



- (51) **International Patent Classification:**
H04L 9/30 (2006.01)
- (21) **International Application Number:**
PCT/US2013/062064
- (22) **International Filing Date:**
27 September 2013 (27.09.2013)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant:** EMPIRE TECHNOLOGY DEVELOPMENT LLC [US/US]; 2711 Centerville Road, Suite 400, Wilmington, Delaware 19808 (US).
- (72) **Inventor:** KHESIN, Oscar; 4250 Albany Dr., #F303, San Jose, California 95129 (US).
- (74) **Agent:** SU, Gene; Ren-Sheng International, 7F, No. 57, Sec. 2, Dun Hua S. Road, Taipei, 106 (TW).
- (81) **Designated States** (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,

DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) **Title:** INFORMATION PROTECTION METHOD AND SYSTEM

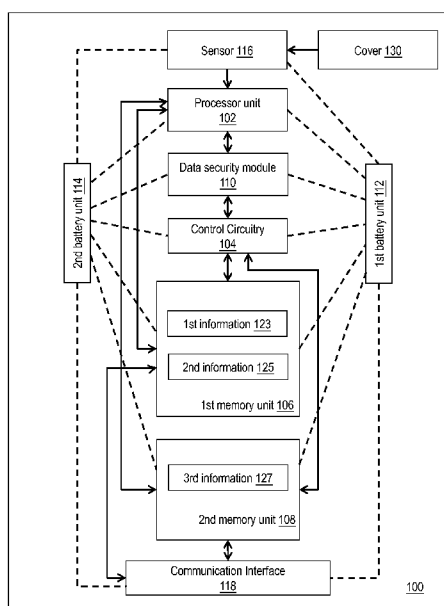


Fig. 1A

(57) **Abstract:** Techniques described herein generally relate to protecting information stored in a mobile communication device. In one embodiment, a mobile communication device may include a data security module, a control circuitry, a first memory unit configured to store a first information, a first battery unit configured to supply power to the mobile communication device, and a second battery unit configured to supply power to the data security module and the control circuitry in response to a trigger event. The data security module is further configured to activate the control circuitry to perform a particular action on the first information, such as at least a partial erasure of the first information.

INFORMATION PROTECTION METHOD AND SYSTEM

BACKGROUND

[0001] Unless otherwise indicated herein, the approaches described in this section are not prior art to the claims in this application and are not admitted to be prior art by inclusion in this section.

[0002] As mobile communication devices become an integral part of our daily lives, more and more information is being stored in these mobile communication devices for convenience.

[0003] However, when a mobile communication device is lost or stolen, sensitive information stored in such a mobile device (such as credit card information or bank account information) may be exposed to unauthorized accesses.

[0004] When an owner of the mobile communication device realizes that his/her mobile communication device may have been misplaced, the owner could possibly locate the mobile communication device and then remotely lock the mobile communication device and/or erase the sensitive information stored in the device. However, locating the mobile communication device may not be a viable option if the mobile communication device is not powered.

[0005] Moreover, even if the mobile communication device is located, and the information stored in the mobile communication device is successfully erased, since all the stored information in the convention approach is erased, irrespective of the sensitivity or confidentiality of the information, recovering and/or rebuilding the erased information can be time consuming and costly.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] So that the manner in which the above recited features of the disclosure can be understood in detail, a more particular description of the disclosure may be had by reference to embodiments, some of which are illustrated in the drawings. It is to be noted, however, that the drawings illustrate only typical embodiments and are therefore not to be considered limiting of its scope, for the disclosure may admit to other equally effective embodiments.

[0007] Fig. 1A is a block diagram of a mobile communication device;

Fig. 1B is a block diagram illustrating certain physical arrangements of parts in a communication device;

Fig. 2 illustrates a flow chart of an example method to protect information stored in a mobile communication device;

Fig. 3 is a block diagram illustrating a computer program product that is arranged to protect information stored in a mobile communication device; and

Fig. 4 is a block diagram illustrating an example computing device that is arranged to protect sensitive data, all arranged in accordance with at least some embodiments of the present disclosure.

DETAILED DESCRIPTION

[0008] Various embodiments are described hereinafter with reference to the figures. It should be noted that the figures are not drawn to scale. It should also be noted that the figures are only intended to facilitate the description of embodiments. They are not intended as an exhaustive description of the disclosure or as a limitation on the scope of the disclosure. In addition, an aspect described in conjunction with a particular embodiment is not necessarily limited to that embodiment and can be practiced in any other embodiments.

[0009] Fig. 1A is a block diagram of a mobile communication device 100, in accordance with at least some embodiments of the present disclosure. The mobile communication device 100 may include a processor unit 102, control circuitry 104, a first memory unit 106, a second memory unit 108, a data security module 110, a first battery unit 112, a second battery unit 114, a sensor 116, and a communication interface 118. The mobile communication device 100 may also include a removable cover, such as a cover 130 (not drawn to scale). Some examples of the mobile communication device 100 may include, without limitation, a smart phone, a tablet device, a laptop computer, a cellular phone, and others.

[0010] For clarity, dotted lines shown in Fig. 1A may correspond to power supplied by the first battery unit 112 and the second battery unit 114, and solid lines shown in Fig. 1A may correspond to data flow among the various illustrated components.

[0011] In some embodiments, the processor unit 102 may be coupled to the sensor 116, the first memory unit 106, the second memory unit 108, and the control circuitry 104. The

control circuitry 104, which may include logic components and a memory controller coupled to the first memory unit 106 and the second memory unit 108 to control erasing/writing/reading to these memory units. The memory units may be coupled to the communication interface 118. The data security module 110 may be coupled to the processor unit 102 and the control circuitry 104. All the components may be coupled to the first battery unit 112, and some or all of the components may be coupled to the second battery unit 114. In the example configuration shown in Fig. 1A, at least the data security module 110, the control circuitry 104, the first memory unit 106, and the second memory unit 108 may be coupled to the second battery unit 114.

[0012] In some other embodiments, the sensor 116 may also be coupled directly to the data security module 110, so that it may be powered by the second battery unit 114. Thus, even if the communication device 100 is turned off normally by its user or if the first battery unit 112 is lost and/or discharged, the sensor 116 may still be functional.

[0013] In some embodiments, the sensor 116 may be configured to detect whether the cover 130 of the mobile communication device 100 has been opened, whether a battery unit has been physically tampered with (e.g., removal or destruction of the first battery unit 112), whether the mobile communication device 100 is outside of its typical coverage area, and other events. Depending on the type of the communication device 100, the range of the typical coverage area may vary. For instance, the communication device 100 may support, without limitation, the third generation of mobile telecommunications technology (3G), the fourth generation of mobile telecommunications technology (4G), Long term Evolution (LTE), Wi-Fi, and Bluetooth. The sensor 116 may be configured to send signals to the processor unit 102 for processing, wherein the signals sent by the sensor 116 may be indicative of these events.

