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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 March 2018 (15.03.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/048563 A1

(51) International Patent Classification:
G06F 21/34 (2013.01) *H04L 9/32* (2006.01)
G06F 21/35 (2013.01)

(21) International Application Number:
PCT/US2017/046124

(22) International Filing Date:
09 August 2017 (09.08.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/384,257 07 September 2016 (07.09.2016) US

(71) Applicant: **TOKENIZE, INC.** [US/US]; 125 Tyech Park Dr., Ste 2137B, Rochester, NY 14623 (US).

(72) Inventors: **SHAPIRO, Steve**; 6488 Coe Rd., Livonia, NY 14487 (US). **SHAPIRO, Melanie**; 6488 Coe Rd., Livonia, NY 14487 (US). **LOURETTE, Richard**; 112 Crossover, Fairport, NY 14450 (US). **ALLEN, Michael, W.**; 83 Booth Street Ext., Shortville, NY 14548 (US). **SCHULTZ, Stephen**; 291 Brooks Road, West Henrietta, NY 14586 (US).

(74) Agent: **BROCKHAUS, Marc, A.**; Dunlap Codding, P.C., P.O. Box 16370, Oklahoma City, OK 73113 (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.

(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))*

(54) **Title:** SYSTEM AND METHOD FOR SUPPLYING SECURITY INFORMATION

(57) **Abstract:** A wearable device having one or more processors configured to receive one or more signals representative of biometric parameter(s) and sensed presence of a user. The one or more processors configured to compare the biometric parameter to a stored user parameter for authentication of the user. Upon authentication, the one or more processors switch from a locked mode to an unlocked mode to enable communication.

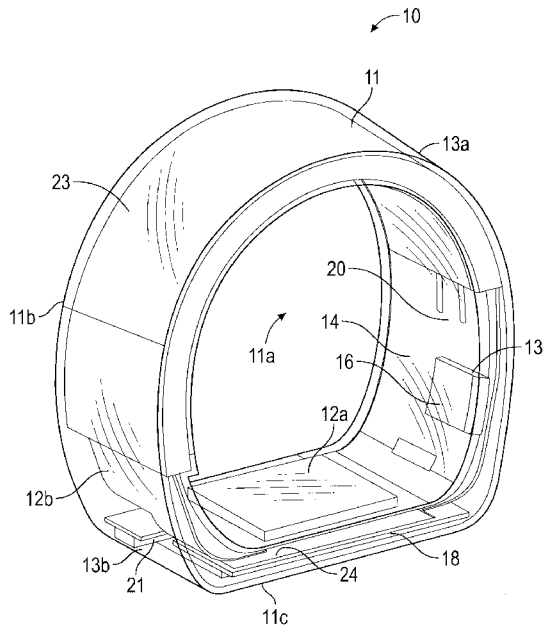

FIG. 1

WO 2018/048563 A1

PATENT

SYSTEM AND METHOD FOR SUPPLYING SECURITY INFORMATION

CROSS-REFERENCE TO RELATED APPLICATION

[0001] The present application claims the benefit of U.S. Serial No. 62/384,257, filed on September 7, 2016, which is hereby incorporated by reference in its entirety.

BACKGROUND

[0002] In the electronic age, the number of keys, whether physical, electronic, or cybernetic, has drastically increased. For example, a given person may carry house keys, car keys, work keys, and/or the like. Additionally, such person may have one or more radio-frequency identification (RFID) badges, access cards, and/or automated teller machine (ATM) cards providing for access to bank lobbies. Further, passwords may be included on phones, computers, online and other accounts being used for any number of purposes. Each of these present security weaknesses. For example, regarding physical keys, possession of the physical key gains access. However, if the physical key is lost or stolen, not only is your access limited, but an outside party may now have access to your house, car or office. In another example, cybernetic keys, such as passwords, may be selected for ease in remembrance. Yet, such passwords may be easily determined and/or hacked. Additionally, use of the same password over multiple accounts may leave such accounts compromised in such an event.

[0003] Several products on the market today attempt to address these issues. For example, “master password” services provide unique, hard to hack passwords for accounts, storing them in an encrypted format in a “password vault” accessible using a “master password.” While this may solve the issue of remembering multiple unique passwords and use of a sole password for multiple accounts, if the master key is ever compromised, all passwords may need changing. Further, a sole “master password” for entrance into the vault provides a point of weakness. Such “master password” systems only involved cybernetic passwords, and do not provide any system for physical and/or electronic keys.

[0004] With the growing number of electronic lock capabilities for cars, homes, offices, and the like, reliance on physical keys may be decreasing. As such, systems

currently available may provide a means to store multiple electronic keys on a single device. This may be beneficial for convenience as it obviates the needs to carry multiple key fobs, access cards, RFID tags, and/or the like. Again, however, such systems present security vulnerability as possession of a master key gains access and if the master key is lost and/or stolen, an outside party may now have access to all electronic locks.

[0005] Multi-factor security may be used to solve these issues. Such three security factors may often be described as "what you have," "what you know," and "who you are." The "what you have" factor refers to possession (e.g., having a physical key granting access). The "what you know" factor refers to something known (e.g., a password, PIN, key phrase, and/or the like, granting access). The "who you are" factor refers to biometrics (e.g., a fingerprint scan, retinal scan, and the like, granting access). Generally, a multi-factor solution may utilize two of the three security factors, with some systems incorporating all three.

[0006] Smartphones have recently added two factor authentication. For example, some forms of keys (e.g., credit cards) may require both possession of a phone and a fingerprint scan with each transaction (e.g., transaction at a contactless payment credit card terminal).

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] These and other objects and features of the present invention will be more fully disclosed or rendered obvious by the following detailed description of the invention, which is to be considered together with the accompanying drawings wherein like numbers refer to like parts, and further wherein:

[0008] Figure 1 is a perspective view of an exemplary wearable device in accordance with the present invention.

[0009] Figure 2 is a block diagram of the exemplary wearable device illustrated in Figure 1.

[0010] Figure 3A is an exemplary circuit diagram of an exemplary communication device for use with the wearable device illustrated in Figure 1.

[0011] Figure 3B is an exemplary graphical representation of impedance in the circuit illustrated in Figure 3A.

[0012] Figure 4 is a circuit diagram illustrating communication between an external charger and the wearable device illustrated in Figure 1.

[0013] Figure 5 illustrates a flow chart of an exemplary method for providing the wearable device in a locked mode and an unlocked mode such that an exemplary wearable device may be configured to process a key request and/or communicate sensitive data.

[0014] Figure 6 illustrates a flow chart of an exemplary method for using an exemplary wearable device to process key requests.

[0015] Figure 7 illustrates a flow chart of an exemplary method for providing confirmation from a user of the wearable device.

[0016] Figure 8 illustrates a flow chart of an exemplary method for providing secure information from an exemplary wearable device to an exemplary paired device.

[0017] Figure 9 illustrates a block diagram of an exemplary wearable device communicating with one or more automobile systems.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

[0018] Before explaining at least one embodiment of the presently disclosed and claimed inventive concepts in detail, it is to be understood that the presently disclosed and claimed inventive concepts are not limited in their application to the details of construction, experiments, exemplary data, and/or the arrangement of the components set forth in the following description or illustrated in the drawings. The presently disclosed and claimed inventive concepts are capable of other embodiments or of being practiced or carried out in various ways. Also, it is to be understood that the phraseology and terminology employed herein is for purpose of description and should not be regarded as limiting.

[0019] In the following detailed description of embodiments of the inventive concepts, numerous specific details are set forth in order to provide a more thorough understanding of the inventive concepts. However, it will be apparent to one of ordinary skill in the art that the inventive concepts within the disclosure may be practiced without these specific details. In other instances, certain well-known features may not be described in detail in order to avoid unnecessarily complicating the instant disclosure.

[0020] As used herein, the terms "comprises," "comprising," "includes," "including," "has," "having," or any other variation thereof, are intended to cover a non-exclusive inclusion. For example, a process, method, article, or apparatus that

comprises a list of elements is not necessarily limited to only those elements but may include other elements not expressly listed or inherently present therein.

[0021] Unless expressly stated to the contrary, "or" refers to an inclusive or and not to an exclusive or. For example, a condition A or B is satisfied by anyone of the following: A is true (or present) and B is false (or not present), A is false (or not present) and B is true (or present), and both A and B are true (or present).

[0022] The term “and combinations thereof” as used herein refers to all permutations or combinations of the listed items preceding the term. For example, “A, B, C, and combinations thereof” is intended to include at least one of: A, B, C, AB, AC, BC, or ABC, and if order is important in a particular context, also BA, CA, CB, CBA, BCA, ACB, BAC, or CAB. Continuing with this example, expressly included are combinations that contain repeats of one or more item or term, such as BB, AAA, AAB, BBC, AAABCCCC, CBBAAA, CABABB, and so forth. A person of ordinary skill in the art will understand that typically there is no limit on the number of items or terms in any combination, unless otherwise apparent from the context.

[0023] In addition, use of the "a" or "an" are employed to describe elements and components of the embodiments herein. This is done merely for convenience and to give a general sense of the inventive concepts. This description should be read to include one or at least one and the singular also includes the plural unless it is obvious that it is meant otherwise.

