



- (51) International Patent Classification: G06Q 10/00 (2012.01)
- (21) International Application Number: PCT/US2017/040304
- (22) International Filing Date: 30 June 2017 (30.06.2017)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 62/356,679 30 June 2016 (30.06.2016) US
- (72) Inventors; and
- (71) Applicants: CAMARGO, Fabian Emilio Philipe [US/US]; 8281 Greensboro Drive, Suite 100, Tysons, Virginia 22102 (US). BROPHY, Michael Montgomery [US/US]; 8281 Greensboro Drive, Suite 100, Tysons, Virginia 22102 (US).
- (74) Agent: MONALDO, Jeremy J. et al.; Fish & Richardson P.C., P.O. Box 1022, Minneapolis, Minnesota 55440-1022 (US).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(54) Title: SCHEDULED TEMPORARY RENTAL PROPERTY ACCESS

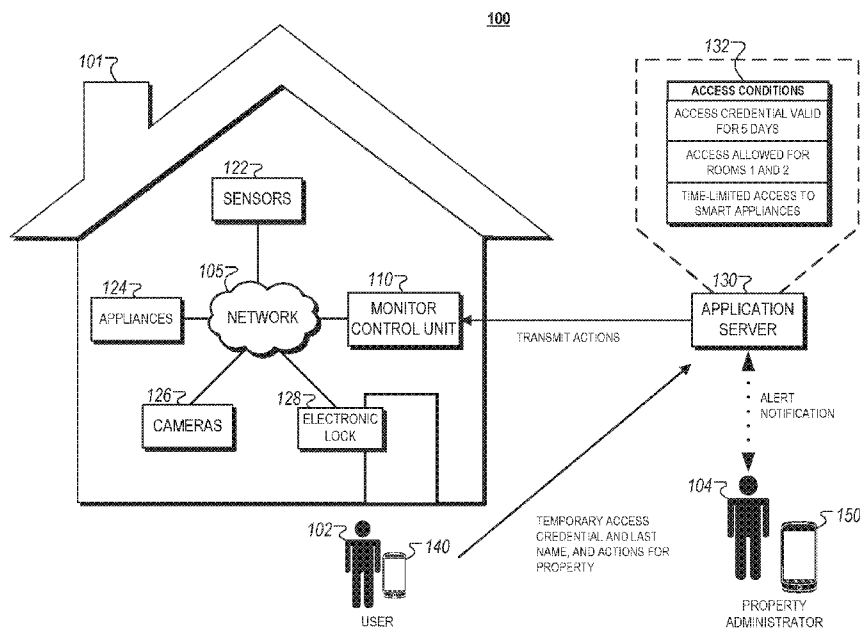


FIG. 1

(57) Abstract: In some implementations, a system is capable of generating and distributing access credentials to users that access a rental property for a limited time period. Users can be provided with access to the rental property through an application or webpage portal without creating a new user account or user login for the application. For example, a user can be granted access to control electronic devices associated with a monitoring system of a rental property without creating a new user account with the monitoring system. Techniques described herein enable such users to more easily access, for example, rental property information that is associated with a monitoring system of the rental property. In this manner, access credentials can be distributed to users through any suitable means, e.g., through email or SMS, and used to temporarily authenticate users.



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

Published:

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

SCHEDULED TEMPORARY RENTAL PROPERTY ACCESS

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of U.S. Non-Provisional Patent Application Serial No. 62/356,679, filed June 30, 2016, entitled "SCHEDULED TEMPORARY RENTAL PROPERTY ACCESS", the entire contents of which are incorporated herein.

TECHNICAL FIELD

[0002] This disclosure application relates generally to rental property management technology.

BACKGROUND

[0003] Properties are often temporarily available for rent to a user by a property owner. In some instances, a property owner may provide a rental property listing to advertise the property to users. Once a user expresses interest in renting an available property, the property owner and the user attempt to reach an agreement on allowing the user temporary physical access to the rental property.

SUMMARY

[0004] Techniques are described for rental property management technology. For example, techniques are described to generate and distribute access credentials to users such as temporary guests or occupants that access a rental property for a limited time period. Users can be provided with access to the rental property through an application or webpage portal without creating a new user account or user login for the application. For example, a user can be granted access through an application or web portal to control electronic devices associated with a monitoring system of a rental property without creating a new user account with the monitoring system. Techniques described herein enable such users to more easily access, for example, rental property information through an application or through a webpage portal that is associated with a monitoring system of the rental property. In this manner, access credentials can be distributed to users through any suitable means, e.g., through email or SMS, and used to temporarily authenticate users without requiring that the user create a user account that enables access to the rental property.

[0005] The access credentials may be generated and distributed to users at various stages of the property rental process. In some instances, the access credential is generated after a user submits a reservation for a rental listing provided by a property administrator. In such instances, the generated access credential is initially associated with the reservation, and then distributed to the user to provide access to an application (or a webpage) to view rental property information. Alternatively, in other implementations, the access credential is pre-generated by the system once a property administrator creates the rental listing prior to any user submitting a reservation request. In such instances, the access credential is assigned and distributed to a user once she/she submits a rental reservation.

[0006] Once the access credential is distributed to a user, the access credential may be used for a variety of functions that are related to property rental. In some instances, the access credential can be used to provide easy access to property information without requiring the user to create a new account to access an application that is capable of exchanging communications with a monitoring system of the rental property. In such instances, the distributed access credential is used to authenticate the user into the application so that he/she can perform actions related to the rental property such as physically accessing the rental property or controlling electronic devices located within the property. In some implementations, user information is obtained from an external source (e.g., an existing user account associated with a rental property listing website or a rental property listing application) and associated with the distributed access credential. In such instances, the user information can be additionally used to authenticate the user into the application.

[0007] In some other instances, once the user has used the access credential to log into the application, the user can use the application to perform actions associated with the rental property. Examples of actions can include transmitting messages to the property administrator, using the application to unlock an electronic lock of the rental property to provide physical access, controlling smart appliances and/or network-enabled devices through commands transmitted from the application, among others.

[0008] In some implementations, the system may generate and provide the access credential in response to receiving an indication that the property administrator has approved the user to rent the corresponding property. The granted access credential can also be used to control the provisioning of services that are associated with the property rental to the user.

[0009] Implementations of the described techniques may include hardware, a method or process implemented at least partially in hardware, or a computer-readable storage medium encoded with executable instructions that, when executed by a processor, perform operations.

[0010] The details of one or more implementations are set forth in the accompanying drawings and the description below. Other features will be apparent from the description and drawings, and from the claims.

DESCRIPTION OF DRAWINGS

[0011] FIG. 1 is a schematic diagram that illustrates an example of a system that enables temporary rental property access.

[0012] FIG. 2-3 are flowcharts that illustrate examples of processes relating to temporary rental property access.

[0013] FIG. 4 is a schematic diagram that illustrates an example of a rental property with multiple access regions.

[0014] FIGS. 5A-5B are schematic diagrams that illustrate examples of user interfaces for an application that is used by a property administrator.

[0015] FIGS. 6A-6B are schematic diagrams that illustrate examples of user interfaces for an application that is used by a user.

[0016] FIG. 7 is a flowchart that illustrates an example of a process for providing temporary access to a property.

[0017] In the drawings, like reference numbers represent corresponding parts throughout.

DETAILED DESCRIPTION

[0018] In general, techniques are described to generate and distribute access credentials to users (e.g., users or users) to more easily access rental property information on an application without requiring the users to create a new account or user login for the application. Each access credential may be associated with a particular rental property and associated with a set of access conditions that are specified by a property administrator.

[0019] The access credentials may be generated and distributed to users at various stages of the property rental process. In some instances, the access credential is generated after a user submits a reservation for a rental listing provided by a property administrator. In such

instances, the generated access credential is initially associated with the reservation, and then distributed to the user to provide access to an application (or a webpage) to view rental property information. Alternatively, in other implementations, the access credential is pre-generated by the system once a property administrator creates the rental listing prior to any user submitting a reservation request. In such instances, the access credential is assigned and distributed to a user once she/she submits a rental reservation.

[0020] Once the access credential is distributed to a user, the access credential may be used for a variety of functions that are related to property rental. In some instances, the access credential can be used to provide easy access to property information without requiring the user to create a new account to access an application that is capable of exchanging communications with a monitoring system of the rental property. In such instances, the distributed access credential is used to authenticate the user into the application so that he/she can perform actions related to the rental property such as physically accessing the rental property or controlling electronic devices located within the property. In some implementations, user information is obtained from an external source (e.g., an existing user account associated with a rental property listing website or a rental property listing application) and associated with the distributed access credential. In such instances, the user information can be additionally used to authenticate the user into the application.

