(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 4 092 637 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
23.11.2022 Bulletin 2022/47

(21) Application number: **21020264.4**

(22) Date of filing: **19.05.2021**

(51) International Patent Classification (IPC):
G07C 9/00 *(2020.01)*

(52) Cooperative Patent Classification (CPC):
G07C 9/00309; G07C 9/00571; G07C 9/00904; G07C 2009/00436; G07C 2009/00785; G07C 2009/00865; G07C 2209/63

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
KH MA MD TN

(71) Applicant: **Lina SAS**
91400 Orsay (FR)

(72) Inventor: **LAZUECH, Théo**
91400 Orsay (FR)

(54) **ACCESS CONTROL MANAGEMENT SYSTEM AND METHOD OF ACCESS CONTROLLER USE**

(57) The present invention provides a method and system for operating an access control management system (1000) having an access controller (6040) coupled with a lock (1002). The access controller (604) is configured to restrict access to an area. The access control management system (1000) provides a two-way communication between the access controller (604) and an electronic device (102) for locking and unlocking the lock (1002). The access controller (604) transmits a unique code to the electronic device (102) via a wireless communication module (1004). The electronic device (102) transmits a trigger key associated with the unique code to the access controller (604) via a visible light module (1006). The access controller (604) transmits the trigger key to a server (608) through a hub (606). The server (608) is enabled to validate the trigger key with a predefined criterion to generate a trigger command. The server (608) transmits the trigger command to the access controller (604) through the hub (606). The trigger command initiates a locking or unlocking of the lock (1002).

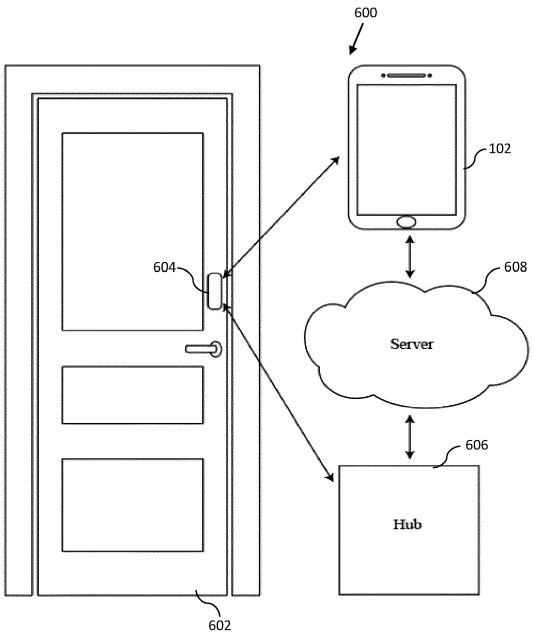

FIG. 6

EP 4 092 637 A1

Description

TECHNICAL FIELD OF THE INVENTION

[0001] The present invention relates to an access control management system having an access controller coupled with a lock, and more particularly to the use of visible light communication to exchange information between the access controller and an electronic device for locking or unlocking the lock.

BACKGROUND OF THE INVENTION

[0002] Currently, a smart door lock is operated via a contactless card, or a digital key to gain access to a restricted area. The contactless card uses an RFID signal, or Wi-Fi signal to exchange information with the smart door lock. However, the contactless card can be easily lost, and card information can be replicated and therefore a severe security problem exists.

[0003] With the continuous development of the communication technology, the intelligent door lock with visible light communication is widely applied. In the prior art, the smart door lock with visible light communication generally utilizes a flash lamp on an electronic device (e.g., a mobile phone) to send a visible light signal to transmit a code for opening or closing of the smart door lock. The smart door lock process the code to generate a trigger command. However, this process is time-consuming, and can easily drain the power of the smart lock door. Further, a security risk also exists.

[0004] A prior art EP3360114A1 discloses an access control system. Authentication information may be transmitted to an electronic locking device configured to restrict access to an entry point of the access control system. In various embodiments, a smart device comprises a light-emitting diode (LED) and a wireless networking radio for exchanging access control information with a remote server. The smart device may receive information from the remote server that configures the LED to present authentication information as an optical signal. The electronic locking device may comprise a photodetector arranged to confront a user holding the smart device to receive an optical signal emitted by the smart device.

[0005] Therefore, there is a need for an access control management system that is secure and provides two-way communication between an access controller and an electronic device, wherein the access controller is coupled with a lock.

SUMMARY OF THE INVENTION

[0006] An object of the present invention is to provide an access control management system configured to lock or unlock a door using an access controller coupled with a door lock. The access controller is capable of selectively restricting access to an area or enclosure (i.e., building, offices, laboratories, restricted areas, home, hotels) and is enabled to exchange information with the electronic device via two-way communication to grant or deny a user access to the area or enclosure. The electronic device is a mobile phone, PDA, tablet, or any other LED-enabled device.

[0007] The present invention provides a method for operating the access control management system, having an access controller coupled with a lock, by two-way communication between the access controller and the electronic device. The method comprising transmitting a unique code to the electronic device, through a wireless communication protocol, by an access controller in response to detecting proximity, by a proximity sensor of the access controller, of the electronic device to the access controller, determining a trigger key, associated with the access controller, in an internal memory of the electronic device corresponding to the unique code received from the access controller by the electronic device, transmitting the trigger key to the access controller through a visible light communication channel of a visible light module by the electronic device in response to determining the trigger key in the internal memory of the electronic device, validating the trigger key, transmitted by the electronic device to the access controller, by a server with a predefined criterion in response to receiving the trigger key by the server from a hub, wherein the hub is coupled with the access controller, transmitting a trigger command to the hub by the server, in response to validating the trigger key by the server, and triggering the lock by the access controller in response to receiving the trigger command from the hub by the access controller. The trigger command is, one of, a command for locking an unlocked lock, a command for unlocking a locked lock or denying permission to access the lock.

[0008] In one exemplary embodiment, a system for operating an access control management system, having an access controller coupled with a lock, by two-way communication between the access controller and an electronic device having a visible light module is provided. The access control management system comprising the access controller, the electronic device, a hub, and a server. The access controller is enabled to transmit a unique code to the electronic device, through a wireless communication protocol, in response to detecting proximity, by a proximity sensor of the access controller, of the electronic device. The wireless communication protocol is one of a Bluetooth protocol, WiFi protocol, NFC protocol, and a light communication protocol. The electronic device is enabled to determine a trigger key, associated with the access controller, in an internal memory of the electronic device corresponding to the unique code received from the access controller. The electronic device is enabled to transmit the trigger key to the access controller through a visible light communication channel of the visible light module in response to determining the trigger key in the internal memory. The access controller is enabled to transmit the trigger key to a hub. The server is enabled to validate the trigger key with a predefined

criterion in response to receiving the trigger key from the hub, wherein the hub is coupled with the access controller. The predefined criterion is matching the trigger key received from the hub with a trigger key stored in a database of the server. Further, the server is enabled to transmit a trigger command to the hub, in response to validating the trigger key. The access controller is enabled to unlock the lock in response to receiving the unlock command from the hub. The trigger command is, one of, a command for locking an unlocked lock, a command for unlocking a locked lock or denying permission to access the lock.

[0009] In one exemplary embodiment, the electronic device is coupled to the server and is enabled to receive a new trigger key after a predefined interval from the server.

[0010] In another exemplary embodiment, the access controller coupled with the door lock comprises a transmission module and a receiver module. The transmission module is enabled to transmit a unique code, stored in a memory of the access controller, to the electronic device through a wireless communication protocol, in response to detecting proximity, by a proximity sensor of the access controller, of the electronic device to the access controller. The wireless communication protocol is one of a Bluetooth protocol, NFC protocol, WiFi protocol, and a light communication protocol. The receiver module is enabled to receive a trigger key through a visible light communication channel from the electronic device in response to transmission of the unique code to the electronic device, wherein the receiver module is further enabled to receive a trigger command from a server, in response to validation of the trigger key with a predefined criterion by the server upon receiving trigger key from a hub, wherein the hub is coupled with the access controller. Further, the transmission module is enabled to transmit the trigger command to (a) unlock the door lock in response to receiving an unlock command from the hub, (b) lock the door in response to receiving a lock command from the hub, or (c) denying permission to access the lock in response to receiving a deny command from the hub.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] The subject matter is particularly pointed out and distinctly claimed at the conclusion of the specification. The foregoing and other features, and advantages of the present disclosure are apparent from the following detailed description taken in conjunction with the accompanying drawings in which:

FIG. 1 is illustrating an electronic device comprising a display screen illustrating an example graphical user interface of a user login interface, in accordance with an exemplary embodiment of the present invention.