[0024] The use of the terms “at least one” and “one or more” will be understood to include one as well as any quantity more than one, including but not limited to each of, 2, 3, 4, 5, 10, 15, 20, 30, 40, 50, 100, and all integers and fractions, if applicable, therebetween. The terms “at least one” and “one or more” may extend up to 100 or 1000 or more, depending on the term to which it is attached; in addition, the quantities of 100/1000 are not to be considered limiting, as higher limits may also produce satisfactory results.

[0025] Further, as used herein any reference to "one embodiment" or "an embodiment" means that a particular element, feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment.

[0026] As used herein qualifiers such as “about,” “approximately,” and “substantially” are intended to signify that the item being qualified is not limited to the

exact value specified, but includes some slight variations or deviations therefrom, caused by measuring error, manufacturing tolerances, stress exerted on various parts, wear and tear, and combinations thereof, for example.

[0027] Certain exemplary embodiments of the invention will now be described with reference to the drawings. In general, such embodiments relate to thermic infusion systems and methods.

[0028] Referring now to the Figures, and in particular FIGS. 1 and 2, illustrated therein is an exemplary wearable device 10 constructed in accordance with the present disclosure. Generally, the wearable device 10 may provide multi-factor security for one or more cybernetic keys, electronic keys, and/or the like. In some embodiments, the wearable device 10 may appear to be an ornament for personal adornment, such as, for example, a ring, bracelet, necklace, earring, cuff link, and/or any article configured to be worn on a person or animal. In some embodiment, the wearable device 10 may be worn and/or positioned adjacent to skin. Use of the wearable device as a multi-factor security system may include, but is not limited to, logical access (e.g., laptop, phone, website), physical access cards, house keys, car keys, transit card, credit cards, passports, drivers licenses, insurance cards, membership/loyalty cards, ticket (e.g., planes, trains, concert, events), medical records, identity artefacts, and/or the like.

[0029] In addition to personal use, the wearable device may also be used within hospitals and other locations wherein access control may be needed. In hospitals, for example, doctors, nurses, and/or other practitioners may be able to use and/or adjust medical devices. Such medical devices may include security limiting access to one or more setting changes. For example, the medical device may provide for a doctor or other medical practitioner to log-in to adjust settings of the medical device. The wearable device may communicate with the medical device to provide authorization of the user (e.g., doctor) when the wearable device is positioned on the practitioner (e.g., placed on finger) and remains authorized while the wearable device remains on the practitioner providing a secure notification to the medical device that the authorized practitioner is present, for example. The wearable device may then deactivate when removed from the practitioner, and communicate with the medical device to provide a notification to the medical device that the practitioner is no longer authorized to change one or more settings. Additionally, in some embodiments, the wearable device may provide one or more

notifications to the medical device as a part of the process for authorizing the practitioner to login into the medical device. For example, the wearable device and/or the medical device may be programmed and provided with suitable sensors, such as a plurality of accelerometers, to sense a predetermined movement of the practitioner as part of the authorization process. For example, the predetermined movements may be the authorized practitioner tapping or manipulating (e.g., rotate) the medical device (e.g., tapping the medical device twice with the hand wearing the wearable device). One or more instructions may be transmitted from the wearable device to send authorization to the requesting medical device, for example. In some embodiments, the wearable device may present a cryptographic challenge and answer for security. As the wearable device includes biometric authorization for authorization of the practitioner, security is at least a two-factor authentication process. In some embodiments, at least a three-factor authentication process may be implemented as a user may provide selected motion to unlock and/or provide authorization of the practitioner. In some embodiments, one or more identifiers may log presence of the practitioner. For example, if a nurse is required to visit specific beds in an Intensive Care Unit at least every thirty minutes, one or more sensors may be positioned within the Intensive Care Unit and/or within the general vicinity of the Intensive Care Unit such that when the wearable device is within a pre-determined proximity to the one or more sensors, one or more identifiers may be transmitted and/or exchanged with the sensors to log presence of the nurse. Identifiers may include, but are not limited to, practitioner identification number, pre-determined code, time stamp, date stamp, and/or the like. In some embodiments, a near field broadcasting device may be used in lieu of or in addition to the one or more sensors. The near field broadcasting device may be active and/or passive. Generally, the wearable device may detect presence of the near field broadcasting device and record the broadcast identification number (e.g., room number), and store the broadcast identification number in the wearable device. Additional information may also be stored including, but not limited to, the current time, date, and/or the like. In some embodiments, broadcast identification number(s) may be downloaded and stored on a main logging system (e.g., head nurse station).

[0030] In some embodiments, the wearable device may be used for identification using digital IDs, including, but not limited to, driver's license, passport, hunting license, identification card, and/or the like. Identifiers may include, but are

not limited to, name, photograph, address, date of birth, eye color, license number, and/or the like. Identifiers may be stored in one or more secure elements (e.g., memory) of the wearable device. In some embodiments, a private key/public key pair and/or checksum may be generated, with the private key being stored in the secure element and the public key and checksum being stored on the wearable device, as well as, in a database at the server for licensing authority (e.g., Department of Motor Vehicles, U.S. Passport Office). In some embodiments, an external device (e.g., smartphone, tablet, computer, reader device, and/or the like), may transmit a challenge to the wearable device. If the wearable device is unlocked, the wearable device may create and transmit a packet of information to the external device. The packet of information may include a public key, the license data, the checksum, the challenge information, and/or a digital signature of the checksum and challenge data. The external device may receive the packet of information, and perform one or more local verifications using information from the packet of information. For example, the external device may verify that the license data transmitted has the same and/or similar checksum contained in the information packet, that the signed content contains the challenge issued and/or checksum as provided, digital signature was generated by the private key associated with the public key, and/or the like. The external device may provide verification by contacting one or more remote database from the licensing authority to verify that the checksum (i.e., verification license information is unaltered) and public key (i.e., verification that license information is unaltered) provided by the wearable device correspond to one or more entries in the database. In some embodiments, one or more photographs may be stored locally in the external device or in the remote database. The one or more photographs may be displayed on the external device such that the requesting individual may perform an additional authentication. In addition to traditional identity requests, multi-factor authentication may be used for "Know Your Customer" applications (e.g., opening bank account, bar authenticating age of individual wearing device, and/or the like). Activation may be via proximity (e.g., pre-determined range to a near field broadcasting device) and/or gesture activated (e.g., knocking twice in proximity of a Bluetooth receiver).

[0031] The wearable device 10 may provide multi-factor security in a manner simplifying carrying of a secure master key while also simplifying validation of the master key. The wearable device 10 may be secured via a biometric signature and

activated solely during use by a user (i.e., activated upon being worn by the user). The wearable device 10 is possessed by the user with biometrics securing information associated with the wearable device 10. Thus, if lost or stolen, the wearable device 10 may be unusable by an outside party as biometric data of the outside party may not validate use of the wearable device 10. In some embodiments, additional validation may be included. For example, one or more optional passwords may be used and entered via a securely paired device, a complex series of motions, and/or the like. With additional validation, three distinct security factors (e.g., user possession factor, user biometric factor, additional validation information including a password, complex series of motions or the like) may be used to authorize one or more transactions.

[0032] In some embodiments, the wearable device 10 may be paired solely to a particular user. In some embodiments, multiple wearable devices 10 may be paired and/or pairable solely to a particular user. As such, transactions initiated and/or confirmed by the wearable device 10 may have multi-factor authentication by possession (e.g., physical possession of the wearable device 10), identity (e.g., confirmation that the user of the wearable device 10 is the particular user), and knowledge (e.g., execution of a known pattern for verification).

[0033] The wearable device 10 may include a housing 11 formed of any material configured to be worn on a user. In some embodiments, the housing 11 may be formed of a waterproof material for protecting one or more components housed within the wearable device 10. In some embodiments, one or more portions of the housing 11 may be formed of a shielded skin (i.e., formed of waterproof material protecting one or more components within the housing 11) and unshielded skin (i.e., open to environment or configured to accept one or more biometric readings from a user). The housing 11 may be formed in any shape including, but not limited to, a sphere, a ring, a cone, a cube, a rectangular prism, a cylinder, a triangular prism, a pyramid, and/or any fanciful shape. In the example depicted in Figure 1, the housing 11 is formed into a shape of a ring defining a passage 11a sized and dimensioned to receive the user's finger. In this example, the housing 11 is formed into a non-cylindrical shape such that the passage 11a is non-circular. For example, the housing 11 may include an arc -shaped portion 11b, and a planar portion 11c.

[0034] Referring to FIGS. 1 and 2, the wearable device 10 may generally include one or more sensors 12, one or more processors 14, one or more memories 16, one or more communication devices 18, and one or more power sources 20 supported by the housing 11. In the example shown, the one or more sensors 12, and the one or more communication devices 18 can be positioned either within or on the planar portion 11c, and the one or more processors 14, one or more memories 16 and the one or more power sources 20 can be positioned within the arc -shaped portion 11b. The one or more sensors 12, the one or more memories 16, and the one or more communication devices 18 may be coupled to the one or more processors 14. For example, in some embodiments, the one or more sensors 12, the one or more memories 16, and/or the one of more communication devices 18 may be coupled to the one or more processors 14 using a bus. In some embodiments, one or more sensors 12 may be supported by the housing 11 yet have a portion exposed to the passage 11a. In these embodiments, the portion of the one or more sensors 12 may be configured to be positioned adjacent to a user's skin. For example, as illustrated in FIG. 1, if the wearable device 10 is a ring to be worn on a user's finger, one or more sensors 12 may be connected to the housing 11, and positioned on an interior surface 13 of the housing 11 of the wearable device 10 such that the sensors 12 are adjacent to a user's skin during use and detect the presence of the user.