[0021] As described herein, a “property administrator” refers to an individual or an entity that controls access to a rental property. For example, in some instances, a property administrator may be a property owner that retains property title to the property to be rented. In other instances, the property administrator may be an authorized agent of the property owner that manages and rents the property on behalf of the property owner. The property administrator specifies a set of access conditions that are associated with the rental of a property. For example, the property administrator may specify the cost of rental, time periods of availability, or services that are offered along with the property rental.

[0022] A “user” (or “guest” or “occupant”) refers to an individual that requests to rent a property that is made available by the property administrator. The user can submit a rental requests through various mediums such as sending a direct email to the property administrator, placing a request through a property rental webpage, and/or through an application that provides property rental services.

[0023] An “access credential” refers to a credential that is associated with a rental property and provides one or more prospective users with temporary access to the rental property with permission from a property administrator. When an access credential is initially generated for a rental property, property information and one or more access conditions that are specified by the property administrator are also associated with the access credential. Once a rental property receives interest from a user through an applicable medium (e.g., through property rental website, property rental application, etc.) and the property administrator approves of a user’s rental request, the access credential can be provided to the user to enable access to rental property services through a separate application without requiring user account creation and/or information submission for the application. In this regard, once a rental agreement has been entered into between a property administrator and a user, the access credential may then be assigned to the user to allow for provisioning of various rental services. In some instances, the access credential can be a uniquely generated personal identifier number (PIN) with a specified number of alphanumeric characters.

[0024] “Access credential activation” refers to a process where a user enters a distributed access credential into a login screen of an application, or some other type of interface, to view and access information related to property rental. In some instances, the distributed access credential becomes activated once a user enters the access credential into an entry form displayed on an application. After submitting the access credential, the user may then view pertinent information associated with the rental property, and/or transmit instructions to devices associated with the rental property to perform particular actions as described in more detail below.

[0025] In addition, an access credential may become inactive in certain situations. For example, an access credential may be associated with an access condition that specifies a fixed time period in which the access credential remains valid. In this example, the access credential may only be activated within the fixed time period, and becomes inactive after expiration of the fixed time period. In another example, an access credential may be inactivated after one or more events specified by the property administrator. For instance, different access credentials may be distributed to different users who have each submitted rental reservations for the same property. In this instance, each respective access credential may be active until one user forms a rental agreement with the property administrator, which

then causes the other access credentials to become invalid because the rental property is no longer available for rent.

[0026] “Access credential enablement” refers to a process by which a distributed access credential is used by a prospective user to physically access the rental property after forming a rental agreement with the property administrator. For instance, in some instances, after a user has activated the access credential by logging into the application, the user may then use the application to transmit an instruction to unlock a front door of the rental property when he/she initially arrives at the property. In this instance, the access credential becomes enabled once the user performs actions that indicate that he/she has obtained possession over the rental property. In this regard, an access credential may be activated but disabled after the user forms a rental agreement but prior to the start of the specified rental period, whereas an access credential may be activated and enabled once the user actually obtains possession over the rental property to initiate the rental period.

[0027] In some instances, an enabled access credential allows the user to perform a greater number of actions on the application compared to an activated (but not enabled) access credential. For instance, because an enabled access credential indicates that the user has physically obtained possession over the rental property, once an access credential is enabled, the application may present the user with options to transmit instructions to connected devices and/or appliances within the property to perform certain actions. Examples of actions may include unlocking an electronic lock of the property, operating smart appliances within the property, among others.

[0028] “Access conditions” refer to features, attributes, or limitations of the property rental that are associated with the access credential and specified by a property administrator. For instance, the access conditions can specify a time period for which access credential remains valid. In other instances, the access conditions may specify limitations on the property rental that are imposed on and agreed upon by the user within a rental agreement. For example, the access conditions may specify geographic rental restrictions (e.g., specific rooms that are accessible to the user), time-based rental restrictions (e.g., use of particular appliances within the property during a specified period of time), or actions during the rental that are strictly prohibited by the property administrator. As described in more detail below, access conditions specified by a property administrator may be associated with a distributed access

credential to effectively enforce rental restrictions without requiring a property owner's presence.

[0029] FIG. 1 illustrates a diagram of an example of a property management system 100 that is associated with a property 101. Although this disclosure is written in the context of controlling access to rental property, systems and techniques described herein can also be used for controlling access to properties for purchase (e.g., condos, houses, and/or commercial headquarters). Although FIG. 1 illustrates one property for brevity, the application server 130 may also manage electronic locks and energy consuming devices for multiple properties and/or structures. For example, the application server 130 may communicate directly with the monitor control unit 110 or through other communications media and protocol (e.g., through the network 105, over Bluetooth, Zigbee, etc.).

[0030] The system 100 may include a monitor control unit 110, sensors 122, appliances 124, cameras 126, an electronic lock 128, and an application server 130 connected over a network 105. The network 105 enables the monitor control unit 110, sensors 122, appliances 124, cameras 126, the electronic lock 128, and the application server 130 to exchange data communications related to rental reservations and/or information related to the rental reservations. The network 105 also enables the system 100 to maintain data that defines a set of access conditions associated with an access credential that is distributed to a particular user that requests to rent the property 101.

[0031] In general, the architecture of the system 100 enables a property administrator 104 to rent the property 101 to a user 102 by use of a distributed access credential that is associated with the property 101 to the user 102, and specification of a set of access conditions 132 associated with property rental. The property administrator 104 may use a rental property management portal to specify the set of access conditions 132, which are then stored on the application server 130. The rental property management portal is described more particularly with respect to FIGS. 5A-5B.

[0032] As described above, the access credentials associated with rental property may be generated and distributed in a variety of ways during a property rental process. In some implementations, the access credential is generated in response to a user submitting a reservation to the rent the property 101 on a rental listing provided by the property administrator. In this example, an access credential may be generated for each reservation for the property 101, and then distributed to the corresponding users that submitted each

reservation. Once each user receives the distributed access credential, the user may then use the distributed access credential to view rental property information on an application that may independent from the rental listing.

[0033] Alternatively, in other implementations, the access credential may be pre-generated by the system once the property administrator creates a new rental listing for the property 101 and prior to receiving any rental reservations from users. In these implementations, once a user submits a rental reservation in response to the rental listing, the access credentials may then be associated with the rental reservations, and distributed to the corresponding user.

[0034] Once a rental agreement and/or confirmation has been formed between the user 102 and the property administrator 104, the access credential associated with the property to be rented is then distributed to the user 102. The access credential may be distributed with the use of various communication mediums such as transmitting an email to the user, sending an SMS message to a mobile device associated with the user, initiating a system-generated telephone call to deliver the access credential to the mobile device associated with the user, among others.

[0035] When the access credential is distributed to the user, the communication may further include an instruction and/or reference to download an application on a device associated with the user. In some instances, the reference can include a deeplink to redirect the user to an application store page to download and install an application on the device. In other instances, the reference can instead be a hyperlink to a webpage that enables the user to submit the distributed access credential and other user-specific information to system 100. More particular discussions related to access credential submission and the application are described with respect to FIGS. 6A and 6B.

[0036] The distributed access credential provides a means to authenticate a user into the system 100 to obtain information related to the rental property and/or utilize services offered as a part of the rental agreement. For example, as described more particularly with respect to FIG. 6B, the access credential enables the user to use a device to transmit instructions to the system 100 of the rental property to perform particular actions. Such actions can include enabling or disabling operation of connected devices inside the rental property, locking or unlocking electronic locks to gain access to regions within the property, among others. Greater discussion of functions of the particular components of the system 100 in relation to the access credentials distributed to users is provided below.

[0037] After the access credentials are generated and distributed to users, there may be different "states" associated with the access credentials. For instance, an access credential may initially be "inactive" prior to the user using the access credential to log into the application as described above. Once the user logs into the application using the access credential, its associated state may change to "active" to reflect that the user has obtained access to rental property information that is provided on the application. As described above, an "active" access credential may remain in such a state for a fixed time period (e.g., as defined by an associated access condition), or until a specified event takes place to revert the access credential to an inactive state (e.g., inactivating the distributed access credentials to other users for a rental property once one of the users has formed a rental agreement with the property administrator). Once the user obtains physical possession over the property, the state of the access credential is adjusted to "enabled," indicating that the start of the actual rental period. As described more particularly below, an "enabled" access credential may provide the user with a greater set of features on the application compared to an "active" access credential since the user has started the rental period.