FIG. 2 illustrates one example of a user interface for displaying access control information to the administrator via the software application, in accordance with an exemplary embodiment of the present invention.

FIG. 3 is illustrating an example graphical user interface showing access control information associated with an access controller coupled with a lock, in accordance with an exemplary embodiment of the present invention.

FIG. 4 is illustrating an example graphical user interface wherein access control associated with the access controller coupled with lock is assigned to a user, in accordance with an exemplary embodiment of the present invention.

FIG. 5 illustrates an example graphical user interface showing a user accessing the software application of the access control management system, in accordance with an exemplary embodiment of the present invention.

FIG. 6 is a block diagram (600) of an access control management system, in accordance with an exemplary embodiment of the present invention.

FIG. 7 is a flow chart illustrating the method for operating an access control management system, in accordance with an exemplary embodiment of the present invention.

FIG. 8 is a block diagram of a printed circuit board of the access controller in accordance with an exemplary embodiment of the present invention.

FIG. 9 illustrates a database of the server storing access information, in accordance with an exemplary embodiment of the present invention.

FIG. 10 is a block diagram of the access control management system, in accordance with a preferred embodiment of the present invention.

DESCRIPTION OF EMBODIMENTS

[0012] Technical solutions in the embodiments of the present disclosure will be described below with reference to the accompanying drawings in the embodiments of the present disclosure. Embodiments of the present invention relate to a method for operating an access control management system having an access controller coupled with a lock, by two-way communication between the access controller and an electronic device, wherein the electronic device having a visible light module. Some embodiments of the present invention provide a system for operating the access control management system, having the access controller coupled with a door lock, by

two-way communication between the access controller and the electronic device having the visible light module. The electronic device can be a smartphone, mobile phone, PDA, smartwatch, or any other operating system-enabled device having a visible light module.

[0013] The access controller is capable of selectively restricting access to an area or enclosure (i.e., building, offices, laboratories, restricted areas, home, hotels) and is enabled to exchange information with the electronic device via two-way communication to grant or deny a user access to the area or enclosure.

[0014] The access control management system is enabled to track and record user's entry information into the area or enclosure using the access controller. In some instance, an administrator of the system is enabled to use or analyze the information at end of the day or end of the month.

[0015] In accordance with some exemplary embodiments, a system administrator or other user of the access control management system is enabled to provide one or more trigger keys corresponding to one or more access controllers to one or more users of the system. The user is enabled to unlock a lock associated with the access controller using an associated trigger key. The administrator has the authority to control who accesses a particular access controller, such as where the administrator has installed the access controller on the administrator's office or home. The administrator is enabled to control access to the access controller coupled with lock by modifying access control permissions for the office doors by communicating with a server (i.e., grant or revoke permission for entry to a particular access controller). In one embodiment, the administrator is enabled to communicate with the server using a web browser application or any other mobile application software application executing on any electronic device capable of communicating with the server.

[0016] FIG. 1 is illustrating an electronic device (102) comprising a display screen illustrating an example graphical user interface of a user login interface (100), in accordance with an exemplary embodiment of the present invention. The administrator or any other user of the system is enabled to login into a software application or web browser application of the access control management system, or the administrator is enabled to register a new account (104). The administrator is enabled to view and/or modify access control information by login into the access control management system. The administrator is enabled to provide login credentials (106) i.e., a username and password prior to accessing access control information. Upon, providing valid login credentials, a server of the system is enabled to provide the administrator with the access control information associated with all access controllers of the system.

[0017] FIG. 2 illustrates one example of a user interface for displaying access control information (200) to the administrator via the software application, in accordance with an exemplary embodiment of the present invention. Each access controller is having a unique code that acts as identifying information for the access controller coupled with a lock. For instance, a particular lock is labeled as "Front Door", Door 1, Door 2 allowing the administrator to quickly identify where the particular access controller is installed within the access control management system, or which area it is intended to secure. The access controller that a user has permission to open is further differentiated by the degree of control that the user may exert over the access controller. The access control information (200) is showing various locks, and users of the system. The administrator is enabled to give or revoke access of the access controller to the user by using the setting tab. The administrator is enabled to restrict area using "Add lock" button and register a door name to restrict access to that door. The access controllers are installed on entry points owned or administered by the administrator i.e., lock - "Front Door", "Door 1", and "Door 2".

[0018] As shown in FIG. 2, the access controller installed on the "Front Door" (202) provides entry access to seven users, and the access controller installed on the "Door 1" (204) provides entry access to three users. The administrator is enabled to modify access permission for certain access controllers coupled with the "Front Door" by selecting, the button labeled "Allowed" proximate to the "Front Door" label to view information associated with that particular access controller. The administrator is enabled to view more access controller information by clicking on the view more button. In various embodiments, the administrator is enabled to view and modify the access control information for the access controller owner by the administrator that is labeled as "My locks" and enabled to only view, but not modify, the access control information for the access controller's owned by other users labeled as "Other Locks". Further, the administrator wishes to open a door entry for the "Front Door", the administrator is enabled to select the appropriate "Open" button.

[0019] In one exemplary embodiment, the server is configured to display information associated with "Door 1" via a webpage accessible from the software application executing on the electronic device. FIG. 3 is illustrating an example graphical user interface showing access control information (300) associated with an access controller coupled with a lock "Door 1", in accordance with an exemplary embodiment of the present invention. The server provides a webpage including information associated with the access controller coupled with the "Door 1", such as a list of users that presently have permission to open the Door 1. The information (i.e., "access overview for "Door 1" (302)) shows a table having columns such as user's name, relation with the administrator, and the trigger key identifier associated with the access controller. The employee Mary is enabled to enter through the Door 1 by transmitting a trigger key (i.e., 0B2#) to the access controller through a flashlight of the electronic device i.e., mobile phone. For the access controller cou-

pled with the "Door 1", the trigger key to lock or unlock the "Door 1" can be the same or different. For example, for the "Door 1" the trigger key for employee Joe is 0B2# and the trigger key for friend Anna is 6DFe.

[0020] In another exemplary embodiment, the administrator is enabled to modify access permission for a particular access controller coupled with the lock, for example, to provide another user with access to the open door lock. FIG. 4 is illustrating an example graphical user interface (400) wherein access control associated with the access controller coupled with lock is assigned to a user, in accordance with an exemplary embodiment of the present invention. The administrator wishes to provide his friend Anna access to a "Door 2". The administrator selects the user labeled as Anna and the administrator is enabled to initiate modification of the access permission associated with the "Door 2" i.e., give access to "Door 2" for a time period of six months (402). The administrator is enabled to set a time period for which access permission is valid such as 1 hour, 1 day, 1 week 1 month, 2 months, 6 months, or 1 year and select a door name from a drop-down menu for which permissions need to be given. The administrator then selects Give button to give Anna a permission to unlock "Door 2". The selected "Door 2" trigger key is shared with the Anna. In one embodiment, the administrator is enabled to select a trigger key for the associated door and share it with the user.

[0021] FIG. 5 illustrates an example graphical user interface (500) showing a user accessing the software application of the access control management system, in accordance with an exemplary embodiment of the present invention. The user "Anna" is enabled to login into the software application of the system to view her profile and access permission related to the access controllers coupled with the door locks. The graphical user interface (500) shows user Anna's profile, her contact number, and access lock details (502). The access lock details show a Door label, its associated unique code, its associated trigger key, and a time period for which Anna has access to the particular Door lock. "Door 1" having a unique code: D1@, a trigger key: 6DFe, a time validity of 8 months. "Door 2" having a unique code: D2@, a trigger key: 4kg$, a time validity of 6 months.