[0035] The power source 20 may be any source configured to supply electrical energy to components of the wearable device 10. For example, in some embodiments, the power source 20 may be a rechargeable battery. In some embodiments, the power source 20 may include a battery 23 formed to the shape of at least a portion of the housing 11 as shown in FIG. 1. For example, when the housing 11 has an arc-shaped portion 12b, the power supply 20 (e.g., the battery 23) may have an arcuate shape.

[0036] The one or more sensors 12 may occupy a small amount of space relative to the wearable device 10 and have low power consumption in standby mode and during use. The one or more sensors 12 may be configured to determine pressure, temperature, light, speed, electrical capacity, and/or the like and transmit a signal to the one or more processors 14. In some embodiments, the one or more sensors 12 may be a transducer configured to convert a biometric parameter (e.g., , acoustic signal from a user's voice and/or the like) of a person into an electric signal.

For example, a first sensor 12a may include a transducer configured to convert an acoustic signal into an electric signal. Alternatively, the first sensor 12a may be implemented in other ways, including, but not limited to a fingerprint scanner, a retinal scanner, a face scanner, and/or other biometric scanner. In some embodiments, the biometric scan may include a cryptographic hash function (e.g., digital hash). By using a cryptographic hash function, as further described in U.S. Serial no. 15/269,554, the entire disclosure of which is herein incorporated by reference in its entirety, the biometric hash may be used to both unlock the wearable device 10 and to secure sensitive data on the wearable device 10.

[0037] In some embodiments, the first sensor 12a (e.g., biometric scanner) may be activated upon a user placing the wearable device 10 on the body. For example, with a user sliding the wearable device 10 onto a finger, a fingerprint scan may be obtained. As such, the first sensor 12a may have a planar configuration, and may be positioned on the interior surface 13 in the planar portion 11c of the housing 11 of the wearable device 10.

[0038] In some embodiments, a second sensor 12b (e.g., wear sensor) may be configured to monitor if the wearable device 10 is currently in use. Use of the wearable device 10 may include substantially constant contact with skin, kinetic motion, and/or the like. To that end, the second sensor 12b may be implemented in a variety of manners including, but not limited to, external capacitance change detection (Cap Sense), inductance change detection, biometric sensing (e.g., thermal sensor, heart beat sensor, blood oxygen sensor), and/or the like. In some embodiments, a biometric scanner, such as a fingerprint scanner, may be used to monitor if the wearable device 10 is currently in use (e.g., contact with skin, kinetic motion). In some embodiments, one single sensor 12 may be used to unlock the wearable device 10 and monitor if the wearable device 10 is currently in use. In the example shown in Fig. 1, the arc-shaped portion 11b is formed of a shielded skin (i.e., formed of waterproof material protecting one or more components within the housing 11) and the planar portion 11c is formed with unshielded skin overlying the first sensor 12a and the second sensor 12b to permit the first sensor 12a and the second sensor 12b to sense the biometric information, and the presence of the user. In this example, shielded skin surrounds, and protects the communication device 18.

[0039] In some embodiments, one or more sensors 12 may be located external and at a distance from the wearable device 10. For example, one or more

sensors 12 may be positioned in a paired device 19. In some embodiments, the paired device 19 may be positioned at a stationary location separate from a user's body. In some embodiments, the paired device 19 may be worn on the user's body. Generally, the paired device 19 may be located in proximity to the wearable device 10. In some embodiments, the paired device 19 may be located remotely from the wearable device 10 and communicate with the wearable device 10 via the communication device 18, one or more networks, and/or the like. In some embodiments, the paired device 19 may be a smartphone or a tablet computer, for example.

[0040] In some embodiments, in addition to the one or more sensors 12, the wearable device 10 may include one or more indicators 21 configured to provide specific information on a state or condition of the wearable device 10. The one or more indicators 21 may be visual, auditory, haptic and/or the like. For example, the one or more indicators 21 may include a visual indicator, such as an LED, or other type of light. In some embodiments, multiple visual indicators may provide information on a plurality of states or conditions of the wearable device 10. For example, a multi-color LED device may be used to provide information on a plurality of states or conditions of the wearable device 10.

[0041] In another example, the one or more indicators 21 may include a haptic indicator, such as a vibration or pulse. In some embodiments, the one or more indicators 21 may include a visual screen. The visual screen may include a graphical user interface, for example.

[0042] In some embodiments, one or more indicators 21 may be included in the paired device 19 (e.g., smartphone). The one or more indicators 21 may provide information to the user regarding state or condition of the wearable device 10 via output received by the paired device 19 (e.g., smartphone). Additionally, a user may be able to provide input to the wearable device 10 via the paired device 19. For example, confirmation of receipt of information regarding the state or condition of the wearable device 10 may be input via a tap or rotation of the paired device 19. Such input may be communicated to the wearable device 10 from the paired device 19.

[0043] In some embodiments, a secure connection may be established between the paired device 19 and the wearable device 10 prior to initial communication between the paired device 19 and the wearable device 10. The secure connection may decrease security breaches, such as, malware intended to

damage or disable systems (e.g., malware on the paired device 19). The secure connection may be obtained via multiple methods. For example, a cryptographic key pair may be shared between the wearable device 10 and the paired device 19 (e.g., an application running on the paired device 19). The cryptographic key pair may be configured to validate that authorized software is running on the paired device 19.

[0044] In some embodiments, to establish a secure connection, the wearable device 10 may provide information that a user enters on the paired device 19 such that the information may be communicated to the wearable device 10 allowing each of the wearable device 10 and the paired device 19 to be in control of the same user. For example, the indicator 21 on the wearable device 10 may include a plurality of separate LED colors. A pattern of LED colors may be flashed. The user of the wearable device 10 may then select corresponding colors on an application running on the paired device 19. In some embodiments, this process may be repeated multiple times to ensure the wearable device 10 and the paired device 19 are both controlled by the user. For example, the process may be repeated four different cycles. Additionally, the paired device 19 may request action of the user with regard to the wearable device 10. For example, the paired device 19 may request the user to rotate the wearable device 10 or tap the wearable device 10 in a particular pattern or a set number of times. After performing the request, the wearable device 10 may communicate to the paired device 19 that the wearable device 10 is controlled by the user. In some embodiments, this process may be repeated multiple times (e.g., three unique motions requested).

[0045] The one or more processors 14 may include a single processor or multiple processors working independently and/or together to execute the logic described herein. In some embodiments, the one or more processors may or may not be located in a single physical location. Additionally, multiple processors may or may not be located in a single physical location. In some embodiments, the one or more processors may be partially or completely network-based and/or cloud-based. As used herein, the terms “network-based,” “cloud-based,” and any variations thereof, may include the provision of configurable computational resources on demand via interfacing with a computer and/or computer network, with software and/or data at least partially located on the computer and/or computer network, by pooling processing power of two or more networked processors.

[0046] The one or more memories 16 may be implemented as a conventional non-transitory memory, such as, for example, random access memory (RAM), read only memory (ROM), flash memory, combinations thereof, and/or the like, for example. The term non-transitory computer readable medium, as used herein, may be implemented as a single physical device or multiple physical devices of a distributed system that may or may not be logically related. To that end, the one or more memories 16 may be located in the same physical location. Alternatively, the one or more memories 16 may be located in a different location and communicate via a network. Additionally, one or more of the memories 16 may be implemented as a "cloud memory" (i.e., one or more memories may be partially or completely based on or accessed using a network, for example).

[0047] The one or more memories 16 may store processor executable code and/or information comprising one or more databases and program logic. In some embodiments, the processor executable code may be stored as a data structure, such as a database and/or data table, for example. In some embodiments, a first memory 16a may be designated a permanent memory and a second memory 16b may be designated a temporary memory as illustrated in FIG. 2. Logic may be embodied in the form of software instructions and/or firmware, and may be executed on appropriate hardware. For example, logic embodied in the form of software instructions or firmware may be executed via the one or more processors 14. In some embodiments, logic may be implemented in a stand-alone environment operating on a single processor 14 and/or logic may be implemented in a networked environment, such as a distributed system using multiple processors 14.

[0048] The communication device 18 may be a system configured to provide communication and charging capabilities for the wearable device 10. For example, in some embodiments, the communication device 18 may include a dual use of a near field communications antenna for communications and for charging. While the use of the communication device 18 is described in relation to the wearable device 10 herein, it should be apparent to one skilled in the art that the communication device 18 may be used in other ring devices, small wearable device, and/or wearable and non-wearable devices in general needing to minimize space constraints by combining communication and charging capabilities into a single device.

[0049] FIG. 3A illustrates an exemplary circuit diagram 22 of an exemplary communication device 18a for use with the wearable device 10. Generally, the communication device 18a may include one or more receiving coils 24 used in Near Field Communications (NFC). Referring to FIGS. 2 and 3, in some embodiments, the recharge of the power source 20 may occur at about 13.56 MHz. In some embodiments, the recharge of the power source 20 may occur at a resonant frequency (e.g., at about the 6.78 MHz ISM band frequency).