[0038] The network 105 is configured to enable exchange of electronic communications between devices connected to the network 105. For example, the network 105 may be configured to enable exchange of electronic communications between the monitor control unit 110, the sensors 122, the appliances 124, the cameras 126, the electronic lock 128 and the application server 130. The network 105 may include, for example, one or more of the Internet, Wide Area Networks (WANs), Local Area Networks (LANs), analog or digital wired and wireless telephone networks (e.g., a public switched telephone network (PSTN), Integrated Services Digital Network (ISDN), a cellular network, and Digital Subscriber Line (DSL)), radio, television, cable, satellite, or any other delivery or tunneling mechanism for carrying data. The network 105 may include multiple networks or subnetworks, each of which may include, for example, a wired or wireless data pathway.

[0039] The network 105 may also include a circuit-switched network, a packet-switched data network, or any other network able to carry electronic communications (e.g., data or voice communications). For example, the network 105 may include networks based on the Internet protocol (IP), asynchronous transfer mode (ATM), the PSTN, packet-switched networks based on IP, X.25, or Frame Relay, or other comparable technologies and may support voice using, for example, VoIP, or other comparable protocols used for voice communications.

The network 105 may include one or more networks that include wireless data channels and wireless voice channels. The network 105 may be a wireless network, a broadband network, or a combination of networks including a wireless network and a broadband network.

[0040] The monitor control unit 110 may be an electronic device that coordinates and/or monitors the operations of the components of the system 100 through a set of data transmissions with each of the components of the system 100. The monitor control unit 110 includes a controller and a network module. The controller is configured to control a system 100 (e.g., a home alarm or security system) that includes the monitor control unit 110. In some examples, the controller may include a processor or other control circuitry configured to execute instructions of a program that controls operation of an alarm system. In these examples, the controller may be configured to receive input from sensors, detectors, or other devices included in the alarm system and control operations of devices included in the alarm system or other household devices (e.g., a thermostat, an appliance, lights, etc.). For example, the controller may be configured to control operation of the network module included in the monitor control unit 110.

[0041] The network module is a communication device configured to exchange communications over the network 105. The network module may be a wireless communication module configured to exchange wireless communications over the network 105. For example, the network module may be a wireless communication device configured to exchange communications over a wireless data channel and a wireless voice channel. In this example, the network module may transmit alarm data over a wireless data channel and establish a two-way voice communication session over a wireless voice channel. The wireless communication device may include one or more of a LTE module, a GSM module, a radio modem, cellular transmission module, or any type of module configured to exchange communications in one of the following formats: LTE, GSM or GPRS, CDMA, EDGE or EGPRS, EV-DO or EVDO, UMTS, or IP.

[0042] The network module may also be a wired communication module configured to exchange communications over the network 105 using a wired connection. For instance, the network module may be a modem, a network interface card, or another type of network interface device. The network module may be an Ethernet network card configured to enable the monitor control unit 110 to communicate over a local area network and/or the Internet.

The network module also may be a voice-band modem configured to enable the alarm panel to communicate over the telephone lines of Plain Old Telephone Systems (POTS).

[0043] The monitor control unit 110 also may include a communication module that enables the monitor control unit 110 to communicate other devices of the system 100. The communication module may be a wireless communication module that allows the monitor control unit 110 to communicate wirelessly. For instance, the communication module may be a Wi-Fi module that enables the monitor control unit 110 to communicate over a local wireless network at the property 101. The communication module further may be a 900 MHz wireless communication module that enables the monitor control unit 110 to communicate directly with a monitor control unit. Other types of short-range wireless communication protocols, such as Bluetooth, Bluetooth LE, Zwave, ZigBee, etc., may be used to allow the monitor control unit 110 to communicate with other devices in the property 101.

[0044] In some examples, the monitor control unit 110 may include data capture and recording devices. In these examples, the monitor control unit 110 may include one or more cameras 126, one or more motion sensors, one or more microphones, one or more biometric data collection tools, one or more temperature sensors, one or more humidity sensors, one or more air flow sensors, and/or any other types of sensors that may be useful in capturing monitoring data related to the property 101 and users in the property.

[0045] The monitor control unit 110 further may include processor and storage capabilities. The monitor control unit 110 may include any suitable processing devices that enable the monitor control unit 110 to operate applications and perform the actions described throughout this disclosure. In addition, the monitor control unit 110 may include solid state electronic storage that enables the monitor control unit 110 to store applications, configuration data, collected sensor data, and/or any other type of information available to the monitor control unit 110.

[0046]

[0047] The monitor control unit 110 may exchange communications with the sensors 122, the appliances 124, the cameras 126, the electronic lock 128, and the application server 130 using multiple communication links. The multiple communication links may be a wired or wireless data pathways configured to transmit signals from sensors 122, the appliances 124, the cameras 126, the electronic lock 128, and the application server 130 to the controller. The

sensors 122, the appliances 124, the cameras 126, the electronic lock 128, and the application server 130 may continuously transmit sensed values to the controller, periodically transmit sensed values to the monitor control unit 110, or transmit sensed values to the monitor control unit 110 in response to a change in a sensed value.

[0048] In some implementations, the monitor control unit 110 may additionally be used to perform routine surveillance operations on a property. For instance, the monitor control unit 110 may be assigned to one or more particular properties within a geographic location and may routinely collect surveillance footage during specified time periods (e.g., after dark), which may then be transmitted to the application server 130 for transmitting back to each particular property owner. In such implementations, the property owner may receive the surveillance footage over the network 105 as a part of a service provided by a security provider that operates the application server 130. For example, transmissions of the surveillance footage collected by the monitor control unit 110 may be part of a premium security service package provided by a security provider in addition to the routine drone emergency response service.

[0049] In some implementations, the monitor control unit 110 may monitor the operation of the electronic devices of the system 100 such as sensors 122, the appliances 124, the cameras 126, the electronic lock 128, and the application server 130. For instance, the monitor control unit 110 may enable or disable the devices of the system 100 based on a set of rules associated with energy consumption, user-specified settings, and/or other information associated with the conditions near or within the property 101 where the system 100 is located. In some examples, the monitor control unit 110 may be used as a replacement to a traditional security panel (or monitor control unit) that is used to monitor and control the operations of the system 100. In other examples, the monitor control unit 110 may coordinate monitoring operations with a separate security panel of the system 100. In such examples, the monitor control unit 110 may monitor particular activities of the devices of the system 100 that are not monitored by the security panel, or monitor the operation of particular devices that are not monitoring by the security panel.

[0050] As described above, the property 101 may include various monitoring devices that are each capable of performing individual monitoring operations and/or capable to performing a set of coordinated operations based on instructions received from either the monitor control unit 110 or the application server 130. For instance, the property 101 may include the sensors

122, the appliances 124, the cameras 126, the electronic lock 128, the application server 130 and other devices that provide monitoring data associated with devices, areas, or individuals located nearby or within the premises of the property 101. As an example, the cameras 126 located on the property 101 may provide video, still images, or other monitoring data, and may provide data via a live feed, transmit data to be stored in a remote location, store data locally for review at a later time, etc. As another example, the sensors 122 located on the property 101 may include motion sensors, heat sensors, pressure sensors, resistive sensors, etc. that periodically collected sensed data indicating conditions of the property 101. The sensors 122 may communicate with the system 100 and transmit monitoring data for processing to the monitoring control unit 110. In some examples, the sensors 122 may store collected data locally or transmit monitoring data to be stored in a remote location (e.g., the application server 130).

[0051] The multiple communication links may further include a local network within the network 105. For instance, the monitor control unit 110, the sensors 122, the appliances 124, the cameras 126, the electronic lock 128, and the application server 130 may exchange data and commands over the local network as described herein. The local network may include 802.11 “Wi-Fi” wireless Ethernet (e.g., using low-power Wi-Fi chipsets), Z-Wave, Zigbee, Bluetooth, “Homeplug” or other “Powerline” networks that operate over AC wiring, and a Category 5 (CAT5) or Category 6 (CAT6) wired Ethernet network. The local network may be a mesh network constructed based on the devices connected to the mesh network.

