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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 October 2017 (26.10.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/184513 A1

(51) International Patent Classification:
G07C 9/00 (2006.01) *H04M 1/725* (2006.01)

(21) International Application Number:
PCT/US2017/027938

(22) International Filing Date:
17 April 2017 (17.04.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/324,484 19 April 2016 (19.04.2016) US

(71) Applicant: **SPECTRUM BRANDS, INC.** [US/US]; 3001 Deming Way, Middleton, Wisconsin 53562 (US).

(72) Inventor: **BROWN, Troy M.**; 197 Woodcrest Lane, Aliso Viejo, California 92656 (US).

(74) Agent: **WEVER, Michael E.**; BARNES & THORNBURG LLP, 888 S. Harrison Street, Suite 600, Fort Wayne, Indiana 46802 (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, 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).

(54) Title: LOCKSET WITH INTEGRATED WIRELESS SIGNALS ANALYSIS FEATURE AND METHOD

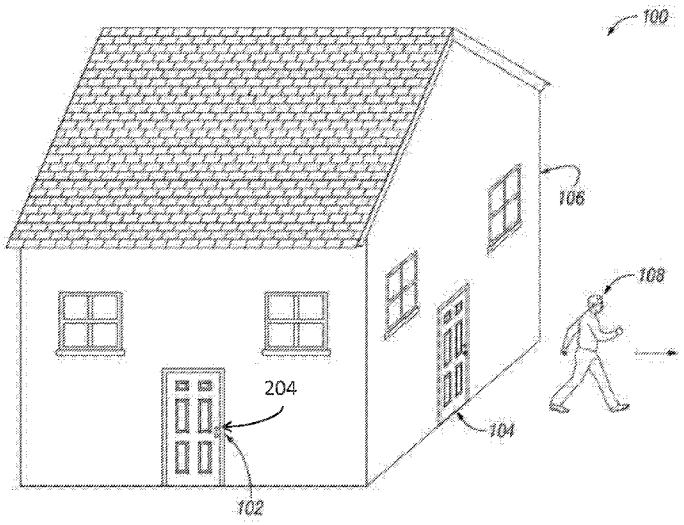

Figure 1

(57) Abstract: A wireless lockset with integrated wireless signals analysis and method is described herein. The analysis integrated into the wireless lockset allows remote monitoring of a building or dwelling. A user can track and be notified of the state of occupancy of a dwelling based upon when specific un-associated devices that are within range of the lockset.

WO 2017/184513 A1

[Continued on next page]

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

LOCKSET WITH INTEGRATED WIRELESS SIGNALS ANALYSIS FEATURE AND METHOD

Related Applications

[0001] This application claims priority to U.S. Application No. 62/324,484, filed April 19, 2016, which is hereby incorporated herein by reference in its entirety.

Technical Field

[0002] The present disclosure relates generally to locking devices; in particular, this disclosure relates to an electronic locking device for wirelessly detecting known and unknown devices.

Background

[0003] Electronic locking systems are in widespread use in residential and commercial markets. In some cases, electronic locks control mechanical locking assemblies, such as movement of a deadbolt between its extended and retracted positions. These locking systems control ingress through doors in a building by requiring certain credentials. These credentials may include keyed or keyless entry types. Some keyless entry types include a keypad in which a user may gain access by entering a code. In some cases, for example, the credentials and/or commands may be provided wirelessly to a lockset, such as disclosed in U.S. Patent No. 9,024,759 for a "Wireless Lockset With Integrated Antenna, Touch Activation, and Light Communication Method," filed March 10, 2014 and U.S. Pre-Grant Publication No. 2012/0234058 for a "Wireless Access Control System and Related Methods," filed March 8, 2012, both of which are hereby incorporated by reference.

[0004] Many existing electronic locks include a notification feature. The notification feature typically allows a user with administrator privileges to be notified, such as with a text message, email, etc., when other users operate the lock. For example, when a user unlocks

the electronic lock, the administrator user may receive a text message or email that someone operated the lock, and in some cases, which user has operated the lock.

[0005] Although this type of notification feature allows limited remote monitoring, there are several challenges. One challenge is that the remote monitoring is limited to the door on which the electronic lock is installed. Typically, there may be many entrances to a building and no notification will be generated if a user enters/exits through an entrance not having the electronic lock installed. Another challenge is that existing electronic locks require pairing of devices (e.g., key fob, smartphone app, etc.) with the electronic lock to determine which user is operating the lock.

Summary

[0006] According to the present disclosure, a door lock system is provided that periodically scans and analyzes devices within a certain range of the door lock hardware system. In one exemplary embodiment, the door lock hardware system may include a radio that periodically scans and analyzes all known and unknown devices within a specific range of the door lock hardware system. All devices, known or unknown, may be assigned an identification code that is presented to a user via a graphical user interface. The user may adjust settings to pick and choose which devices to have tracked by the door lock hardware system using the graphical user interface. In a further embodiment, the user may adjust settings to pick and choose which devices trigger notifications by the door lock system to the user or another user. Other actions may be triggered in response to the detection of devices, known or unknown, within range of the door lock hardware.

Brief Description of the Figures

[0007] The detailed description makes references to the accompanying figures in which:

[0008] Figure 1 is an exemplary environment in which a lock assembly may operate according to one embodiment of this disclosure;

[0009] Figure 2 is a simplified block diagram of an example system for determining proximate devices within range of the lock assembly according to an embodiment of this disclosure;

[00010] Figure 3 is a side view of an electronic lock assembly and corresponding hardware in accordance with an embodiment of the present disclosure, installed on a door and with the door shown in phantom lines;

[00011] Figure 4 is a flow diagram of an example method for determining a list of devices within a proximate range of the lock hardware according to an embodiment of this disclosure;

[00012] Figure 5 is a flow diagram of an example method for the triggering alert notifications based on predefined user settings according to an embodiment of this disclosure;

[00013] Figure 6 is a flow diagram of an example method for a user receiving a list of devices and creating user settings for alert notifications according to an embodiment of this disclosure; and

[00014] Figure 7 is a simplified block diagram of an exemplary computing environment in connection with at least one embodiment of the lock assembly of Figure 1.

Detailed Description

[00015] The figures and descriptions provided herein may have been simplified to illustrate aspects that are relevant for a clear understanding of the herein described devices, systems, and methods, while eliminating, for the purpose of clarity, other aspects that may be found in typical devices, systems, and methods. Those of ordinary skill may recognize that other elements and/or operations may be desirable and/or necessary to implement the devices, systems, and methods described herein. Because such elements and operations are well

known in the art, and because they do not facilitate a better understanding of the present disclosure, a discussion of such elements and operations may not be provided herein. However, the present disclosure is deemed to inherently include all such elements, variations, and modifications to the described aspects that would be known to those of ordinary skill in the art.

