

(51) International Patent Classification:
G06F 7/04 (2006.01)

(21) International Application Number:

PCT/US2015/033833

(22) International Filing Date:

2 June 2015 (02.06.2015)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/006,801

2 June 2014 (02.06.2014)

US

(71) Applicant: **SCHLAGE LOCK COMPANY LLC**
[US/US]; 2720 Tobey Drive, Indianapolis, IN 46219 (US).(72) Inventors: **RETTIG, Raymond, F.**; 9605 Valley Springs
Blvd., Fishers, IN 46037 (US). **VICKREY, Michelle**;
8615 W. Lockerbie Drive, Indianapolis, IN 46234 (US).
CAHILL, Michael; 801 Walkabout Circle N., 1a, Carmel,
IN 46032 (US).(74) Agent: **SCHEPERS, Brad, A.**; Taft Stettinius & Hollister
LLP, One Indiana Square, Suite 3500, Indianapolis, IN
46204-2023 (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, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR,
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,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR SIGNIFYING INTENT FOR LOCK OPERATION

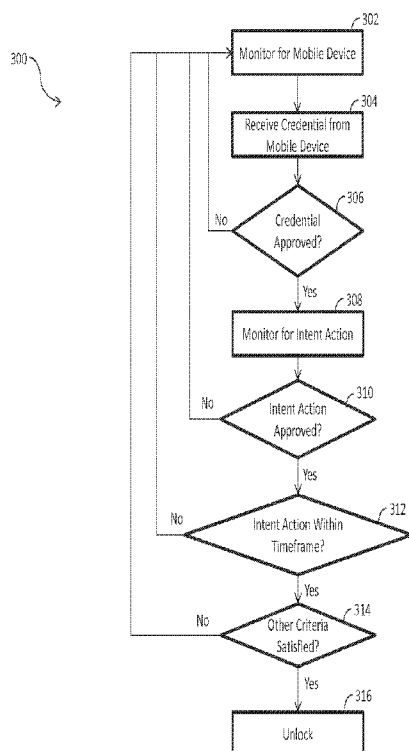


FIG. 3

(57) Abstract: A lock device is configured to receive a credential from a mobile device. The lock device is configured to monitor the distance between the mobile device and the lock device. The lock device is configured to detect an intent action by a user of the mobile device and unlock the lock device if the mobile device is within a predetermined distance from the lock device and the intent action is an approved intent action.

WO 2015/187731 A1



SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, **Published:**
GW, KM, ML, MR, NE, SN, TD, TG).

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

SYSTEM AND METHOD FOR SIGNIFYING INTENT FOR LOCK OPERATION

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims the benefit of U.S. Provisional Patent Application No. 62/006,801 filed on June 2, 2014, the contents of which are hereby incorporated by reference in their entirety.

BACKGROUND

[0002] The present application generally relates to operation of a lock, and more particularly relates to unlocking a lock or access control device with a mobile device. Locks may be unlocked in various ways. Some existing systems have various shortcomings relative to certain applications. Accordingly, there remains a need for further contributions in this area of technology.

BRIEF SUMMARY

[0003] One embodiment of the present invention is directed to a unique system and method for controlling operation of a lock. Other embodiments include apparatuses, systems, devices, hardware, methods, and combinations for controlling operation of a lock. Further embodiments, forms, features, aspects, benefits, and advantages of the present application shall become apparent from the description and figures provided herewith.

BRIEF DESCRIPTION OF THE FIGURES

[0004] The description herein makes reference to the accompanying figures wherein like reference numerals refer to like parts throughout the several views, and wherein:

[0005] FIG. 1 is a schematic block diagram of an exemplary system;

[0006] FIG. 2 is a schematic block diagram of an exemplary computing device; and

[0007] FIG. 3 is a schematic flow diagram of an exemplary process for unlocking a lock device.

DESCRIPTION OF THE ILLUSTRATED EMBODIMENTS

[0008] For the purposes of promoting an understanding of the principles of the invention, reference will now be made to the embodiments illustrated in the drawings and specific language will be used to describe the same. It will nevertheless be understood that no limitation of the scope of the invention is thereby intended, any alterations and further modifications in the illustrated embodiments, and any further applications of the principles of the invention as illustrated therein as would normally occur to one skilled in the art to which the invention relates are contemplated herein.