[0052] Referring now to the sensors 122, the system 100 may include one or more of a contact sensor, a motion sensor, a glass break sensor, an occupancy sensor, or any other type of sensor that can be included in an alarm or security system. The sensors 122 may also include an environmental sensor, such as a temperature sensor, a water sensor, a rain sensor, a wind sensor, a light sensor, a smoke detector, a carbon monoxide detector, an air quality sensor, etc. The sensors 122 may further include a health monitoring sensor, such as a prescription bottle sensor that monitors taking of prescriptions, a blood pressure sensor, a blood sugar sensor, a bed mat configured to sense presence of liquid (e.g., bodily fluids) on the bed mat, etc. In some examples, the sensors 122 may include a radio-frequency identification (RFID) sensor that identifies a particular article that includes a pre-assigned RFID tag.

[0053] The appliances 124 may be home automation devices connected to the network 105 that are configured to exchange electronic communications with other devices of the system 100. The appliances 124 may include, for example, connected kitchen appliances, controllable light sources, safety and security devices, energy management devices, and/or other types of electronic devices capable of exchanging electronic communications over the network 105. In some instances, the appliances 124 may periodically transmit information and/or generated data to the monitor control unit 110 such that the monitor control unit 110 can automatically control the operation of the appliances 124 based on the exchanged communications. For example, the monitor control unit 110 may operate one or more of the appliances 124 based on a fixed schedule specified by the user. In another example, the monitor control unit 110 may enable or disable one or more of the appliances 124 based on received sensor data from the sensors 122.

[0054] The cameras 126 may be video/photographic cameras or other type of optical sensing devices configured to capture images. For instance, the cameras 126 may be configured to capture images of an area within a building monitored by the monitor control unit 110. The cameras 126 may be configured to capture single, static images of the area and also video images of the area in which multiple images of the area are captured at a relatively high frequency (e.g., thirty images per second). The cameras 126 may be controlled based on commands received from the monitor control unit 110.

[0055] The cameras 126 may be triggered by several different types of techniques. For instance, a Passive Infra Red (PIR) motion sensor may be built into the cameras 126 and used to trigger the cameras 126 to capture one or more images when motion is detected. The cameras 126 also may include a microwave motion sensor built into the camera and used to trigger the cameras 126 to capture one or more images when motion is detected. The cameras 126 may have a “normally open” or “normally closed” digital input that can trigger capture of one or more images when external sensors (e.g., the sensors 122, PIR, door/window, etc.) detect motion or other events. In some implementations, the cameras 126 receives a command to capture an image when external devices detect motion or another potential alarm event. The cameras 126 may receive the command from the controller or directly from one of the sensors 122.

[0056] In some examples, the cameras 126 trigger integrated or external illuminators (e.g., Infra Red, Z-wave controlled “white” lights, etc.) to improve image quality when the scene is

dark. An integrated or separate light sensor may be used to determine if illumination is desired and may result in increased image quality.

[0057] The cameras 126 may be programmed with any combination of time/day schedules, system “arming state”, or other variables to determine whether images should be captured or not when triggers occur. The cameras 126 may enter a low-power mode when not capturing images. In this case, the cameras 126 may wake periodically to check for inbound messages from the controller. The cameras 126 may be powered by internal, replaceable batteries if located remotely from the monitor control unit 110. The cameras 126 may employ a small solar cell to recharge the battery when light is available. Alternatively, the cameras 126 may be powered by the controller’s 112 power supply if the cameras 126 is co-located with the controller.

[0058] In some implementations, the cameras 126 communicates directly with the application server 130 over the Internet. In these implementations, image data captured by the cameras 126 does not pass through the monitor control unit 110 and the cameras 126 receives commands related to operation from the application server 130.

[0059] The electronic lock 128 may be an electronic computing device that is placed on the exterior of the property 101 and configured to provide access to a user with the presentation of a distributed access credential through the user device 140. For example, once the prospective receives a distributed access credential and enters the distributed access credential into an application, the access credential may be considered to be in an “active” state, indicating that the user has used the distributed access credential to view property information related to the property 101. In response, the information associated with the activated access credential (e.g., access conditions specified by the property administrator 104, user information associated with the distributed access credential, etc.) may then be transmitted to the monitor control unit 110 of the property 101. The transmitted information may include a stored access credential that is then used by the electronic lock 128 to establish communications with the user device 140 when the user 102 (previously, the user) first accesses the property 101 to initiate the rental period.

[0060] The application server 130 is an electronic device configured to provide monitoring services by exchanging electronic communications with the monitor control unit 110 and the user device 140 over the network 105. For example, the application server 130 may be configured to monitor events (e.g., start or end of a rental period, user activity data collected

during a rental period) generated by the monitor control unit 110 and/or other devices connected over the network 105. In this example, the application server 130 may exchange electronic communications with the network module included in the monitor control unit 110 to receive information regarding events detected by the monitor control unit 110. The application server 130 also may receive information regarding events from the user device 150 of a property administrator 104 (e.g., rental property information, access credentials distributed to users, and/or access conditions associated with access credentials for the property).

[0061] The applications server 130 may also exchange data communications with the user device 140 associated with the user 102. For instance, after the user 102 activates the distributed access credential on an application running on the user device 140 (depicted more particularly in FIG. 6A), the applicant may transmit the activated access credential and user-specific information (e.g., username, last name, password, etc.) to the application server 130. The application server 130 may store the received access credential and determine a set of access conditions 132 that are associated with an access credential for the property 101. As described herein, one or more access credentials are created for the property 101 once the property 101 becomes available for rent (e.g., an online listing on a property rental website).

[0062] Prior to generation of the access credential, the property administrator 104 may specify access conditions 132 to specify attributes and/or limitations associated with the property rental. For example, as described more particularly with respect to FIG. 5A, the property administrator 104 may use a rental property management portal to specify the access conditions 132 on the user device 150. In response, the specified access conditions 132 are then transmitted and stored on the application server 130.

[0063] The access conditions 132 refer to specifications and/or limitations associated with a property rental. In the examples depicted in FIG. 1, the access conditions 132 may include attributes associated with the access credential (e.g., time period of activation), indications as to whether the property rental is for the entire property or a particular region within the property (e.g., limiting access to particular rooms), ancillary services that are included with the property rental (e.g., time-limited access to the appliances 124), among other types of rental specifications.

[0064] Once the communication pathway between the user device 140 and the application server 130 has been established (e.g., by activation of the distributed access credential on an

application running on the user device 140), the user 102 may transmit instructions to perform actions related to the property rental. Examples of actions may include signals to operate the appliances 124, locking and unlocking the electronic lock 128, among others. In such examples, the application running on the user device 140 may present a user interface with user-selectable options to perform particular actions. The instructions to perform the may then be transmitted to either the application server 130 (e.g., when a user 102 physically accesses the property 101 for the first time or in cases where the user device 140 does not directly communicate with the monitor control unit 110), or directly to the monitor control unit 110 or other devices connected over the network 105 (e.g., after the user device 140 has already established communications with the monitor control unit 110).

[0065] In some implementations, the application server 130 stores sensor and image data received from the monitor control unit 110 and performs analysis of the received sensor and image data. Based on the analysis, the application server 130 may communicate with and control aspects of the monitor control unit 110 or the user device 140.

[0066] The user device 140 may be an electronic device associated with a user or the user 102 and the user device 150 may be an electronic device associated with the property administrator 104. The user devices 140, 150 that exchange network communications over the network 105. For example, the user devices 140, 150 may be one or more of a smartphone, tablet, personal computer (PC), network-enabled media player, home entertainment system, cloud storage device, and other types of network devices. The user devices 140, 150 may access an application made available by the application server 130 on the network 105, such as an application (depicted in FIGS. 5A-5B and 6A-6B). The data generated by the user devices 140, 150 may include over the network 105, which may be monitored by the monitor control unit 110.

[0067] The user devices 140, 150 can include a native application. The native application refers to a software/firmware program running on the corresponding mobile device that enables the user interface and features described throughout. The user devices 140, 150 may load or install the native surveillance application based on data received over a network (e.g., the network 105) or data received from local media. The native application is capable of operating on various mobile devices platforms. The native application also enables the user devices 140, 150 to receive and process rental property data from the system 100.

[0068] In some implementations, the user devices 140, 150 communicate with and receive system data from the monitor control unit 110 or the application server 130 using a communication link. For instance, the user devices 140, 150 may communicate with the monitor control unit 110 using various local wireless protocols such as Wi-Fi, Bluetooth, Zwave, Zigbee, HomePlug (Ethernet over powerline), or wired protocols such as Ethernet and USB, to connect the user devices 140, 150 to local security and automation equipment. The user devices 140, 150 may connect locally to the system 100 and sensors 122 and other devices. The local connection may improve the speed of status and control communications because communicating through the network 105 with a remote server (e.g., the application server 130) may be significantly slower.