[00016] References in the specification to "one embodiment," "an embodiment," "an illustrative embodiment," etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but every embodiment may or may not necessarily include that particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to effect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described. Additionally, it should be appreciated that items included in a list in the form of "at least one of A, B, and C" can mean (A); (B); (C); (A and B); (A and C); (B and C); or (A, B, and C). Similarly, items listed in the form of "at least one of A, B, or C" can mean (A); (B); (C); (A and B); (A and C); (B and C); or (A, B, and C).

[00017] In the drawings, some structural or method features may be shown in specific arrangements and/or orderings. However, it should be appreciated that such specific arrangements and/or orderings may not be required. Rather, in some embodiments, such features may be arranged in a different manner and/or order than shown in the illustrative figures. Additionally, the inclusion of a structural or method feature in a particular figure is not meant to imply that such feature is required in all embodiments and, in some embodiments, may not be included or may be combined with other features.

[00018] Referring now to the drawings and particularly to Figure 1, there is shown an exemplary environment in which a locking assembly 204 may operate according to an embodiment of this disclosure. A typical environment 100 may include a single dwelling 106. In other embodiments, the environment may include multiple dwellings in close proximity with one another, such as an apartment complex, one or more townhomes and/or commercial building. Typically, the dwelling may include more than one entryway. For example, the dwelling 106 may include a front door 102, a side door 104, another door in the rear of the dwelling (not shown), a door coming in from a garage (not shown), and/or other doors providing ingress/egress to the dwelling 106. One advantage of the lock assembly 204 is that it only needs to be installed on one of the doors while monitoring other doors that provide ingress/egress to the dwelling 106. Consider an example in which the lock assembly 204 is installed on the front door 102. Even though a user 108 is shown leaving the dwelling 106 using the side door 104, which is a door that does not have the lock assembly 204 installed, the user 108 may still be detected by the locking assembly 204 on the front door 102 as leaving the dwelling 106 from the side door 104. As described below, the lock assembly 204 can detect the user by wirelessly scanning for devices in proximity such as a user carrying a wireless device (e.g., a smart phone, key fob, etc.), which is detected by the lock assembly 204 installed on the front door 102 using, for example, an integrated radio. The lock assembly 204 is shown installed on the front door 102 for purposes of example, but could be installed on any door in the dwelling 106.

[00019] Referring now to Figure 2, there is shown an example system configuration 200 for synchronizing information. In the example shown, the system includes a user device 202 that may receive proximate device list information determined by and from the lock assembly 204, via a network 206. The network 206 may be any type of network known to one of ordinary skill, such as a local area network or the Internet. The lock assembly 204

may include a wireless communication module (see Figure 7) that facilitates wireless communications with the user device 202 through a desired wireless communications protocol. In an another embodiment, the user device 202 may synchronize directly with the lock assembly 204 using an any desired protocol, such as Bluetooth™, Zigbee™, or Z-wave™.

[00020] Referring now to Figure 3, there is shown an example electronic lock 300 in accordance with an embodiment of the present disclosure for mounting on a door 302, which includes an interior chassis 304, a removable cover 306, a manual turnpiece 308, a bolt 310, a face plate 312, user input 314, an exterior chassis 316, mechanical locking assembly 318, and a removable key 320. The interior chassis 304 may include the electronic circuitry for an integrated radio. The integrated radio may have the ability to scan one or more frequency bands for the detection of proximate devices, such as smart phones, PDAs, key fobs, or the like. The integrated radio may typically use Bluetooth or Wi-Fi for the scanning of proximate devices. Additional devices, such as LED's, switches, other integrated circuits, antenna and others are designed into the electronic circuitry. The door lock assembly 204 may be installed on the exterior portion of the door, the interior, or a combination of exterior/interior installation.

[00021] Figure 4 is a simplified flow chart showing an example of the integrated radio of the door hardware performing a scan for proximate devices and compiling a list of detected devices. In this example, the method 400 begins with block 402 by periodically scanning for devices. The integrated radio may scan a frequency band, or bands, of interest and record the unique signatures of any other wireless device in that same frequency band. In step 404, if no devices are detected, the process restarts at block 402. If any devices are detected, the process moves to step 406. In step 406, a list of devices is created. For each device, the integrated radio may assign a unique identification code. Each device may also

be categorized with certain characteristics. These characteristics may include, but are not limited to, ID, name, range, time of detection, dwell time, device type, and operating system. In some embodiments, the system attempts to identify as many characteristics as possible of the detected devices, especially in instances where a device is an unknown device. The characteristics may be saved, along with the device list, within a memory of the lock assembly 204. The device list may be saved within the memory of the lock assembly 204 for a certain period of time, such as 24 hours, a week, a month, or the like, to provide a history of detected proximate devices. The history may also be saved to a cloud server for access by the user device 202 at a later time. After the list is determined, the process moves to step 408 and the list may be sent to a cloud server for synchronization of a user device, such as a user's smartphone. In another embodiment, the list may be synchronized with a user's device when the user's device comes within a certain proximity of the lock assembly 204, such as using a near field communications protocol (e.g., Bluetooth™, etc.). In step 410, the user may decide, after viewing the list of devices to create notifications, which is described in further detail below in conjunction with Figure 6.

[00022] Figure 5 is a simplified flowchart showing an example of alert notifications being triggered based on the detection of certain devices. In this example, the method 500 starts with step 502, the reception of the device list, which could be, for example, the list created in Figure 4, step 408. The reception may be made either at a remote server, or locally within the hardware of the lock assembly itself 204. In step 504, the device list is analyzed based on user settings created by a user, which is described in further detail below in conjunction with Figure 6. In step 506, the lock assembly 204 determines, for each device in the list, whether an alert should be triggered. If no alerts are to be triggered, the process goes back to start. If alerts are to be triggered, the process moves to step 510 and the appropriate alert, or notification, is sent. For example, a user may want to be notified when their child's

cell phone is within range of the lock assembly 204. A user, therefore, creates a setting to be notified when the child's device is on the list of devices and may receive an appropriate notification (e.g., SMS, text, email, etc.). In another exemplary embodiment, a user may choose to be notified every time an unknown, or new, device is determined to be within range of the lock hardware. Once an unknown, or new, device is determined to be on the list, the user may be notified accordingly (e.g., SMS, text, email, etc.). Even further, the lock assembly 204 may be in communication with a home automation system. So while the user may be notified of the unknown device, a command may also be triggered to the home automation system to lock all doors/windows or even close an open garage door.