[0022] FIG. 6 is a block diagram (600) of an access control management system, in accordance with an exemplary embodiment of the present invention. The access control management system comprising an access controller (604) coupled with a door lock (602), an electronic device (102), a hub (606), and a server (608). The access control management system provides two-way communication between the access controller (604) and the electronic device (102) having a visible light module. The access controller (604) comprises a proximity sensor to detect the proximity of the electronic device (102). The access controller (604) is enabled to transmit a unique code to the electronic device (102) through a wireless communication protocol. The wireless communication protocol is one of a Bluetooth protocol, WiFi protocol, NFC protocol, and a light communication protocol. The electronic device (102) is enabled to determine a trigger key associated with the access controller (604), in an internal memory of the electronic device (102) corresponding to the unique code received from the access controller (604). The electronic device (102) is enabled to transmit the trigger key to the access controller (604) through a visible light communication channel of the visible light module (i.e., LED flashlight) in response to determining the trigger key in the internal memory of the electronic device (102). The access control (604) is enabled to transmit the trigger key to the hub (606). The hub is enabled to transmit the trigger key to the server (608). The server (608) is enabled to validate the trigger key with a predefined criterion wherein the predefined criterion is whether the trigger key corresponding to the unique code of the access controller exists in a database and it is matching with a trigger key stored in the database of the server (608). Based on the validation, the server (608) transmits a trigger command to the hub (606). The hub (606) transmits the trigger command to the access controller (604). The trigger command can be (a) unlock the door lock (602), (b) lock the unlock door lock (602), or (c) denying permission to access the door lock (602). The access controller (604) triggers the door lock (602) based on the trigger command received from the hub (606).

[0023] In one exemplary embodiment, the electronic device (102) is coupled to the server (608) and is enabled to receive a new trigger key after a predefined interval from the server (608). The server (608) is enabled to periodically update the trigger keys corresponding to the unique codes of the access controllers.

[0024] In another exemplary embodiment, in a building premises, for each floor access controllers, a central hub is provided to communicate with the server.

[0025] In another exemplary embodiment, a method for operating the access control management system, having an access controller coupled with a lock, by two-way communication between the access controller and the electronic device having a visible light module is provided. FIG. 7 is a flow chart illustrating the method (700) for operating an access control management system, in accordance with an exemplary embodiment of the present invention. At step (702), transmitting a unique code to the electronic device, through a wireless communication protocol, by an access controller in response to detecting proximity, by a proximity sensor of the access controller, of the electronic device to the access controller. The electronic device is a mobile phone, PDA, tablet, or any other LED-enabled device. The wireless communication protocol is one of a Bluetooth protocol, WiFi protocol, NFC protocol, and a light communication protocol. At step (704), determining a trigger key, associated with the access controller, in an internal memory of the electronic device corresponding to the unique code received from the access controller by the electronic device. At

step (706), transmitting the trigger key to the access controller through a visible light communication channel of the visible light module by the electronic device in response to determining the trigger key in the internal memory of the electronic device. At step (708), validating the trigger key, transmitted by the electronic device to the access controller, by a server with a predefined criterion in response to receiving the trigger key by the server from a hub, wherein the hub is coupled with the access controller. The predefined criterion is matching the trigger key received from the hub with a trigger key stored in the database of the server. At step (710), transmitting a trigger command to the hub by the server, in response to validating the trigger key by the server. At step (712), triggering the lock by the access controller in response to receiving the trigger command from the hub by the access controller. The trigger command is, one of, a command for locking an unlocked lock, a command for unlocking a locked lock or denying permission to access the lock. In one example, the electronic device is coupled to the server and is enabled to receive a new trigger key after a predefined interval from the server.

[0026] In another exemplary embodiment, the access controller coupled with the door lock comprises a transmission module and a receiver module. The transmission module is enabled to transmit a unique code, stored in a memory of the access controller, to the electronic device through a wireless communication protocol, in response to detecting proximity, by a proximity sensor of the access controller, of the electronic device to the access controller. The wireless communication protocol is one of a Bluetooth protocol, NFC protocol, WiFi protocol, and a light communication protocol. The receiver module is enabled to receive a trigger key through a visible light communication channel from the electronic device in response to transmission of the unique code to the electronic device. The receiver module is further enabled to receive a trigger command from a server, in response to validation of the trigger key with a predefined criterion by the server upon receiving trigger key from a hub, wherein the hub is coupled with the access controller. Further, the transmission module is enabled to transmit the trigger command to (a) unlock the door lock in response to receiving an unlock command from the hub, (b) lock the door in response to receiving a lock command from the hub, or (c) denying permission to access the lock in response to receiving a deny command from the hub.

[0027] FIG. 8 is a block diagram (800) of a printed circuit board of the access controller (604) in accordance with an exemplary embodiment of the present invention. The access controller (604) is capable of restricting access to an area, enclosure, or item thereof. The printed circuit board comprises a microcontroller (802) that is operatively associated with a plurality of components using wired links, wireless links, or a combination thereof. The access controller (604) comprises a proximity sensor (812), a memory (816), a LED flash (814), a wireless communication module (806), a buzzer (804), a real-time clock (808), a battery (810), a LED indicator (818), and a switch (820). The proximity sensor (812) is configured to detect the proximity of the electronic device. The memory (816) is configured to store the access controller's unique code, access control information, for example, a time of an entry and exit of the electronic device from the door, access given and denied information. The battery (810) is configured to power the access controller (604). The battery (810) is a rechargeable battery. The LED indicator (818) is configured to indicate when the locking command or unlocking command is triggered by the access controller. For example, a green indicator indicates a door is opened for the user of the electronic device, and a red indicator indicates that the door denies access permission. The access controller (604) is enabled to determine the door lock is being vandalized i.e., detection of forces applied to the door lock and locks the door permanently via the switch (820). The access control (604) is enabled to send alert to the user to alert the user the that an act of vandalism is occurring using the wireless communication module (806).

[0028] In one exemplary embodiment, the door lock can be an electromagnetic lock, an electromechanical lock, or any other type of lock. An electric motor is configured to perform locking and unlocking operations of the electromechanical door. In one example, one or more magnets are used to perform locking and unlocking operations of the electromagnetic door.

[0029] FIG. 9 illustrates a database (908) of the server (608) storing access information, in accordance with an exemplary embodiment of the present invention. The access information comprises an access controller (902), its associated unique code (904), and trigger key (906). The unique code (904) and trigger key (906) is alphanumeric and can be any combination of the 0-9 characters, A-Z, a-z alphabets. The trigger key is periodically updated by the server (608) and is transmitted to the electronic device. The unique code is enabled to uniquely identify access controller coupled with locks on the same floor of the building. As shown in the FIG. 9, the access controller installed in "Front Door" has a unique code: DF$, and a trigger key Z4>$. The access controller installed in "Door 1" having a unique code: D1@, and a trigger key 6DFe. The access controller installed in "Door 2" having a unique code: D2@, and a trigger key 4Kg$. The access controller installed in "Door 3" having a unique code: D3#, and a trigger key X#2@. The server (608) is configured to match the trigger key received from the electronic device with a trigger key stored in the database (908) of the server (608) to generate a trigger command. If the trigger key is matched with the trigger key stored in the database (908) of the server (608), then the trigger command is unlocking the locked door, and If the trigger key does not match with the trigger key stored in the database (908) of the server (608), then the trigger command is locking an unlocked door. If the trigger key is not present in the database (908) of the server (608), then the trigger command is denying permission to access the

lock.

[0030] FIG. 10 is a block diagram of the access control management system (1000), in accordance with a preferred embodiment of the present invention. The system comprises of an access controller (604) coupled with a lock (1002), an electronic device (102) having a visible light module (1006), a hub (606) and a server (608). The access controller (604) comprises a proximity sensor (812) configured to detect proximity of the electronic device (102) to the access controller (604). The access controller (604) is enabled to transmit a unique code to the electronic device (102) through a wireless communication protocol (1004) in response to detecting proximity by a proximity sensor (812) of the access controller (604). The wireless communication protocol (1004) is one of a Bluetooth protocol, WiFi protocol, NFC protocol, and a light communication protocol. The electronic device (102) is enabled to determine a trigger key, associated with the access controller (604), in an internal memory of the electronic device (102) corresponding to the unique code received from the access controller (604) by the electronic device (102). The electronic device (102) is enabled to transmit the trigger key to the access controller (604) through a visible light communication channel of the visible light module (1006) in response to determining the trigger key in the internal memory of the electronic device (102). The access controller (604) is coupled to the hub (606). The access controller (604) is enabled to transmit the trigger key to the hub. The hub (606) is enabled to transmit the trigger key to the server (608) through a network (1008). The network (1008) may be 3G, 4G, 3G/4G, WHDMI, Bluetooth, WiFi, SuperWiFi, WiMax, 5G, and other wireless network. The server (608) is enabled to validate the trigger key with a predefined criterion in response to receiving the trigger key from the hub (606). The predefined criterion is matching the trigger key received from the hub with a trigger key stored in a database (908) of the server (608). Further, the server (608) is enabled to transmit a trigger command to the hub (606) through the network (1008), in response to validating the trigger key. The access controller (604) is enabled to receive the trigger command from the hub (606). The trigger command is, one of, a command for locking an unlocked lock, a command for unlocking a locked lock or denying permission to access the lock. The electronic device (102) is coupled to the server (608) and is enabled to receive a new trigger key after a predefined interval from the server (608) through the network (1008).