[0009] The present application is generally directed to signifying intent for operating a lock device or an access control device. FIG. 1 illustrates a system 100 including a lock device 102, a mobile device 104, and a door 106. The lock device 102 is located on or near the door 106 to control access to the area protected by the door 106. The system 100 is configured as an access control system. However, in other embodiments, the system 100 may be a payment system, a transportation system, or any other type of access control system known to those having skill in the art.

[00010] The lock device 102 may be an electronic lock, a reader, a payment terminal, and/or any other type of device that can communicate with the mobile device 104. The lock device 102 may include a transceiver 108 to communicate with a transceiver 110 of the mobile device 104 via a communication protocol such as, for example, Bluetooth, near field communication (NFC), Wi-Fi, and other communication protocols. The lock device 102 may also include a lock mechanism 103 such as, for example, a latch, a bolt, and the like that is used to lock and unlock the lock device 102 for restricting access to the door 106. The lock device 102 may also include an accelerometer 105 to detect an intent action. The intent action may be used, among other information, by the lock device 102 to determine whether the lock device 102 should unlock the lock mechanism 103 so that the user of the mobile device 104 may have access to the area protected by the door 106.

[00011] The mobile device 104 may be a smartphone, a mobile phone, a tablet computer, a watch, smartcard, and/or any other device capable of transmitting a credential 112 to the lock device 102. The credential 112 is capable of indicating to the lock device 102 from a relatively great distance (e.g., several meters) that a user of the mobile device 104 is authorized to access the area protected by the door 106 such as, for example, when the lock device 102 and the

mobile device 104 pair with one another via Bluetooth communication. The credential 112 may be a unique number, a unique identifier, a personal identification number (PIN), an address and/or any other type of information that uniquely identifies the mobile phone 104. In one example, the mobile device 104 may transmit the credential 112 to the lock device 102 in order for the mobile device 104 and the lock device 102 to be paired together using, for example, Bluetooth communication. In this example, the credential 112 constitutes unique information that facilitates pairing or wirelessly connecting the mobile device 104 and the lock device 102.

[00012] In one embodiment, as a user is located relatively close to the door 106, the lock device 102 automatically unlocks the lock mechanism 103. The lock device 102 may connect with the mobile device 104 from a relatively long range (>10m) to determine that the credential 112 is approaching the lock device 102. The lock device 102 can determine that the mobile device 104 is approaching by analyzing the radio signal strength (e.g., received signal strength indicator (RSSI)) received at the lock device 102 or at higher abstracted levels such as Apple's iBeacon technology.

[00013] In some circumstances, a user could walk past a door not intending to unlock the door or lock device such as, for example, when the user is located inside a house and a stranger is located outside of the house. The lock device 102 may use the accelerometer 105 to detect or identify an intent action from a user. The intent action indicates to the lock device 102 to unlock the lock mechanism 103 once the lock device 102 detects or recognizes the user has approached the door 106.

[00014] The accelerometer 105 in the lock device 102 may detect the intent action by the user of the mobile device 104. For example, when the user is located close to the door 106, the lock device 102 may unlock the lock mechanism 103 when the accelerometer 105 detects an intent action (e.g., a specific vibration signature) such as the rotation of a lever on the door 106. Any one or combination of intent actions (e.g., specific vibration signatures) could be sensed such as, for example, rotating a knob or lever on the lock device 102 or the door 106, pressing a thumb-piece on the lock device 102, kicking the door 106, knocking on the door 106, and/or bumping a car key fob to the door 106, among other vibrations or intent actions.

[00015] This technique may be used for approaching the door 106 from either the outside or inside. In some cases, the user may approach the door 106 and be located near it, but may change their mind and stay by the door 106 to talk to a neighbor or change direction and move

away. For these cases, it may not be desirable to allow the lock device 102 to forever be looking for the intent action. This circumstance may be addressed in at least two ways: (1) an intent time window could be constructed so that if the user arrives at the door 106 and does not perform the intent action within a specific amount of time, then the intent action will not be recognized by the lock device 102 to unlock; or (2) the distance between the mobile device 104 and the lock device 102 could be monitored so that if the user is detected as moving away from the door 106, then any intent action will not be recognized by the lock device 102 to unlock.

