US Patent & Trademark Office
Patent Public Search | Text View

BUILDING ACCESS USING A MOBILE DEVICE

Abstract

Methods and systems for unlocking an access point of a facility with a mobile device. Permissions and locations of access points of the facility that are accessible to a user of a particular mobile device may be downloaded and a location of the particular mobile device determined. The mobile device may identify one or more access points of the facility that are accessible by the user of the mobile device based on the location of the mobile device and the downloaded permissions and locations of the access points. The method may include displaying on the mobile device a notification of the access points that are identified by the mobile device, receiving a selection of one of the displayed access points from the user via a user interface of the mobile device, sending a command from the mobile device to unlock the selected access point, and unlocking the selected access point.

Inventors: **Coniff; Michael (Louisville, KY), Murthy; Krishna (Bangalore, IN), Raman; Sreedhar (Bangalore, IN), Harpanhalli; Karthik (Bangalore, IN)**

Applicant: **Honeywell International Inc.** (Charlotte, NC)

Family ID: **1000008578341**

Appl. No.:   **19/198728**

Filed: **May 05, 2025**

Related U.S. Application Data

parent US continuation 18674464 20240524 PENDING child US 19198728
parent US continuation 18353700 20230717 parent-grant-document US 12027007 child US 18674464
parent US continuation 17188695 20210301 parent-grant-document US 11749045 child US 18353700

Publication Classification

Int. Cl.: **G07C9/28** (20200101); **G07C9/27** (20200101); **H04W4/029** (20180101)

U.S. Cl.:

CPC   **G07C9/28** (20200101); **G07C9/27** (20200101); **H04W4/029** (20180201);

Background/Summary

[0001] This is a continuation of co-pending U.S. patent application Ser. No. 18/674,464, filed May 24, 2024, and entitled "BUILDING ACCESS USING A MOBILE DEVICE", which is a continuation of co-pending U.S. patent application Ser. No. 18/353,700, filed Jul. 17, 2023, and entitled "BUILDING ACCESS USING A MOBILE DEVICE", now U.S. Pat. No. 12,027,007, which is a continuation of co-pending U.S. patent application Ser. No. 17/188,695, filed Mar. 1, 2021, and entitled "BUILDING ACCESS USING A MOBILE DEVICE", now U.S. Pat. No. 11,749,045, all of which are incorporated herein by reference.

TECHNICAL FIELD
[0002] The disclosure is directed to providing building access through a mobile device.
BACKGROUND
[0003] Physical access control systems are designed to provide access to buildings and/or specific areas of a building for individuals who are authorized to access such areas and to deny access to buildings and/or specific areas of the building to individuals who are not authorized to access such areas. For example, certain individuals may be authorized to access a secure area of a building, whereas other individuals may not be allowed to access the secure area. In another example, certain individuals may be authorized to access a first building but not a second building, whereas other individuals may not be allowed to access either building. In some cases, access may be granted only during certain times.
[0004] Current approaches to physical access control systems often rely on users (e.g., employees) carrying physical access cards (e.g., physical badge) to gain entry to areas of a building. For example, a user can swipe a physical access card in an access card reader at a security door to gain entry to an area of a building. However, issuing and managing physical access card can be time consuming, cumbersome and error prone. What would be desirable is a system which allows a user's mobile device to act as an access credential with current building access systems.
SUMMARY
[0005] This disclosure is directed to providing and/or managing access control, and more particularly to methods and systems for using a user's mobile device as an access credential to gain access to one or more authorized areas.
[0006] An example method for managing access to a facility may include selecting a commissioning mode in an application running on a mobile device. When in the commissioning mode, displaying via a user interface of the mobile device a list of access points associated with the facility, receiving a selection of an access point from the list of access points via the user interface of the mobile device, physically placing the mobile device adjacent to the selected access point, capturing and storing a current location of the mobile device and thus a location of the selected access point, associating the captured location of the mobile device with the selected access point, repeating the receiving, placing, capturing and associating steps for each of two or more access points in the list of access points, and uploading the associations between the captured locations of the mobile device and each of the two or more access points. These associations may be used in

controlling access to the facility.

[0007] In some cases, the method may include subsequently receiving a registration request from a user via a user interface of a user mobile device, associating the user and the user mobile device with one or more access points from the list of access points based on one or more user permissions, displaying on the user mobile device at least some of the one or more access points that the user is associated based on one or more user permissions, selecting via the user interface of the user mobile device one of the displayed access points to unlock, and sending a request to unlock the selected access point.

[0008] In some cases, the method may include determining a current location of the user mobile device and determining a distance between the current location of the user mobile device and the location captured in the commissioning mode and associated with each of the two or more access points. The access points that are displayed on the user interface of the user mobile device may be those that are within a threshold distance of the current location of the user mobile device.

[0009] In another example, a method for unlocking an access point of a facility may include downloading permissions and locations of access points of the facility that are accessible to a user of a particular mobile device and receiving a location of the particular mobile device. The particular mobile device may determine one or more access points of the facility based on the location of the particular mobile device and the downloaded permissions and locations of the access points of the facility. The method may further include displaying on the particular mobile device a notification of the one or more access points that are determined by the particular mobile device, receiving a selection of one of the displayed access points from the user via a user interface of the particular mobile device, sending a command from the particular mobile device to unlock the selected access point, and unlocking the selected access point. Prior to unlocking the selected access point, the method may further include verifying one or more access credential of the user.

[0010] In some cases, the notification of one or more access points may identify those access points that are within a predetermined distance from the particular mobile device and may not include those access points that are not within the predetermined distance from the particular mobile device. Alternatively, the notification of one or more access points may include all access points in the facility that are accessible by the user.