[0014] By applying electromagnetic principals, the sensor 116 may be implemented using an inductive coil micro sensor, and a magnetic, such as ferrite, strip/plate may be installed on the cover 130, so that the magnetic strip/plate may be aligned across this inductive coil micro sensor. Depending on the vicinity of the magnetic strip/plate in relation to the inductive coil sensor, e.g., depending on the cover 130 being opened or closed, the difference in the inducted current may generate the signal corresponding to the “cover open/closed” event.

[0015] Alternatively, the sensor 116 may be implemented using an integrated light-emitting diode (LED)/photo-detector, and a LED/photo-detector reflective strip/plate (e.g., mirror) may be installed on the cover 130, so that the reflective strip/plate may be aligned to the LED/photo-detector. In such a case, opening the cover 130 may result in the loss of the reflected light by photo-detector, which may generate the signal corresponding to the “cover open” event.

[0016] In other embodiments, the sensor 116 may be implemented using an electromechanical micro switch, so that when the cover 130 is opened, the current may flow through the sensor 116, leading to the generation of the signal corresponding to the “cover open” event.

[0017] In some embodiments, the first memory unit 106 and the second memory unit 108 may be configured to store information with varying levels of sensitivity and/or confidentiality. For example, at the time the information is stored in the mobile communication device 100, the person using the mobile communication device 100 may be prompted to assign levels of sensitivity and/or confidentiality to the information to be stored. Depending on the assigned level of sensitivity and/or confidentiality, the information may be stored in different locations. To illustrate, the more sensitive and/or confidential information, such as first information 123 and second information 125 may be stored in the first memory unit 106, and the less sensitive and/or confidential information, such as the third information 127, may be stored in the second memory unit 108. A person's bank account information may be viewed to be more sensitive than the person's haircut appointment information, for example. A person's business proposal may be viewed to be more confidential than a random digital coupon received by the person, for example. In the example configuration of Fig. 1A, the first information 123 may correspond to the personal information of the owner, and the second information 125 may correspond to information of the owner's business. The third information 127 may correspond to information relating to the owner's friends. Additional security and/or confidentiality levels may be assigned within a set of information, such that for instance, the first information 123 may further include sets of information having different security and/or confidentiality levels.

[0018] As an example, suppose the first information 123 is associated with a security level of five (5) and above; the second information 125 is associated with a security level of seven (7) and above; and the third information 127 is associated with a security level of three (3) and below, with relatively higher security and/or confidentiality levels being indicated by

these higher numerical levels and relatively lower security and/or confidentiality levels being indicated by these lower numerical levels. The first information 123 may further include multiple sets of information. One set may include the owner's financial information, such as bank account numbers, credit card numbers, and others, having a security level of 7, for example. Another set may include the owner's identification information, such as his/her driver's license number, passport number, and others, having a security level of 6, for example. The second information 125 may include tax information of the owner's business, for example. The third information 127 may include articles written by the owner's friends, for example.

[0019] Another example of sensitive and/or confidential information may include status history and authentication results associated with the mobile communication device 100. For example, the second information 124 may include status history of the mobile communication device 100 (e.g., how long the mobile communication device 100 may have lost power from the first battery unit 112) and authentication results (e.g., how many times the entry of authentication information prompted by the data security module 110 has failed). Such status history and authentication results may be usable to determine whether to entirely or partially erase the first information 123. Additional details relating to the erasure of information from the mobile communication device 100 will be discussed in the subsequent paragraphs.

[0020] In some embodiments, when a trigger event (e.g., physical tampering of the first battery unit 112, opening of the cover 130 of the mobile communication device 100, leaving the typical coverage area by the mobile communication device 100, and/or others) is detected, and the trigger event is authenticated within a certain period of time, the second battery unit 114 may be configured to supply power to components such as the processor unit 102, the control circuitry 104, the data security module 110, the first memory unit 106, the second memory unit 108, and the communication interface 118. The second battery unit 114 may be placed in a location inside the mobile communication device 100 that is not easily accessible. For example, the second battery unit 114 may not be visible once the cover 130 of the mobile communication device 100 is opened, and accessing the second battery unit 114 may require disassembly of physical parts of the mobile communication device 100. As a result, an unauthorized user of the mobile communication device 100 may not be aware of the existence of the second battery unit 114, and even when he/she is

aware of its existence, he/she may not be able to quickly interrupt the power supplied by the second battery unit 114 to the mobile communication device 100.

[0021] In some embodiments, the first battery unit 112, the second battery unit 114, the first memory unit 106, and/or the second memory unit 108 may be coin-like sized. Fig. 1B is a block diagram illustrating certain physical arrangements of parts in the mobile communication device 100, in accordance with at least some embodiments of the present disclosure. The mobile communication device 100 may have a case 150 and a display screen 152. The cover 130 and the case 150 may form an enclosure for the various parts of the mobile communication device 100, such as, without limitation, a printed circuit board 158, the first memory unit 106 (and/or the second memory unit 108, not shown in Fig. 1B), the first battery unit 112, the second battery unit 114, and other components 160. Opposite from the cover 130, the first memory unit 106 and/or the second battery unit 114 may be placed within a holder 154. The first memory unit 106 and/or the second battery unit 114 may also be sealed, for instance, by epoxy glue. With such an example configuration, time is required to disassemble the mobile communication device 100 to find and remove the first memory unit 106 and/or the second battery unit 114.

[0022] The data security module 110 may be configured to evaluate trigger events and protect the sensitive and/or confidential information of the mobile communication device 100 by potentially instructing the control circuitry 104 to erase certain information from the memory units of the mobile communication device 100. Thus, even if an unauthorized user of the mobile communication device 100 successfully removes the first battery unit 112, this user still may not be able to retrieve any sensitive and/or confidential information. An example process that the data security module 110 may follow to protect the sensitive and/or confidential information of the mobile communication device 100 is illustrated in at least Fig. 2 and detailed in subsequent paragraphs.

[0023] The data security module 110 illustrated in Fig. 1A may be implemented as an Application-Specific Integrated Circuit (ASIC). Alternatively or additionally, the data security module 110 may also be implemented in software or other computer-readable instruction stored on a computer-readable medium (such as the first memory unit 106, the second memory unit 108, or other memory unit) and executable by the processor unit 104, or implemented in a combination of hardware and software. For instance, using the example configuration shown in Fig. 1A, the second memory unit 108 may contain executable instructions for evaluating trigger events and protecting the sensitive and/or confidential

information of the mobile communication device 100. When the executable instructions are executed by the processor unit 102, the processor unit 102 may be configured to process the signals generated by the sensor 116 and interact with the control circuitry 104, the memory units, and/or the communication interface 118. The combination of the executable instructions and the processor unit 102 may support the functions of the data security module 110.

[0024] In the above-mentioned software implementation, since the second memory unit 108 may store both the executable instructions and potentially less sensitive and/or confidential information (e.g., the third information 127), the content of the second memory unit 108 may not be erased entirely when the mobile communication device 100 is determined to have been lost or stolen.