[00023] Figure 6 is a simplified flowchart showing an example from a user's point of view utilizing a user device having a software application that interacts, either directly or indirectly, with the lock assembly 204. In this example, the process 600 starts with step 602 and receiving a device list which may be viewed on a screen of the user's device via a software application, or "app." The device list essentially represents the state of occupancy of a certain dwelling, such as all of the devices within a certain range of the dwelling 106 of Figure 1. In step 604, the user may decide to update or create settings to establish notifications and/or alerts to occur when devices are detected within a certain proximity of the lock assembly 204. If the user elects not to make any changes, the process moves back to step 602. If the user elects to make changes, the process moves to step 606 to update/create alerts. As mentioned above, the user may elect to receive certain notifications (e.g., SMS, text, email) when certain devices are determined to be within range of the lock hardware. Other settings may be established as well; for example, the proximity range to being a certain area, based on the size of the dwelling, or command settings to be sent to a home automation system based on certain detected devices. Once settings are complete, the process moves to

step 608 and the elected alerts/notifications are saved. In step 610, the saved alerts/notifications may be synchronized with a cloud server and/or the lock assembly 204.

[00024] Referring now to Figure 7, a simplified block diagram of an exemplary computing environment 700 for the lock assembly 204, in which the door lockset application, is shown. The illustrative implementation 700 includes a lock assembly 204, which may be in communication with one or more other computing systems or devices 742 via one or more networks 740. As shown, the lock assembly 204 comprises storage media 720.

[00025] The illustrative lock assembly 204 includes at least one processor 712 (e.g. a microprocessor, microcontroller, digital signal processor, etc.), memory 714, and an input/output (I/O) subsystem 716. Although not specifically shown, it should be understood that the I/O subsystem 716 may include, among other things, an I/O controller, a memory controller, and one or more I/O ports. The processor 1012 and the I/O subsystem 716 are communicatively coupled to the memory 714. The memory 714 may be embodied as any type of suitable computer memory device (e.g., volatile memory such as various forms of random access memory).

[00026] The I/O subsystem 716 is communicatively coupled to a number of components including one or more user input devices 718 (e.g., a touchscreen, keyboard, virtual keypad, microphone, etc.), one or more storage media 720, one or more output devices 722 (e.g., speakers, LEDs, etc.), one or more sensing devices 724, 726, 728, one or more camera or other sensor applications 730 (e.g., software-based sensor controls), and one or more network interfaces 732.

[00027] The storage media 720 may include one or more hard drives or other suitable data storage devices (e.g., flash memory, memory cards, memory sticks, and/or others). In some embodiments, portions of systems software (e.g., an operating system, etc.), framework/middleware (e.g., APIs, object libraries, etc.). Portions of systems software or

framework/middleware may be copied to the memory 714 during operation of the computing device 710, for faster processing or other reasons.

[00028] The one or more network interfaces 732 may communicatively couple the computing device 710 to a network, such as a local area network, wide area network, personal cloud, enterprise cloud, public cloud, and/or the Internet, for example. Accordingly, the network interfaces 732 may include one or more wired or wireless network interface cards or adapters, for example, as may be needed pursuant to the specifications and/or design of the particular computing system 700. The network interface(s) 732 may provide short-range wireless or optical communication capabilities using, e.g., Near Field Communication (NFC), wireless fidelity (Wi-Fi), radio frequency identification (RFID), infrared (IR), or other suitable technology. Further, the wireless communications may use the Zigbee or Z-Wave protocols.

[00029] The other computing system(s) 742 may be embodied as any suitable type of computing system or device such as any of the aforementioned types of devices or other electronic devices or systems. For example, in some embodiments, the other computing systems 742 may include one or more server computers used to store portions of the data stored in storage media 720. Further, computing device 742 may further include application 744 to provide an interface for display to a user to implement the embodiments of the disclosure set forth. The computing system 700 may include other components, sub-components, and devices not illustrated in Figure 7 for clarity of the description. In general, the components of the computing system 700 are communicatively coupled as shown in Figure 7 by electronic signal paths, which may be embodied as any type of wired or wireless signal paths capable of facilitating communication between the respective devices and components.

EXAMPLES

[00030] Illustrative examples of the wireless lockset with integrated wireless signals disclosed herein are provided below. An embodiment of the wireless lockset may include any one or more, and any combination of, the examples described below.

[00031] Example 1 is a system including an electronic lock for use with a mobile device. The system includes a locking device movable between a locked position and an unlocked position and an electronic lock with an integrated radio. The electronic lock configured to: scan a proximate area for known and unknown devices, wherein the proximate area is a predefined area within range of the electronic lock; determine a list of known and unknown devices within the proximate area; synchronize the list of known and unknown devices with the mobile device; and trigger one or more alerts based on the list of known and unknown devices.

[00032] In Example 2, the subject matter of Example 1 is further configured such that the proximate device list is synchronized with the user device via the Internet.

[00033] In Example 3, the subject matter of Example 1 is further configured such that the proximate device list is synchronized with the user device via Bluetooth.

[00034] In Example 4, the subject matter of Example 1 is further configured such that the mobile device is configured to: receive the list of known and unknown devices; create or update, by a user of the mobile device, user settings defining alerts or notifications associated with one or more of the known and unknown devices.

[00035] In Example 5, the subject matter of Example 4 is further configured such that each device is categorized with one or more characteristics, the one or more characteristics being an ID, name, range, time of detection, dwell time, device type, and operating system.

[00036] In Example 6, the subject matter of Example 5 is further configured such that the one or more alerts triggered are further based on the user settings.

[00037] In Example 7, the subject matter of Example 1 is further configured such that all determined proximate devices are stored in a master list for a period of time.

[00038] Example 8 is an electronic lock comprising at least one processor and a non-transitory computer-medium comprising a plurality of instructions that in response to being executed by the at least one processor to perform: scanning a proximate area for known and unknown devices, wherein the proximate area is a predefined area within range of the electronic lock; determining a list of known and unknown devices within the proximate area; synchronizing the list of known and unknown devices with the mobile device; and triggering one or more alerts based on the list of known and unknown devices.

[00039] In Example 9, the subject matter of Example 8 is further configured such that the proximate device list is synchronized with the user device via the Internet.