[0031] Any reference in this disclosure to "one embodiment," "an embodiment," "some embodiments," "various embodiments," etc., means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of this disclosure. The appearances of such phrases, and variations thereof, including references to "implementations," are not necessarily all referring to the same embodiment or implementation. When a particular feature, structure, or element is described in connection with any embodiment or implementation, it is understood that it is within the purview of persons of skill to affect such feature, structure, or element in connection with any of the other embodiments and implementations.

[0032] Although embodiments have been described with reference to a number of illustrative embodiments and implementations thereof, it will be appreciated that numerous other modifications and embodiments can be devised by skilled persons without departing from the spirit and scope of the underlying principles of this disclosure. The scope of this disclosure should, therefore, be determined only by the following claims.

Claims

1. A method for operating an access control management system (1000), having an access controller (604) coupled with a lock (1002), by a two-way communication between the access controller (604) and a device (102) having a visible light module (1006), the method comprising:

   transmitting a unique code to the device (102), through a wireless communication protocol (1004), by the access controller (604) in response to detecting proximity, by a proximity sensor (812) of the access controller (604), of the device (102) to the access controller (604);
   determining a trigger key, associated with the access controller (604), in an internal memory of the device (102) corresponding to the unique code received from the access controller (604) by the device (102);
   transmitting the trigger key to the access controller (604) through a visible light communication channel of the visible light module (1006) by the device (102) in response to determining the trigger key in the internal memory of the device (102);
   validating the trigger key, transmitted by the device (102) to the access controller (604), by a server (608) with a predefined criterion in response to receiving the trigger key by the server (608) from a hub (606), wherein the hub (606) is coupled with the access controller (604);
   transmitting a trigger command to the hub (606) by the server (608), in response to validating the trigger key by the server (608); and
   triggering the lock (1002) by the access controller (604) in response to receiving the trigger command from the hub (606) by the access controller (604).

2. The method of claim 1, wherein the wireless communication protocol (1004) is one of a Bluetooth protocol, WiFi protocol, NFC protocol, and a light com-

munication protocol.

3. The method of claim 1, wherein the device (102) is coupled to the server (608) and is enabled to receive a new trigger key after a predefined interval from the server (608).

4. The method of claim 1, wherein the predefined criterion is matching the trigger key received from the hub (606) with a trigger key (906) stored in a database (908) of the server (608).

5. The method of claim 1, wherein the device (102) is an LED (814) enabled device (102).

6. The method of claim 1, wherein the trigger command is, one of, a command for locking an unlocked lock, command for unlocking a locked lock, and command for denying permission to access the lock (1002).

7. A system for operating an access control management system (1000), having an access controller (604) coupled with a lock (1002), by a two-way communication between the access controller (604) and a device (102) having a visible light module (1006), the system comprising:

the access controller (604), enabled to transmit a unique code to the device (102), through a wireless communication protocol (1004), in response to detecting proximity, by a proximity sensor (812) of the access controller (604), of the device (102) to the access controller (604);
the device (102), enabled to determine a trigger key, associated with the access controller (604), in an internal memory of the device (102) corresponding to the unique code received from the access controller (604) by the device (102), wherein the device (102) is enabled to transmit the trigger key to the access controller (604) through a visible light communication channel of the visible light module (1006) by the device (102) in response to determining the trigger key in the internal memory of the device (102);
a server (608), enabled to validate the trigger key, transmitted by the device (102) to the access controller (604), with a predefined criterion in response to receiving the trigger key by the server (608) from a hub (606), wherein the hub (606) is coupled with the access controller (604);
wherein the server (608) is enabled to transmit a trigger command to the hub (606) by the server (608), in response to validating the trigger key by the server (608); and
the access controller (604) is enabled to unlock the lock (1002) in response to receiving the unlock command from the hub (606) by the access controller (604).

8. The system of claim 7, wherein the wireless communication protocol (1004) is one of a Bluetooth protocol, WiFi protocol, NFC protocol, and a light communication protocol.

9. The system of claim 7, wherein the device (102) is coupled to the server (608) and is enabled to receive a new trigger key after a predefined interval from the server (608).

10. The system of claim 7, wherein the predefined criterion is matching the trigger key received from the hub (606) with a trigger key (906) stored in a database (908) of the server (608).

11. The system of claim 7, wherein the device (102) is an LED enabled (814) device (102).

12. The system of claim 7, wherein the trigger command is, one of, a command for locking an unlocked lock, command for unlocking a locked lock, and command for denying permission to access the lock (1002).

13. An access controller (604), enabled to operate in a two-way communication with a device (102) having a visible light module (1006), the access controller (604) comprising:

a transmission module, enabled to transmit a unique code, stored in a memory (816) of the access controller (604), to the device (102) through a wireless communication protocol (1004), in response to detecting proximity, by a proximity sensor (812) of the access controller (604), of a device (102) to the access controller (604);
a receiver module, enabled to receive a trigger key through a visible light communication channel from the device (102) in response to transmission of the unique code to the device (102), wherein the receiver module is further enabled to receive a trigger command from a server (608), in response to validation of the trigger key with a predefined criterion by the server (608) upon receiving trigger key from a hub (606), wherein the hub (606) is coupled with the access controller (604), and
wherein the transmission module is enabled transmit the trigger command to unlock the door lock (1002) in response to receiving the unlock command from the hub (606).

14. The access controller of claim 13, wherein the wireless communication protocol (1004) is one of a Bluetooth protocol, NFC protocol, WiFi protocol, and a light communication protocol.

15. The access controller of claim 13, wherein the trigger

command is, one of, a command for locking an unlocked lock, command for unlocking a locked lock, and command for denying permission to access the lock (1002).

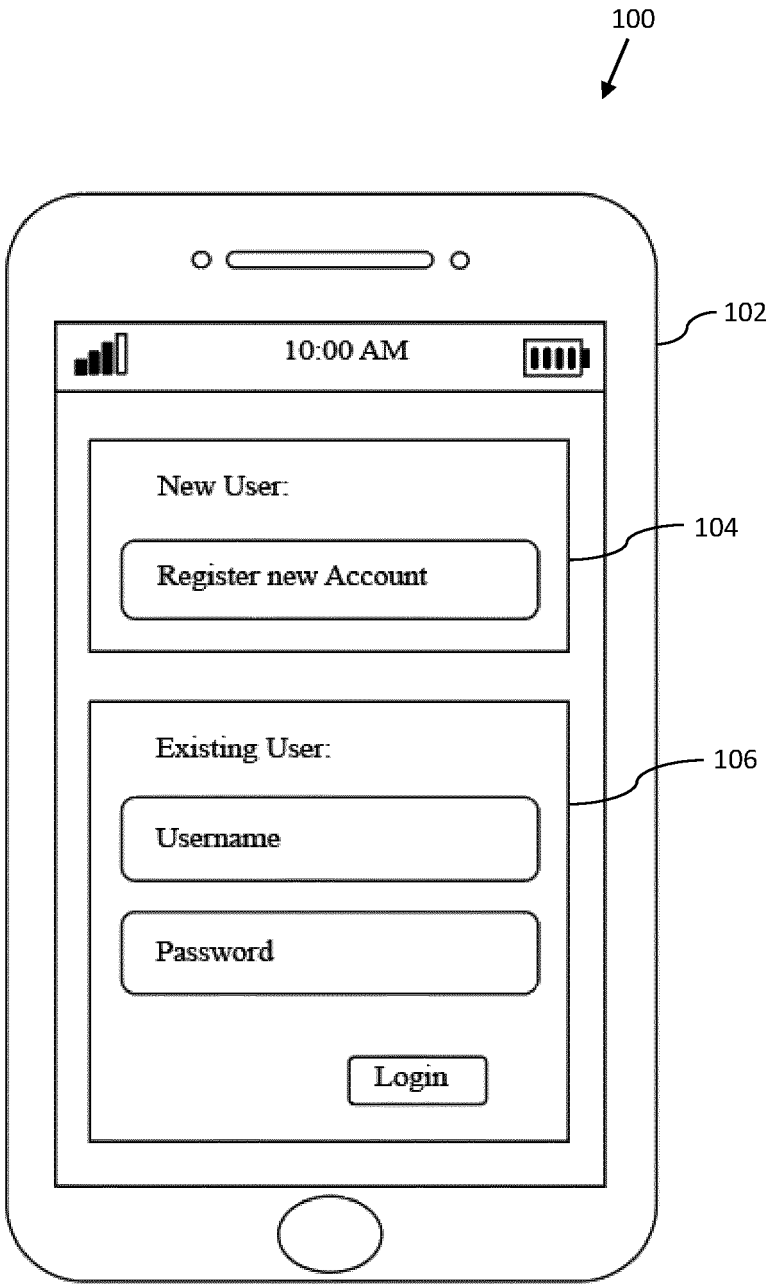
100
102
10:00 AM
New User:
104
Register new Account
Existing User:
106
Username
Password
Login