[0050] Additionally, one or two resonant traps 26 (i.e., tank circuits, parallel LC circuit) coupled to the receiving coil 24 may be configured to isolate NFC transaction circuity 28 from charging circuity 30 as illustrated in FIG. 3A. In the presence of an alternating voltage (i.e., AC signal), the impedance of the circuit 22 may identify with the graphical representation shown in FIG. 3B. At the point of resonance, the circuit 22 may identify with an infinite resistance (e.g., essentially an open circuit or disconnected switch). The resonant traps 26 may be set to a resonant frequency of 13.56 MHz. With a "perfect" inductor and capacitor, components on a first side 25 of the resonant traps 26 may be isolated from the NFC on a second side 27 of the resonant traps 26. As such, energy may remain with the NFC such that range (i.e. distance) of transactions may be increased. In particular, in FIG. 3A, elements of the circuit 22 on the first side 25 include diodes D1 and D2 and capacitors C1 and C2. The purpose of D2 may be to clamp the voltage at a node N between the two diodes D1 and D2 from going negative resulting in capacitor C2 being charged positively. When the coil voltage changes polarity, the voltage on capacitor C2 may be added to the switched voltage (e.g., doubling the voltage) with a resulting peak voltage rectified by diode D1 charging capacitor C1. The coil voltage may reverse and capacitor C2 may again be charged with the process repeated. As the resonant traps 26 may not resonant at the 6.78MHz frequency, the resonant traps 26 may pass energy such that voltage on the coil and capacitor C2 may pass to the diodes D1 and D2. The resonant traps 26 may be combined with the diodes D1 and D2 and the capacitor C2 to form a voltage doubler circuit. At the NFC frequency, energy may then be clocked from flowing to the diodes D1 and D2. For example, with charging frequency of 6.78 MHz, the resonant trap(s) 26 pass energy to the charging circuity 30 providing the power source 20 to be charged at the non-resonant 6.78 MHz ISM band frequency. Further, in some embodiments, the communication

device 18a may default to a charging mode if the power source 20 has a charge below a predetermined baseline, e.g., devoid of charge.

[0051] Referring to FIG. 4, the wearable device 10 may be configured to discern between the NFC transaction and charging due to detection of the non-resonant charging frequency with the signal rectified by a diode. An external charger 32 may include a drive coil 34 with the wearable device 10 having the receiving coil 24. In some embodiments, an RF connection may be used to communicate battery voltage and/or battery current. In some embodiments, the wearable device 10 may signal the battery voltage to the external charger 32 via light emitting diode (LED) signalling. In some embodiments, passive or active near field load modulation may be used for communication between the wearable device 10 and the external charger 32.

[0052] To further reduce circuitry needed to charge the power source 20, the external charger 32 may include one or more intelligent chargers. Intelligent chargers may communicate with the wearable device 10 and vary energy during charging to maintain proper current and/or voltage levels to the power source 20.

[0053] In some embodiments, the one or more processors 14 may determine and report voltage level at the power source 20 to the external charger 32. In some embodiments, if the power source 20 is devoid of charge, and as such, at least one processor 14 is inoperable, charging operation may be initiated with a pre-charge level of Radio Frequency (RF) energy to the coil 24. This energy level may provide 0.05C to 0.1C current, for example, to pre-charge the power source 20 until a predetermined voltage level is reached (e.g., pre-charge termination voltage). At the predetermined voltage level, the processor 14 within the wearable device 10 may communicate voltage level of the power source 20 via the communication device 18 to the external charger 32. Once the predetermined voltage level is reached and the wearable device 10 communicates the voltage to the external charger 32, RF drive level may be altered to achieve a charging current of approximately 0.5C. In some embodiments, the wearable device 10 may monitor and report to the external charger 32 current into the power source 20 to monitor charging current. In some embodiments, drive energy of the external charger 32 may be monitored to determine energy being absorbed by the wearable device 10. Correlation of the drive energy to the power source 20 may be used to determine charging current.

[0054] In some embodiments, a pre-determined target charge level (e.g., 0.5C) may be maintained until the power source 20 reaches a charge termination voltage (e.g., 4.2V). The wearable device 10 may report the voltage to the external charger 32 via the communication device 18 such that charge current may be reduced (e.g., by 50%) and charging may continue until voltage of the power source 20 again reaches termination voltage. At this point, drive level may be reduced while the process of monitoring of voltage and reducing drive level may continue until a minimum drive level (e.g., minimum battery current) is reached and charging discontinues.

[0055] Alternatively, drive level may be adjusted to maintain a constant voltage on the power source 20 until a minimum drive level (e.g., battery current) may be achieved and charging discontinues. During this process, the wearable device 10 may determine and report voltage to the external charger 32 such that a closed loop feedback operation may continue.

[0056] FIG. 5 illustrates a flow chart 40 of an exemplary method for providing the wearable device 10 in a locked mode and an unlocked mode such that the processor 14 may be capable of processing at least one key request and/or communicating sensitive data (i.e., data needing security). Because the wearable device 10 is activated with a fingerprint scan and having the wearable device 10 also proves possession, in this embodiment, the wearable device 10 is always providing at least two factors of authentication. Those two factors may be protecting one or more cybernetic keys, electronic keys, and/or the like in a multi-key security protocol.

[0057] In a step 42, the first sensor 12a (e.g., biometric sensor), may determine a biometric parameter and transmit a signal to the processor 14. In a step 44, the processor 14 may compare the biometric parameter to one or more stored user parameters for confirmation of the user. In some embodiments, validation of the biometric parameters may be determined using the algorithm described in U.S. Serial no. 15/269,554, which is hereby incorporated by reference in its entirety. The method described therein may also be used to differentiate biometric parameters, validate biometric parameters, and/or supply a biometric key for use in decrypting secure information. In a step 46, the processor 14 may authenticate the user and switch to an unlock mode, allowing the processor 14 to communicate sensitive data. The wearable device 10 may remain in the unlocked mode as long as the wearable device 10 is still being worn. In a step 48, the second sensor 12b, may determine

whether the wearable device 10 is still in contact with the user. The step 48 can be repeated periodically, randomly or on a schedule to determine at a variety of instants of time whether the wearable device 10 is still in contact with the user. In a step 50, if the wearable device 10 is not in contact with the user, the processor 14 may switch into a locked mode wherein the processor 14 may not communicate secure data. The user may then re-authenticate the wearable device 10 as indicated by arrow 52.

[0058] FIG. 6 illustrates a flow chart 60 of an exemplary method for using the wearable device 10 to process key requests. By processing key requests, the wearable device 10 may be used as multi-factor security for one or more cybernetic keys, electronic keys, and/or the like. In a step 62, sensitive data may be stored in one or more memories 16. In some embodiments, sensitive data may be stored in an encrypted form in the permanent memory 16a. In a step 64, the wearable device 10 may be switched to the unlocked mode. In a step 66, with the wearable device 10 in the unlocked mode, the sensitive data may be temporarily decrypted and stored in the temporary memory 16b. Decryption may be by using biometric data and the biometric data hashing verification and security process described in U.S. Serial No. 15/269,554, which is hereby incorporated by reference in its entirety. In some embodiments, the processor 14 may transmit decrypted sensitive information to one or more external systems, such as the paired device 19. In other embodiments, the processor 14 is configured to receive a cryptographic challenge from one or more external system, such as the paired device 19, determine whether the cryptographic challenge corresponds to the decrypted sensitive information, and respond to the cryptographic challenge in a first manner when the cryptographic challenge corresponds to the decrypted sensitive information, or in a second manner when the cryptographic challenge does not correspond to the decrypted sensitive information. The response in the first manner can be used by the paired device 19, for example, to authorize a transaction. The response in the second manner can be used by the paired device 19 to decline a transaction. In a step 68, the wearable device 10 may be returned to the locked mode (e.g., powered off, taken off) with the unencrypted sensitive data being discarded from the temporary memory 16b.

[0059] In another example, for authentication, a unique private cryptographic key may be stored for each use (e.g., website password, credit card data, access card data). Each private cryptographic key may include a corresponding public cryptographic key. The processor 14 may provide the corresponding public

cryptographic key to an external system (e.g., NFC device). For logging in, for example, the external system may provide a challenge. The processor 14 in the unlocked mode may sign the challenge with the private cryptographic key as an answer to the challenge. The external system may use the public cryptographic key to verify that the challenge was signed with the private cryptographic key. As such, only the public cryptographic key may be used to verify the signature and the private cryptographic key remains in the processor 14. In another example, for authentication, secret protocols may be used wherein sensitive data may be shared by the processor 14 during one or more authentications (e.g., passwords, pin codes, identification numbers). Data may be the pass code instead of using of a cryptographic key, such as, for example, in a sequence of events.

[0060] FIG. 7 illustrates a flow chart 70 of an exemplary method for providing user confirmation from the user of the wearable device 10. By providing user confirmation from the user, the wearable device 10 may be used as multi-factor security for one or more cybernetic keys, electronic keys, credit cards, office access cards, transit cards, door lock keys, and/or the like. For example, by providing user confirmation from the user of the wearable device 10, a portable mock point of sale terminal or similar device used within close proximity of the wearable device 10 may be prevented from being inserted into transactions without the user's knowledge. In a step 72, the user may be positioned in proximity to a Near Field Communication (NFC) device. In a step 74, the user may provide a positive action (e.g., tapping the wearable device 10) to initiate a transaction with the NFC device. In some embodiments, one or more prompts from the wearable device 10 and/or the NFC device may be used to initiate the positive action by the user. In some embodiments, the wearable device 10 may include motion sensing capability. As such, movements of the wearable device 10 by the user, such as rotation (e.g., clockwise, counter clockwise), may be used. To that end, it may be possible to include a third factor of authentication by requiring that for selected transactions, a movement password may be executed. For example, a user may flip the wearable device 10 over clockwise once, tap twice, and rotate the wearable device 10 counter-clockwise back to the original orientation. When combined with possession of the wearable device 10, and identity of the user established via sensors 12, three factor authentication may be used for selected or all transactions.