[0025] In conjunction with Fig. 1A, Fig. 2 illustrates a flow chart of an example method 200 to protect information stored in a mobile communication device, in accordance with at least some embodiments of the present disclosure. The method 200 may include one or more operations, functions, or actions as illustrated by one or more of blocks 204, 206, 208, 210, 212, 214 and/or 216. Although the blocks are illustrated in a sequential order, these blocks may also be performed in parallel, and/or in a different order than those described herein. Also, the various blocks may be combined into fewer blocks, divided into additional blocks, and/or eliminated based upon the particular implementation. Additional blocks representing other operations, functions, or actions may be provided.

[0026] The method 200 may begin in block 204 “prompt for authentication information.” Block 204 may be followed by block 208 “timely authenticated?”

[0027] If the received authentication information is timely authenticated, block 208 may also be followed by block 206. Otherwise, block 208 may be followed by block 210 “instruct second battery unit to supply power.” Block 210 may be followed by block 212 “instruct control circuitry to perform action on first set of information,” which may be followed by block 214 “instruct control circuitry to perform action on second set of information.” Block 214 may be followed by block 216 “transmit signal via communication interface.”

[0028] In block 204, the data security module 110 may be configured to prompt for authentication information from a user of the mobile communication device 100. The authentication information may be, for example, a password, a user override command, or

other input from the user to indicate that the detected event is for a legitimate purpose. In one embodiment, the authentication (e.g., password entry) may need to be performed within a particular timeframe and/or within a number of attempts within the particular timeframe.

[0029] In some embodiments, the data security module 110 may be configured to perform the operations of block 204 in response to a trigger event. Some examples of a trigger event may include, without limitation, physical tampering of the first battery unit 112, opening of the cover 130 of the mobile communication device 100, leaving the typical coverage area by the mobile communication device 100, and/or other events. Either the processor unit 102 or the data security module 110 may be configured to process information collected by the sensor 116 and determine whether such a trigger event has been detected or has otherwise occurred.

[0030] If the authentication information received by the mobile communication device 100 is accurate and timely received in block 208, then the data security module 110 may determine that normal operations may continue in block 206, including enabling the user to remove or replace the first battery unit 112 and/or the second battery unit 114 without causing an unintended erasure of data.

[0031] On the other hand, suppose an unauthorized user has figured out the authentication information (e.g., such as a password) but exceeded the required period of time to figure out and enter the password. In block 210, the data security module 110 may be configured to instruct the second battery unit 114 to supply power to the mobile communication device 110. It should be noted that the switch from the first battery unit 112, which may power the mobile communication device 100 when the mobile communication device operates routinely, to the second battery unit 114 may take place irrespective of whether the first battery unit 112 is removed from the mobile communication device 100, so long as the received authentication information is inaccurate and/or the required period of time is expired before receiving the authentication information.

[0032] In block 212, the data security module 110 may be configured to instruct the control circuitry 104 to perform an action on a first set of information (e.g., the first information 123). The action to be performed may include entirely or partially erasing the first information 123 from the first memory unit 106. Erasing the first information 123 (and/or erasing the information from any of the other memory units) may involve redundant overwriting, physical

destruction, reformatting, and/or other operation to remove or to otherwise make the first information 123 unreadable, inaccessible, or unavailable.

[0033] In block 214, the data security module 110 may be configured to instruct the control circuitry 104 to perform an action on a second set of information (e.g., the second information 125). The action to be performed may include entirely or partially erasing the second information 125 from the second memory unit 108.

[0034] In some embodiments, the action performed in block 212 may take place prior to the action performed in block 214, because the sensitivity and/or confidentiality level of the first information 123 may be higher than the level of the second information 125. In other words, the more sensitive and/or confidential information may be erased first.

[0035] In some embodiments, as discussed above, the first information 123 or the second information 125 may include additional levels of sensitivity and/or confidentiality. For example, suppose the first information 123 includes a first subset of information having a higher sensitivity and/or confidentiality level than a second subset of information. In such an arrangement, the first subset of information may be erased ahead of the second subset of information.

[0036] In some embodiments, the action to be performed on the first set of information in block 212 may be based on the second set of information. As discussed above, the second set of information (e.g., the second information 125) may include status history of the mobile communication device 100 (e.g., how long the mobile communication device 100 may have lost power from the first battery unit 112) and authentication results (e.g., how many times the entry of authentication information prompted by the data security module 110 has failed). The data security module 110 may be configured to determine whether to partially or entirely erase the first set of information in block 212 based on such status history and authentication results.

[0037] Through the powered communication interface 118, in block 216, the data security module 110 may be configured to generate and transmit a signal, such as an alert signal or a positional signal, so that the mobile communication device 100, which may have been stolen or lost, may be located. Such signal may be sent to another device of the rightful owner of the mobile communication device, to a service provider, to law enforcement, and/or to some other entity.

[0038] Fig. 3 is a block diagram illustrating a computer program product 300 that is arranged to protect information stored in a mobile communication device, in accordance with at least some embodiments of the present disclosure. Computer program product 300 may include signal bearing medium 304, which may include one or more sets of executable instructions 302 that, when executed by, for example, the processor unit 102 of the mobile communication device 100 of Fig. 1A, may provide at least the features described above and illustrated in Fig. 2.

[0039] In some implementations, signal bearing medium 304 may encompass non-transitory computer readable medium 308 or another similar recordable medium 310, such as, but not limited to, a hard disk drive, a Compact Disc (CD), a Digital Versatile Disk (DVD), a digital tape, memory, etc. In some implementations, signal bearing medium 304 may encompass recordable medium 310, such as, but not limited to, memory, read/write (R/W) CDs, R/W DVDs, etc. In some implementations, signal bearing medium 304 may encompass communications medium 306, such as, but not limited to, a digital and/or an analog communication medium (e.g., a fiber optic cable, a waveguide, a wired communications link, a wireless communication link, etc.)

[0040] FIG. 4 is a block diagram illustrating an example computing device 400 that is arranged to protect sensitive data, in accordance with at least some embodiments of the present disclosure. In a very basic configuration 402, computing device 400 typically includes one or more processors 404 and a system memory 406. A memory bus 408 may be used for communicating between processor 404 and system memory 406.

[0041] Depending on the desired configuration, processor 404 may be of any type including but not limited to a microprocessor (μ P), a microcontroller (μ C), a digital signal processor (DSP), or any combination thereof. Processor 404 may include one more levels of caching, such as a level one cache 410 and a level two cache 412, a processor core 414, and registers 416. An example processor core 414 may include an arithmetic logic unit (ALU), a floating point unit (FPU), a digital signal processing core (DSP Core), or any combination thereof. An example memory controller 418 may also be used with processor 404, or in some implementations memory controller 418 may be an internal part of processor 404.