[00016] Additionally, there are at least two ways to address situations where a stranger approaches the door 106 from the outside and the user approaches the door 106 from the inside. In one embodiment, the system 100 could be designed with a lockout feature where if one or more intent actions (e.g., certain signatures) are detected at the door 106 before the credential 112 arrives at the door 106, then the lock device 102 would ignore the intent action(s) even if the credential 112 comes to the door 106 shortly afterwards. In one example, a stranger comes to the door 106 and knocks. The knock is sensed by the accelerometer 105, but because there is no credential 112 near lock device 102, the lock device 102 disables any response or ignores the intent action. Then, if the user inside hears the knock and approaches the door 106 with the mobile device 104 and credential 112, any further intent actions by the stranger will be ignored or not recognized as an intent action for the lock device 102 to unlock.

[00017] In another embodiment, the lock device 102 may be configured to require two or more intent actions to signify intent within a predetermined timeframe of one another. For example, the lock device 102 could be configured such that the user normally bumps his or her knuckle to the door 106 and then rotates the lever within two (2) seconds. A stranger on the outside would have to do this specific action to gain access.

[00018] In some embodiments, the detection of signatures yields application usage data for doors that have a thumb-piece on the outside of the door and a lever on the inside of the door, which could inform the system if ingress or egress is occurring.

[00019] FIG. 2 is a schematic block diagram of a computing device 200. The computing device 200 is one example of a lock device and/or mobile device that may be utilized in connection with the lock device 102 and/or the mobile device 104 shown in FIG. 1. Computing device 200 includes a processing device 202, an input/output device 204, memory 206, and

operating logic 208. Furthermore, computing device 200 communicates with one or more external devices 210.

[00020] The input/output device 204 allows the computing device 200 to communicate with the external device 210. For example, the input/output device 204 may be a transceiver, network adapter, network card, interface, or a port (e.g., a USB port, serial port, parallel port, an analog port, a digital port, VGA, DVI, HDMI, FireWire, CAT 5, or any other type of port or interface). The input/output device 204 may be comprised of hardware, software, and/or firmware. It is contemplated that the input/output device 204 will include more than one of these adapters, cards, or ports.

[00021] The external device 210 may be any type of device that allows data to be inputted or outputted from the computing device 200. For example, the external device 210 may be a mobile device, lock device, a reader device, equipment, a handheld computer, a diagnostic tool, a controller, a computer, a server, a processing system, a printer, a display, an alarm, an illuminated indicator such as a status indicator, a keyboard, a mouse, or a touch screen display. Furthermore, it is contemplated that the external device 210 may be integrated into the computing device 200. It is further contemplated that there may be more than one external device in communication with the computing device 200.

[00022] Processing device 202 can be a programmable type, a dedicated, hardwired state machine; or a combination of these; and it can further include multiple processors, Arithmetic-Logic Units (ALUs), Central Processing Units (CPUs), Digital Signal Processors (DSPs), or the like. Processing devices 202 with multiple processing units may utilize distributed, pipelined, and/or parallel processing. Processing device 202 may be dedicated to performance of just the operations described herein or may be utilized in one or more additional applications. In the depicted form, processing device 202 is of a programmable variety that executes algorithms and processes data in accordance with operating logic 208 as defined by programming instructions (such as software or firmware) stored in memory 206. Alternatively or additionally, operating logic 208 for processing device 202 is at least partially defined by hardwired logic or other hardware. Processing device 202 can be comprised of one or more components of any type suitable to process the signals received from input/output device 204 or elsewhere, and provide desired output signals. Such components may include digital circuitry, analog circuitry, or a combination of both.