FIG. 1

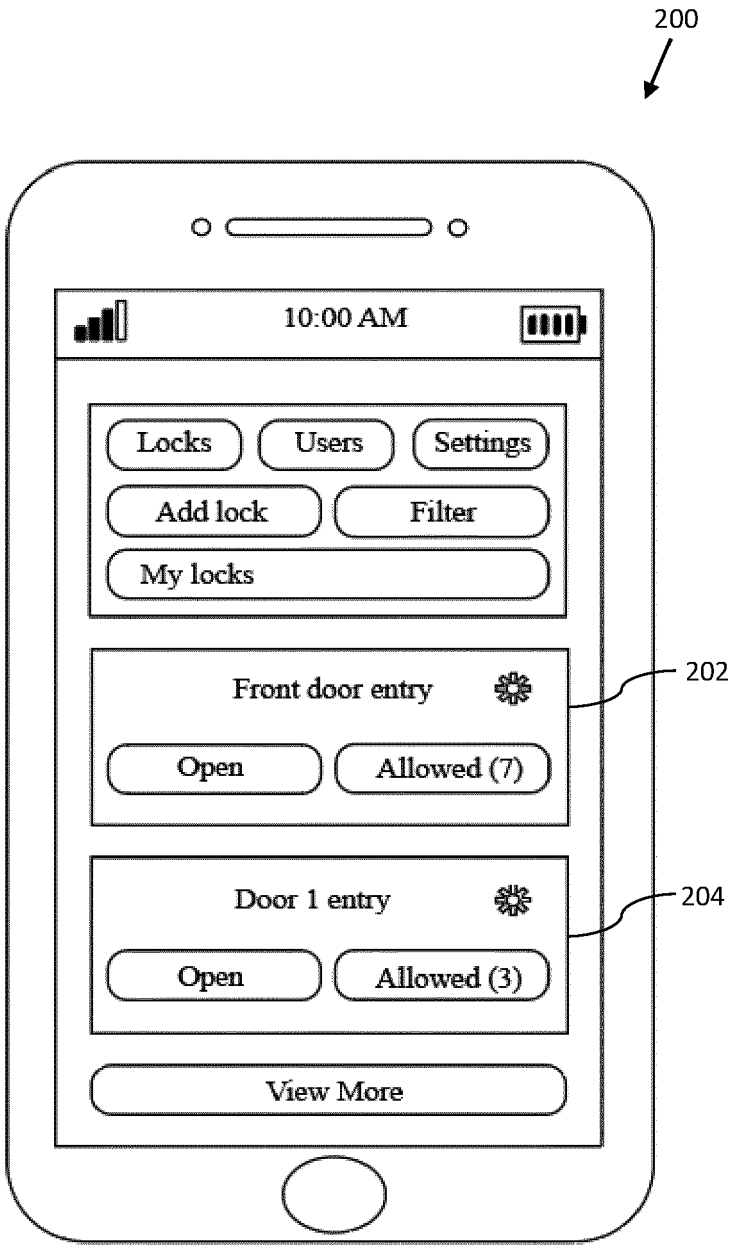
200
10:00 AM
Locks
Users
Settings
Add lock
Filter
My locks
Front door entry
Open
Allowed (7)
202
Door 1 entry
Open
Allowed (3)
204
View More

FIG. 2

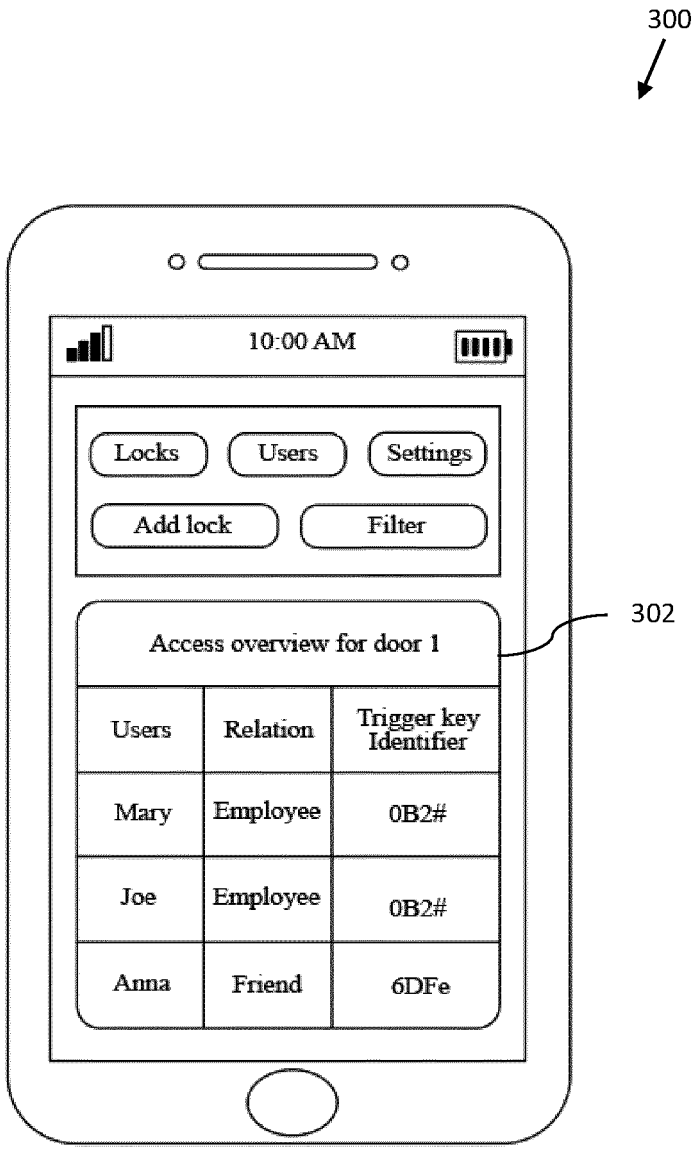
300
10:00 AM
Locks
Users
Settings
Add lock
Filter
Access overview for door 1
302
Users
Relation
Trigger key Identifier
Mary
Employee
0B2#
Joe
Employee
0B2#
Anna
Friend
6DFe

FIG. 3

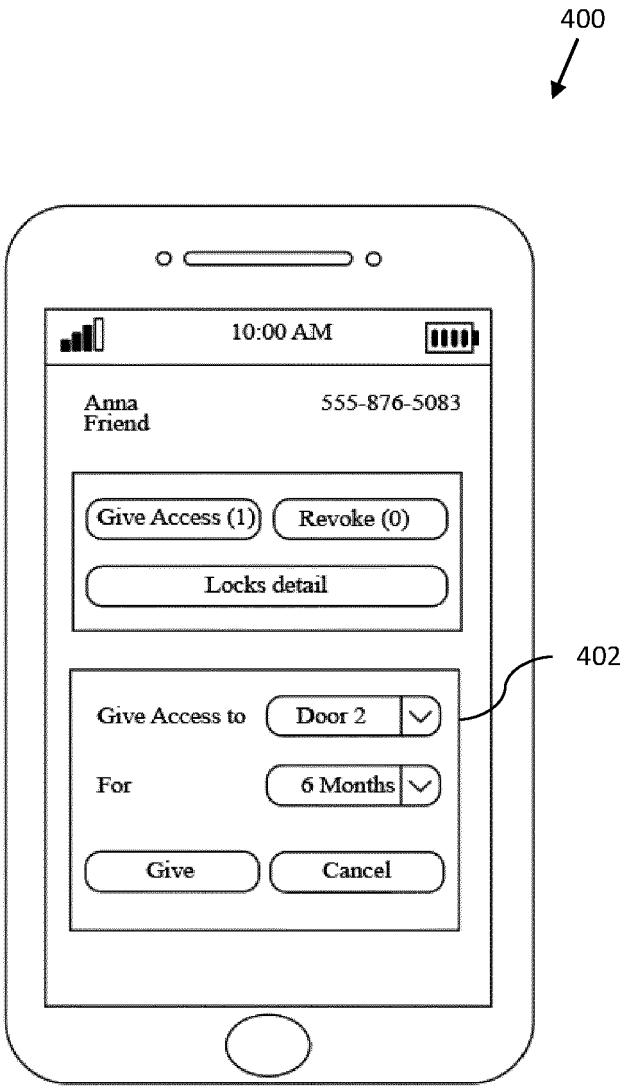
400
10:00 AM
Anna
Friend
555-876-5083
Give Access (1)
Revoke (0)
Locks detail
402
Give Access to
Door 2
For
6 Months
Give
Cancel