[0042] Depending on the desired configuration, system memory 406 may be of any type including but not limited to volatile memory (such as RAM), non-volatile memory (such as ROM, flash memory, etc.) or any combination thereof. System memory 406 may include an

operating system 420, one or more applications 422, and program data 424. Application 422 may include a data protection algorithm 426 that is arranged to perform the functions as those described with respect to at least method 200 of Fig. 2. Program data 424 may be useful for operation with data protection algorithm 426 as is described herein. In some embodiments, application 422 may be arranged to operate with program data 424 on operating system 420. This described basic configuration 402 is illustrated in Fig. 4 by those components within the inner dashed line.

[0043] Computing device 400 may have additional features or functionality, and additional interfaces to facilitate communications between basic configuration 402 and any required devices and interfaces. For example, a bus/interface controller 430 may be used to facilitate communications between basic configuration 402 and one or more data storage devices 432 via a storage interface bus 434. Data storage devices 432 may be removable storage devices 436, non-removable storage devices 438, or a combination thereof. Examples of removable storage and non-removable storage devices include magnetic disk devices such as flexible disk drives and hard-disk drives (HDD), optical disk drives such as compact disk (CD) drives or digital versatile disk (DVD) drives, solid state drives (SSD), and tape drives to name a few. Example computer storage media may include volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information, such as computer readable instructions, data structures, program modules, or other data.

[0044] System memory 406, removable storage devices 436 and non-removable storage devices 438 are examples of computer storage media. Computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which may be used to store the desired information and which may be accessed by computing device 400. Any such computer storage media may be part of computing device 400.

[0045] Computing device 400 may also include an interface bus 440 for facilitating communication from various interface devices (e.g., output devices 442, peripheral interfaces 444, and communication devices 446) to basic configuration 402 via bus/interface controller 430. Example output devices 442 include a graphics processing unit 448 and an audio processing unit 450, which may be configured to communicate to various external devices such as a display or speakers via one or more A/V ports 452. Example peripheral

interfaces 444 include a serial interface controller 454 or a parallel interface controller 456, which may be configured to communicate with external devices such as input devices (e.g., keyboard, mouse, pen, voice input device, touch input device, etc.) or other peripheral devices (e.g., printer, scanner, etc.) via one or more I/O ports 458. An example communication device 446 includes a network controller 460, which may be arranged to facilitate communications with one or more other computing devices 462 over a network communication link, such as, without limitation, optical fiber, Long Term Evolution (LTE), 3G, WiMax, via one or more communication ports 464.

[0046] The network communication link may be one example of a communication media. Communication media may typically be embodied by computer readable instructions, data structures, program modules, or other data in a modulated data signal, such as a carrier wave or other transport mechanism, and may include any information delivery media. A “modulated data signal” may be a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media may include wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, radio frequency (RF), microwave, infrared (IR) and other wireless media. The term computer readable media as used herein may include both storage media and communication media.

[0047] Computing device 400 may be implemented as a portion of a small-form factor portable (or mobile) electronic device such as a cell phone, a personal data assistant (PDA), a personal media player device, a wireless web-watch device, a personal headset device, an application specific device, or a hybrid device that include any of the above functions. Computing device 400 may also be implemented as a personal computer including both laptop computer and non-laptop computer configurations.

[0048] There is little distinction left between hardware and software implementations of aspects of systems; the use of hardware or software is generally (but not always, in that in certain contexts the choice between hardware and software can become significant) a design choice representing cost vs. efficiency tradeoffs. There are various vehicles by which processes and/or systems and/or other technologies described herein can be effected (e.g., hardware, software, and/or firmware), and that the preferred vehicle will vary with the context in which the processes and/or systems and/or other technologies are deployed. For example, if an implementer determines that speed and accuracy are paramount, the implementer may opt for a mainly hardware and/or firmware vehicle; if flexibility is

paramount, the implementer may opt for a mainly software implementation; or, yet again alternatively, the implementer may opt for some combination of hardware, software, and/or firmware.

[0049] The foregoing detailed description has set forth various embodiments of the devices and/or processes via the use of block diagrams, flowcharts, and/or examples. Insofar as such block diagrams, flowcharts, and/or examples contain one or more functions and/or operations, it will be understood by those within the art that each function and/or operation within such block diagrams, flowcharts, or examples can be implemented, individually and/or collectively, by a wide range of hardware, software, firmware, or virtually any combination thereof. In one embodiment, several portions of the subject matter described herein may be implemented via Application Specific Integrated Circuits (ASICs), Field Programmable Gate Arrays (FPGAs), digital signal processors (DSPs), or other integrated formats. However, those skilled in the art will recognize that some aspects of the embodiments disclosed herein, in whole or in part, can be equivalently implemented in integrated circuits, as one or more computer programs running on one or more computers (e.g., as one or more programs running on one or more computer systems), as one or more programs running on one or more processors (e.g., as one or more programs running on one or more microprocessors), as firmware, or as virtually any combination thereof, and that designing the circuitry and/or writing the code for the software and or firmware would be well within the skill of one of skill in the art in light of this disclosure. In addition, those skilled in the art will appreciate that the mechanisms of the subject matter described herein are capable of being distributed as a program product in a variety of forms, and that an illustrative embodiment of the subject matter described herein applies regardless of the particular type of signal bearing medium used to actually carry out the distribution. Examples of a signal bearing medium include, but are not limited to, the following: a recordable type medium such as a floppy disk, a hard disk drive, a Compact Disc (CD), a Digital Video Disk (DVD), a digital tape, a computer memory, etc.; and a transmission type medium such as a digital and/or an analog communication medium (e.g., a fiber optic cable, a waveguide, a wired communications link and/or channel, a wireless communication link and/or channel, etc.).

[0050] Those skilled in the art will recognize that it is common within the art to describe devices and/or processes in the fashion set forth herein, and thereafter use engineering practices to integrate such described devices and/or processes into data processing

systems. That is, at least a portion of the devices and/or processes described herein can be integrated into a data processing system via a reasonable amount of experimentation. Those having skill in the art will recognize that a typical data processing system generally includes one or more of a system unit housing, a video display device, a memory such as volatile and non-volatile memory, processors such as microprocessors and digital signal processors, computational entities such as operating systems, drivers, graphical user interfaces, and applications programs, one or more interaction devices, such as a touch pad or screen, and/or control systems including feedback loops and control motors (e.g., feedback for sensing position and/or velocity; control motors for moving and/or adjusting components and/or quantities). A typical data processing system may be implemented utilizing any suitable commercially available components, such as those typically found in data computing/communication and/or network computing/communication systems.