[00023] Memory 206 may be of one or more types, such as a solid-state variety, electromagnetic variety, optical variety, or a combination of these forms. Furthermore, memory 206 can be volatile, nonvolatile, or a combination of these types, and some or all of memory 206 can be of a portable variety, such as a disk, tape, memory stick, cartridge, or the like. In addition, memory 206 can store data that is manipulated by the operating logic 208 of processing device 202, such as data representative of signals received from and/or sent to input/output device 204 in addition to or in lieu of storing programming instructions defining operating logic 208, just to name one example. As shown in FIG. 2, memory 206 may be included with processing device 202 and/or coupled to the processing device 202.

[00024] FIG. 3 illustrates a schematic flow diagram of an exemplary process 300 for unlocking a lock device. Operations illustrated for all of the processes in the present application are understood to be exemplary only, and operations may be combined or divided, and added or removed, as well as re-ordered in whole or in part, unless explicitly stated to the contrary.

[00025] Process 300 begins with operation 302 in which the lock device 102 monitors for a mobile device 104 to connect to wirelessly such as, for example, via Bluetooth communication. It is contemplated that in some embodiments, the mobile device 104 may be monitoring for a lock device 102 to connect to over Bluetooth communication or another protocol.

[00026] Process 300 proceeds from operation 302 to operation 304. At operation 304, during the setup of the wireless connection or after the connection is established between the lock device 102 and the mobile device 104, the mobile device 104 transmits a credential 112 to the lock device 102. In some embodiments, the mobile device 104 may transmit the credential 112 to the lock device 102 as part of the pairing or connecting process. In other embodiments, the mobile device 104 may transmit the credential 112 to the lock device 102 after the two devices are connected or paired.

[00027] Process 300 proceeds from operation 304 to operation 306. At operation 306, the lock device 102 determines whether the credential 112 is valid or authenticates the credential 112. For example, the lock device 102 may determine whether the credential 112 represents a piece of unique information so that the lock device 102 and the mobile device 104 may be paired (e.g., via Bluetooth) or otherwise form a wireless connection. The lock device 102 may also receive the credential 112 after a connection is established and look up in a database whether the credential 112 has sufficient rights to access the door 106. If the credential 112 is approved,

process 300 proceeds to operation 308. If the credential 112 is not approved, process 300 proceeds to operation 302 where the lock device 102 monitors for a mobile device 104.

[00028] At operation 308, the lock device 102 may use the accelerometer 105 to monitor or detect an intent action (e.g., a particular vibration signature) by the user. One or more types of intent actions may be detected such as rotating a lever on the lock device 102 or door 106, pressing a thumb-piece on the lock device 102, kicking the door 106, knocking on the lock device 102 or door 106, bumping a car key fob to the door 106, and/or any other action that the accelerometer 106 may detect. Once the intent action has been received, process 300 proceeds from operation 308 to operation 310. It is contemplated that if no intent action is received within a certain amount of time and/or the mobile device 104 moves away from the lock device 102, process 300 may proceed back to operation 302.

[00029] At operation 310, the lock device 102 determines whether the intent action detected is a valid or approved intent action. The lock device 102 may have a list of valid or approved intent actions that the lock device 102 uses to compare to the intent action detected by the accelerometer 105. It is contemplated that the lock device 102 monitors or analyzes data from the accelerometer 105 to determine whether a valid intent action occurred.

[00030] Process 300 proceeds from operation 310 to operation 312. At operation 312, the lock device 102 determines whether one or more intent action(s) were received within a predetermined timeframe from receipt of the credential 112. For example, if the lock device 102 received the credential 112 from the mobile device 104 when the mobile device 104 was several meters from lock device 102, it may take a user a few seconds walk up to the door 106 and perform an intent action. However, if the user stands near the door 106 for a prolonged period of time without performing an intent action, this may indicate that the user does not wish to access the area protected by the door 106. If the intent action was received within the timeframe, process 300 proceeds from operation 310 to operation 312. If the intent action was not received within the timeframe, then process 300 will proceed to operation 302.

[00031] At operation 314, the lock device 102 may determine whether one or more other criteria are met before deciding whether to unlock the lock mechanism 103. For example, the lock device 102 may ensure that the credential 112 was received before the intent action. In some embodiments, if the lock device 102 receives an intent action before the mobile device 104 approaches the door 106, all subsequent intent actions may be ignored for a period of time.