[0011] In another example, a non-transitory computer-readable medium having instructions stored thereon that when executed by a mobile device may be configured to receive a user credentials from a user via a user interface of the mobile device to verify an identity of the user, verify the received user credentials of the user, receive a current location of the mobile device from a location service of the mobile device, determine a distance between the current location of the mobile device and each of one or more access points of a facility, and display on the user interface of the mobile device one or more of the access points of the facility. The one or more access points that are displayed may be those that are accessible to the user based on one or more access point permissions associated with the user, and in some cases are within a threshold distance from the current location of the mobile device. The user interface of the mobile device may receive a selection of one of the displayed access points to unlock, and the mobile device may send a request to unlock the selected access point to an access control system of the building.

[0012] The preceding summary is provided to facilitate an understanding of some of the features of the present disclosure and is not intended to be a full description. A full appreciation of the disclosure can be gained by taking the entire specification, claims, drawings, and abstract as a whole.

Description

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] The disclosure may be more completely understood in consideration of the following detailed description of various embodiments in connection with the accompanying drawings, in which:

[0014] FIG. **1** is a schematic diagram of an illustrative access control system for accessing multiple buildings via mobile device;

[0015] FIG. **2** is a flow chart of an illustrative method for commissioning an access control system;

[0016] FIGS. **3-5** are illustrative screen captures of an application for commissioning the access control system for use by an installer;

[0017] FIG. **6** is a flow chart of an illustrative method for using a user's mobile device to access a building;

[0018] FIG. **7** is an illustrative setup portal for an access control system for use by an administrator;

[0019] FIG. **8** is a flow chart of another illustrative method for using a user's mobile device to access a building; and

[0020] FIGS. **9-12** are illustrative screen captures of an application running on a user's mobile device to access a building.

[0021] While the disclosure is amenable to various modifications and alternative forms, specifics thereof have been shown by way of example in the drawings and will be described in detail. It should be understood, however, that the intention is not to limit aspects of the disclosure to the particular embodiments described. On the contrary, the intention is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of the disclosure.

DESCRIPTION

[0022] For the following defined terms, these definitions shall be applied, unless a different definition is given in the claims or elsewhere in this specification.

[0023] All numeric values are herein assumed to be modified by the term "about", whether or not explicitly indicated. The term "about" generally refers to a range of numbers that one of skill in the art would consider equivalent to the recited value (i.e., having the same function or result). In many instances, the term "about" may be indicative as including numbers that are rounded to the nearest significant figure.

[0024] The recitation of numerical ranges by endpoints includes all numbers within that range (e.g., 1 to 5 includes 1, 1.5, 2, 2.75, 3, 3.80, 4, and 5).

[0025] Although some suitable dimensions ranges and/or values pertaining to various components, features and/or specifications are disclosed, one of skill in the art, incited by the present disclosure, would understand desired dimensions, ranges and/or values may deviate from those expressly disclosed.

[0026] As used in this specification and the appended claims, the singular forms "a", "an", and "the" include plural referents unless the content clearly dictates otherwise. As used in this specification and the appended claims, the term "or" is generally employed in its sense including "and/or" unless the content clearly dictates otherwise.

[0027] The following description should be read with reference to the drawings in which similar elements in different drawings are numbered the same. The drawings show by way of illustration how one or more embodiments of the disclosure may be practiced. The illustrative embodiments depicted are intended only as exemplary. Selected features of any illustrative embodiment may be incorporated into an additional embodiment unless clearly stated to the contrary.

[0028] User interaction with a door access control system can be streamlined using capabilities offered by mobile devices. For example, in some embodiments, global positioning system (GPS), WiFi, Bluetooth, and/or other location functionalities provided by a mobile device may allow the automatic determination of user location (e.g., without user input). Thus, in some cases, rather than

physically presenting a card (or other device) for access to an area or facility, the user may simply move within a particular distance of a door and be automatically presented with an option to unlock the door. Rather than using "card readers", embodiments of the present disclosure allow a user's mobile device to perform the function of an access card. It is contemplated that the embodiments of the present disclosure may be utilized with a variety of access systems. In some cases, embodiments of the present disclosure may be used with or in place of systems with door access card readers (those with and/or without Bluetooth® capabilities). Alternatively, or additionally, embodiments of the present disclosure may be used with systems that only include an actuatable lock mechanism (e.g., no card readers present).

[0029] The present disclosure is generally directed towards methods and systems for allowing secure access to one or more access points using a mobile device. It is contemplated that the system may allow a user to access two different buildings having two different access control providers using the same mobile device. In some cases, the buildings may belong to the same entity (e.g., company and corporation) or the buildings may belong to different entities, as may be the case for a person servicing certain building equipment that is use in many buildings. Generally, access points may be tagged with a geographic location (e.g., latitude, longitude, and/or altitude) and a door name. These access points may be selectively made available to users via the user's mobile device. Actuation of an unlock button on the mobile device may result in the unlocking of the door.

[0030] Embodiments of the present disclosure can reduce the need to issue a physical badge for every location or facility that a person (e.g., an employee, a contractor, a repair person, etc.) needs to access. Embodiments of the present disclosure can be retrofit to existing access control systems with and/or without smart reader systems without having to add additional hardware. Further, embodiments of the present disclosure may streamline or facilitate access requests for access to facilities and/or locations.

[0031] FIG. **1** is a schematic diagram of an illustrative access control system **10** for multiple buildings **20**, **30** via a user's mobile device **40**. A facility or building, as used herein, can refer to one or more buildings, businesses, homes, plants, hospitals, refineries, etc. Facilities can include indoor and/or outdoor areas. The illustrative system **10** may include a first facility **20**, a second facility **30**, a mobile device **40**, a first door access control system (ACS) **50** optionally including at least one card reader **51** and in communication with one or more relays **22***a*, **22***b* (collectively **22**), and a second door access control system (ACS) **60** optionally including at least one card reader **61** and in communication with one or more relays **32***a*, **32***b* (collectively, **32**). While the illustrative system **10** includes a first and a second facility **20**, **30**, it should be understood that the system **10** may be applied to fewer than two facilities or more than two facilities, such as, but not limited to three or more, 10 or more, 20 or more, 50 or more, etc. Similarly, while the illustrative system **10** is illustrated as having a first and a second access system **50**, **60**, it should be understood that the system **10** may be applied to less or more than two or more than two access systems. In some cases, the number of access systems may correspond to the number of facilities in the system **10**. While the access control systems **50**, **60** are described as door access control systems, the access control systems **50**, **60** may control other means of entry into a building or area, including, but not limited to, turnstiles or baffle gates, revolving doors, gates, etc.

