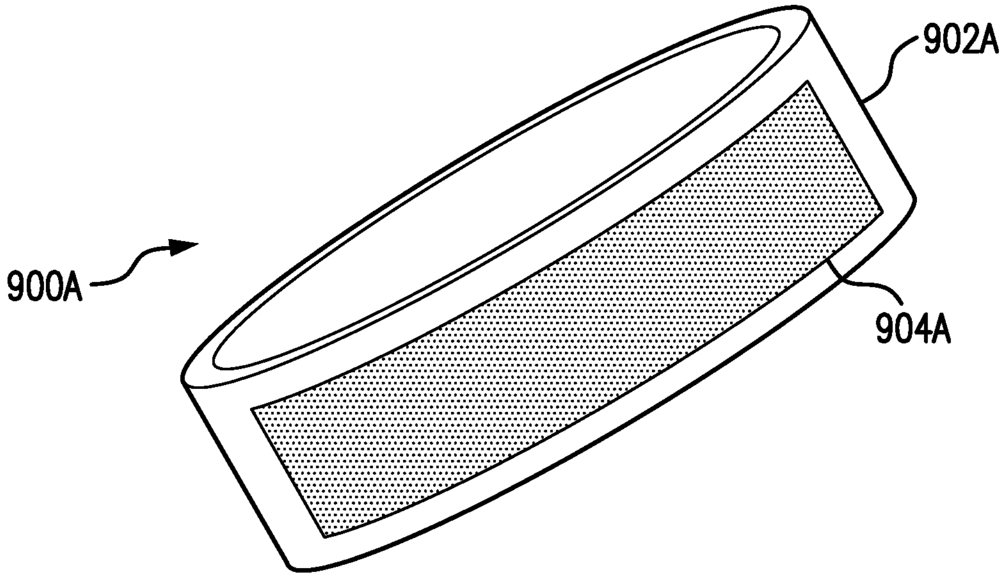

FIG. 9A

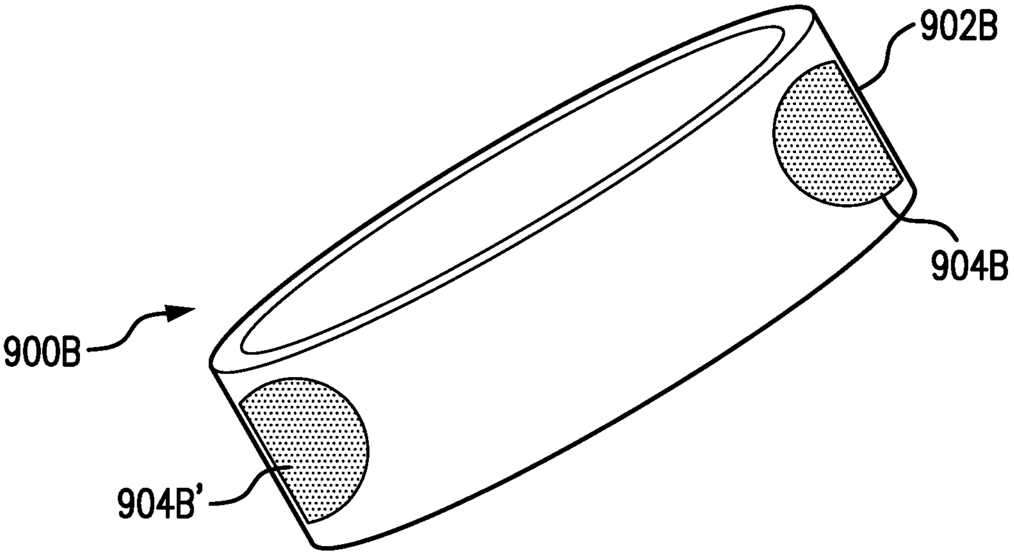

FIG. 9B

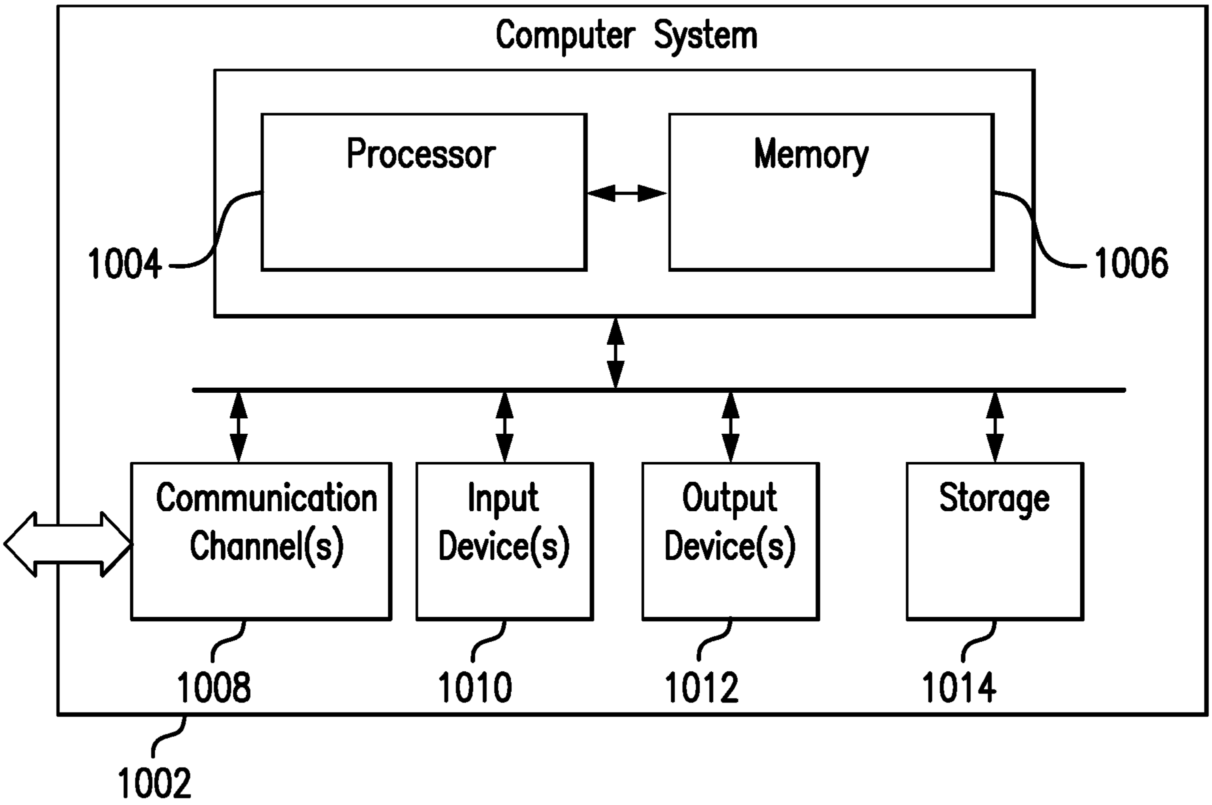
Computer System
Processor
Memory
1004
1006
Communication Channel(s)
Input Device(s)
Output Device(s)
Storage
1008
1010
1012
1014
1002

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2019/023506

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/40(2012.01)i, G06Q 20/38(2012.01)i, G06Q 20/20(2012.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q 20/40; A61B 5/00; G06F 17/60; G06F 3/01; G06Q 20/32; H04B 5/00; H04L 29/06; H04W 12/06; G06Q 20/38; G06Q 20/20

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: wearable device, authentication, payment, fingerprint, biometric template

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2014-0273961 A1 (TYFONE, INC.) 18 September 2014 See paragraphs [0025]-[0080], claim 14 and figures 4,10-13.	1-28
Y	US 2017-0068956 A1 (BANK OF AMERICA CORPORATION) 09 March 2017 See paragraphs [0043],[0073],[0084], claims 1-4 and figures 2A-2B.	1-28
A	US 2016-0191511 A1 (PAYPAL INC.) 30 June 2016 See paragraphs [0062],[0067]-[0072] and figures 1-5.	1-28
A	US 2015-0288687 A1 (INVENSENSE, INCORPORATED) 08 October 2015 See paragraphs [0066]-[0069] and figures 2,6.	1-28