[00032] In another example, if the lock device 102 does not sense the mobile device 104 approach relatively close to the door 106 before detecting the intent action, the lock device 102 may ignore or disable recognizing intent actions for a period of time.

[00033] In yet another example, the lock device 102 may ensure that the mobile device 104 does not come closer to the lock device 102 and then move further away from the lock device 102, which may in turn indicate that the user does not wish to access the area protected by the door 106.

[00034] In another example, the lock device 102 may be configured to require two or more intent actions to signify intent within a predetermined timeframe of one another.

[00035] Other types of criteria are also contemplated. If the other criteria are satisfied, process 300 proceeds from operation 314 to operation 316. If the other criteria are not satisfied, process 300 proceeds from operation 314 to operation 302.

[00036] At operation 316, the lock device 102 unlocks the lock mechanism 103 to allow the user of the mobile device 104 access to the area protected by the door 106.

[00037] It is contemplated that in some embodiments, the mobile device 104 may be considered to be the credential 112.

[00038] While the invention has been illustrated and described in detail in the drawings and foregoing description, the same is to be considered as illustrative and not restrictive in character, it being understood that only certain exemplary embodiments have been shown and described and that all changes and modifications that come within the spirit of the inventions are desired to be protected.

[00039] In reading the claims, it is intended that when words such as “a,” “an,” “at least one,” or “at least one portion” are used there is no intention to limit the claim to only one item unless specifically stated to the contrary in the claim. When the language “at least a portion” and/or “a portion” is used the item can include a portion and/or the entire item unless specifically stated to the contrary.

CLAIMS

1. A method, comprising:
receiving, with a lock device, a credential from a mobile device;
monitoring, with the lock device, a distance of the mobile device from the lock device;
detecting, with the lock device, an intent action by a user of the mobile device; and
unlocking the lock device if the mobile device is within a predetermined distance from the lock device and the intent action is an approved intent action.
2. The method of claim 1, wherein the lock device and the mobile device communicate via Bluetooth communication.
3. The method of claim 1, wherein the mobile device is a smartphone.
4. The method of claim 1, wherein the credential must be received by the lock device before the intent action is detected by the lock device in order for the lock device to unlock.
5. The method of claim 1, wherein the credential must be received and the intent action must be detected within a predetermined timeframe.
6. The method of claim 1, wherein the lock device includes an accelerometer structured to detect the intent action of the user.
7. The method of claim 1, wherein the intent action includes at least one of rotating a lever, pressing a thumbpiece on the lock device, kicking a door, knocking on the door, and bumping a car key fob to the door.
8. The method of claim 1, further comprising:
ignoring all subsequent intent actions for a period of time if a first intent action was received by the lock device before the credential.

9. The method of claim 1, wherein the lock device is structured to require two or more intent actions within a predetermined period of time to unlock.

10. An apparatus, comprising:
a lock device configured to receive a credential from a mobile device, monitor a distance between the mobile device and the lock device, detect an intent action by a user of the mobile device, and unlock a lock mechanism of the lock device if the mobile device is within a predetermined distance from the lock device and the intent action is an approved intent action.

11. The apparatus of claim 10, wherein the lock device and the mobile device communicate via Bluetooth communication.

12. The apparatus of claim 10, wherein the credential must be received by the lock device before the intent action is detected by the lock device in order for the lock device to unlock.

13. The apparatus of claim 10, wherein the credential must be received and the intent action must be detected within a predetermined timeframe.

14. The apparatus of claim 10, wherein the lock device includes an accelerometer structured to detect the intent action of the user.

15. The apparatus of claim 10, wherein the intent action includes at least one of rotating a lever, pressing a thumbpiece on the lock device, kicking a door, knocking on the door, and bumping a car key fob to the door.

16. The apparatus of claim 10, wherein the lock device is further configured to ignore all subsequent intent actions for a period of time if a first intent action was received by the lock device before the credential.

17. The apparatus of claim 10, wherein the lock device is structured to require two or more intent actions within a predetermined period of time to unlock.

18. A system, comprising:
a smartphone; and
a lock device configured to receive a credential from the smartphone, monitor a distance between the smartphone and the lock device utilizing a received signal strength indicator, detect an intent action by a user of the smartphone utilizing an accelerometer, and unlock a lock mechanism of the lock device if the smartphone is within a predetermined distance from the lock device and the intent action is an approved intent action.