[0032] Though in the example illustrated in FIG. **1** the first ACS **50** is shown external to the first facility **20** (e.g., remote with respect to the first facility **20**) and the second ACS **60** is shown external to the second facility **30** (e.g., remote with respect to the second facility **30**), embodiments of the present disclosure are not so limited. In some cases, the first ACS **50** and/or the second ACS **60** are internal to the first facility **20** (e.g., local with respect to the first facility **20**) and/or the second facility **30** (e.g., local with respect to the second facility **30**), respectively.

[0033] The mobile device **40** may be a client device carried or worn by a user. It should be understood that more than one mobile device **40** may be utilized with the access control system **10**. For example, each user may have their own particular or unique mobile device **40**. The mobile

device **40** may be a phone (e.g., smartphone), personal digital assistant (PDA), tablet, and/or wearable device (e.g., wristband, watch, necklace, etc.). These are just examples. The mobile device **40** may include a user interface including a display and a means for receiving user input (e.g., touch screens, buttons, keyboards, etc.). The mobile device **40** may further have locations services. For example, the mobile device **40** may use a built-in global positioning system (GPS) in combination with GPS satellites to pinpoint a location of the mobile device **40**. In other cases, the location of the mobile device **40** may be estimated based on a direction of the signal and a distance from one or more cell towers. The mobile device **40** can include one or more software applications (e.g., apps) **46** stored within a memory **42** of the mobile device **40** that can define and/or control communications between the mobile device, the first ACS **50**, the second ACS **60**, and/or other devices. In some cases, the mobile device **40** may communicate with the first ACS **50**, the second ACS **60**, and/or other devices via a remote or cloud server **70**, as will be described in more detail herein. Apps **46** may be received by the mobile device **40** from the first ACS **50** and/or the second ACS **60**, for instance, although this is not required. In other embodiments, the application **46** may be downloaded from an app store, such as, but not limited to ITUNES® or GOOGLE PLAY®, or an access control service provider's web site.

[0034] In some embodiments, the application **46** may be an integrated security platform which may include access control and security system components. Users may manage the access control system and/or the security system from the app **46** and/or via a web browser, as desired. In some cases, the app **46** may present different features based upon a user's login credentials. It is contemplated that the amount and type of information that is visible to a user of the app **46** may be based, at least in part, on the permissions assigned to the particular user. For example, a member of a security team may have access to the security system components while a routine building user may not. Further, some users may be capable of accessing a commissioning mode while other users may not. In some cases, different applications **46** may be available for regular employees and visitors.

[0035] Apps **46** may be launched by a user and/or responsive to some other condition (e.g., the interaction between the mobile device **40** and a device within the door access system, such as a controller or relay, or when the location services of the mobile device detects the location of the mobile device is near a facility in which the user is registered to access). In some embodiments, apps **46** can be executing as background apps. As used herein, at least one of the apps **46** includes a digital identifier. In some cases, the digital identifier may be a unique device identifier provided by the phone operating system (e.g., Android™ (Android is a trademark of Google LLC), iOS® (IOS is a trademark of Cisco and used under license by Apple), etc.) to uniquely identify a mobile device. In other cases, a digital identifier may include, but is not limited to a phone number and/or an International mobile equipment identity (IMEI) number. In some cases, at least one of the apps **46** may include more than one digital identifier.

[0036] In the example shown, the relays **22**, **32** can be actuated by variation in conditions of one or more electric circuits. In some examples, the relays **22**, **32** can be a locking device (e.g., for a door). In some examples, the relays **22**, **32** can include one or more actuating mechanisms. The relays **22**, **32** can be associated with one or more controlled functionalities. As used herein "controlled functionality" refers to a functionality under the control of the first ACS **50** and/or the second ACS **60**. For instance, an electronic door lock may include a relay that is controlled by the first ACS **50** and/or the second ACS **60** to lock/unlock a door.

[0037] The relays **22***a*, **32***a* can be associated with an entry point (e.g., an exterior door) of the respective facility **20**, **30**, and/or the relays **22***b,* **32***b* can be associated with a specific area **24**, **34** of the respective facility **20**, **30**. As referred to herein, an area can be a portion of a facility. In some embodiments, the area **24**, **34** can be a room, a plurality of rooms, a wing, a building, a plurality of buildings, a campus, etc. In some embodiments, the area **24**, **34** can be defined by physical boundaries (e.g., walls, doors, etc.). In some embodiments, the area **24**, **34** can be defined by

logical and/or geographic boundaries (e.g. geofence). The area **24**, **34** can be defined by a user, by a Building Information Model (BIM) associated with the respective facility **20**, **30**, by the first ACS **50** and/or the second ACS **60**, and/or in any other suitable way.

[0038] The first ACS **50** and/or the second ACS **60** can control (e.g., manage) access to a number of areas (e.g., the area **24**, **34**) and/or a number of entry points of the respective facility **20**, **30**. As previously discussed, the first ACS **50** and/or the second ACS **60** can be remote with respect to the facility **20**, **30** and/or local with respect to the facility **20**, **30**. In some embodiments, the first ACS **50** and/or the second ACS **60** can be cloud-based. In some embodiments, the first ACS **50** and/or the second ACS **60** can manage access to one or more areas across a plurality of facilities. It is further contemplated that the first ACS **50** and the second ACS **60** may be configured to accept different credentials and/or may have different connectivity, although this is not required.