FIG. 4

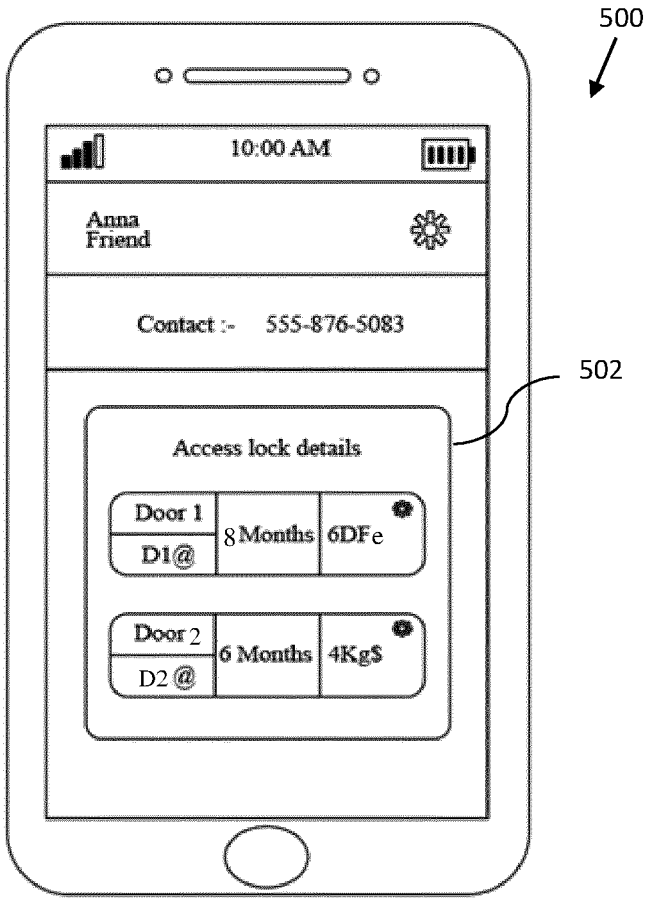
500
10:00 AM
Anna
Friend
Contact :- 555-876-5083
502
Access lock details
Door 1
D1@
8 Months
6DFe
Door 2
D2 @
6 Months
4Kg$