[0051] The herein described subject matter sometimes illustrates different components contained within, or connected with, different other components. It is to be understood that such depicted architectures are merely examples and that in fact many other architectures can be implemented which achieve the same functionality. In a conceptual sense, any arrangement of components to achieve the same functionality is effectively "associated" such that the desired functionality is achieved. Hence, any two components herein combined to achieve a particular functionality can be seen as "associated with" each other such that the desired functionality is achieved, irrespective of architectures or intermedial components. Likewise, any two components so associated can also be viewed as being "operably connected", or "operably coupled", to each other to achieve the desired functionality, and any two components capable of being so associated can also be viewed as being "operably couplable", to each other to achieve the desired functionality. Specific examples of operably couplable include but are not limited to physically mateable and/or physically interacting components and/or wirelessly interactable and/or wirelessly interacting components and/or logically interacting and/or logically interactable components.

[0052] With respect to the use of substantially any plural and/or singular terms herein, those having skill in the art can translate from the plural to the singular and/or from the singular to the plural as is appropriate to the context and/or application. The various singular/plural permutations may be expressly set forth herein for sake of clarity.

[0053] It will be understood by those within the art that, in general, terms used herein, and especially in the appended claims (e.g., bodies of the appended claims) are generally

intended as "open" terms (e.g., the term "including" should be interpreted as "including but not limited to," the term "having" should be interpreted as "having at least," the term "includes" should be interpreted as "includes but is not limited to," etc.). It will be further understood by those within the art that if a specific number of an introduced claim recitation is intended, such an intent will be explicitly recited in the claim, and in the absence of such recitation no such intent is present. For example, as an aid to understanding, the following appended claims may contain usage of the introductory phrases "at least one" and "one or more" to introduce claim recitations. However, the use of such phrases should not be construed to imply that the introduction of a claim recitation by the indefinite articles "a" or "an" limits any particular claim containing such introduced claim recitation to inventions containing only one such recitation, even when the same claim includes the introductory phrases "one or more" or "at least one" and indefinite articles such as "a" or "an" (e.g., "a" and/or "an" should typically be interpreted to mean "at least one" or "one or more"); the same holds true for the use of definite articles used to introduce claim recitations.

[0054] In addition, even if a specific number of an introduced claim recitation *is* explicitly recited, those skilled in the art will recognize that such recitation should typically be interpreted to mean *at least* the recited number (e.g., the bare recitation of "two recitations," without other modifiers, typically means *at least* two recitations, or *two or more* recitations). Furthermore, in those instances where a convention analogous to "at least one of A, B, and C, etc." is used, in general such a construction is intended in the sense one having skill in the art would understand the convention (e.g., "a system having at least one of A, B, and C" would include but not be limited to systems that have A alone, B alone, C alone, A and B together, A and C together, B and C together, and/or A, B, and C together, etc.). In those instances where a convention analogous to "at least one of A, B, or C, etc." is used, in general such a construction is intended in the sense one having skill in the art would understand the convention (e.g., "a system having at least one of A, B, or C" would include but not be limited to systems that have A alone, B alone, C alone, A and B together, A and C together, B and C together, and/or A, B, and C together, etc.). It will be further understood by those within the art that virtually any disjunctive word and/or phrase presenting two or more alternative terms, whether in the description, claims, or drawings, should be understood to contemplate the possibilities of including one of the terms, either of the terms, or both terms. For example, the phrase "A or B" will be understood to include the possibilities of "A" or "B" or "A and B."

[0055] While various aspects and embodiments have been disclosed herein, other aspects and embodiments will be apparent to those skilled in the art. The various aspects and embodiments disclosed herein are for purposes of illustration and are not intended to be limiting, with the true scope and spirit being indicated by the following claims.

I Claim:

1. A mobile communication device, comprising:
 - a data security module;
 - control circuitry;
 - a first memory unit configured to store first information;
 - a first battery unit configured to supply power to the mobile communication device;
 - a second battery unit configured to supply power to the data security module and the control circuitry in response to a trigger event; and
 - the data security module configured to activate the control circuitry to perform a particular action on the first information.
2. The mobile communication device of claim 1, wherein the trigger event corresponds to detection by a sensor of the mobile communication device of an opening of a cover of the mobile communication device.
3. The mobile communication device of claim 2, wherein the trigger event further includes interruption of the power supplied by the first battery unit to the mobile communication device due to physical tampering of the first battery unit.
4. The mobile communication device of claim 1, wherein the particular action comprises a wipe out of the first information entirely or partially or erasing an entire content of the first memory unit based on second information stored in the first memory unit.
5. The mobile communication device of claim 4, wherein the second information comprises status history and a previous authentication result.
6. The mobile communication device of claim 1, wherein the first information comprises a first set of classified information associated with a first sensitivity level and a second set of classified information associated with a second sensitivity level.
7. The mobile communication device of claim 6, wherein the control circuitry is configured to perform the particular action on the first set of classified information ahead of the second set of classified information in response to the first sensitivity level being higher than the second sensitivity level.

8. The mobile communication device of claim 1, wherein the data security module is configured to authenticate information received by the mobile communication device within a period of time before activating the control circuitry to perform the particular action on the first information.
9. The mobile communication device of claim 1, wherein the second battery unit is disposed at a sealed location inside the mobile communication device that is reachable by removal or disassembly of a plurality of internal components located inside of a housing of the mobile communication device.
10. The mobile communication device of claim 1, wherein the data security module is configured to cause the control circuitry to power a communication interface of the mobile communication device to send out positional information of the mobile communication device.
11. The mobile communication device of claim 1, wherein the trigger event corresponds to the mobile communication device being out of communication coverage of a communication network of the mobile communication device.
12. The mobile communication device of claim 1, wherein the data security module is configured to prompt for an input of an authentication information before having the second battery unit supply power to the data security module and the control circuitry.
13. A method to protect sensitive data of a mobile communication device having a data security module, control circuitry, a first memory unit, a first battery unit, and a second battery unit, comprising:
- prompting for an authentication information;
 - after failing to receive the prompted authentication information within a period of time, delivering power of the second battery unit to the data security module and the control circuitry; and
 - using the powered data security module to activate the control circuitry to perform a particular action on a first information stored in the first memory unit, wherein the particular action includes wiping out the first information entirely or partially.

14. The method of claim 13, wherein prompting for the authentication information includes prompting for the authentication information in response to a detected trigger event, and wherein the trigger event corresponds to a sensor of the mobile communication device detecting opening of a cover of the mobile communication device.
15. The method of claim 14, wherein the trigger event further includes power supplied by the first battery unit to the mobile communication device being interrupted due to physical tampering of the first battery unit.
16. The method of claim 13, wherein comprises wiping out the first information entirely includes erasing an entire content of the first memory unit based on a second information stored in the first memory unit.
17. The method of claim 16, wherein the second information comprises status history and a previous authentication result.
18. The method of claim 13, wherein the first information comprises a first set of classified information associated with a first sensitivity level and a second set of classified information associated with a second sensitivity level.
19. The method of claim 18, wherein wiping out the first information entirely or partially includes wiping out the first set of classified information ahead of the second set of classified information in response to the first sensitivity level being higher than the second sensitivity level.
20. The method of claim 13, wherein prompting for the authentication information includes prompting for the authentication information in response to a detected trigger event, and wherein the trigger event corresponds to the mobile communication device being out of communication coverage of a communication network of the mobile communication device.
21. A non-transitory computer readable medium having executable instructions that, in response to execution by a processor, cause the processor to perform a method to protect sensitive or confidential data of a mobile communication device having a data security

module, control circuitry, a first memory unit, a first battery unit, and a second battery unit, the method comprising:

- prompting for an authentication information;
- after failing to receive the prompted authentication information within a period of time, delivering power of the second battery unit to the data security module and the control circuitry; and
- using the powered data security module to activate the control circuitry to perform a particular action on a first information stored in the first memory unit, wherein the particular action includes wiping out the first information entirely or partially.