[0039] The mobile device **40** can communicate with (e.g., exchange data with) the first ACS **50** and/or the second ACS **60** via a wired and/or wireless connection, for instance. In some cases, the communication may occur via a cloud server **70**. For example, the mobile device **40** may transmit information to the cloud server **70**, the cloud server **70** may process the information and subsequently transmit a command to the appropriate ACS **50**, **60**. In some embodiments, the mobile device **40** can communicate using one or more communication modules (e.g., cellular, WiFi, etc.). The first ACS **50** and/or the second ACS **60** can communicate with the relays **22**, **32** via a wired and/or wireless connection, for instance. Communication between various devices herein can be carried out over a wireless and/or a wired network. A wireless network, as used herein, can include WiFi, Bluetooth, Cellular or any other suitable means to wirelessly transmit and/or receive information.

[0040] The illustrative mobile device **40** includes a memory **42** and a processor **44**. The processor **44** is configured to execute executable instructions stored in the memory **42** to perform various tasks. Data may also be stored in the memory **42** to be used in executing the instructions. For example, in some embodiments, the memory **42** stores instructions executable by the processor **44** to provide data in the form of a specific user identity assigned to the mobile device to the access control system. The memory **42** can be any type of non-transitory storage medium that can be accessed by the processor **44** to perform various examples of the present disclosure. For example, the memory **42** can be a non-transitory computer readable medium having computer readable instructions (e.g., computer program instructions) stored thereon that are executable by the processor **44**. The execution of the computer readable instructions may result in the actuation of a relay **22**, **32** which in turn allows entrance to a facility **20**, **30** and/or an area **24**, **34** of said facility **20**, **30**.

[0041] The memory **42** can be volatile or nonvolatile memory. The memory **42** can also be removable (e.g., portable) memory, or non-removable (e.g., internal) memory. For example, the memory **42** can be random access memory (RAM) (e.g., dynamic random access memory (DRAM) and/or phase change random access memory (PCRAM)), read-only memory (ROM) (e.g., electrically erasable programmable read-only memory (EEPROM) and/or compact-disc read-only memory (CD-ROM)), flash memory, a laser disc, a digital versatile disc (DVD) or other optical storage, and/or a magnetic medium such as magnetic cassettes, tapes, or disks, among other types of memory.

[0042] In addition to, or in place of, the execution of executable instructions, various functions of the present disclosure can be performed via one or more devices (e.g., one or more controllers) having logic. As used herein, "logic" is an alternative or additional processing resource to execute the actions and/or functions, etc., described herein, which includes hardware (e.g., various forms of transistor logic, application specific integrated circuits (ASICs), etc.), as opposed to computer executable instructions (e.g., software, firmware, etc.) stored in memory and executable by a processor. It is presumed that logic similarly executes instructions for purposes of the embodiments of the present disclosure.

[0043] In some cases, the memory **42** can store data in the form of a digital identifier that is associated with an application **46** that is also stored in memory **42** on the mobile device **40**. The memory **42** can also include instructions executable by the processor **44** to provide this information to an access control system when the application **46** is in use and the user has met certain conditions that enable the user to request that the digital identifier be sent to the access control system. In some cases, the user must authenticate himself to the mobile device by entering a password or fingerprint scan to unlock the mobile device **40** and/or the application **46**, before the application **46** will initiate any sending of an identifier and/or unlock command.

[0044] FIG. **2** is a flow chart of an illustrative method **100** for commissioning an access control system (such as, but not limited to ACS **50** and/or ACS **60**) for use with a mobile device **40** and application **46**. While one or more access control systems **50**, **60** may be commissioned with a same app or by a same person, for the sake of brevity, description of the commissioning procedure will be described with respect to a single access control system **50**. In some cases, the method **100** for commissioning an access control system may be performed by an installer or other designated personnel. However, this is not required. To begin, the user may select a commissioning mode in an application (e.g., app **46**) running on a mobile device **40**, where the mobile device includes both a user interface and a location service. Prior to entering or once in the commissioning mode, the application may be configured to display available systems of a facility (e.g., access control systems, security systems, etc.) to the user. In some cases, the commissioning mode may be entered after selection of a particular system. FIG. **3** is an illustrative screen capture **200** of a summary screen that may be displayed on the mobile device **40** by the application **46** for a particular building (e.g., facility **20**) when a supervising user or installer has entered their user credentials (e.g., username and password, facial recognition, fingerprint recognition, etc.). The application **46** may be configured to display a status of a security system **202**, a number of access points **204** connected to the access control system **50**, cameras or other devices associated with a security system **206**, a number of people in the facility **208**, and/or a summary of activities **210**. These are just examples. Some information may be omitted or additional information included, as desired. In some cases, the summary screen **200** may be based on user defined settings or preferences.

[0045] Returning to FIG. **2**, in the commissioning mode, a list of access points associated with the facility may be displayed on the user interface of the mobile device **40**, as shown at block **104**. FIG. **4** is an illustrative screen capture **220** of a list of access points **222** associated with the facility **30**. This screen **220** may be reached by selecting the access points **204** on screen **200** of FIG. **3**. Returning to FIG. **2**, a selection of an access point from the list of access points may be received via the user interface of the mobile device **40**, as shown at block **106**. The access points are not required to have a card reader to be displayed. For example, any access point capable of having a remotely actuated locking mechanism may be displayed. FIG. **5** is an illustrative screen capture **230** of details for a selected access point. In the illustrative embodiment, the "building access" access point was selected from the list illustrated in screen capture **220** of FIG. **4**. In the illustrative embodiment, the user has the option to select an "actions" button **232** or to select a "TAG location" button **234**. Returning to FIG. **2**, the mobile device **40** may be carried and physically placed adjacent to the selected access point, as shown at block **108**. In some cases, the user may need to travel to the selected access point in order to place the mobile device **40** adjacent thereto. It is contemplated that the list of access points **222** may be dynamically updated as the installer moves through the facility **20** to display only access points in close proximity to the installer, although this is not required. In some cases, the list of access points **222** may display all access points in the facility **20**.