FIG. 5

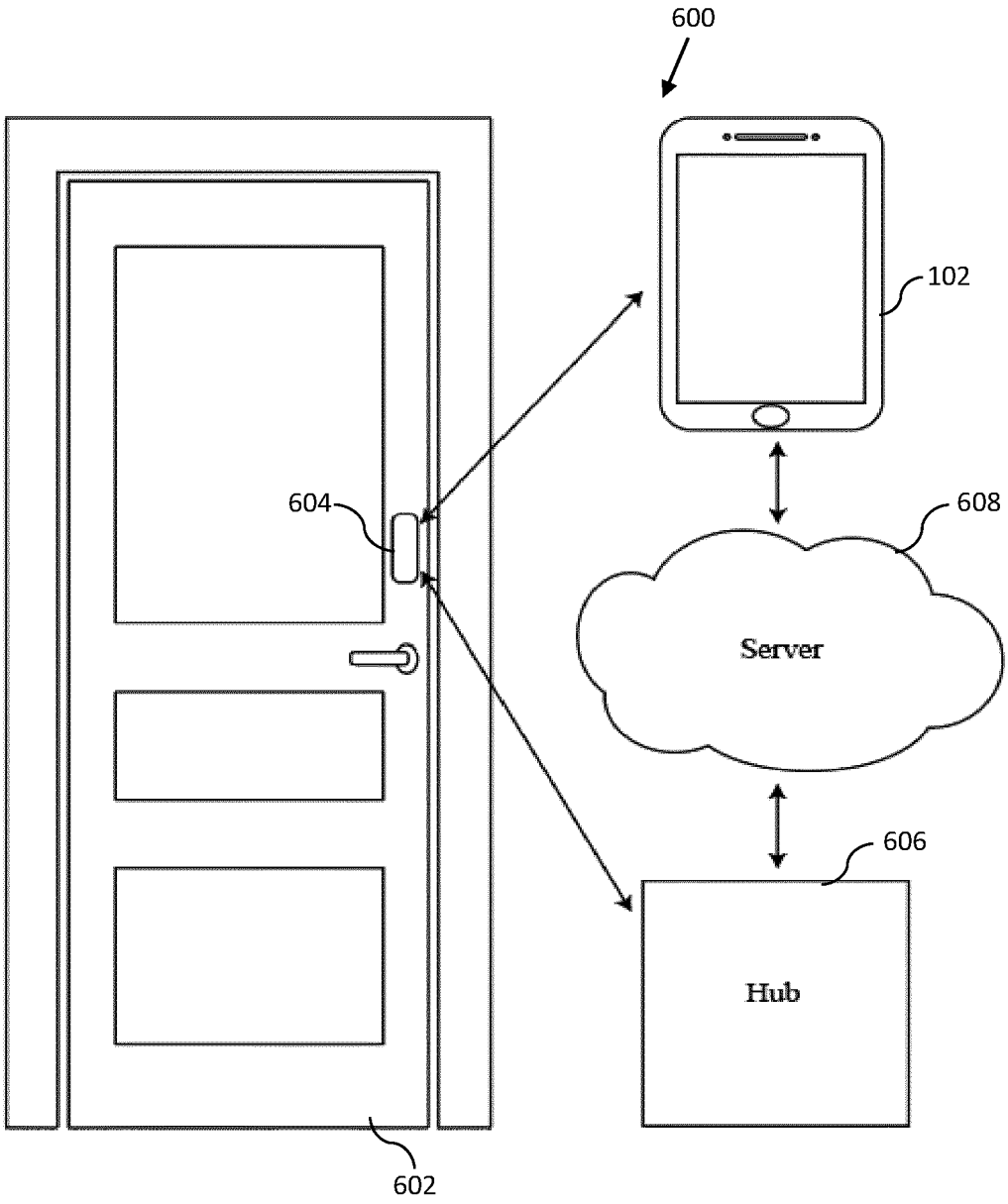

FIG. 6

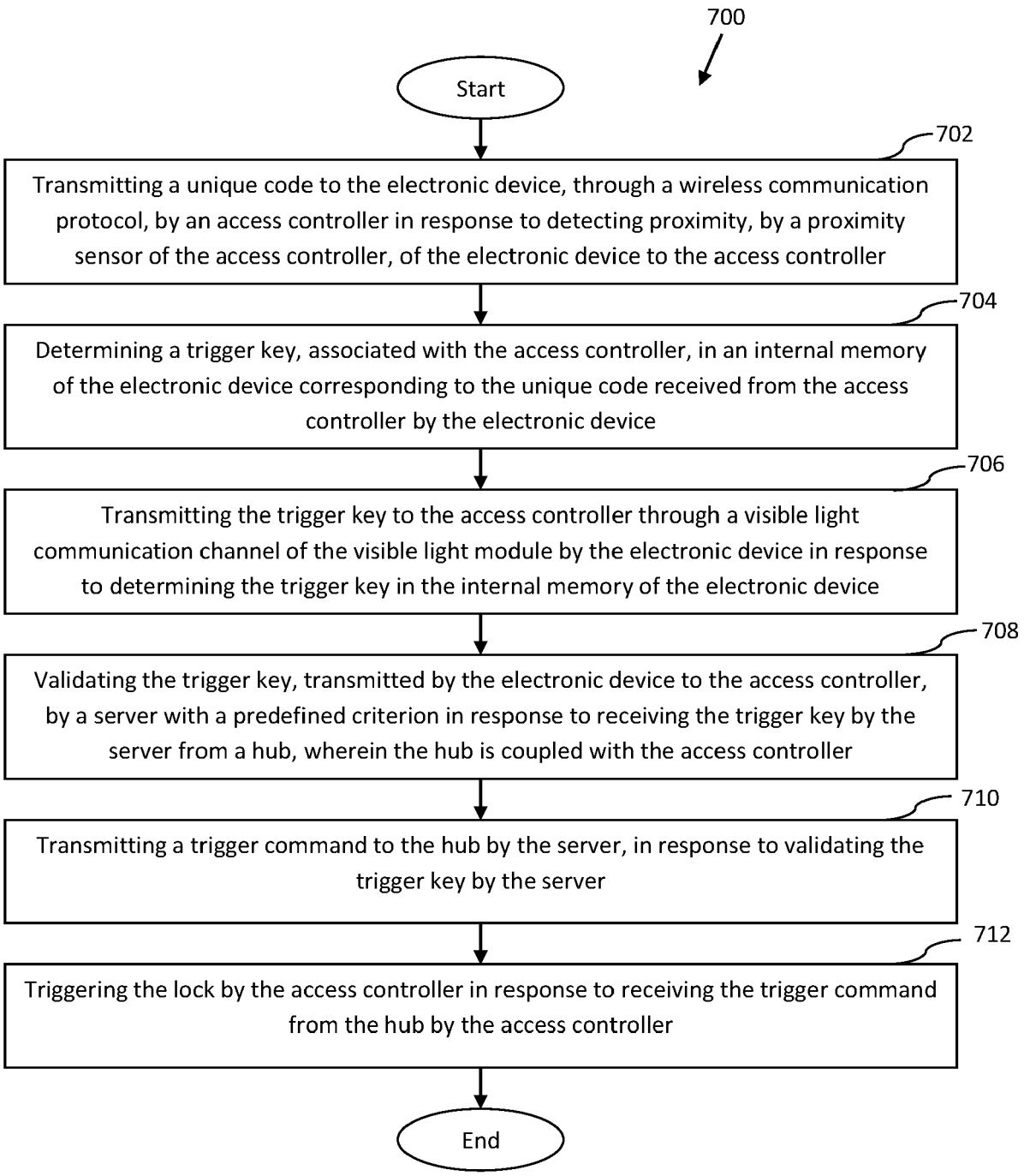
700
Start
702
Transmitting a unique code to the electronic device, through a wireless communication protocol, by an access controller in response to detecting proximity, by a proximity sensor of the access controller, of the electronic device to the access controller
704
Determining a trigger key, associated with the access controller, in an internal memory of the electronic device corresponding to the unique code received from the access controller by the electronic device
706
Transmitting the trigger key to the access controller through a visible light communication channel of the visible light module by the electronic device in response to determining the trigger key in the internal memory of the electronic device
708
Validating the trigger key, transmitted by the electronic device to the access controller, by a server with a predefined criterion in response to receiving the trigger key by the server from a hub, wherein the hub is coupled with the access controller
710
Transmitting a trigger command to the hub by the server, in response to validating the trigger key by the server
712
Triggering the lock by the access controller in response to receiving the trigger command from the hub by the access controller
End

FIG. 7

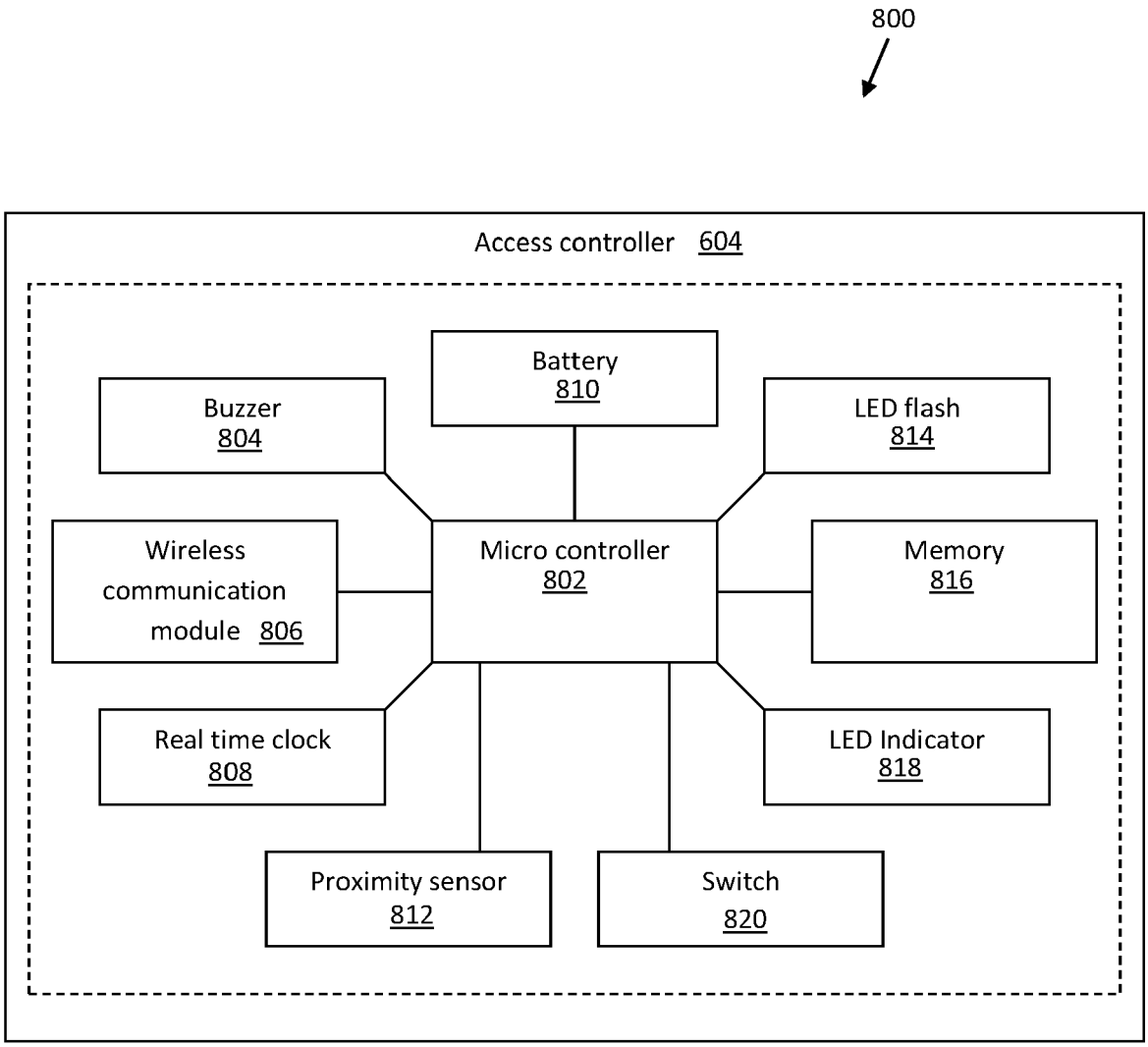
800
Access controller 604
Battery 810
Buzzer 804
LED flash 814
Wireless communication module 806
Micro controller 802
Memory 816
Real time clock 808
LED Indicator 818
Proximity sensor 812
Switch 820