[0061] FIG. 8 illustrates a flow chart 80 of an exemplary method for providing secure information from the wearable device 10 to the paired device 19. In a step 82, the wearable device 10 may switch to the unlocked mode. In a step 84, the wearable device 10 may establish a secure connection with the paired device 19. In a step 86, the paired device 19 may prompt the user to provide additional security information for access. For example, the user may set up an account such that any transaction over an established amount requires the user to enter a 4-digit PIN to authorize the transaction. As such, the wearable device 10 would need to be in the unlocked mode to provide the sensitive information, and also the user may need to enter a 4-digit PIN into the paired device 19 through an application running on the paired device 19 in order to complete a transaction. In some embodiments, a hashed password may be transmitted to gain admittance. The hashed password may be entered by the user whenever access is requested. In some embodiments, a challenge and answer method may be used to obtain the password. In a step 88, the paired device 19 may provide sensitive information from the wearable device 10 to a third party system. For example, the paired device 19 may provide sensitive information from the wearable device 10 to a payment processing network or access granting system via the Internet. If the third party system is unable to receive communications directly form the wearable device 10, but is able to communicate via the Internet, the paired device 19 may provide sensitive information from the wearable device 10 to the third party system via the Internet. Additionally, the third party system may communicate with the wearable device 10 via the paired device 19.

[0062] In some embodiments, the secure connection between the wearable device 10 and the paired device 19 may be used to unlock a password vault system such that the user may use randomly generated complex passwords stored either in the wearable device 10 in an encrypted format or stored on the paired device 10 in an encrypted format. When a password is needed, a request may be made from the password vault. If the password vault is stored in memory 16 on the wearable device 10, the corresponding password may be selected and decrypted internally using a secure element stored key, biometric hash key, and decrypted password sent via the secure connection to the paired device 19. If the password is on the paired device 19, a stored master password within the memory 16 of the wearable device 10 may be decrypted using the secure element stored key or the biometric

hash key, and the decrypted master password may then be transmitted via the secure connection to the password vault within the paired device 19. The decrypted master password may then be used to decrypt the corresponding password stored in the paired device 19.

[0063] In some embodiments, the wearable device 10 may be used to operate a keyless fob for automobiles, home entry, and/or the like. For example, in home entry system, the NFC antenna for the home lock may be installed into the door handle such that when the user grasps the door handle with the hand wearing the wearable device 10, the wearable device 10 may enter the antenna range of the NFC antenna and the door may be unlocked using the multi-factor authorization of the wearable device 10.

[0064] Referring to FIG. 9, in another example, for automotive systems, the wearable device 10 may communicate with one or more sensors (e.g., capacitive sensors) located within a door lock 90 of an automobile, one or more proximity sensors 92 on or within the automobile, the ignition starter 94 (e.g., start button), and/or the like. In some embodiments, a secondary installed device 96 may be positioned within the automobile, for example, on a dashboard or windshield. The secondary installed device 96 may alternatively be connected to an OBD-II diagnostics port, fuse panel, and/or the like. In some embodiments, the secondary installed device may emit an identification signal (e.g., Bluetooth Low Energy (BLE). The wearable device 10 may detect the identification signal, and connect to the secondary installed device 96. A secure connection may be established using multi-factor authentication described herein. The wearable device 10 may either have a continuous active radio, periodically active radio, or gesture activated radio (e.g., double knock) such that the wearable device 10 may be configured to conserve power.

[0065] Once authenticated, the secondary installed device 96 may power the fob circuitry, for example, thus indicating the fob is in proximity to the automobile. This may unlock doors of the automobile, start the automobile, and/or the like. The fob may remain active while the automobile is in operation. If the wearable device 10 leaves the proximity of the automobile (e.g., user stops driving and walks away from the automobile), the BLE connection may be disconnected causing the second installed device 96 to initiate a lock sequence and disable the fob circuit. In some embodiments, a motion sequence (e.g., a double knock) may be used to start a timer

98 such that a user has a pre-determined amount of time to leave the vehicle prior to the secondary installed device 96 initiating another unlock sequence. For example, a first motion sequence, such as a double knock, may be used to unlock the car and activate the start button, followed by a second motion sequence, such as a double knock, to deactivate the start button and lock the car.

[0066] In some embodiments, the secondary installed device 96 may include a power source 100. The power source 100 may be configured to recharge using power from the automobile, may be connected directly into the automobile, and/or may be recharged using solar cells, and/or the like. In some embodiments, the secondary installed device 96 may be built inside a tamper-resistant enclosure, such as, for example, FIPS 140-2 level 3 compliant, that may be configured to destroy the fob circuitry upon tampering. In some embodiments, the fob circuitry may be made by either altering an aftermarket fob or by using an existing fob and inserting the PCB into the installed device.

[0067] In some embodiments, the wearable device 10 may be used to unlock a smartphone, tablet, and/or the like. For example, the paired device 19 may be a smartphone, tablet, and/or the like, and the secure connection may be established between the wearable device 10 and the paired device 19. Further, settings may be altered such that the wearable device 10 need not provide the security password after the secure connection has been established between the wearable device 10 and the paired device 19. The same protocol may be used to unlock a desktop system.

[0068] From the above description, it is clear that the inventive concepts disclosed and claimed herein are well adapted to carry out the objects and to attain the advantages mentioned herein, as well as those inherent in the invention. While exemplary embodiments of the inventive concepts have been described for purposes of this disclosure, it will be understood that numerous changes may be made which will readily suggest themselves to those skilled in the art and which are accomplished within the spirit of the inventive concepts disclosed and claimed herein.

What is claimed is:

1. A wearable device, comprising:

a housing configured to be worn by a user;

at least one sensor supported by the housing and configured to sense presence of a user in contact with the housing, and at least one biometric parameter of a user in contact with the wearable device and output one or more signals representative of the biometric parameter;

a communication device configured to provide wireless communication signals;

at least one data processing system having one or more processors configured to receive the one or more signals representative of the biometric parameter and sensed presence of the user and compare the biometric parameter to a stored user parameter for authentication of the user, wherein upon authentication by the one or more processors, the one or more processors are configured to switch from a locked mode to an unlocked mode to enable the one or more processors to communicate data, via the communication device, indicative of at least two factors conforming to the requirements of a multi-factor authentication scheme, and to switch from the unlocked mode to the locked mode in absence of the at least one sensor device sensing the presence of the user, at least one of the one or more processors and the communication device being disabled from communicating data indicative of the factor in the locked mode; and,

a power source providing energy to the sensor and the at least one data processing system.

2. The wearable device of claim 1, wherein the housing is a ring.

3. The wearable device of any one of claims 1-2, wherein the at least one sensor includes a first sensor and a second sensor, and wherein the second sensor is configured to continuously sense proximity of the user.

4. The wearable device of any one of claims 1-3, wherein at least one of the sensor and the one or more processors are configured to transform the biometric parameter with a cryptographic hash function.

5. The wearable device of any one of claims 1-4, wherein the at least one sensor includes a first sensor and a second sensor, and wherein the second sensor is positioned externally and at a distance from the wearable device.

6. The wearable device of any one of claims 1-5, further comprising at least one indicator coupled to the one or more processors and configured to provide one or more states of the wearable device.

7. The wearable device of claim 6, wherein the at least one indicator comprises a secondary indicator positioned on a paired device and wherein the at least one indicator and the secondary indicator establish a secure connection between the communication device and the paired device.

8. The wearable device of any one of claims 1-7, further comprising at least one indicator positioned externally and at a distance from the wearable device and configured to provide one or more states of the wearable device.

9. The wearable device of any one of claims 1-8, wherein the communication device transmits wirelessly using a protocol conforming to the requirements of low energy bluetooth.

10. The wearable device of any one of claims 1-9, wherein the communication device includes a near field communications antenna.

11. The wearable device of claim 10, wherein the near field communications antenna includes one or more resonant coils.

12. The wearable device of claim 11, further comprising charging circuitry and NFC transaction security, and wherein the communication device further includes one or more resonant traps coupled to charging circuitry and the NFC transaction security and configured to isolate signals intended for the NFC transaction circuitry from the charging circuitry.

13. The wearable device of claim 12, wherein recharge of the power source occurs at a frequency that is not resonant with the one or more resonant coils.

14. The wearable device of claim 10, wherein the communication device is configured to discern between communication signals including sensitive data and energy for the power source via detection of a non-resonant charging frequency.

15. The wearable device of any one of claims 1-14, wherein the wearable device further comprises a temporary memory and a permanent memory wherein temporary memory stores unencrypted sensitive information when the one or more processors are in an unlocked mode and discards unencrypted sensitive information when the one or more processors are in a locked mode.

16. The wearable device of any one of claims 1-15, wherein the at least one sensor supported by the housing and configured to sense presence of a user in contact with the housing is a fingerprint scanner.

17. The wearable device of any one of claims 1-16, wherein the multi-factor authentication scheme includes identity and verification of car security access.

18. The wearable device of any one of claims 1-17, wherein the multi-factor authentication scheme includes identity and verification of lock access.

19. The wearable device of any one of claims 1-18, wherein the multi-factor authentication scheme includes identity and verification of user account access.