[00040] In Example 10, the subject matter of Example 8 is further configured such that the proximate device list is synchronized with the user device via Bluetooth.

[00041] In Example 11, the subject matter of Example 8 is further configured such that the instructions when executed by the processor further perform: receiving the list of known and unknown devices; creating or updating, by a user of the mobile device, defining alerts or notifications associated with one or more of the known and unknown devices.

[00042] In Example 12, the subject matter of Example 11 is further configured such that each device is categorized with one or more characteristics, the one or more characteristics being an ID, name, range, time of detection, dwell time, device type, and operating system.

[00043] In Example 13, the subject matter of Example 12 is further configured such that the one or more alerts triggered are further based on the user settings.

[00044] In Example 14, the subject matter of Example 8 is further configured such that all determined proximate devices are stored in a master list for a period of time.

[00045] Example 15 is a method for determining a list of devices proximate to an electronic lock. The method includes the steps of: scanning a proximate area for devices, wherein the proximate area is a predefined area within range of the electronic lock; determining a list of known and unknown devices within the proximate area; synchronizing the list of known and unknown devices with the mobile device; and triggering one or more alerts based on the list of known and unknown devices.

[00046] In Example 16, the subject matter of Example 15 is further configured such that the proximate device list is synchronized with the user device via the Internet.

[00047] In Example 17, the subject matter of Example 15 is further configured such that the proximate device list is synchronized with the user device via Bluetooth.

[00048] In Example 18, the subject matter of Example 15 is further configured such that the method includes the steps of: receiving the list of known and unknown devices; and creating or updating, by a user of the mobile device, defining alerts or notifications associated with one or more of the known and unknown devices.

[00049] In Example 19, the subject matter of Example 18 is further configured such that each device is categorized with one or more characteristics, the one or more characteristics being an ID, name, range, time of detection, dwell time, device type, and operating system.

[00050] In Example 20, the subject matter of Example 19 is further configured such that the one or more alerts triggered are further based on the user settings.

[00051] Although the present disclosure has been described with reference to particular means, materials and embodiments, from the foregoing description, one skilled in the art can easily ascertain the essential characteristics of the present disclosure and various changes and modifications may be made to adapt the various uses and characteristics without departing from the spirit and scope of the present invention as set forth in the following claims.

WHAT IS CLAIMED IS:

1. A system comprising an electronic lock for use with a mobile device, the system comprising:

a locking device movable between a locked position and an unlocked position;

the electronic lock comprising an integrated radio, the electronic lock configured to:

scan a proximate area for known and unknown devices, wherein the proximate area is a predefined area within range of the electronic lock;

determine a list of known and unknown devices within the proximate area;

synchronize the list of known and unknown devices with the mobile device; and

trigger one or more alerts based on the list of known and unknown devices.

2. The system of claim 1, wherein the proximate device list is synchronized with the mobile device via the Internet.

3. The system of claim 1, wherein the proximate device list is synchronized with the mobile device via Bluetooth.

4. The system of claim 1, wherein the mobile device is configured to:

receive the list of known and unknown devices;

create or update, by a user of the mobile device, user settings defining alerts or notifications associated with one or more of the known and unknown devices.

5. The system of claim 4, wherein each device is categorized with one or more characteristics, the one or more characteristics being an ID, name, range, time of detection, dwell time, device type, and operating system.

6. The system of claim 5, wherein the one or more alerts triggered are further based on the user settings.

7. The system of claim 1, wherein all determined proximate devices are stored in a master list for a period of time.

8. An electronic lock comprising at least one processor and a non-transitory computer-medium comprising a plurality of instructions that in response to being executed by the at least one processor to perform:

scanning a proximate area for known and unknown devices, wherein the proximate area is a predefined area within range of the electronic lock;

determining a list of known and unknown devices within the proximate area;

synchronizing the list of known and unknown devices with a mobile device; and

triggering one or more alerts based on the list of known and unknown devices.

9. The electronic lock of claim 8, wherein the proximate device list is synchronized with the mobile device via the Internet.

10. The electronic lock of claim 8, wherein the proximate device list is synchronized with the mobile device via Bluetooth.

11. The electronic lock of claim 8, wherein the instructions when executed by the processor further perform:

receiving the list of known and unknown devices;

creating or updating, by a user of the mobile device, defining alerts or notifications associated with one or more of the known and unknown devices.

12. The electronic lock of claim 11, wherein each device is categorized with one or more characteristics, the one or more characteristics being an ID, name, range, time of detection, dwell time, device type, and operating system.

13. The electronic lock of claim 12, wherein the one or more alerts triggered are further based on the user settings.

14. The electronic lock of claim 8, wherein all determined proximate devices are stored in a master list for a period of time.

15. A method for determining a list of devices proximate to an electronic lock, the method comprising:

scanning a proximate area for devices, wherein the proximate area is a predefined area within range of the electronic lock;

determining a list of known and unknown devices within the proximate area;

synchronizing the list of known and unknown devices with a mobile device; and

triggering one or more alerts based on the list of known and unknown devices.

16. The method of claim 15, wherein the proximate device list is synchronized with the mobile device via the Internet.

17. The method of claim 15, wherein the proximate device list is synchronized with the mobile device via Bluetooth.

18. The method of claim 15, further comprising:

receiving the list of known and unknown devices;

creating or updating, by a user of the mobile device, defining alerts or notifications associated with one or more of the known and unknown devices.

19. The method of claim 18, wherein each device is categorized with one or more characteristics, the one or more characteristics being an ID, name, range, time of detection, dwell time, device type, and operating system.