[0046] Once the mobile device **40** is adjacent to the selected access point, the current location of the mobile device **40** and thus a location of the selected access point may be captured and stored, as shown at block **110**. In some cases, this may be performed through selection of the TAG location button **234** on the user interface of the mobile device **40**. The location of the mobile device **40** may

be determined using a GPS location of the mobile device **40** using location services of the mobile device **40**. The GPS location may include latitude, longitude, and altitude as shown in FIG. **5**. The captured location of the mobile device **40** may be associated with the selected access point, as shown at block **112** of FIG. **2**. In some cases, the captured location may be stored with the selected access point in a database in the cloud server **70**. In other cases, the captured location may be stored locally within the facility **20** and/or at any other suitable location.

[0047] Next, it may be determined if a location has been captured and stored for each access point of the facility **20** desired to be accessible via a mobile device, as shown at block **114** of FIG. **2**. If not all of the access points have been captured, the steps of receiving a selection of an access point **106**, placing the mobile device **40** adjacent to the selected access point **108**, capturing and storing a location **110** of the mobile device **40**, and associating the captured location of the mobile device **40** with the selected access point **112** may be repeated for each access point desired to be accessible via a mobile device **40**. In some cases, the receiving **106**, placing **108**, capturing **110**, and associating **112** steps may be repeated for each of two or more access points in the list of access points shown in FIG. **4**.

[0048] The associations between the captured locations of the mobile device **40** and each of the access points may then be uploaded, as shown at block **116**. In some cases, the captured locations of the mobile device and each of the access points may be uploaded to a remote cloud server **70**. In other cases, the captured locations of the mobile device and each of the access points may be uploaded to a server or storage device located locally to the facility. Once the associations have been stored, they may be used to control access to and within the facility **20**, as shown at block **118**.

[0049] In some cases, a subsequent user may be required to register with an access control system **50** to use a mobile device **40** to access a facility **20** or an area **24** within the facility **20**. FIG. **6** is an illustrative flow chart **300** of a method for registering a user to the ACS **60** and accessing an access point. To begin, a registration request may be received from a user, as shown at block **302**. In some cases, the user may initiate the user registration request via the app **46** used to access one or more access points in the facility **20**. In other cases, the user may initiate the user registration request via a web browser, email or any other suitable mechanism. In some cases, a supervising user may initiate the registration request on behalf of the user. Once the user request is received, the user and the user's mobile device **40** may be associated with one or more access points, as shown at block **304**. It is contemplated that a quantity of access points or which particular access points may be associated with a user may be determined, at least in part, on an employment status and/or a hierarchical level of the user. For example, a regular employee may have the ability to access more access points than a contract employee who in turn may have the ability to access more access points than a visitor. This is just one example.

[0050] In some cases, the registration process may be performed by a supervising or administrative user. For example, an administrative user may utilize a mobile device access setup portal to associate a user and/or a user's mobile device with access permissions. FIG. **7** is a screenshot of an illustrative mobile device access setup portal **350** for use by an administrator. The setup portal **350** may include a list or menu **352** of selectable options. For example, the menu **352** may allow the supervising user to view detailed information related to building sites **20**, **30** and/or access control systems **50**, **60** thereof. In some cases, the menu **352** may include an option to allow the supervising user to view and/or edit "people" **354** (among other options) associated with the organization. In the illustrative embodiment of FIG. **7**, people **354** has been selected and detailed information regarding people associated with the organization is displayed. For example, the setup portal **350** includes a list of people **356**. The list may include an image **358** of each particular person and an employment status **360** (e.g., visitor, regular employee, contract employee, temporary employee, etc.) This list **356** may also include access credentials **362** associated with the particular person. Selection of a particular person may allow the administrative user to edit the information and/or permissions associated with the particular person.

[0051] In the illustrative embodiment of FIG. **7**, a new user is being added in region **364** of the screen. The administrative user may generate a profile for the new user through the selection of the profile tab **366** and may add permissions through the selection of the permissions tab **368**. In the illustrative embodiment of FIG. **7**, the permissions tab **368** has been selected. The supervising user may add a card-based access credential **370** that is assigned to the new user, although this is not required. The supervising user may also add information that associates a specific mobile device **40** with the new user, such as, but not limited to a unique device identifier **372** and/or a mobile device telephone number **374** of the user's mobile device. In some cases, the unique device identifier **372** may be automatically detected via the application **46** and transmitted with the user request. The supervising user may also assign the user to a permissions group **376** which determines which access points or group of access points the user is authorized to access with the mobile device **40** (and/or access card). For example, the user and the user mobile device **40** may be associated with one or more access points from the list of access points **376** based on one or more user permissions. In some cases, the user may not be granted door access. In other cases, the user may be assigned a custom permissions group. The administrative user may also select an activation date **378** and/or an expiration date **380** to further customize a user's access permissions. It is further contemplated that the supervising user may assign time windows during which the user may utilize the access points. For example, the user may be allowed to use access points during predetermined hours and/or predetermined days.

[0052] In some cases, a visitor to the facility **20** may be capable of submitting an access request for preapproval. It is contemplated that when the visitor request is approved and credentials assigned, the visitor may receive an email or a text message with a link to download the app **46** as well as login credential information. In other cases, the visitor may register or submit a visit request using the application **46**. This may facilitate visitor access during high volume hours.