[0069] Although the user devices 140, 150 are shown as communicating with the application server 130, the user devices 140, 150 may also communicate directly with the sensors 122 and other devices controlled by the monitor control unit 110 when the user devices 140, 150 are near the property 101. For example, the user devices 140, 150 may exchange communications with the devices of the system 100 over the network 105.

[0070] In some implementations, the user devices 140, 150 receive system data captured by the monitor control unit 110 through the network 105. The user devices 140, 150 may receive the data from the monitor control unit 110 through the network 105 or the application server 130 may relay data received from the monitor control unit 110 to the user devices 140, 150 through the network 105. In this regard, the application server 130 may facilitate communication between the user devices 140, 150 and the system 100.

[0071] In some implementations, the system 100 intelligently leverages the monitor control unit 110 to aid in security monitoring, property automation, and property management. For example, the monitor control unit 110 may aid in investigating alarm events detected at the property 101 by the monitor control unit 110. In this example, the monitor control unit 110 may detect an alarm event (e.g., a fire alarm, an entry into the property 101 when the system is armed "Stay," etc.) and, based on the detected alarm event, control the monitor control unit 110 to attempt to identify persons in the property 101 at the time of the alarm event. Specifically, the monitor control unit 110 may send a control command that causes the sensors 122 and the cameras 126 to perform a coordinated and automated search for persons in the property 101. Based on the control command received, each of the cameras 126 captures images of the property 101.

[0072] FIG. 2 illustrates an example of a process 200 for generating a unique access credential for a user that requests to rent a property. Briefly, the process 200 may include receiving input from a property administrator 104 specifying one or more access conditions associated with a property (210), accessing rental data associated with the property from a user (220), generating a unique access credential for the user (230), and transmitting the unique access credential to a device associated with the user (240).

[0073] In more detail, the process 200 may include receiving input from a property administrator 104 specifying one or more access conditions associated with a property (210). For instance, the user device 150 may receive input from the property administrator 104 that specify the access conditions 132 associated with the property 101 on an application running on the user device 150. In some instances, the application may be an application that is configured to exchange communications with the monitor control unit 110 or the application server 130. As described herein with respect to FIG. 1, the input from the property administrator 104 may include selections of user-selectable interface objects that are associated with rental property specifications (e.g., rental time period, ancillary services available during the rental period, scope of rental within the property, etc.).

[0074] The process 200 may include accessing rental data associated with the property from a user (220). For instance, the application server 130 may receive data from the user device 140 associated with a user that indicates that the user is renting the property 101. In some examples, the rental data may include a rental start date and time and a rental end date and time.

[0075] The process 200 may include generating a unique access credential for the user (230). For instance, the application server 130 may generate a user-specific access credential for the user associated with the user device 140. As described herein with respect to FIG. 1, the generated access credential may be used as a user credential used to authenticate the user as the person that made the reservation. The generated access credential may have attributes that control its use with components of the monitor control unit. For example, the generated access credential may be associated with the access conditions 132 specified by the property administrator 104.

[0076] The process 200 may include transmitting the unique access credential to a device associated with the user (240). For instance, after generating the access credential for the user, the application server 130 may then distribute the generated access credential to the user

device 140. As described herein, the distribution of the generated access credential may include a transmission of an email to an email address corresponding to the user, a SMS message using the mobile capabilities of the user device 140, or other type of electronic formats.

[0077] FIG. 3 illustrates an example of a process 300 for enabling a user to access information associated with a rental property. Briefly, the process 300 may include receiving an access credential submitted by a user (310), obtaining rental data associated with a property (320), determining that user information included in the rental data matches user information specified by a property administrator (330), providing access to an application (340), and performing one or more action associated with the user (350).

[0078] In more detail, the process 300 may include receiving an access credential submitted by a prospective (310). For instance, once an access credential is distributed to the user device 140 associated with a user, the user device 140 may also receive a link to install an application associated with the application server 130 on the user device 140. The user may be directed to install the application on the user device 140 through a webpage or through a deep-link that redirects the user to a page in an application store. After installing the application on the user device 140, the user may submit the distributed access credential on the application, which is then transmitted to the application server 130.

[0079] The process 300 may include receiving user rental data associated with a property (320). For instance, after receiving the submitted access credential from the application running on the user device 140, the application server 130 may identify the rental property (e.g., property 101) associated with the submitted access credential and obtain rental data stored a database that includes rental data for all properties of the property administrator 104 that are available for rent. For example, the rental data may include information associated with the property 101, user information for any users, or information submitted by the property administrator 104 on a rental property listing.

[0080] The process 300 may include determining that the user information included in the rental data matches user information specified by a property administrator (330). For instance, in response to obtaining rental data associated with the property 101, the application server 130 may identify user information associated with the submitted access credential (e.g., last name of the user) that is included in the obtained rental data. The application server 130 may also identify user information that is specified by the property administrator 104,

and compare the user information associated with the submitted access credential and the user information submitted by the property administrator 104. For example, the comparison may be used to detect fraudulent attempts to rent the property 101 by unauthorized entities (e.g., any individual that the property administrator 104 does not designate as the user to receive the distributed access credential). If the user information associated with the submitted access credential matches the user information submitted by the property administrator, then the application server 130 determines a successful attempt to access property information related to the property 101. For example, the application server 130 may have a reservation with an access credential of "1234" associated with the user "John Doe" and receive an access credential of "1234" and last name of "Doe" and determine that the received last name of "Doe" matches the last name of "Doe" associated with the reservation associated with the access credential of "1234." In another example, the application server 130 may have a reservation with an access credential of "1234" associated with the user "John Doe" and receive an access credential of "1234" and last name of "Smith" and determine that the received last name of "Smith" does not match the last name of "Doe" associated with the reservation associated with the access credential of "1234."

[0081] The process 300 may include providing access to an application (340). For instance, in response to determining that the user information associated with the submitted access credential matches the user information submitted by the property administrator 104, the application server 130 may provide access to an application through which the user submitted the access credential. More particular descriptions related to the application are described with respect to FIGS. 6A-6B.

[0082] The process 300 may include performing one or more action associated with the user (350). For instance, as described herein with respect to FIG. 1, once the user has obtained access to the application running on the user device 140, the user may transmit instructions to perform actions related to the property 101 through the application. For example, the user may transmit an instruction to operate one of the appliances 124 within the property, which is then transmitted either to the application server 130, or directly to the monitor control unit 110 or the particular appliance. In this example, the established communication pathway between the user device 140, the application server 130, and the monitor control unit 110 may be over the network 105 once the user obtains access to the application used to perform actions related to property rental at or near the property 101.

[0083] FIG. 4 illustrates an example of a rental property 410 that includes multiple access regions. For instance, the rental property 410 includes regions one and two, which can be separately rented to different user users, and a common region that is accessible to all user users. For example, the regions one and two can represent different bedrooms within a rental property that is rented to different users during an overlapping rental period. In other examples, the region one and two can represent different floors, sub-units, or other types of divisions within a single property or dwelling.

[0084] Access to the premises and different regions within the property 410 can be controlled using electronic locks 422, 424, and 426. In some instances, the electronic locks 422, 424, and 426 correspond to the electronic lock 128 as described herein with respect to FIG. 1. In the example, the electronic lock 422 provides access to the common region of the property 410, the electronic lock 424 provides access to region one, and the electronic lock 426 provides access to region two. As described herein, an access credential distributed to a user can be used to configure a device associated with the user such that the user device can unlock the applicable electronic devices using instructions transmitted through the device. For example, the user may use an application that is enabled by the distributed access credential to transmit an instruction to a system 100 (e.g., the system 100) associated with property 410.

[0085] In the example depicted in FIG. 4, the system 100 identifies access credential information for three users that have access to the property 410, which are shown in tables 432, 434, and 436. The tables each identify user-specific information associated with respective access credentials (e.g., user IDs) and specifies a permission level that dictates privileges to access various regions of the property 410. In this example, user A represents a property administrator 104 that has privileges to access all regions of the property 410. In contrast, users B and C represent users that rent different regions (e.g., regions one and two) of the property 410. In some instances, the users B and C may be co-users that both rent the different regions of the property 410 during an overlapping period of time. In such instances, the regions one and two can represent different rooms within the property 410 that are made available for rent by the property administrator 104.

[0086] As depicted, the tables 432, 434, and 436 identify respective access privileges that are specified by the corresponding access credential for each user. For example, the access credential distributed to user B indicates that he/she has access to region one but not to region

two, and whereas the access credential distributed to user C indicates that he/she has access to region two but not to region one.