22. An apparatus, comprising:

- a data security module;
- control circuitry;
- a first memory unit coupled to the control circuitry and configured to store first information; and
- a plurality of internal components coupled to the first memory unit and configured to support mobile communication,
- wherein the first memory unit and at least some of the plurality of internal components are configured to be powered by a first battery unit, and
- wherein the data security module and the control circuitry are configured to be powered by a second battery unit in response to a trigger event, and the data security module is further configured to activate, in response to the trigger event, the control circuitry to perform at least a partial erasure of the first information stored in the first memory unit.

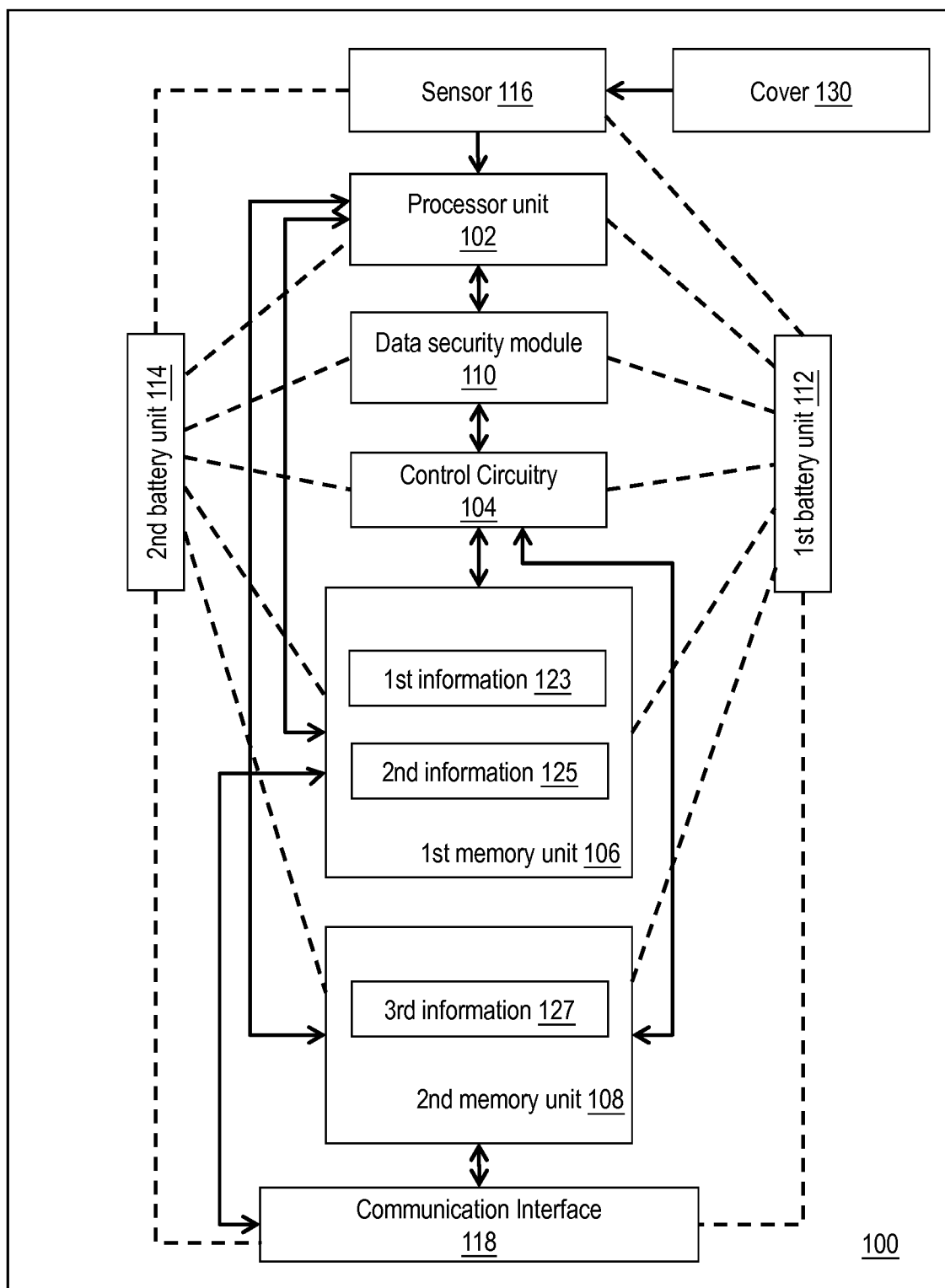
23. The apparatus of claim 22, further comprising:

- a housing having a cover and configured to contain the data security module, the control circuitry, the first memory unit, and the plurality of internal components; and
- a sensor coupled to the cover,
- wherein the trigger event includes an opening of the cover as detected by the sensor and a failure to receive valid authentication information within a timeframe.

24. The apparatus of claim 23, wherein the second battery unit is disposed at a sealed location inside the housing, the sealed location being reachable by removal or disassembly of at least one of the plurality of internal components contained in the housing.

25. The apparatus of claim 24, further comprising:
a printed circuit board; and
a holder coupled to the printed circuit board, wherein at least one of the second battery unit and the first memory unit is sealed within the holder.
26. The apparatus of claim 23, wherein the sensor is one of an inductive micro sensor, an integrated light-emitting diode and photo-detector, and an electromechanical micro switch.