20. The method of claim 19, wherein the one or more alerts triggered are further based on the user settings.

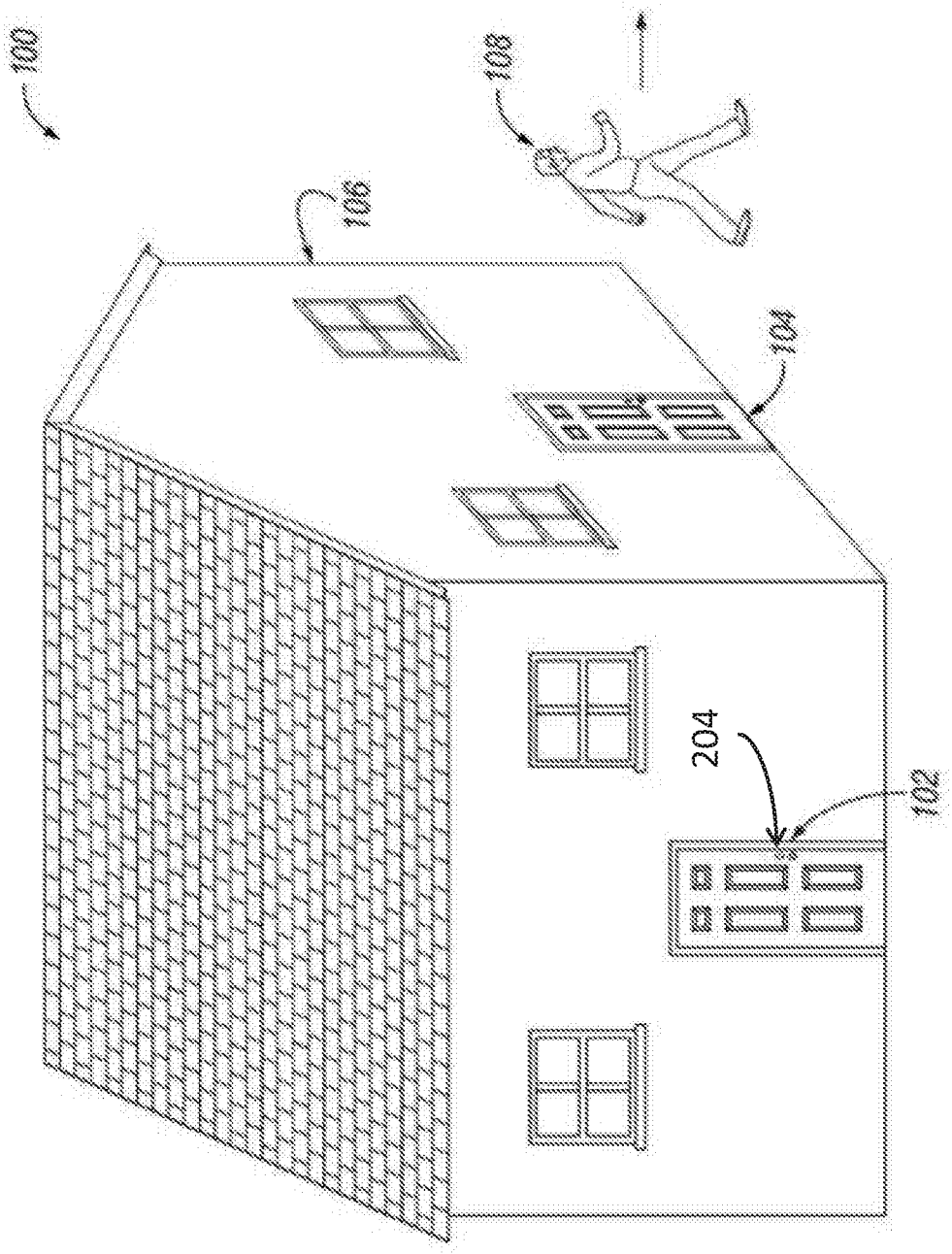

Figure 1

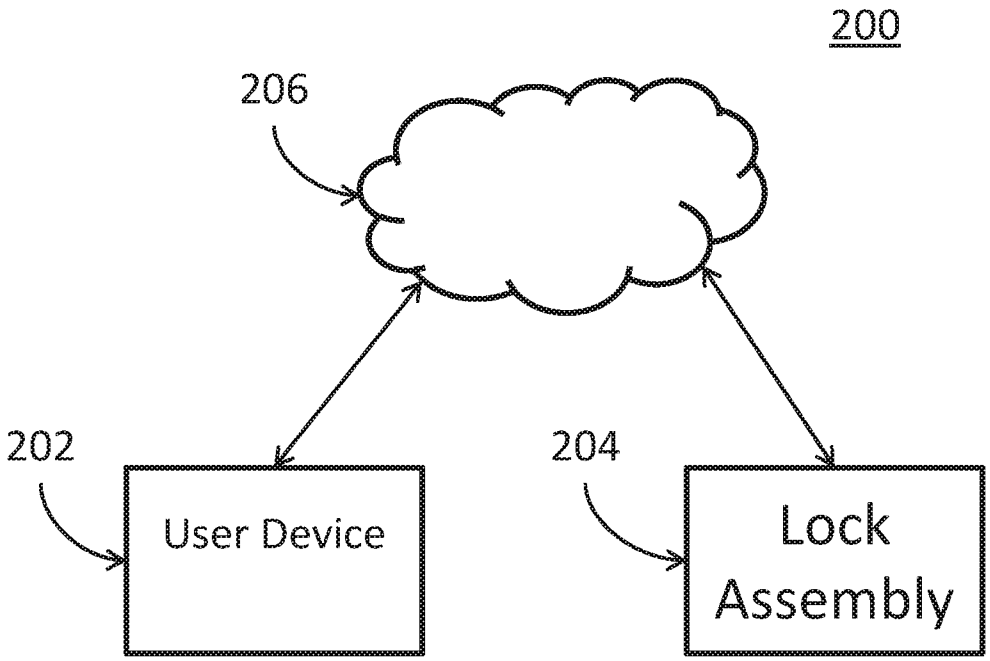

Figure 2

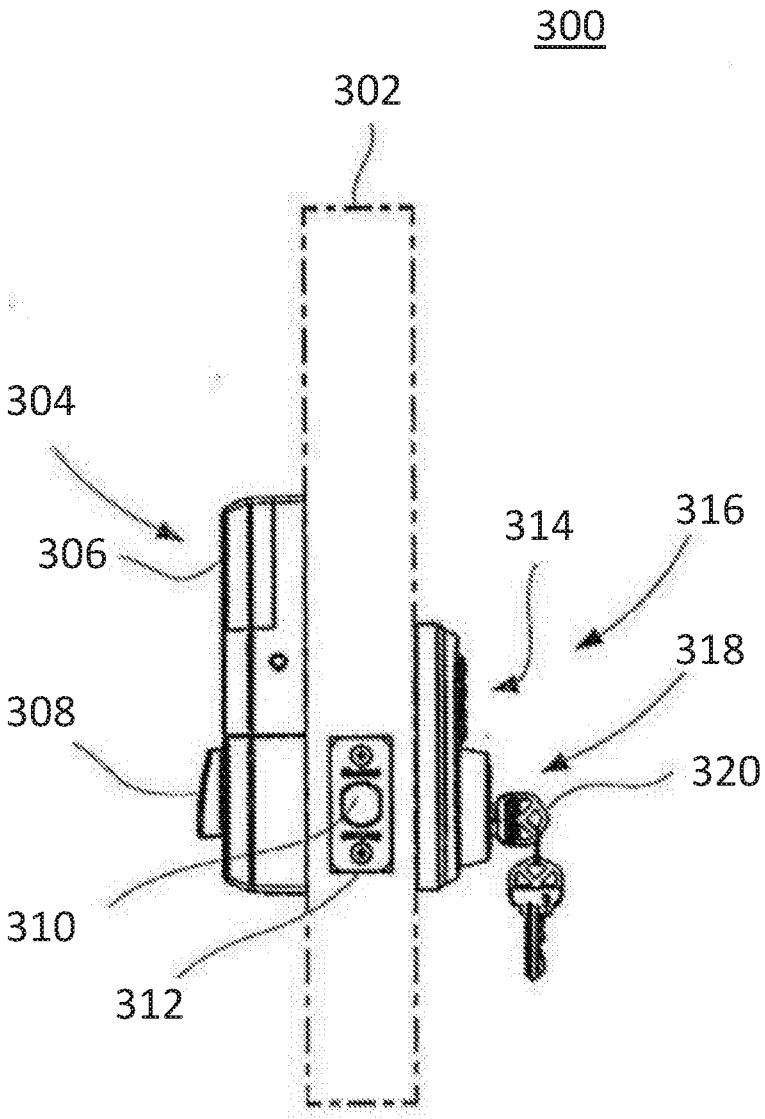