20. A method comprising:

determining, by a first sensor on a wearable device, a biometric parameter of a user and transmitting the biometric parameter to one or more processors, at least one of the processors positioned in the wearable device;

determining, by a second sensor on the wearable device, continuous presence of the user;

authenticating, by the one or more processors, the user using the biometric parameter and one or more stored parameters;

switching the one or more processors from a locked mode to an unlocked mode responsive to authenticating the user; and,

maintaining the one or more processors in the unlocked mode by monitoring the continuous biometric parameter via the second sensor.

21. The method of claim 20, wherein the wearable device includes a rechargeable power source and a communication device, and further comprising recharging the power source on the wearable device by the communication device.

22. The method of any one of claims 20-21, further comprising discerning, by a communication device in the wearable device, between a NFC transaction and charging due to detection of a non-resonant charging frequency.

23. The method of any one of claims 20-22, further comprising the step of transmitting, by the one or more processors in the unlocked mode, sensitive information stored in a temporary memory to a paired device.

24. The method of claim 23, further comprising the step of discarding, by the temporary memory the sensitive information when the one or more processors are switched to the locked mode.

25. A wearable device, comprising:

a housing configured to be worn by a user;

at least one sensor supported by the housing and configured to obtain one or more biometric parameters from a user in contact with the wearable device;

at least one processor coupled to the housing and having circuitry that receives and utilizes the biometric parameters to configure the processor in an unlocked mode and a locked mode, wherein in the unlocked mode the processor decrypts sensitive information and stores the decrypted sensitive information in a temporary memory;

a power source coupled to the housing; and,

a communication device coupled to the housing and configured to receive and provide communication signals related to the sensitive information.

26. The wearable device of claim 25, wherein at least one processor is configured to transmit the decrypted sensitive information to one or more external systems.

27. The wearable device of any one of claims 25-26, wherein the at least one processor is configured to receive a cryptographic challenge from one or more external system, determine whether the cryptographic challenge corresponds to the decrypted sensitive information, and respond to the cryptographic challenge in a first manner when the cryptographic challenge corresponds to the decrypted sensitive information, or in a second manner when the cryptographic challenge does not correspond to the decrypted sensitive information.

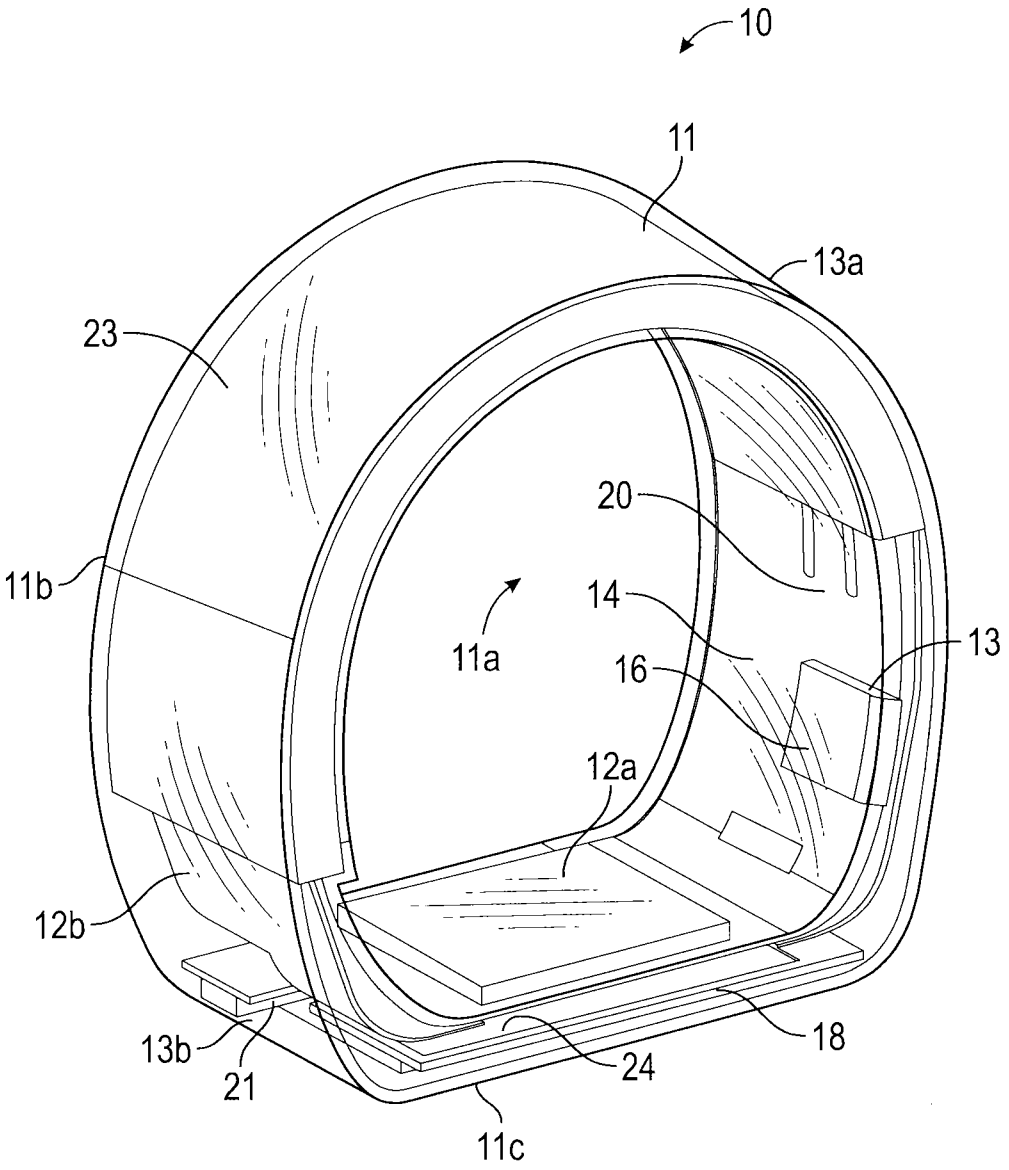

FIG. 1

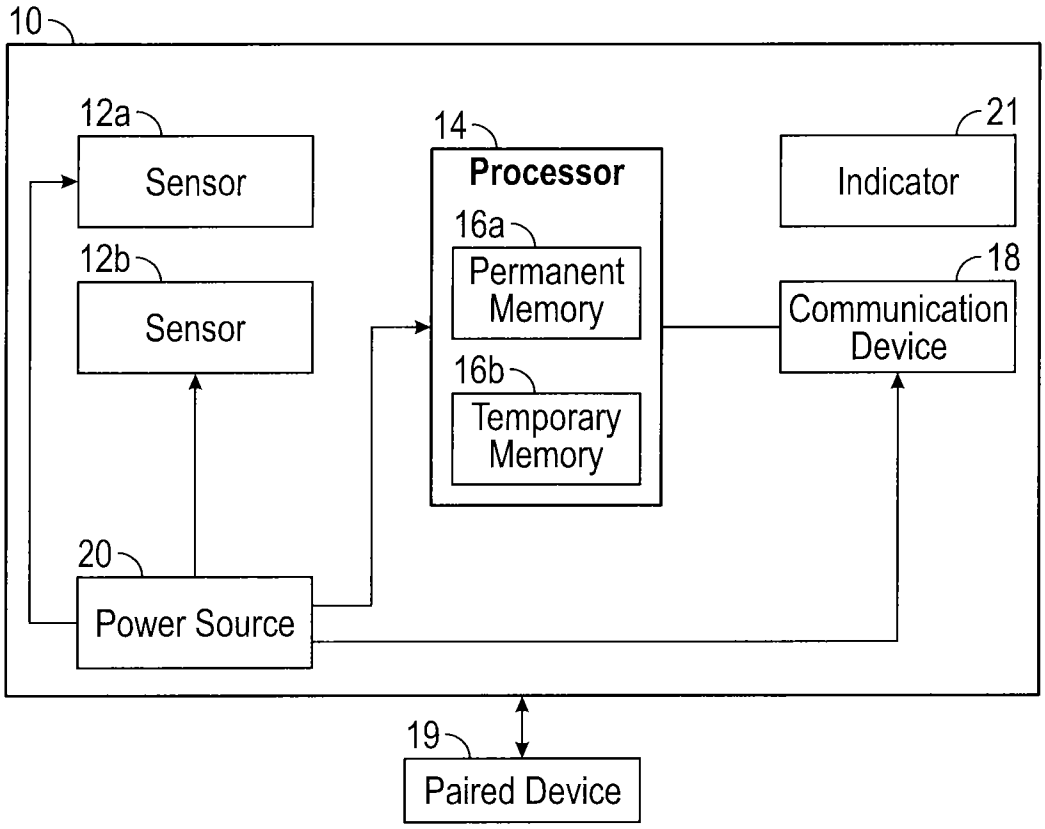
10
12a
Sensor
12b
Sensor
14
Processor
16a
Permanent Memory
16b
Temporary Memory
21
Indicator
18
Communication Device
20
Power Source
19
Paired Device