[0053] Returning to FIG. **6**, once a user and the user mobile device have been associated with one or more access points, the user may begin to use the mobile device **40** to open one or more access points. Generally, the user may open the application **46** on the mobile device **40** to display on the user mobile device **40** at least some of the access points available to the user, as shown at block **306**. It is contemplated that not all of the access points available to the user (based on the user permissions) will be displayed simultaneously. For example, the current location of the user mobile device **40** may be used select a subset of the available access points to be displayed. A distance between the current location of the user mobile device **40** (as determined by the location services of the user mobile device **40**) and the locations of the access points captured in the commissioning mode (and associated with access points) may be determined. Access points that are within a threshold distance of the current location of the user mobile device **40** may be displayed on the user interface of the user mobile device **40**. It is contemplated that the threshold distance is programmable. This may facilitate the locating of the access point that is desired to be opened by reducing the number of access points visible to the user. The user may then select one of the displayed access points unlock, as shown at block **308**. The request to unlock the access point may be sent to the ACS **60**, in some cases, via an intermediate cloud server **70**, as shown at block **310**. In some cases, the user may receive a confirmation on the user mobile device **40** that the access point has been unlocked.

[0054] FIG. **8** is a flow chart of another illustrative method **400** of using a user's mobile device **40** to access a building. It should be understood that actions performed at the mobile device **40** is accomplished by the processor **44** executing executable instructions stored in a memory **42** of the mobile device **40** and/or logic of the mobile device **40**. To begin, permissions and locations of access points of the facility that are accessible to the user of a particular mobile device **40** are downloaded to the particular mobile device **40**, as shown at block **402**. It is contemplated that this step may not be needed each time the user accesses the application **46**. A user may present user credentials to the application **46** via a user interface of the mobile device **40** in order to authenticate

themselves to the application **46** to verify the users identify. This may include providing a username and password and/or using biometric identification such as, but not limited to fingerprint recognition and/or facial recognition. In some cases, the user credentials may be verified by comparing the provided credentials to credentials saved at the mobile device **40** or at the cloud server **70**, as desired. Once the user is authenticated, the permissions and locations of access points in the facility that are accessible to the user (for example, as defined in the setup portal) may be downloaded (e.g., from the cloud server **70** or local facility storage) to the user mobile device **40** and saved in the memory **42** thereof. This may allow quicker response times during use of the application **46** but may not be required. For example, the application **46** may access permissions and locations stored remotely, for example, at the cloud server **70**. The access permissions and locations may include, but are not limited to, which access points are available to the user, GPS locations of those access points, employment status of the user, access time windows, etc.

[0055] The location of the particular mobile device **40** may be received or determined, as shown at block **404**. For example, the application **46** may receive the GPS location of the mobile device from the location services of the mobile device **40**. In some cases, the mobile device **40** may be configured to recognize a measure of error in the current location of the mobile device **40**. In some cases, the particular mobile device **40** may then determine one or more access points of the facility to display to the user based on the location of the particular mobile device, the downloaded permissions, and locations of the access points of the facility, as shown at block **406**. For example, the particular mobile device **40** may determine which access points are accessible to the user (based on assigned permissions) and/or within a predetermined threshold distance of the user. It is contemplated that the threshold distance may take into consideration the measure of error that may occur when locating the position of the mobile device **40**. For example, the threshold distance may be based at least in part on the identified measure of error in the current location of the mobile device. In some cases, the mobile device **40** may be configured to determine a distance between the current location of the mobile device **40** and each of one or more access points of a facility. A notification of the one or more access points that are determined by the particular mobile device may be displayed on the particular mobile device, as shown at block **408**.

[0056] In some cases, the notification may identify those access points that are within a predetermined distance from the particular mobile device **40** and does not include those access points that are not within the predetermined distance from the particular mobile device **40**. In some embodiments, the notification identifies or includes all access points in the facility that are accessible by the user. In some cases, the access points that are displayed on the user interface of the user device **40** may be those that are accessible to the user based on one or more access point permissions associated with the user and are within a threshold distance from the current location of the mobile device **40**. It is contemplated that the displayed access points may be continually or repeatedly updated based on the current location of the mobile device **40**. For example, as the mobile device **40** moves away from a particular access point, the particular access point may be removed from the notification, and additional access points may be added as the mobile device **40** comes within the threshold distance.

[0057] FIG. **9** is a screen capture **450** of a notification or list of available access points **452** that may be displayed to the user on the particular mobile device. The list of available access points **452** may vary from user to user based on user location and/or user permissions. In some cases, the particular mobile device **40** may also display the current GPS location **454** of the mobile device **40** as shown. It is contemplated that each access point of the list of available access points **452** may include a selectable button **456** configured to transmit an unlock or lock request, as will be described in more detail herein. It is contemplated that the list of available access points **452** may be based, at least in part, on the assigned permissions including, but not limited to, a current time falling within the one or more access time windows assigned to the user or an employment status of the user. In some embodiments, some access points may be displayed which are not available to the

user. In such an instance, the selectable button **460** may be omitted or grayed out and unselectable.

[0058] In some cases, the notification may be a pop-up alert that access points have been identified. The identified access points may be those that are accessible to the user and within a threshold distance of the mobile device **40**. FIG. **10** is a screen capture **500** of a mobile device **40** including pop-up alert **502**. In the illustrative example, the user interface of the mobile device **40** also displays a list **504** of access points available to the user and the GPS location **506** of the user mobile device. However, this is not required.

[0059] It is contemplated that the notification or list of available access points **452** may be automatically displayed as the user approaches an access point, without user input. In some cases, the available access points **452** that are displayed may be ranked, with the closest access point placed at the top of the list (if more than one access points are listed). When so provided, the user need not have to click through various menus of the application to identify a button to open a particular door. Instead, the application may automatically present an appropriate button to the user to unlock a door as the user approaches the door.