Figure 3

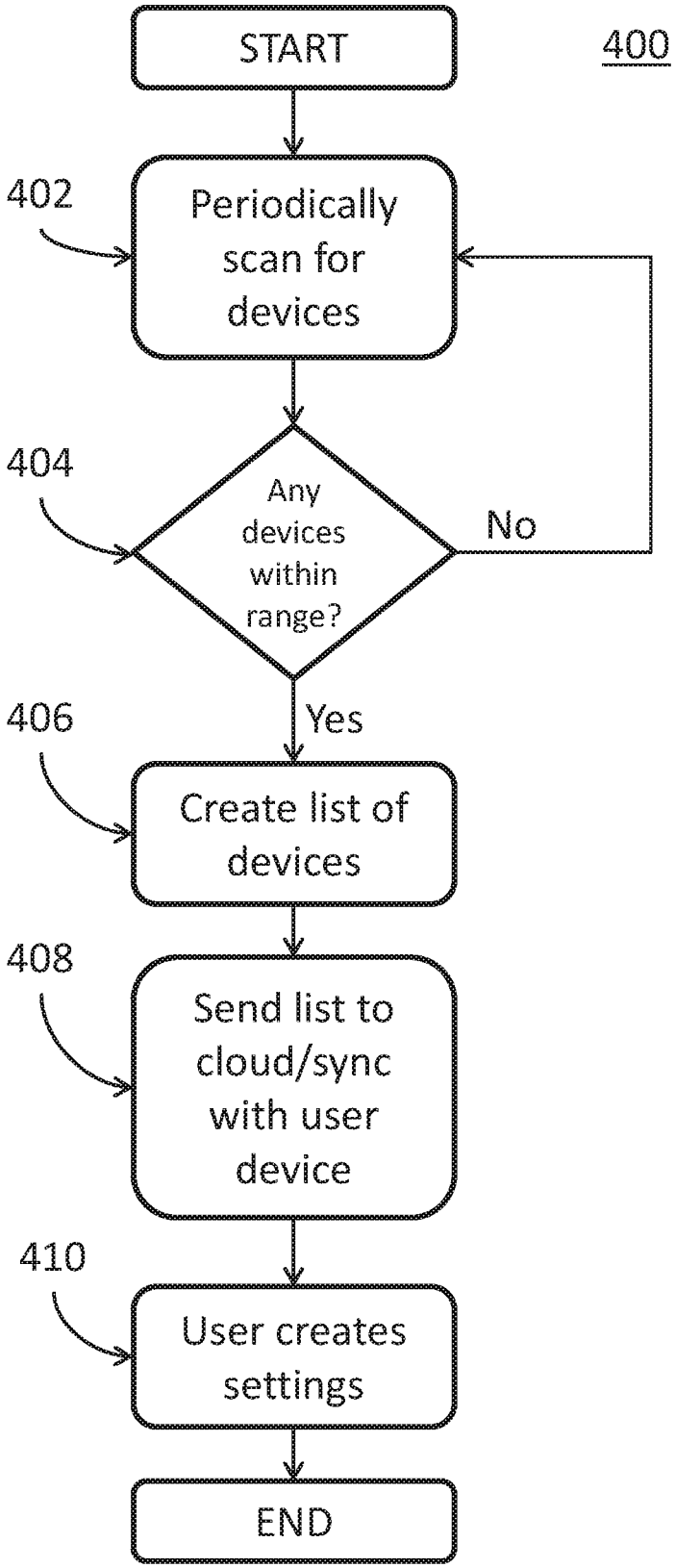
START
400
402
Periodically scan for devices
404
Any devices within range?
No
Yes
406
Create list of devices
408
Send list to cloud/sync with user device
410
User creates settings
END