FIG. 2

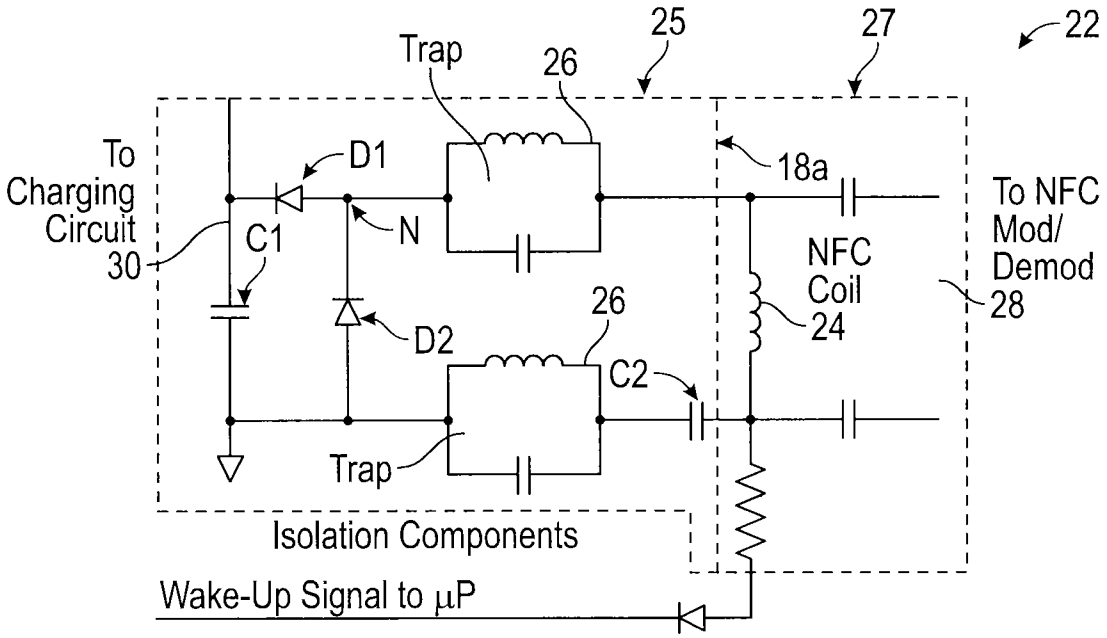
22
25
27
Trap
26
To Charging Circuit 30
D1
C1
N
18a
To NFC Mod/ Demod 28
NFC Coil 24
D2
26
C2
Trap
Isolation Components
Wake-Up Signal to μP

FIG. 3A

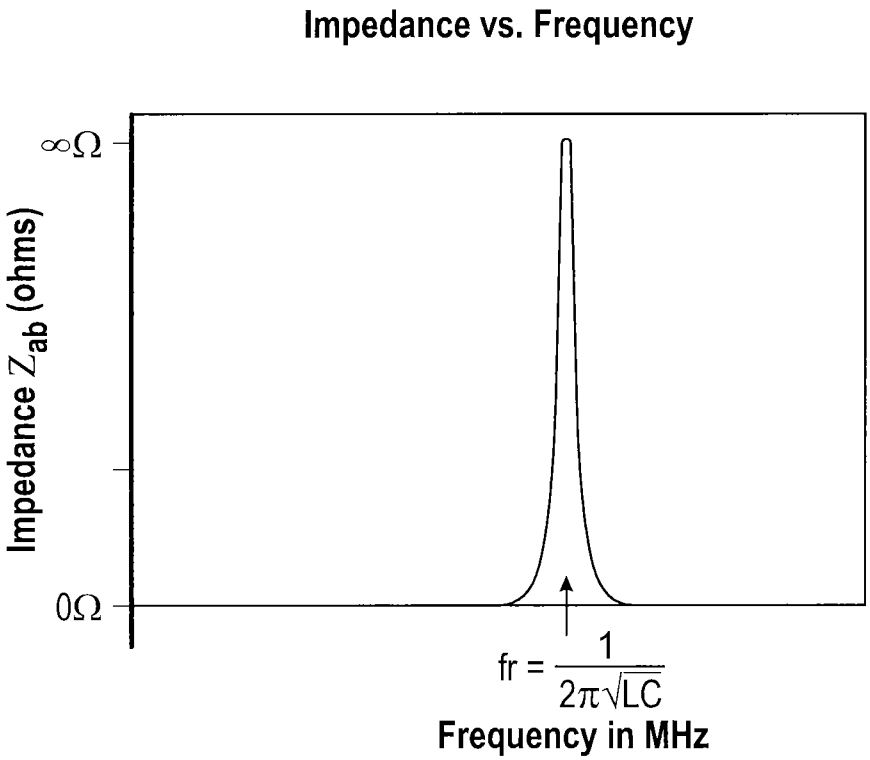
Impedance vs. Frequency
∞Ω
0Ω
Impedance Z_{ab} (ohms)
$fr = \frac{1}{2\pi\sqrt{LC}}$
Frequency in MHz

FIG. 3B

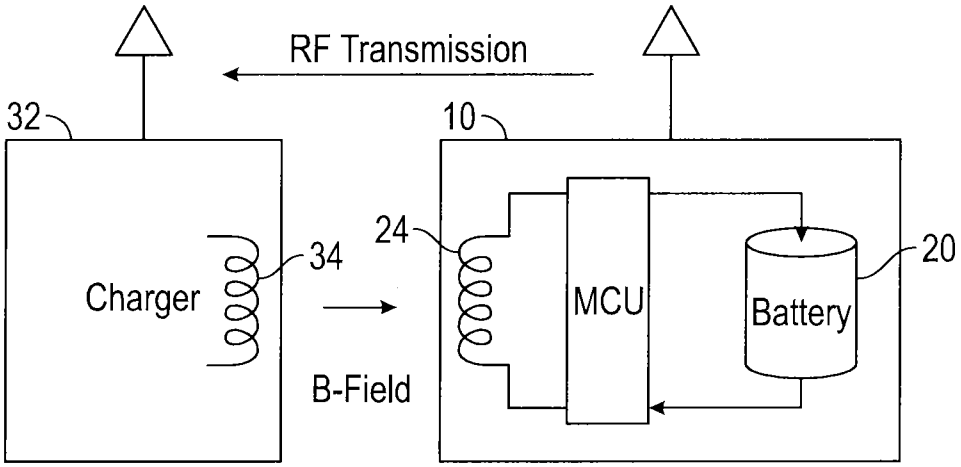
RF Transmission
32
10
Charger
34
24
MCU
Battery
20
B-Field

FIG. 4

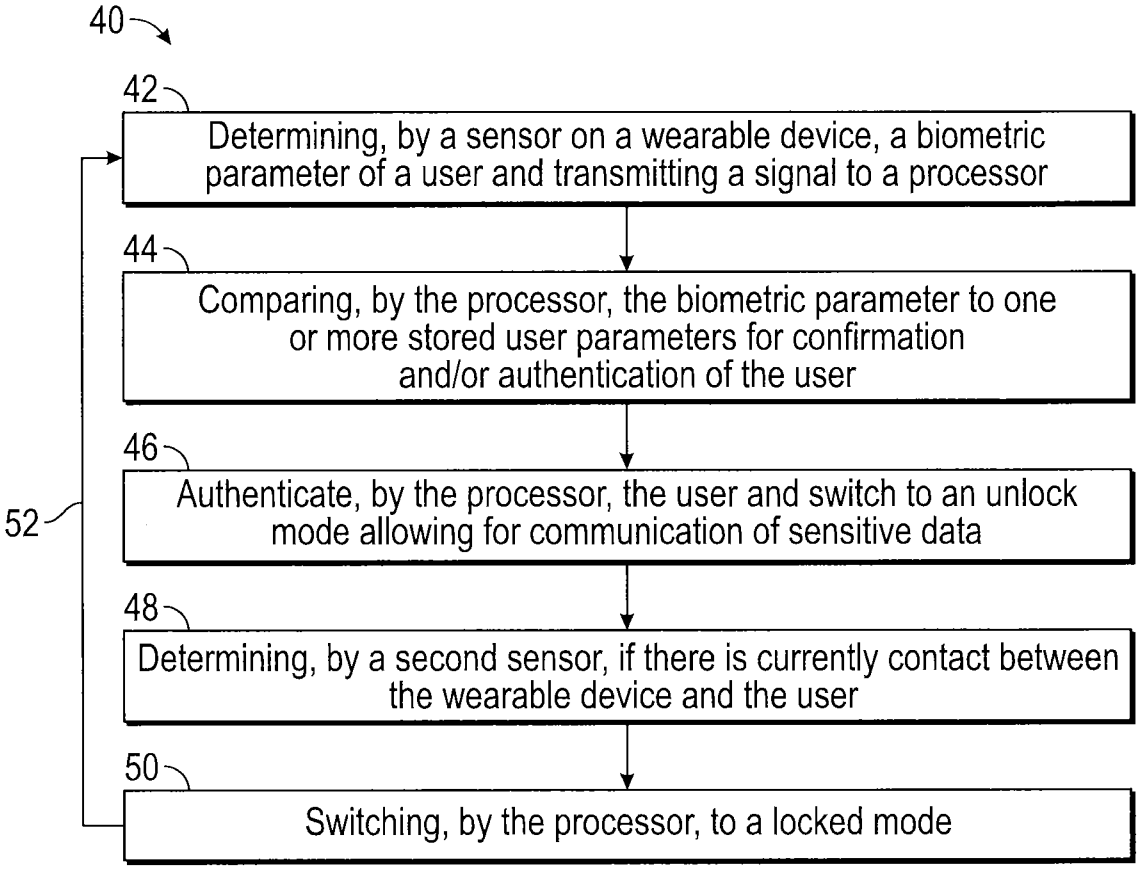
40
42
Determining, by a sensor on a wearable device, a biometric parameter of a user and transmitting a signal to a processor
44
Comparing, by the processor, the biometric parameter to one or more stored user parameters for confirmation and/or authentication of the user
46
Authenticate, by the processor, the user and switch to an unlock mode allowing for communication of sensitive data
52
48
Determining, by a second sensor, if there is currently contact between the wearable device and the user
50
Switching, by the processor, to a locked mode