[0060] Returning back to FIG. **8**, a selection of one of the displayed access points from the user via a user interface of the particular mobile device may be received, as shown at block **410**. For example, the user may select the "unlock" button **460** adjacent to Door B **458** as shown in FIG. **9**. Alternatively, the user may select the pop-up notification **502** illustrated in FIG. **10**. This may cause the mobile device **40** to display that the door that has been found. FIG. **11** is an illustrative screen capture **510** of the mobile device **40** upon selection (e.g., tapping) of the pop-up notification **502**. The mobile device **40** may be configured to display the "found" or nearby door **512** along with a selectable unlock button **514**. The user may select the unlock button **514** associated with Door B in FIG. **11**. In some cases, the unlock buttons **460**, **514** may not be selectable until the mobile device **40** is within a threshold distance of the access point to prevent unauthorized users from gaining entry if an unlock button is selected before the user is ready to enter the access point.

[0061] Returning again to FIG. **8**, upon selection of an access point to unlock (e.g., selection of unlock button **460** or unlock button **514**), the mobile device may send a command to unlock the selected access point, as shown at block **412**. The mobile device **40** may transmit the command to the cloud server **70**, although this is not required. In some cases, the cloud server **70** may validate the permissions of the mobile device **40** making the unlock request. For example, the cloud server **70** may compare the mobile device identifier to a list of identifiers allowed to access the selected access point. This may also include verifying that the identifier can use the access point at the current time. In response to the command to unlock the selected access point, the selected access point may be unlocked, as shown at block **414**. For example, after validation of the mobile device **40**, the cloud server **70** may transmit a command to the ACS **50** to actuate the relay associated with the selected access point. It is contemplated that a user may use the mobile device **40** to lock an access point that is not automatically secured in a manner similar to the unlocking procedure. In some cases, the mobile device **40** may be configured to receive and display a notification or confirmation that the selected access point has been unlocked. FIG. **12** is an illustrative screen capture **520** of the mobile device **40** displaying a pop-up notification **522** indicating that the access point has been unlocked. It is contemplated that the ACS **50** may transmit a message to the cloud server **70** that the selected access point was unlocked. The cloud server **70** may relay this message to the mobile device **40** where it is received and displayed to the user via the user interface.

[0062] Those skilled in the art will recognize that the present disclosure may be manifested in a variety of forms other than the specific embodiments described and contemplated herein. Accordingly, departure in form and detail may be made without departing from the scope and spirit of the present disclosure as described in the appended claims.

Claims

1. A non-transitory computer readable medium storing instructions thereon that when executed by one or more processors of a mobile device, which mobile device has a designated unique device identifier, causes the mobile device to: wirelessly receive an access permission that grants access rights to the mobile device having the designated unique device identifier to unlock a particular wireless locked device during a designated future time window; receive a designated user input via a user interface of the mobile device; determine a time that the designated user input was received via the user interface; identify whether the mobile device is within a threshold range of the particular wireless locked device; wirelessly send a signal to the particular wireless locked device to unlock the particular wireless locked device when: the time that the designated user input is received via the user interface is within the designated future time window defined by the received access permission; and the mobile device is determined to be located within the threshold range of the particular wireless locked device.

2. The non-transitory computer readable medium of claim 1, wherein the designated user input includes one or more of a PIN and a biometric identifier.

3. The non-transitory computer readable medium of claim 1, wherein the designated user input includes a user selection to unlock the particular wireless locked device.

4. The non-transitory computer readable medium of claim 1, wherein at least part of the designated unique device identifier of the mobile device includes an International mobile equipment identity (IMEI) number of the mobile device.

5. The non-transitory computer readable medium of claim 1, wherein at least part of the designated unique device identifier of the mobile device is generated by an operating system of the mobile device.

6. The non-transitory computer readable medium of claim 1, wherein at least part of the designated unique device identifier of the mobile device includes a phone number associated with the mobile device.

7. The non-transitory computer readable medium of claim 1, wherein the designated future time window corresponds to one or more predetermined hours and/or one or more predetermined days.

8. The non-transitory computer readable medium of claim 1, wherein the instructions when executed by one or more processors of the mobile device causes the mobile device to: display via the user interface of the mobile device an unlock button that is associated with the particular wireless locked device; and receive via the user interface of the mobile device a selection of the unlock button that is associated with the particular wireless locked device, wherein the selection of the unlock button includes at least part of the designated user input.

9. The non-transitory computer readable medium of claim 1, wherein the instructions when executed by one or more processors of the mobile device causes the mobile device to: concurrently display via the user interface of the mobile device a plurality of wireless locked devices including the particular wireless locked device; visually distinguish the particular wireless locked device on the user interface of the mobile device when the mobile device is located within the threshold range of the particular wireless locked device at a time that is within the designated future time window defined by the access permission; and receive a selection of the particular wireless locked device while the particular wireless locked device is visually distinguished on the user interface of the mobile device, wherein the selection of the particular wireless locked device includes at least part of the designated user input.

10. The non-transitory computer readable medium of claim 9, wherein the instructions when executed by one or more processors of the mobile device causes the mobile device to: concurrently display via the user interface of the mobile device the plurality of wireless locked devices including the particular wireless locked device in a ranked order from nearest to furthest from the mobile device.

11. The non-transitory computer readable medium of claim 9, wherein each of plurality of wireless

locked devices concurrently displayed via the user interface of the mobile device correspond to wireless locked devices that the mobile device has previously received an access permission that grants access rights for the mobile device to unlock the respective wireless locked device.

12. The non-transitory computer readable medium of claim 1, wherein the instructions when executed by one or more processors of the mobile device causes the mobile device to: concurrently display via the user interface of the mobile device an unlock button for each of a plurality of wireless locked devices including the particular wireless locked device, wherein the unlock button for each of the plurality of wireless locked devices is unselectable; change the unlock button that is associated with the particular wireless locked device from unselectable to selectable when the mobile device is located within the threshold range of the particular wireless locked device at a time that is within the designated future time window defined by the access permission; and receive via the user interface of the mobile device a selection of the selectable unlock button that is associated with the particular wireless locked device, wherein the selection of the selectable unlock button that is associated with the particular wireless locked device includes at least part of the designated user input.