1/5

**Fig. 1A**

100

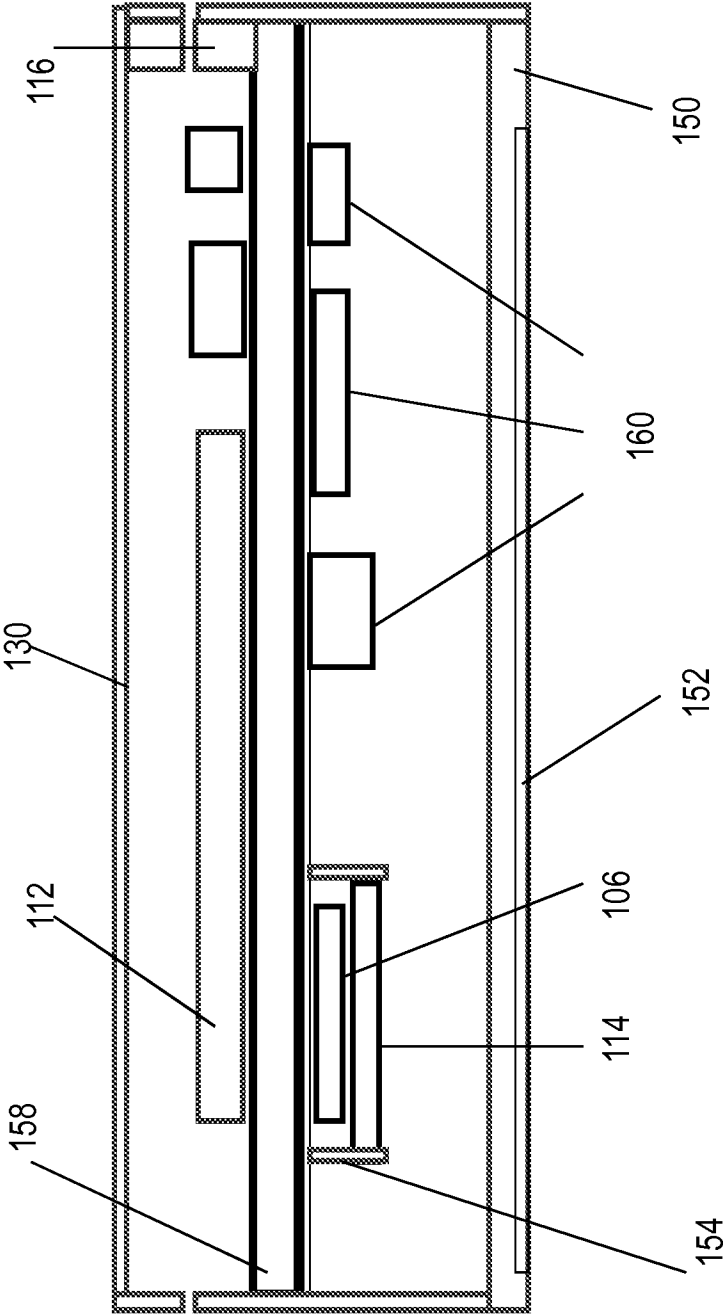
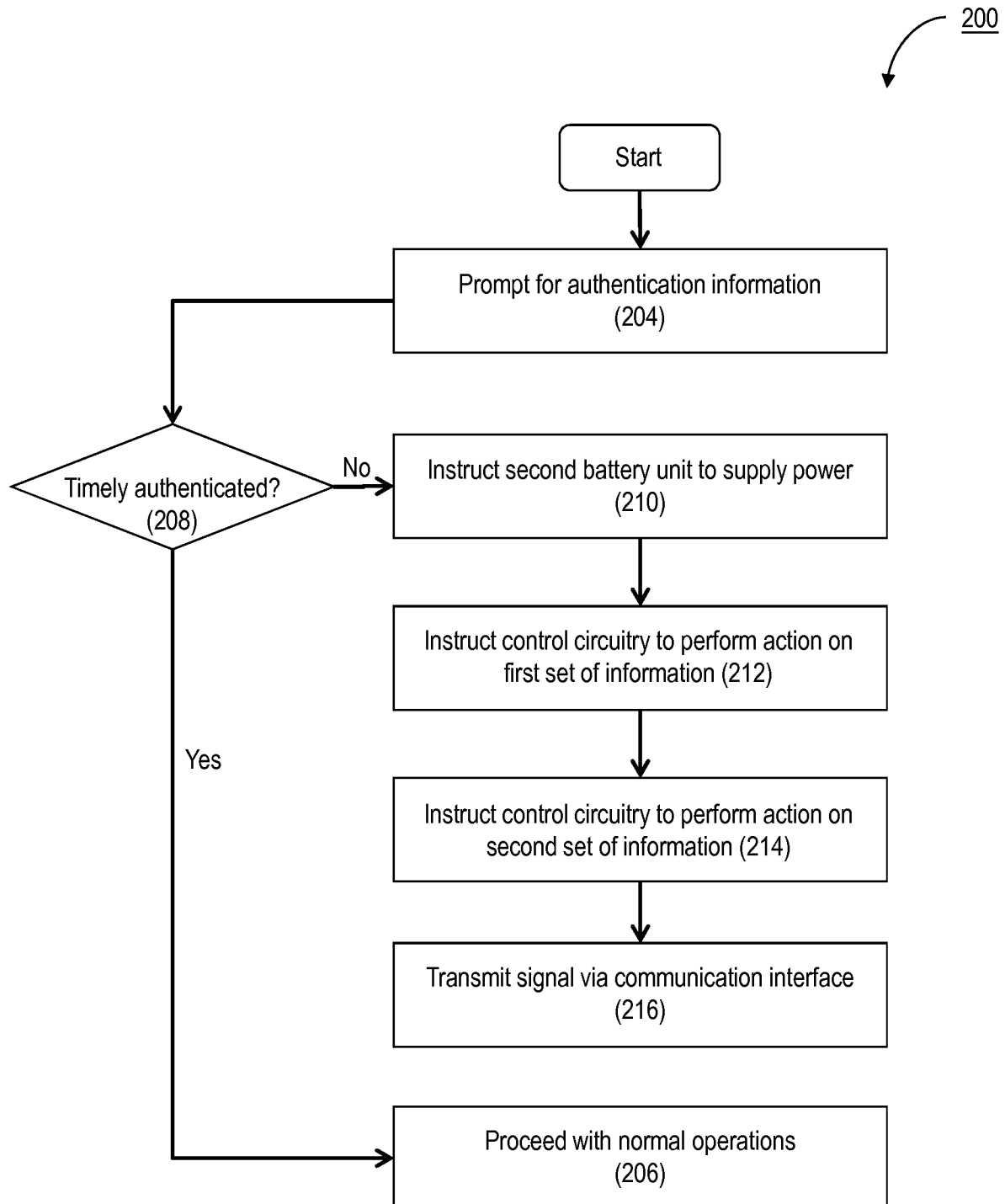
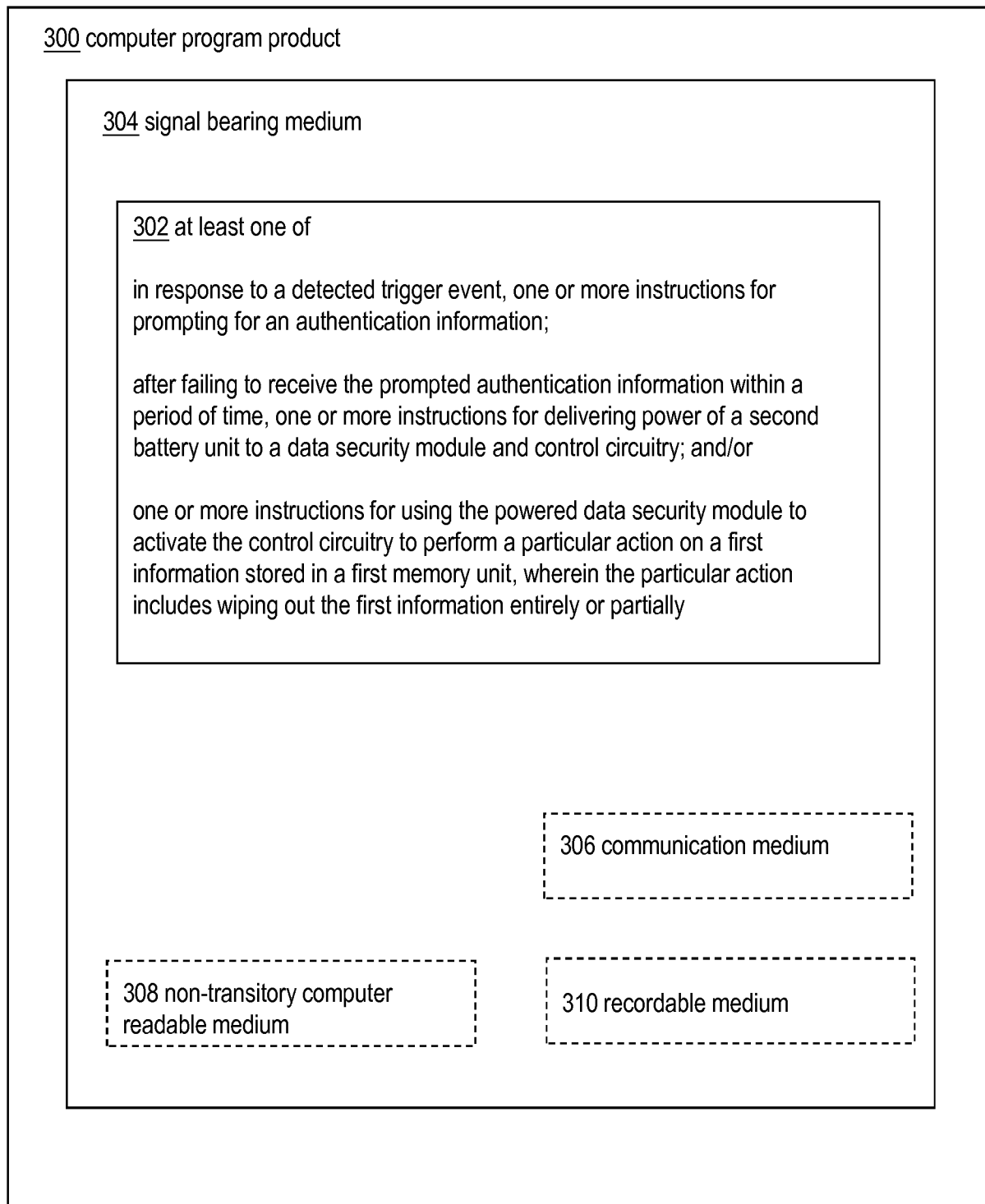