[0087] In addition to specifying the access privileges for each user, the tables 432, 434, and 436 specify the type of access credential distributed to each user. For example, user A has a permanent access credential that provides access to the property 410, whereas user B has a temporary access credential that provides access on a daily basis, and user C has a temporary access credential that provides access to the property 410 on a monthly basis. In this regard, access credential distribution can be used to specify different types of tenancies of the property 410 (e.g., temporary, at-will, lease, etc.), while also enabling the property administrator 104 to specify the level of access to provide with each type of tenancy (e.g., access to the entire premises for daily periods, or access to a particular region for monthly periods).

[0088] In some implementations, the property administrator 104 may receive various alerts or notifications based on the activity of users at or near the property 410. For example, the property administrator 104 may initially receive an alert 440 when a user initially unlocks the lock 422 and to obtain possession over the property 410. In other examples, the property administrator 104 may also receive alerts when a user attempts to perform actions that are prohibited by the access conditions described herein. For instance, if the access credential distributed to a particular user indicates that they cannot access a specific region within the property, then the system 100 (e.g., the system 100) of the property 410 may perform one or more monitoring operations to detect if and when the particular user attempts to access the prohibited region. In response to detecting an unauthorized access attempt, the system 100 may then transmit an alert to a device associated with the property administrator 104 indicating information such as, for example, the number of unauthorized actions attempted, timestamps associated with the actions attempted, among other types of information. In some implementations, the monitoring operations can additionally or alternatively include obtaining data collected by the devices associated with the system 100 (e.g., obtaining sensor data collected by the sensors 122, or collecting video data collected by the cameras 126).

[0089] FIGS. 5A-5B illustrate examples of user interfaces 500A and 500B of an application that includes a rental property management portal used by a property administrator 104. For instance, interface 500A enables a property administrator 104 to view the statuses associated with a list of rental properties, and interface 500B enables the property administrator 104 to

view detailed rental information associated with a single property. Although FIGS. 5A-5B illustrate the interfaces 500A and 500B being displayed on an application running on a device 502, in other implementations, the interfaces 500A and 500B can also be displayed in other electronic formats such as a desktop application, a webpage, or other types of content distribution interfaces. In some instances, the device 502 corresponds to the user device 150 described herein with respect to FIG. 1.

[0090] Referring initially to FIG. 5A, the interface 500A includes a reservation management page that displays an overview of all available rental properties that are either managed or owned by the property administrator 104. For instance, table 510 identifies each rental property and indicates a rental/access status associated with each rental property. The rental/access status indicates whether a user has activated a distributed access credential for a corresponding rental property and the access period specified by the distributed access credential. For example, the table 510 specifies an “INACTIVE (NO RESIDENTS)” status for the “123 MAIN ST” property, indicating that the system has not yet distributed an access credential for the property to a user. In another example, the table 510 specifies an “ACTIVE – USER HAS ACTIVATED TOKEN (MONTHLY)” status for the “9 FIRST ST, APT. 3” property, indicating that the system has distributed a single access credential for the rental property on a monthly basis to a user, who has activated the distributed access credential. In yet another example, the table 510 specifies an “ACTIVE – MULTIPLE ACCESS CREDENTIALS ACTIVATED (DAILY)” status for the “15 SECOND DR.” property, indicating that the system has distributed multiple access credentials for the rental property on a daily basis to multiple co-users that each rent a particular region of the rental property.

[0091] Referring now to FIG. 5B, the interface 500B includes a property detail page that allows a property administrator to view and adjust property-specific information associated with a rental property. For instance, the property detail page includes property information 512, user information 514, and an alert button 516. In the example depicted, the property information 512 specifies a property address (e.g., “15 Second Drive, Washington, DC 20001”), a property type (e.g., a house), and/or other information (e.g., 3-bedroom, 2-bath).

[0092] The user information 514 includes a username associated with a user and specifies access credential information associated with the user. In the example depicted in FIG. 5B, the access credential information for the user “USER001” indicates that the access credential is “ACTIVE (NOT ENABLED).” In this example, this indicates that the user has entered a

distributed access credential into an application (e.g., into the interface 600A depicted in FIG. 6A), but has not yet used the access credential to physically access the property thereby initiating the rental period.

[0093] The user information 514 further specifies a set of specifications and services that are associated with the property rental by the user 102. In the examples depicted in FIG. 5B, such specifications may include the time period for rental (e.g., 5-day access), ancillary services that are included within the rental (e.g., access to appliances), and/or the scope of access within the property that is covered under a rental agreement (e.g., partial property access).

[0094] The user information 514 may provide the property administrator 104 with an option to adjust preconfigured access settings during various time points of a rental agreement (e.g., after a rental agreement has been formed but before the start of the rental period, or during the rental period, etc.). For instance, a property administrator 104 may choose an option to adjust access settings during a rental period by selecting the “ADJUST ACCESS SETTINGS” button, which then redirects the property administrator 104 to an access configuration page that allows the property administrator 104 to specify specifications associated with the property rental. In response to receiving an updated selection of rental specifications, the system 100 may then provide an additional notification to the user 102, and/or dynamically reconfigure the system 100 associated with the property 101 to effectuate the updated rental specifications. In one example, a property administrator 104 may wish to restrict access to a particular appliance within the property 101 after a rental agreement that includes access to the particular appliance has been formed. In this example, once the property administrator 104 updates the access settings, the application server 130 may transmit an instruction to the monitor control unit 110 to adjust a set of access configurations associated with the distributed access credential. Once the user 102 subsequently uses the distributed access credential through the user device 140 to transmit an instruction to operate the particular appliance, the monitor control unit may use the set of adjusted access configurations to restrict access to the particular appliance.

[0095] The alert button 516 provides the property administrator 104 with the option to transmit notifications, alerts, and/or other supplemental information to all users associated with the particular rental property displayed within the property detail page. For example, the property administrator 104 may use the alert button 516 to transmit property-related

information (e.g., maintenance updates, payment reminders, updates on user service requests, etc.).

[0096] FIGS. 6A-6B illustrate examples of user interfaces 600A and 600B, respectively, for an application that is used by users such as temporary guests of a rental property.

Specifically, interface 600A enables a user to submit an access credential for authentication purposes to obtain access to the application. The interface 600B enables the user to view and access rental property information after gaining access to the application using the submitted access credential. Although FIGS. 6A-6B illustrate the interfaces 600A and 600B being displayed on an application, in other implementations, the interfaces 600A and 600B can also be displayed in other electronic formats such as through a webpage portal.

[0097] Referring initially to FIG. 6A, the interface 600A represents a login page of the application that runs on a user device 602. The user can access the interface 600A on the user device 602 to submit an access credential 612 for authentication into the application. The application is capable of exchanging communications with an application server associated with a monitoring system of the rental property, as depicted in FIG. 1. In this regard, access to the application through the interface 600A enables the user to, for example, control electronic devices of the monitoring system using actions presented through application. For example, the user can use the application to gain physical access to the property (e.g., by unlocking an electronic lock), control electronic devices located within the property (e.g., by submitting remote instructions through the application), among others.

[0098] In some implementations, the actions may include all actions that users are permitted to trigger in the property. In other implementations, such actions can include viewing and accepting the terms of a rental agreement, accessing additional property information, exchanging communications with the property administrator 104, among other types of actions.

[0099] As described herein with respect to FIG. 1, the user 102 may initially receive a distributed access credential in response to submitting an inquiry related to a rental property (e.g., a reservation request submitted for an electronic rental listing for the rental property). In some implementations, the distributed access credential is associated with external account information of the user (e.g., username, last name, etc.) such as a user account for a rental property listing website or a rental property listing application.

[00100] Referring now to the example depicted in FIG. 6A, the user submits an access credential 612 that includes PIN number and a last name. Once the user has submitted the access credential 612 on the login page, the distributed access credential becomes “active.” As discussed previously with respect to FIG. 1, in some implementations, the activated access credential refers to an indication that a user has used a distributed access credential to access an application. In this regard, an activated access credential provides the property administrator 104 with an indication that the user may have an interest in renting the rental property. In such instances, multiple access credentials may be distributed for a single property (e.g., to multiple users), and once a particular user agrees to enter into a rental agreement, the corresponding access credential becomes “enabled,” indicating that the rental property is no longer available for rent to other users. In response to a rental agreement being formed between a user 102 and a property administrator 104, the system 100 may automatically deactivate all other access credentials that have been previously distributed to other users.