19. The system of claim 18, wherein the intent action includes at least one of rotating a lever, pressing a thumbpiece on the lock device, kicking a door, knocking on the door, and bumping a car key fob to the door.

20. The system of claim 18, wherein the smartphone is the credential.

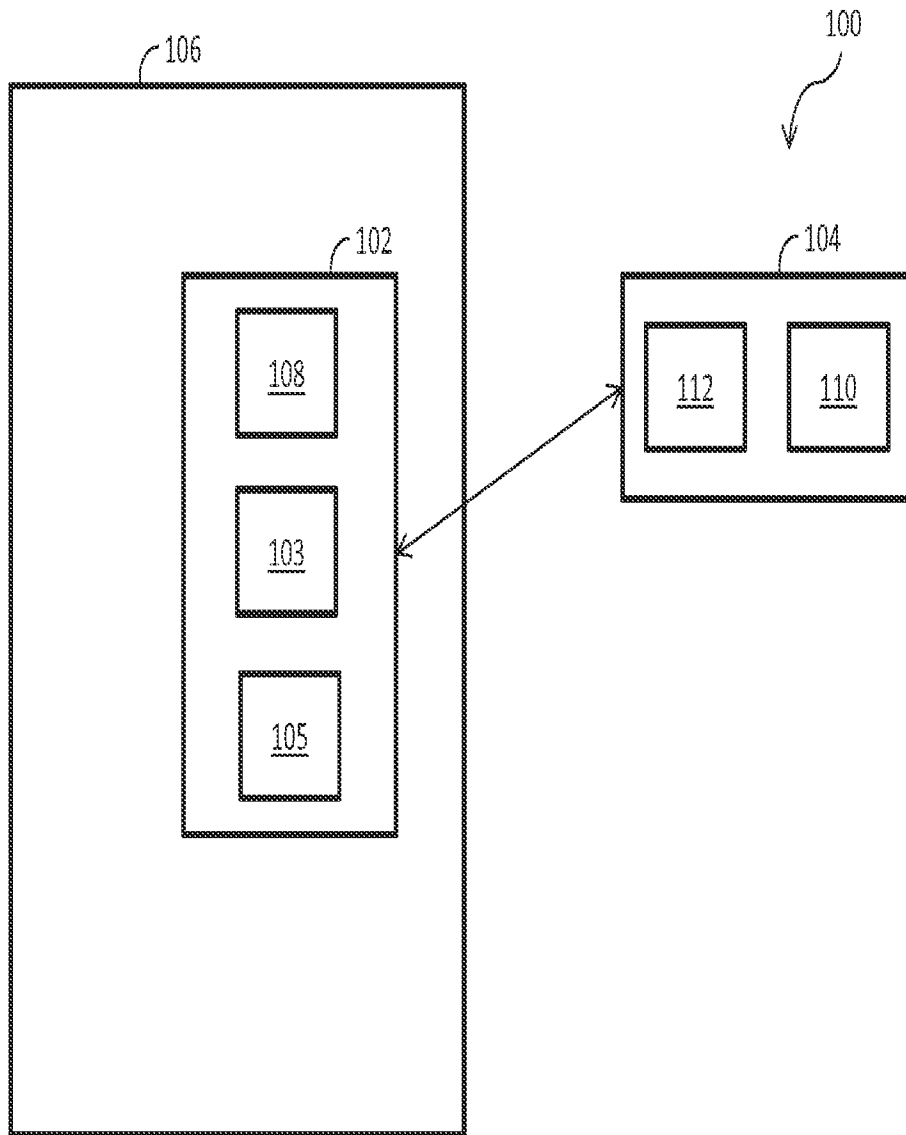
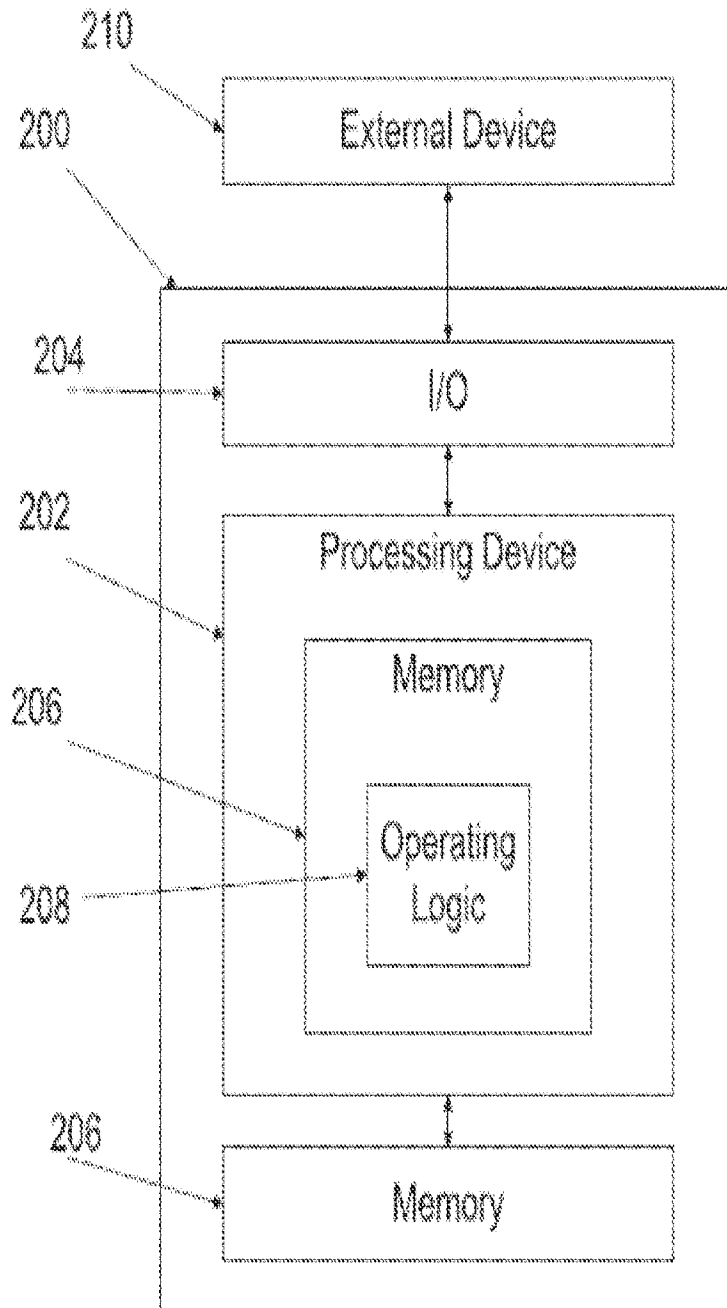