A	US 2003-0046228 A1 (JEAN-MARC BERNEY) 06 March 2003 See paragraphs [0029]-[0032] and figures 3-7.	1-28

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

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

Date of the actual completion of the international search 28 June 2019 (28.06.2019)	Date of mailing of the international search report **28 June 2019 (28.06.2019)**
Name and mailing address of the ISA/KR International Application Division Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea Facsimile No. +82-42-481-8578	Authorized officer KANG, Min Jeong Telephone No. +82-42-481-8131

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2019/023506

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014-0273961 A1	18/09/2014	US 10211988 B2	19/02/2019
		US 2016-0197727 A1	07/07/2016
		US 2018-0183598 A1	28/06/2018
		US 9319881 B2	19/04/2016
		US 9906365 B2	27/02/2018
		WO 2014-150535 A1	25/09/2014
US 2017-0068956 A1	09/03/2017	None	
US 2016-0191511 A1	30/06/2016	US 10135819 B2	20/11/2018
		US 2017-0111356 A1	20/04/2017
		WO 2016-105892 A1	30/06/2016
US 2015-0288687 A1	08/10/2015	WO 2015-157083 A1	15/10/2015
US 2003-0046228 A1	06/03/2003	CN 1610920 A	27/04/2005
		EP 1421543 A1	26/05/2004
		JP 2005-528662 A	22/09/2005
		KR 10-2004-0034677 A	28/04/2004
		WO 03-021523 A1	13/03/2003