Figure 4

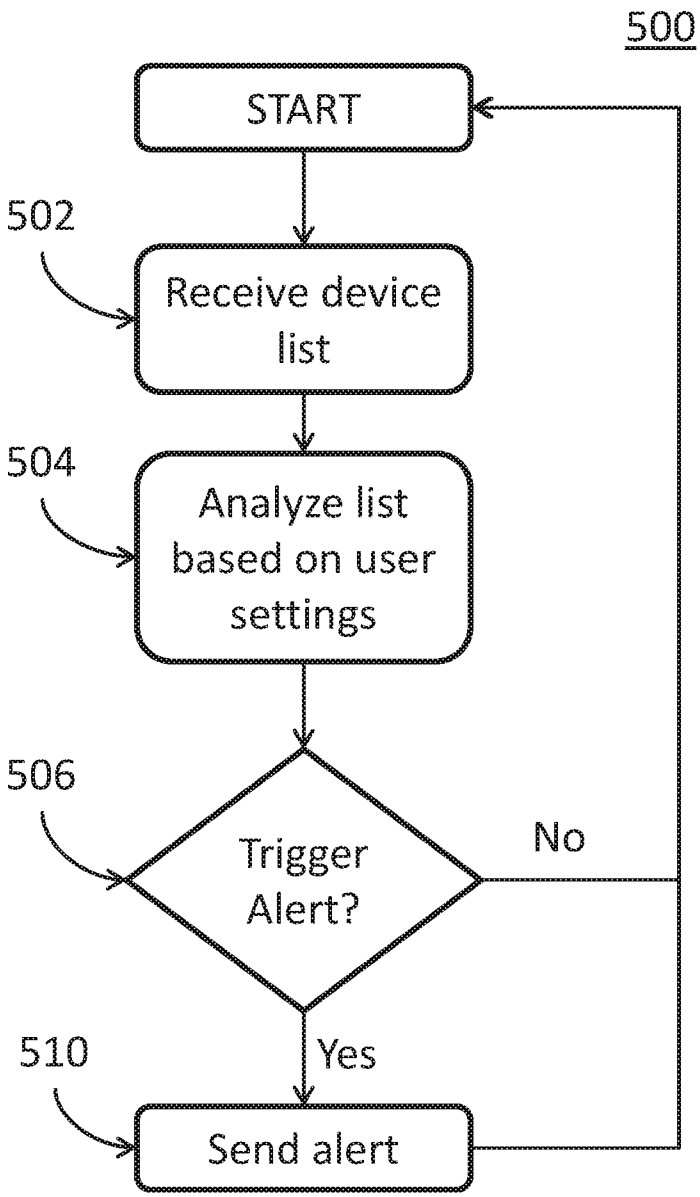
500
START
502
Receive device list
504
Analyze list based on user settings
506
Trigger Alert?
No
Yes
510
Send alert

Figure 5

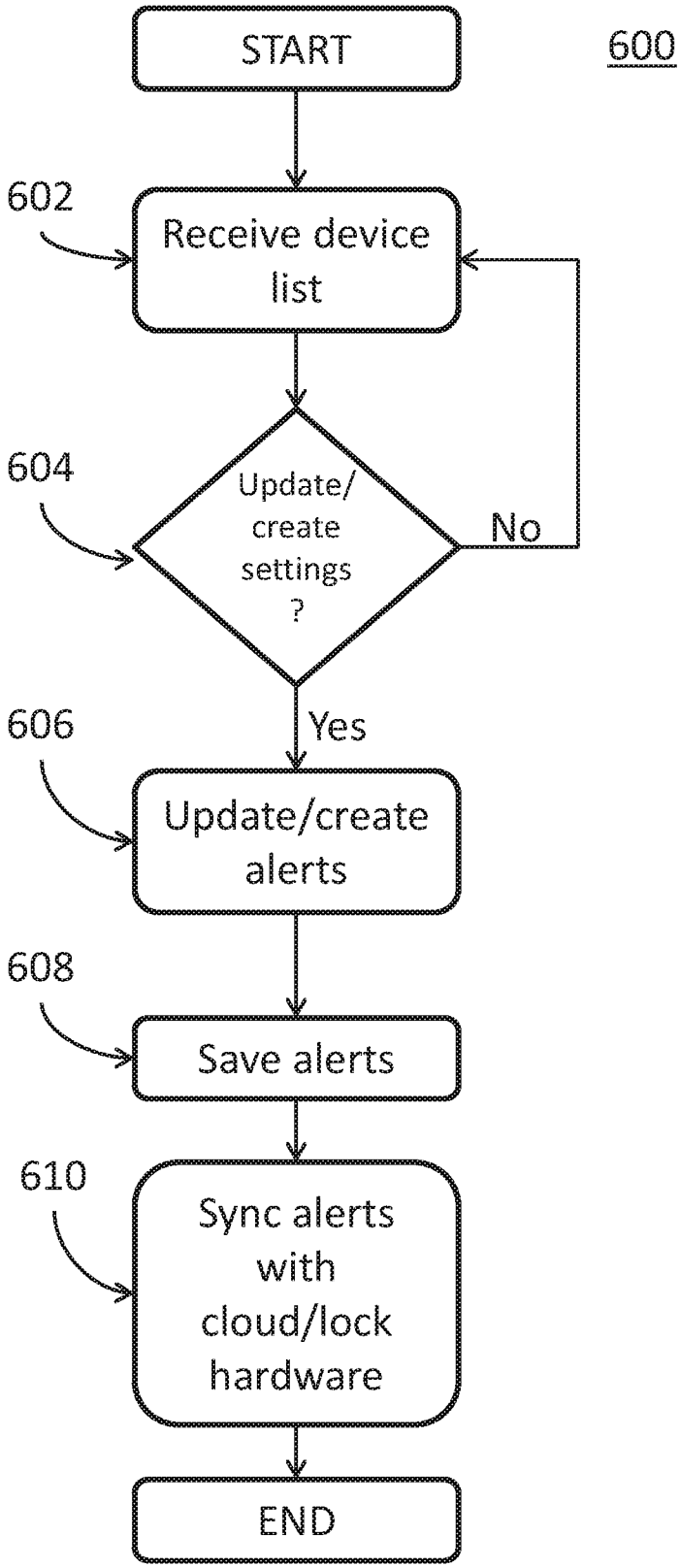
START
600
602
Receive device list
604
Update/ create settings ?
No
Yes
606
Update/create alerts
608
Save alerts
610
Sync alerts with cloud/lock hardware
END