[00101] Alternatively, in other implementations, an access credential operates as a single-use token that provides only a single user with access to property information on an application. In such implementations, only the user 102 that has already formed a rental agreement with a property administrator 104 is provided a distributed access credential. The distributed access credential can then be used by the user 102 to perform actions that are related to the property rental as described throughout. For example, such actions can include transmitting an instruction to the system 100 to unlock the electronic lock 128 in order to physically access the property 101, transmitting instructions to operate the appliances 124 within the property 101, and/or exchanging communications with the property administrator 104.

[00102] In addition, in some instances, in response to an activation of the access credential by the user 102, the system 100 associated with the property 101 may receive and store user-specific information associated with the distributed access credential (e.g., username, password, last name, etc.) prior to the start of the rental period. Once the user 102 uses the user device 140 to perform actions related to the property 101 (e.g., physically access the property 101, transmit instructions to the monitor control unit 110, etc.), the system 100 may then perform a user verification operation to ensure that the presentation of the access credential is by an authorized user and/or user device. In these instances, the user-specific information may include information that is uniquely available to the user 102 (e.g., answers

to security questions), hardware-related information of the user device 140, among other types of information.

[00103] In some implementations, the system performs different types of verification operations in association with the access credential submitted by the user on the application. For example, in some instances, the system performs a verification operation prior to distributing an access credential to the user and/or allowing the user to access a login page of the application where an access credential can be submitted such as the interface 600A. In such instances, the system initially verifies that the user that is provided the distributed access credential and/or with access to the login page of the application is actually the actual user that that submitted the rental reservation and/or formed the rental agreement. For example, before distributing the access credential, the user may be requested to provide user-specific information that is used to identify the identity of the user (e.g., user-specific information associated with an account for a property listing website). In such instances, the user is distributed the access credential and/or provided with access to the login page of the application where the distributed credential can be submitted only after his/her identity has been verified.

[00104] Alternatively, or in addition, the system performs a verification operation after the user has submitted the access credential on, for example, a login page of the application such as the interface 600A. In such instances, the system can verify either the submitted access credential (e.g., determining whether a submitted PIN code is correct), or verify some other type of externally associated data related the access credential such as uniquely identifiable information for the user submitting the access credential, and/or device data for the user device used to submit the access credential. For example, the user may be requested to provide account information associated with an existing account (e.g., an account associated with a rental listing website), which is then used as a second factor authentication in addition to the submitted access credential. In other examples, the user may be requested to provide identifying information for the rental property (e.g., a property identifier) in order to verify that he/she is attempting to access the correct rental property through the application. In some other examples, sensor data such as location data of the user device can be used to verify the submitted access credential. In such examples, the system determines that the submitted access credential is verified only if the user is within a threshold proximity to the location of the rental property.

[00105] Although the verification operations described above are in relation to the activation of the access credential (e.g., the process by which a user submits the access credential to gain access to the application), in some other implementations, the system can perform verification operations in relation to access credential enablement. The system may perform such verification operations after the access credential has been activated but before the access credential has been enabled to prevent unauthorized users from gaining access to the property. For example, when a user attempts to physically access the rental property, location data of the user device used by the user can be used to determine if he/she is within a threshold proximity (e.g., within 50 feet) of the location of the rental property. In this example, even though the user has previously activated the access credential, he/she can only enable the access credential to gain access to the property if the system verifies that his/her associated device is located nearby the property.

[00106] Referring now to FIG. 6B, the interface 600B provides a rental property access page that provides a user with rental property access information through an application. For instance, the rental property access page may include property information 622, available service information 624, and an alert button 626. In the example depicted, the property information 622 specifies a property address (e.g., "15 Second Drive, Washington, DC 20001"), access credential status and information (e.g., provided on a daily basis and active for four more days), and/or other rental information (e.g., shared rental with one other user).

[00107] The available service information 624 specifies various types of services that are associated with the rental property. For instance, the available service information 624 may specify regions of the property that are physically accessible by the user 102 under the rental agreement (e.g., rooms 1, 2) and associated access information such as the remaining time period that the enabled access credential provides physical access to the user 102 (e.g., four days remaining within a rental period).

[00108] The available service information 624 also specifies a list of appliances and other electronic devices that are available for use by the user 102 during the property rental. In the example depicted, the available service information 624 specifies a list of smart appliances that can be operated by exchanging communications between the system 100 within the property 101 and the user device 602. For example, the user 102 may transmit instructions to the monitor control unit 110 or the application server 130, which then relays the instructions to the appliances 124. In this example, the access credential distributed to the user 102 and

the corresponding specifications provided to the system 100 enables the user 102 to access the appliances 124 that are indicated in the access conditions described herein with respect to FIGS. 5A and 5B. The access conditions provide limitations on access privileges granted by a distributed access credential (e.g., availability from 9AM to 10PM).

[00109] The alert button 626 provides the user 102 to transmit messages, alerts, notifications, or other types of communication to the property administrator 104 in a manner similar to that of the alert button 516 described herein with respect to FIG. 5B, but from the perspective of the user 102.

[00110] FIG. 7 is a flowchart that illustrates an example of a process 700 for providing temporary access to a property. Briefly, the process 700 can include the operations of generating an access credential for a property (710), transmitting data indicating the access credential (720), receiving access data indicating a submitted access credential (730), determining that the submitted access credential is valid (740), and providing access to user interface enabling access to the property (750).

[00111] The operations of the process 700 can generally be executed by one or more components of the system 100 as depicted in FIG. 1. For example, the operations can be performed by the application server 130, the monitor control unit 110, or a combination thereof. The descriptions below are provided in reference to the application server 130 for brevity.

[00112] In more detail, the process 700 can include the operation of generating an access credential for a property (710). For instance, the application server 130 generates an access credential that specifies a time period that the access credential provides access to the property 101. As described herein, the access credential can be generated at various time points in relation to the rental process. In some implementations, the access credential is generated once the property administrator 104 creates an electronic listing for the property 101 on a rental listing website but before a user actually submits a reservation request for the rental listing. Alternatively, in other implementations, the access credential is generated once a user submits a reservation request to the rental listing.

[00113] As described above, the access credential specifies a time period that the access credential can be used to provide the user 102 with access to the property 101. In some instances, the time period corresponds to a rental period during which the user 102 rents the

property 101 under a rental agreement with the property administrator 104. In such instances, the access credential is revoked after the rental period (e.g., the user 102 is unable to use the access credential to access the property 101). In other instances, the time period corresponds to a time period specified by the property administrator 104 irrespective of the rental period.

[00114] As described above, the generated access credential can also have different configurations and/or functions based on their specific application. In some implementations, a generated access credential can be used by multiple users to access rental property information through an application. For example, before a rental agreement has been formed between the property administrator and a user, a single access credential can be used by multiple users to access rental property information over the application. Alternatively, in other implementations, multiple user-specific access credentials can be generated for each user that submits a rental reservation for the same time period before a rental agreement has been formed for the time period. In addition, as discussed above, in some implementations, access credentials may be used multiple times by one or more users. Alternatively, in other implementations, access credentials can be used as single-use tokens that are only capable of used once by a user.

[00115] The format and/or content of the generated access credential can vary across different implementations. In some implementations, the access credential is an alphanumeric code such as a PIN number. In such implementations, the access credential can be distributed to the user device 140 as, for instance, a text message that includes alphanumeric code. In other implementations, the access credential represents a combination of an access code and other association information such as personally identifiable information for the user 102. For example, as depicted in FIG. 6A, the access credential can include both an access code and a last name for the user 102. In some other implementations, the access credential represents a combination of an access code and property-specific information for the property 101 that allows the application to associate the access credential with the property 101. For example, the access credential can include an access code and an identifier for the property 101 that is associated with an electronic rental property listing.

[00116] In some implementations, the access credential specifies one or more access conditions that provide, for example, restrictions for accessing the property using the access credential. For example, as depicted in FIG. 4, the access conditions can specify regions of the property that are accessible by the user 102 using the access credential and other regions

of the property that are inaccessible by the user 102. Other examples of access conditions include the type of access provided by the access credential (e.g., permanent, temporary).

[00117] In some implementations, the specified access conditions can be adjusted during the time period when an access credential is “enabled” (e.g., being used by the user 102 to access the property 101). For example, as depicted in FIG. 5B, the property administrator 104 may adjust access conditions specifying access for the user 102 during the rental period, and in response, the system modifies the access credential distributed to the user 102 to specify the modified access conditions. In such circumstances, the user 102 can either be distributed a second access credential, or the application configuration protocol can be changed and/or updated to implement the modified access conditions specified by the adjusted access credential.