FIG. 8

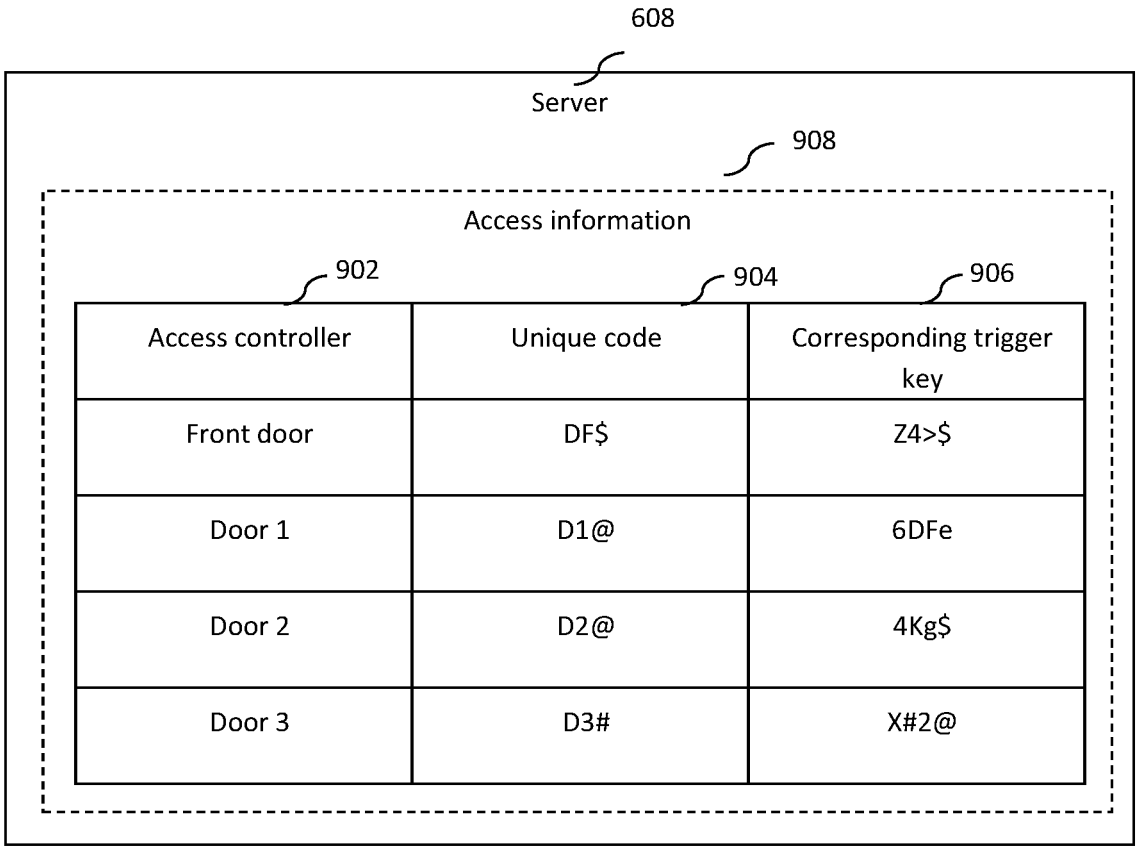
608
Server
908
Access information
902
904
906
Access controller
Unique code
Corresponding trigger key
Front door
DF$
Z4>$
Door 1
D1@
6DFe
Door 2
D2@
4Kg$
Door 3
D3#
X#2@

FIG. 9

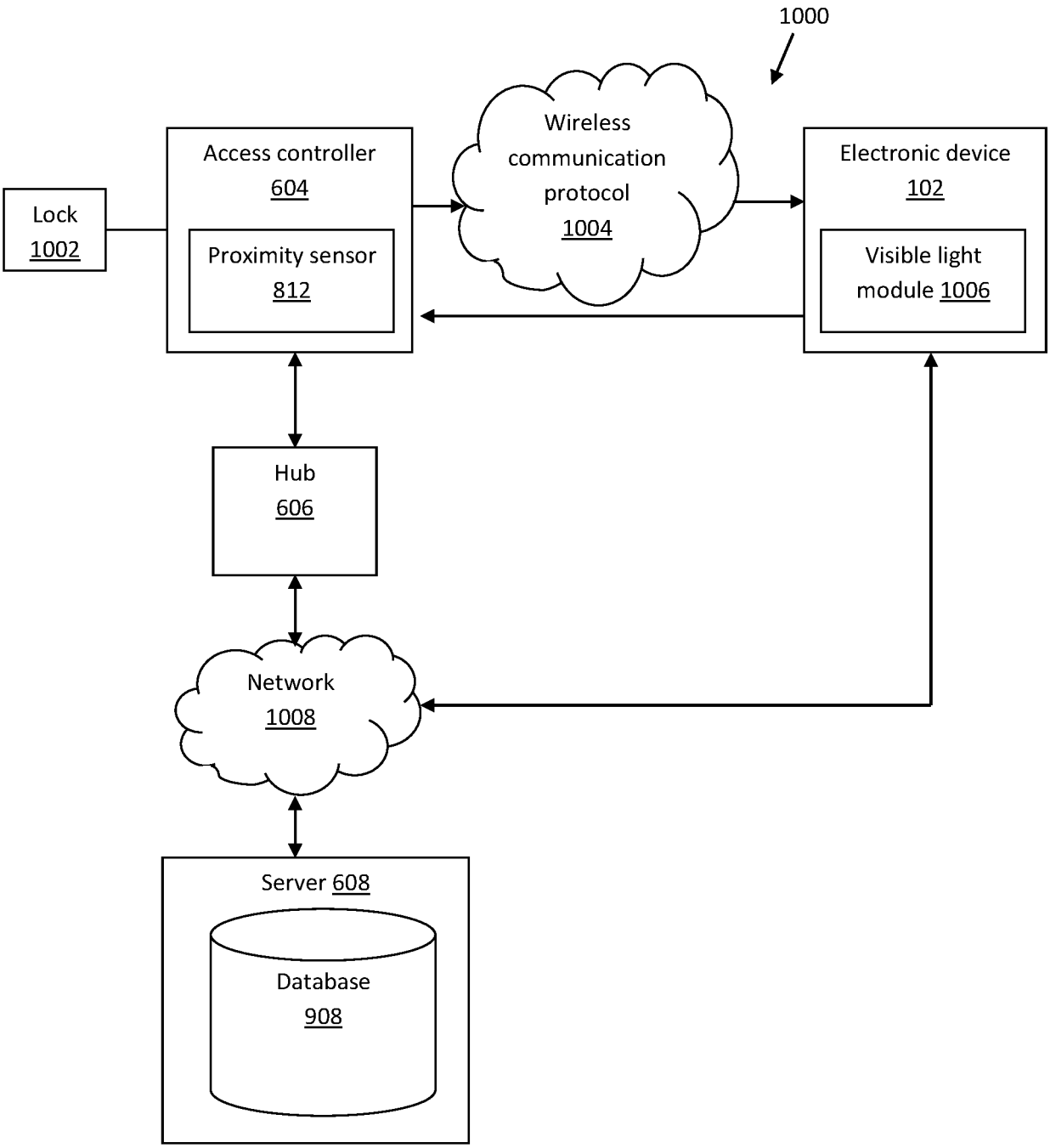
1000
Wireless communication protocol 1004
Access controller 604
Proximity sensor 812
Lock 1002
Electronic device 102
Visible light module 1006
Hub 606
Network 1008
Server 608
Database 908

FIG. 10

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 21 02 0264

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	EP 3 029 906 A1 (KUANG CHI INTELLIGENT PHOTONIC TECHNOLOGY LTD [CN]) 8 June 2016 (2016-06-08) * claims 1, 3, 16, 27, 28 * * figures 1-5 * * paragraph [0017] - paragraph [0034] *	1-15	INV. G07C9/00
X	WO 2017/006172 A1 (ACSYS IP HOLDING INC) 12 January 2017 (2017-01-12) * claims 1, 5 * * figures 4, 5 * * paragraph [0049] - paragraph [0053] * * paragraph [0079] * * paragraph [0090] - paragraph [0098] *	1-15	
X	US 2021/110624 A1 (TAYLOR ROBERT J [US] ET AL) 15 April 2021 (2021-04-15) * claims 12, 13 * * figures 1-4, 7, 8A * * paragraph [0032] * * paragraph [0071] - paragraph [0072] *	1-15	

TECHNICAL FIELDS SEARCHED (IPC)

G07C

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	27 October 2021	Hniene, Badr

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 21 02 0264

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

27-10-2021

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 3029906 A1	08-06-2016	CN 103825871 A	28-05-2014
		EP 3029906 A1	08-06-2016
		JP 2016536889 A	24-11-2016
		KR 20160039227 A	08-04-2016
		US 2016150411 A1	26-05-2016
		WO 2015014232 A1	05-02-2015
WO 2017006172 A1	12-01-2017	CN 107889536 A	06-04-2018
		EP 3266004 A1	10-01-2018
		HK 1248024 A1	05-10-2018
		TW 201712583 A	01-04-2017
		US 2017011573 A1	12-01-2017
		US 2018102009 A1	12-04-2018
		WO 2017006172 A1	12-01-2017
US 2021110624 A1	15-04-2021	US 2020327760 A1	15-10-2020
		US 2021110624 A1	15-04-2021
		WO 2020214646 A1	22-10-2020

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- EP 3360114 A1 **[0004]**