13. The non-transitory computer readable medium of claim 1, wherein the instructions when executed by one or more processors of the mobile device causes the mobile device to store the access permission to a non-volatile memory of the mobile device for subsequent use.

14. The non-transitory computer readable medium of claim 1, wherein the instructions when executed by one or more processors of the mobile device causes the mobile device to: display a notification via the user interface of the mobile device that the particular wireless locked device has been unlocked after successfully wirelessly sending the signal to the particular wireless locked device to unlock the particular wireless locked device.

15. The non-transitory computer readable medium of claim 1, wherein the instructions when executed by one or more processors of the mobile device causes the mobile device to: wirelessly send an access request requesting preapproval for permission to unlock the particular wireless locked device during the designated future time window, wherein the access request includes the designated unique device identifier associated with the mobile device; and in response to sending the access request, wirelessly receive the access permission for use by the mobile device to unlock the particular wireless locked device during the designated future time window.

16. The non-transitory computer readable medium of claim 15, wherein the particular wireless locked device is one of a plurality of wireless locked devices, and wherein the access request includes a locked device identifier that uniquely identifies the particular wireless locked device from the plurality of wireless locked devices.

17. The non-transitory computer readable medium of claim 16, wherein the instructions when executed by one or more processors of the mobile device causes the mobile device to: display a listing of two or more of the plurality of wireless locked devices on the user interface of the mobile device including the particular wireless locked device; receive a first input via the user interface of the mobile device that identifies the particular wireless locked device from the plurality of wireless locked devices; receive a second input via the user interface of the mobile device that identifies the designated future time window; and receive a third input via the user interface of the mobile device that initiates the access request requesting preapproval for permission to unlock the particular wireless locked device during the designated future time window.

18. A server configured to: receive for a particular user pre-approval to access a particular home during a designated future time window; receive a unique device identifier of a mobile device of the particular user; generate an access permission that grants access rights to the mobile device having the unique device identifier to unlock a wireless locked device associated with the particular home during the designated future time window, allowing access to the particular home during the designated future time window; and send the access permission to the mobile device having the unique device identifier, wherein the access permissions permit the mobile device having the

unique device identifier to determine whether the mobile device is within a threshold range of the wireless locked device associated with the particular home during the designated future time window, and when so, wirelessly send a signal to the wireless locked device associated with the particular home that unlocks the wireless locked device associated with the particular home.

19. The server of claim 18, wherein at least part of the unique device identifier of the mobile device includes one or more of: an International mobile equipment identity (IMEI) number of the mobile device; a phone number associated with the mobile device; and a unique device identifier generated by an operating system of the mobile device.

20. The server of claim 18, wherein the access permission includes an identifier that uniquely identifies the wireless locked device associated with the particular home from a plurality of other wireless locked devices not associated with the particular home.

21. The server of claim 18, wherein the server receives the pre-approval from an administrative user that is separate from the particular user.

22. The server of claim 18, wherein the access permission includes a user credential for the particular user, such that the mobile device having the unique device identifier must receive a user input that matches the user credential of the access permission before the mobile device is permitted to send the signal to the wireless locked device associated with the particular home that unlocks the wireless locked device associated with the particular home.

23. The server of claim 18, wherein the unique device identifier of the mobile device of the particular user is received from the mobile device of the particular user.

24. A non-transitory computer readable medium storing instructions thereon that when executed by one or more processors of a mobile device causes the mobile device to: wirelessly receive an access permission that grants access rights to the mobile device to unlock a particular wireless locked device during a designated future time window; store the received access permission in a non-volatile memory of the mobile device for subsequent use; automatically determine that the mobile device is within a threshold range of the particular wireless locked device; authenticate a user to the mobile device; and only after authenticating the user to the mobile device, and during the designated future time window and with the mobile device determined to be within the threshold range of the particular wireless locked device, wirelessly send a signal to unlock the particular wireless locked device.

25. The non-transitory computer readable medium of claim 24, wherein the instructions when executed by one or more processors of the mobile device causes the mobile device to authenticate the user to the mobile device by: receiving one or more of a PIN and a biometric identifier via a user interface of the mobile device; comparing the received one or more of the PIN and the biometric identifier with a known PIN and/or a known biometric identifier, respectively, to identify whether there is a match; and authenticating the user to the mobile device when there is a match.

26. The non-transitory computer readable medium of claim 24, wherein the instructions when executed by one or more processors of the mobile device causes the mobile device to automatically determine that the mobile device is within the threshold range of the particular wireless locked device by: storing a location of the particular wireless locked device in a memory of the mobile device; determining a location of the mobile device; determining a distance between the location of the mobile device and the location of the particular wireless locked device; and determining if the distance is within the threshold range.

27. The non-transitory computer readable medium of claim 24, wherein the instructions when executed by one or more processors of the mobile device causes the mobile device to automatically determine that the mobile device is within the threshold range of the particular wireless locked device by analyzing a received signal transmitted by a signal source.

28. A method for unlocking a particular wireless locked device that is associated with providing access to a facility, the method comprising: a mobile device, having a designated unique device identifier, wirelessly receiving an access permission for use by an application program running on

the mobile device, wherein the access permission grants access rights for the mobile device having the designated unique device identifier to unlock the particular wireless locked device during a requested future time window; after receiving the access permission, the application program running on the mobile device causing the mobile device to wirelessly send a signal to the particular locked device to unlock the particular wireless locked device after: receiving, at a time that is within the requested future time window defined by the access permission, a designated user input via a user interface of the mobile device; and the mobile device is located within a threshold range of the particular wireless locked device.

29. The method of claim 28, wherein the designated user input includes one or more of a PIN and a biometric identifier.

30. The method of claim 28, wherein the designated user input includes a user selection to unlock the particular wireless locked device.