FIG. 5

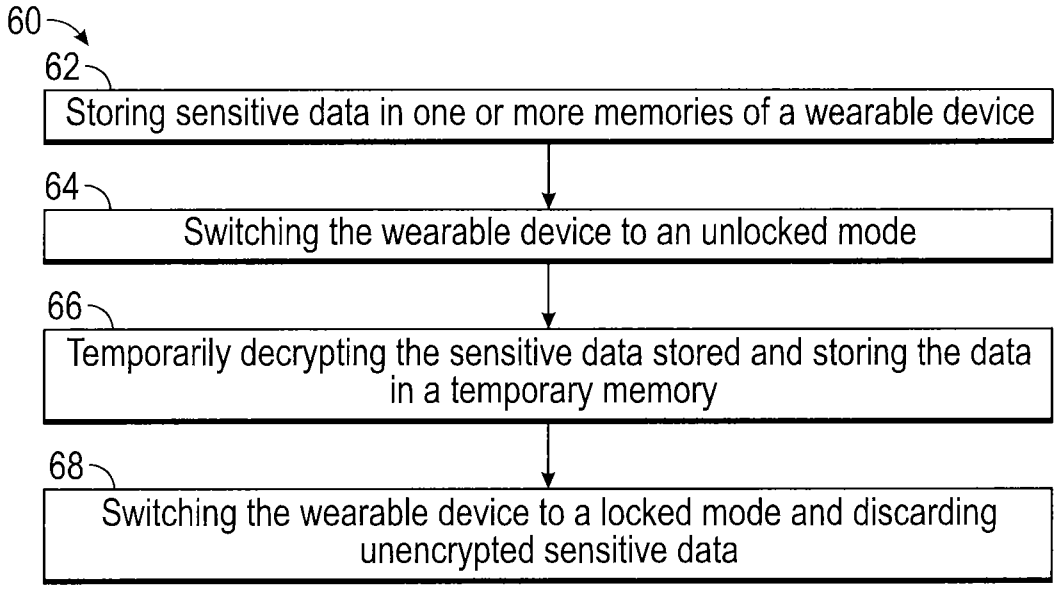
60
62
Storing sensitive data in one or more memories of a wearable device
64
Switching the wearable device to an unlocked mode
66
Temporarily decrypting the sensitive data stored and storing the data in a temporary memory
68
Switching the wearable device to a locked mode and discarding unencrypted sensitive data

FIG. 6

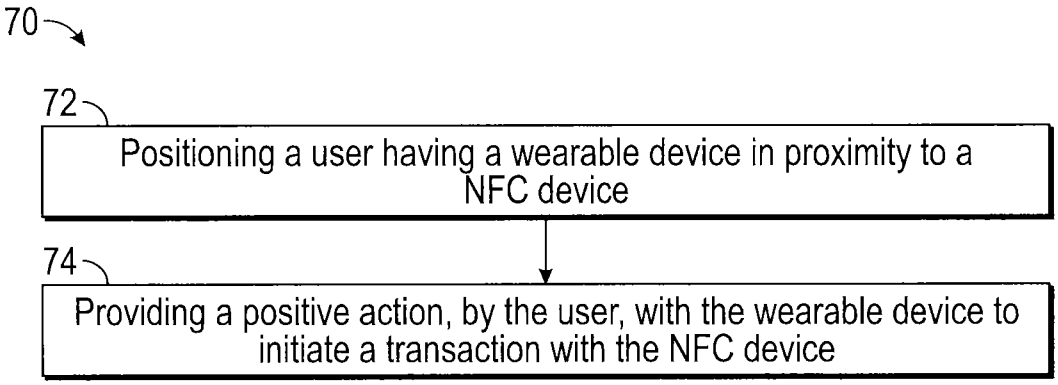
70
72
Positioning a user having a wearable device in proximity to a NFC device
74
Providing a positive action, by the user, with the wearable device to initiate a transaction with the NFC device

FIG. 7

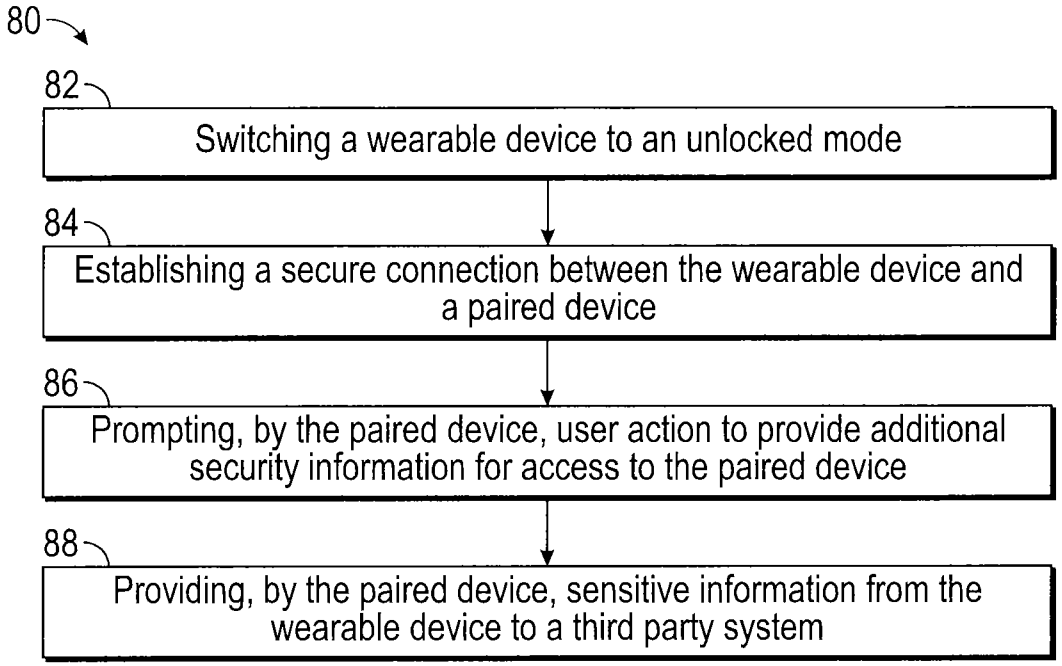
80
82
Switching a wearable device to an unlocked mode
84
Establishing a secure connection between the wearable device and a paired device
86
Prompting, by the paired device, user action to provide additional security information for access to the paired device
88
Providing, by the paired device, sensitive information from the wearable device to a third party system

FIG. 8

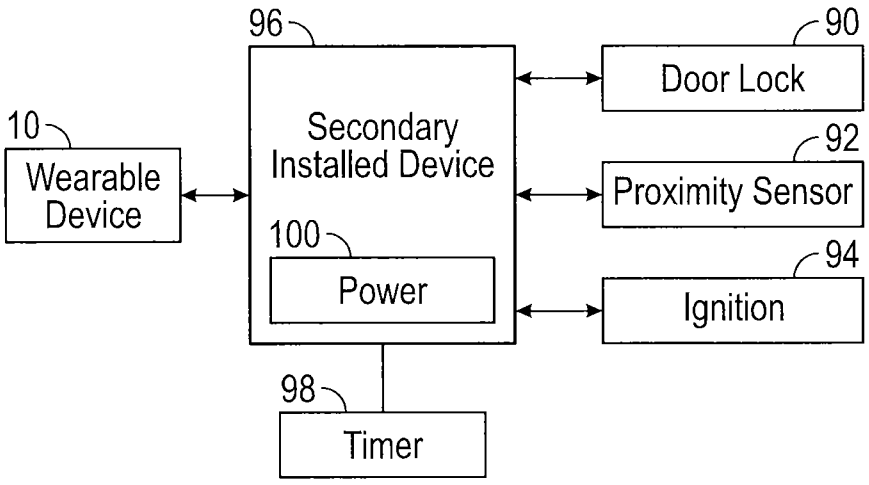
96
90
Door Lock
10
Wearable Device
Secondary Installed Device
92
Proximity Sensor
100
Power
94
Ignition
98
Timer

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2017/046124

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☒ Claims Nos.: 4-19, 23, 24
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2017/046124

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 21/34; G06F 21/35; H04L 9/32 (2017.01)
CPC - G06F 21/32; G07C 9/00087; G07C 9/00158 (2017.08)

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)
See Search History document

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 340/5.530; 340/5.520; 713/186 (keyword delimited)

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2016/0092665 A1 (INTEL CORPORATION) 31 March 2016 (31.03.2016) entire document	1-3, 20, 22 --- 21, 25-27
Y	US 2009/0150667 A1 (BALTZER) 11 June 2009 (11.06.2009) entire document	21, 25-27
A	US 7,898,385 B2 (KOCHER) 01 March 2011 (01.03.2011) entire document	1-3, 20-22, 25-27
A	US 2014/0089672 A1 (LUNA et al) 27 March 2014 (27.03.2014) entire document	1-3, 20-22, 25-27

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

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

Date of the actual completion of the international search	Date of mailing of the international search report
01 October 2017	27 OCT 2017
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450 Facsimile No. 571-273-8300	Authorized officer Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774