Fig. 1B

3/5

**Fig. 2**

**Fig. 3**

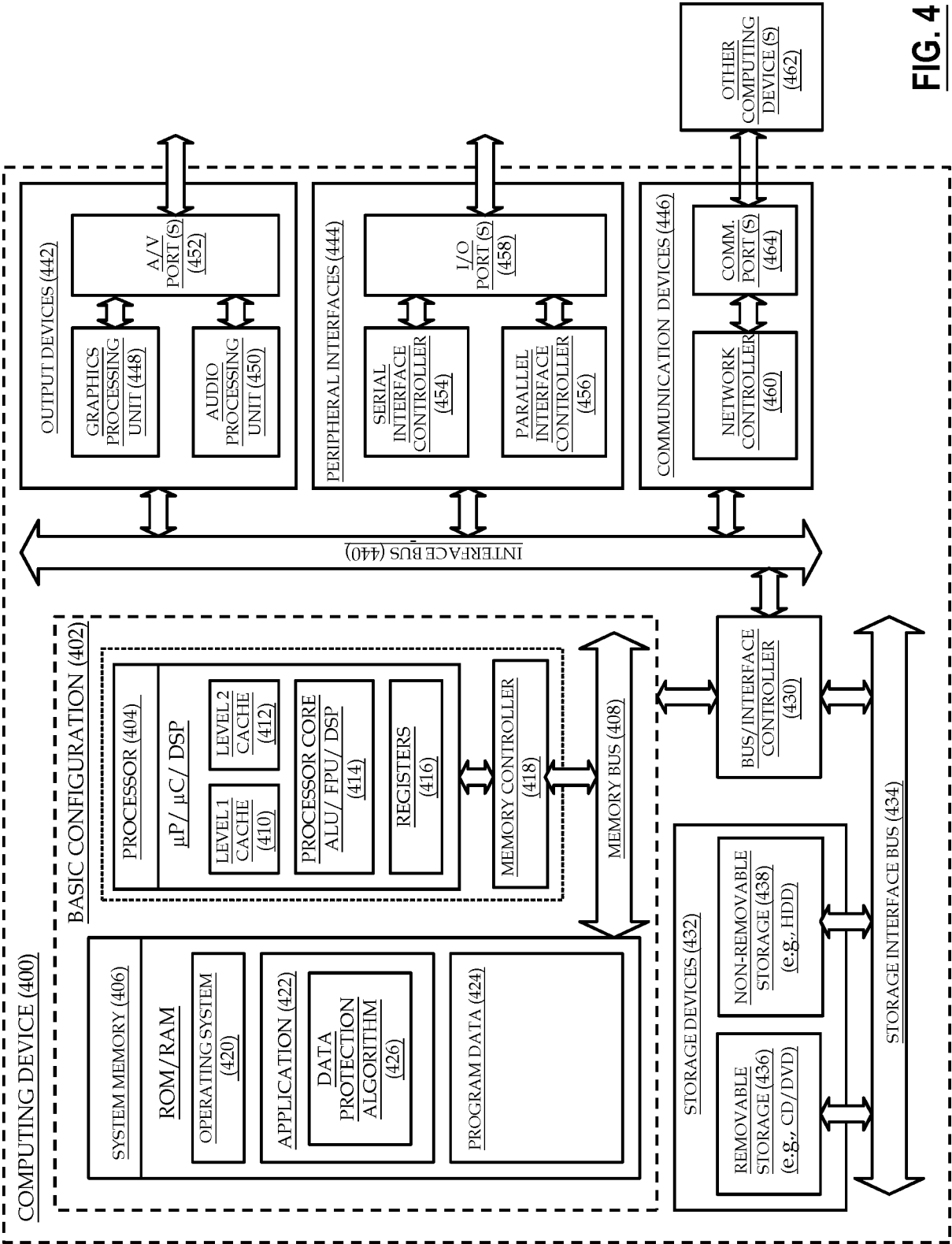


FIG. 4