FIG. 1

FIG. 2



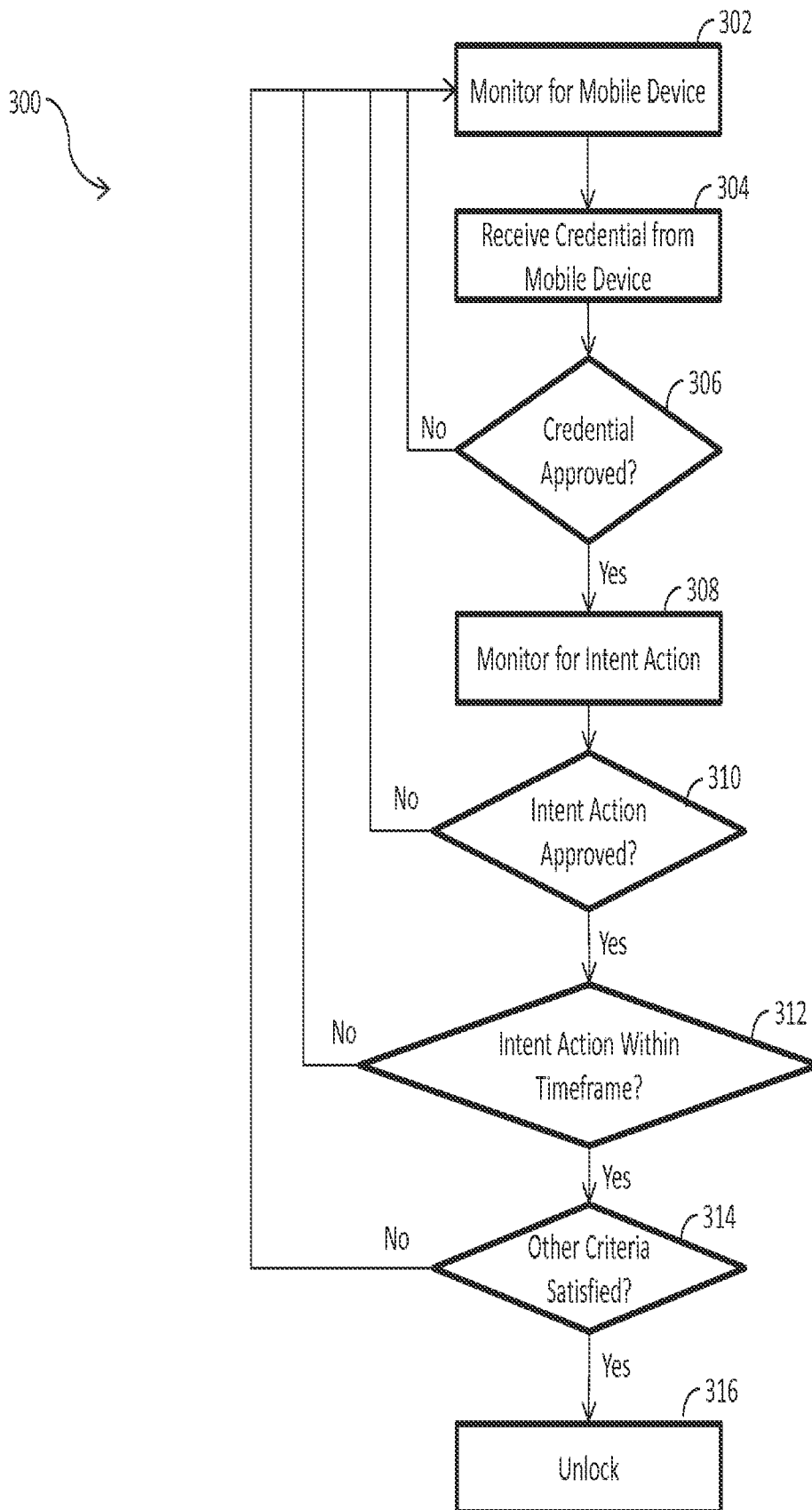


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 15/33833

A. CLASSIFICATION OF SUBJECT MATTER IPC(8) - G06F 7/04 (2015.01) CPC - H04L63/10 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) CPC: H04L63/10; IPC(8): G06F 7/04 (2015.01); USPC: 726/2 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched CPC: H04L63/08, G06F21/6218, G06F21/31, H04L63/083, H04L63/10; USPC: 340/5.6, 340/5.7, 340/5.27, 340/5.5, 340/5.28, 340/5.73, 713/156, 726/2, 713/162, 726/26 (keyword limited; terms below) Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) PatBase; Google Scholar Search Terms: lock, credential, smartphone, iPhone, Blackberry, Android, distance, proximity, near, close, intent, unlock, etc.		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/0077929 A1 (DUMAS et al.) 20 March 2014 (20.03.2014), entire document, especially abstract and para [0050]-[0054], [0056]-[0058], [0061]-[0064], [0070], [0087], [0106], [0116], [0125]-[0127], [0130]-[0131], [0135], Fig. 1, Fig. 6a, Fig. 6b, Fig. 7a, Fig. 17.	1-20
A	US 2012/0234058 A1 (NEIL et al.) 20 September 2012 (20.09.2012), entire document.	1-20
A	US 2013/0257589 A1 (MOHIUDDIN et al.) 03 October 2013 (03.10.2013), entire document.	1-20
☐ Further documents are listed in the continuation of Box C. ☐		
* 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 29 July 2015 (29.07.2015)		Date of mailing of the international search report 03 SEP 2015
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300		Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774