Figure 6

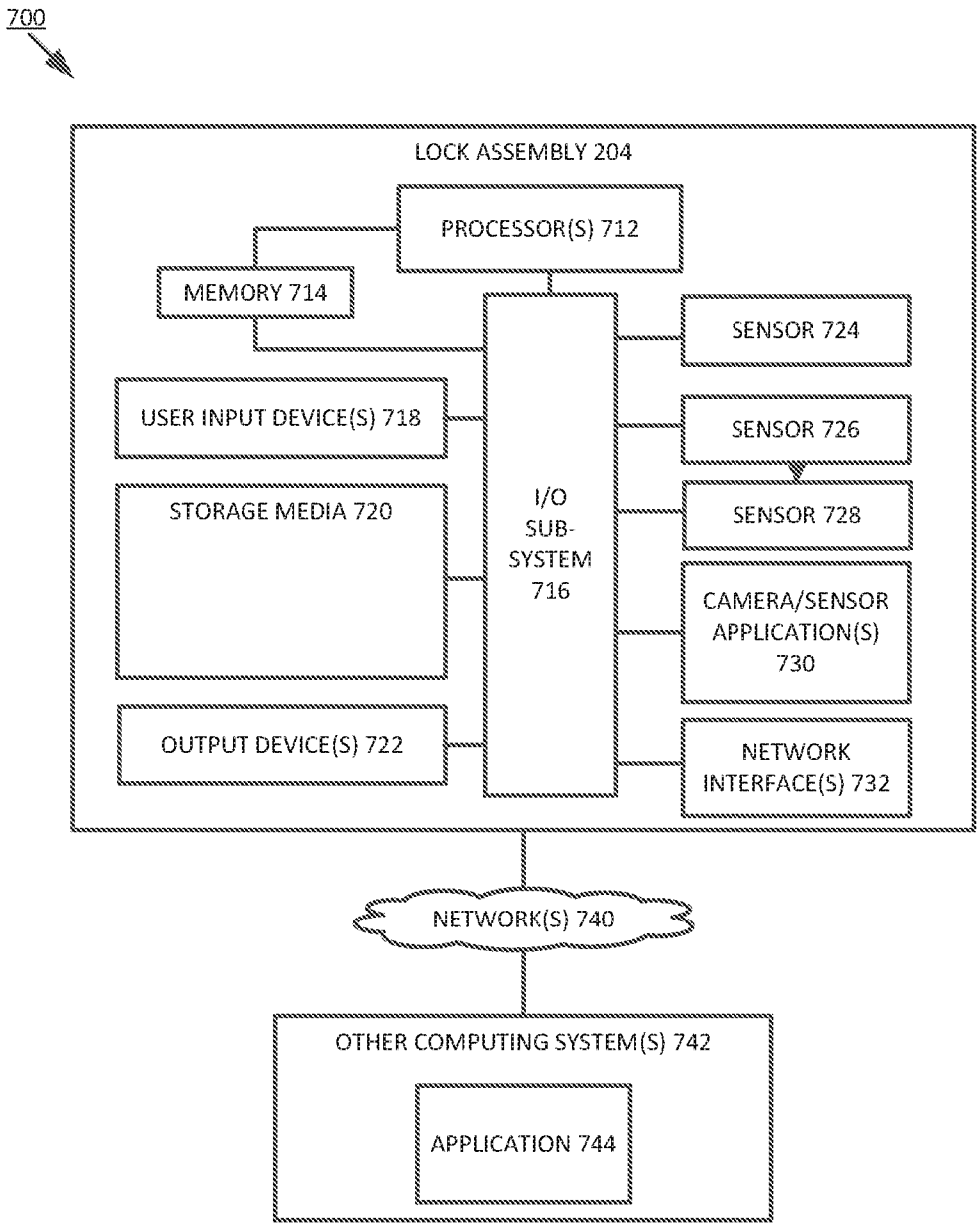
700
LOCK ASSEMBLY 204
PROCESSOR(S) 712
MEMORY 714
SENSOR 724
USER INPUT DEVICE(S) 718
SENSOR 726
STORAGE MEDIA 720
I/O SUB-SYSTEM 716
SENSOR 728
CAMERA/SENSOR APPLICATION(S) 730
OUTPUT DEVICE(S) 722
NETWORK INTERFACE(S) 732
NETWORK(S) 740
OTHER COMPUTING SYSTEM(S) 742
APPLICATION 744

Figure 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2017/027938

A. CLASSIFICATION OF SUBJECT MATTER

G07C 9/00(2006.01)i, H04M 1/725(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G07C 9/00; H04B 5/00; G05B 19/00; E05B 47/00; H04L 9/00; E05B 53/00; G08B 13/00; G06F 7/04; H04M 1/725

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: electronic lock, scanning, synchronizing, triggering, list

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2014-0051355 A1 (SCHLAGE LOCK COMPANY LLC.) 20 February 2014 See paragraphs [0009]-[0023], claims 1-5 and figures 1-3.	1-20
Y	US 2010-0283579 A1 (KEVIN C. KRAUS et al.) 11 November 2010 See paragraphs [0073]-[0081], claims 1-3 and figures 1-2.	1-20
Y	US 2012-0213362 A1 (OLLE BLIDING et al.) 23 August 2012 See paragraphs [0048]-[0056], claim 1 and figures 2-4.	4-7,11-14,18-20
A	US 2013-0063265 A1 (JEFFREY FELDSTEIN et al.) 14 March 2013 See paragraphs [0013]-[0031] and figures 1-3.	1-20
A	KR 10-2012-0074569 A (ZOIT CO., LTD.) 06 July 2012 See paragraphs [0069]-[0085], claim 1 and figures 1-3.	1-20

☐ 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
28 August 2017 (28.08.2017)	**30 August 2017 (30.08.2017)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
KIM, Sung Gon
Telephone No. +82-42-481-8746

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2017/027938

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014-0051355 A1	20/02/2014	AU 2013-302373 A1	02/04/2015
		AU 2013-302373 B2	19/05/2016
		EP 2885679 A1	24/06/2015
		MX 2015002066 A	05/08/2015
		MX 342113 B	14/09/2016
		US 2014-0049368 A1	20/02/2014
		US 2017-0145713 A1	25/05/2017
		US 9262879 B2	16/02/2016
		US 9514585 B2	06/12/2016
		WO 2014-028892 A1	20/02/2014
US 2010-0283579 A1	11/11/2010	AU 2008-347260 A1	16/07/2009
		AU 2008-347260 B2	28/11/2013
		AU 2008-347261 A1	16/07/2009
		AU 2008-347261 B2	28/08/2014
		CA 02711230 A1	16/07/2009
		CA 02711235 A1	16/07/2009
		CA 2711230 C	13/12/2016
		EP 2232779 A2	29/09/2010
		EP 2232779 B1	31/08/2011
		EP 2235886 A1	06/10/2010
		EP 2235886 B1	26/09/2012
		US 2010-0318685 A1	16/12/2010
		US 2013-0014219 A1	10/01/2013
		US 8331544 B2	11/12/2012
		WO 2009-088901 A1	16/07/2009
		WO 2009-088902 A2	16/07/2009
US 2012-0213362 A1	23/08/2012	EP 2478496 A1	25/07/2012
		EP 2478496 A4	19/04/2017
		WO 2011-034482 A1	24/03/2011
US 2013-0063265 A1	14/03/2013	US 2011-0074570 A1	31/03/2011
		US 2015-0077251 A1	19/03/2015
		US 2016-0253898 A1	01/09/2016
		US 8325033 B2	04/12/2012
		US 8902061 B2	02/12/2014
		US 9368023 B2	14/06/2016
KR 10-2012-0074569 A	06/07/2012	KR 10-1256920 B1	02/05/2013