[00118] The process 700 can include the operation of transmitting data indicating the access credential (720). For instance, the application server 130 can transmit data indicating the access credential to the user device 140 of the user 102 using various types of electronic mediums (e.g., e-mail, text message, etc.). As described above, the access credential can be distributed to the user device 140 at different time points of the rental process across different implementations. For example, in some implementations, the access credential is distributed to the user 102 after he/she has submitted a reservation request but prior to the formation of a rental agreement. In such implementations, the user 102 can “activate” the access credential to access an application to view rental property information but is unable to “enable” the access credential to obtain access to the property 101 as described above. In other implementations, the access credential is distributed only after the user 140 has formed a rental agreement with the property administrator 104 to rent the property 101 over a rental period. In such implementations, the user 102 can “activate” the access credential to view property information on the application, and then “enable” the access credential to gain access to the property 101 at the start of his/her rental period under the rental agreement.

[00119] The process 700 can include the operation of receiving access data indicating a submitted access credential (730). For instance, once the access credential has been distributed to the user 102, the application server 130 receives access data from the user device 140 indicating a submitted access credential. For example, as depicted in FIG. 6A, the submitted access credential can be provided through a login page of the application where the

user 102 can submit the access credential that was previously distributed and/or other types of information.

[00120] In some implementations, the access data includes other types of data in addition to the submitted access credential. For example, in some implementations, the access data additionally includes location data indicating a present location of the user device 140 when the user provided the submitted access credential. In other examples, the access data can include user-specific information (e.g., external account information of the user for a rental property website) or property-specific information (e.g., a property identifier for the property 101). In such examples, the user-specific information and/or the property-specific information can be used to validate the received access data.

[00121] The process 700 can include the operation of determining that the submitted access credential is valid (740). For instance, the application server 130 may determine that the submitted access credential is valid based on the access data received at step 730. In some implementations, the application server 130 determines that the submitted access credential is valid based on determining that the submitted access credential matches the access credential that was distributed to the user device 140 at step 720. In other implementations where the received access data includes other information, the application server 130 additionally, or alternatively, determines that the submitted access credential based on verifying the other information. For example, application server 130 may verify location data of the user device 140 based on determining that the present location of the user device 140 is within a threshold proximity of the location of the property 101. In other examples, the application server 130 may verify submitted user information included with the submitted access credential within the access data if the submitted user information matches a set of verified user information obtained from an external user account such as an existing user account with a rental listing website.

[00122] The process 700 can include the operation of providing access to user interface enabling access to the property (750). For instance, in response to determining that the submitted access credential is valid, the application server 130 provides the user 102 with access to a user interface (e.g., the user interface 600B) enabling access to the property for the time period specified by the access credential. Access to the user interface can be provided through a mobile application, as depicted in FIG. 6B, or through a webpage portal, as described above. Once the user 102 has been provided access to the user interface, the

user can, for example, view property information for the rental property or perform actions in association with the rental property such as unlocking an electronic lock for the property to obtain physical access to the property. For example, a user can select a user interface element presented on the user interface that causes the user device 140 to transmit an indication to the application server 130 to relay an instruction to the unlock the electronic lock 128 and provide the user 102 with physical access to the property 101.

[00123] The described systems, methods, and techniques may be implemented in digital electronic circuitry, computer hardware, firmware, software, or in combinations of these elements. Apparatus implementing these techniques may include appropriate input and output devices, a computer processor, and a computer program product tangibly embodied in a machine-readable storage device for execution by a programmable processor. A process implementing these techniques may be performed by a programmable processor executing a program of instructions to perform desired functions by operating on input data and generating appropriate output. The techniques may be implemented in one or more computer programs that are executable on a programmable system including at least one programmable processor coupled to receive data and instructions from, and to transmit data and instructions to, a data storage system, at least one input device, and at least one output device. Each computer program may be implemented in a high-level procedural or object-oriented programming language, or in assembly or machine language if desired; and in any case, the language may be a compiled or interpreted language. Suitable processors include, by way of example, both general and special purpose microprocessors. Generally, a processor will receive instructions and data from a read-only memory and/or a random access memory. Storage devices suitable for tangibly embodying computer program instructions and data include all forms of non-volatile memory, including by way of example semiconductor memory devices, such as Erasable Programmable Read-Only Memory (EPROM), Electrically Erasable Programmable Read-Only Memory (EEPROM), and flash memory devices; magnetic disks such as internal hard disks and removable disks; magneto-optical disks; and Compact Disc Read-Only Memory (CD-ROM). Any of the foregoing may be supplemented by, or incorporated in, specially designed application-specific integrated circuits (ASICs).

[00124] It will be understood that various modifications may be made. For example, other useful implementations could be achieved if steps of the disclosed techniques were performed

in a different order and/or if components in the disclosed systems were combined in a different manner and/or replaced or supplemented by other components. Accordingly, other implementations are within the scope of the disclosure.

CLAIMS

1. A method comprising:
 - generating, by a server system, an access credential that specifies a time period that the access credential provides access to a property;
 - transmitting, by the server system and to a computing device of a user, data indicating the access credential;
 - receiving, by the server system and from the computing device of the user, access data indicating a submitted access credential;
 - determining that the submitted access credential is valid based on the received access data; and
 - in responses to determining that the submitted access credential is valid, providing access to a user interface on the computing device, the user interface enabling the user to access the property for the period of time specified by the access credential.
2. The method of claim 1, wherein the access credential is valid during the time period once the access credential has been used to provide access to the property.
3. The method of claim 1, wherein:
 - the access credential is an alphanumeric code; and
 - data indicating the access credential comprises a text message that includes the alphanumeric code.
4. The method of claim 1, wherein determining that the submitted access credential is valid comprises determining that the submitted access credential matches the access credential.
5. The method of claim 1, wherein the user interface comprises a user interface element that, when selected by the user, provides physical access the property.

6. The method of claim 5, further comprising:
 - obtaining, by the server system and from the computing device of the user, data indicating a user selection of the user interface element through the user interface; and
 - transmitting, by the server system and to a monitoring system of the property, an instruction to unlock an electronic lock that provides access to the property.

7. The method of claim 1, wherein the access credential specifies one or more access conditions specified by a property administrator of the property.

8. The method of claim 7, wherein the one or more access conditions comprises an access condition that specifies one or more regions of the property that are restricted from be accessed during the time period.

9. The method of claim 7, further comprising:
 - after providing access to the user interface on the computing device, receiving, by the server system, data indicating an adjustment to at least one of the one or more access conditions; and
 - modifying, by the server system, the access credential to specify the at least one adjusted access conditions.

10. The method of claim 1, wherein the access credential specifies access to one or more electronic devices associated with a monitoring system of the property through the user interface.

11. The method of claim 1, wherein the user interface is provided on the computing device through an application, the application enabling the computing device to exchange communications with one or more electronic devices associated with a monitoring system of the property.

12. The method of claim 1, further comprising:
receiving, by the server system and from the computing device of the user, data indicating a reservation request to access the property for a rental period;
wherein the access credential is generated in response to receiving the data indicating the reservation request; and
wherein the time period specified by the access credential corresponds to the rental period.
13. The method of claim 1, further comprising:
receiving, by the server system, data indicating an electronic rental listing for the property;
receiving, by the server system and from the computing device of the user, data indicating a reservation request for the electronic rental listing for the property;
wherein the access credential is generated in response to receiving the data indicating the electronic rental listing for the property; and
wherein the access credential is transmitted to the computing device of the user after receiving the data indicating the reservation request.
14. The method of claim 1, wherein the access data indicates a location of the computing device of the user when the submitted access credential is provided by the user on the computing device; and
determining that the submitted access credential is valid comprises determining that the location of the computing device is within a threshold proximity to a location of the property when the submitted access credential is provided by the user on the computing device.
15. A system comprising:
one or more computers; and
one or more storage devices storing instructions that, when executed by the one or more computers, cause the one or more computers to perform operations comprising:
generating, by a server system, an access credential that specifies a time period that the access credential provides access to a property;

transmitting, by the server system and to a computing device of a user, data indicating the access credential;

receiving, by the server system and from the computing device of the user, access data indicating a submitted access credential;

determining that the submitted access credential is valid based on the received access data; and

in responses to determining that the submitted access credential is valid, providing access to a user interface on the computing device, the user interface enabling the user to access the property for the period of time specified by the access credential.

16. The system of claim 15, wherein the access credential is valid during the time period once the access credential has been used to provide access to the property.

17. The system of claim 15, wherein:

the access credential is an alphanumeric code; and

data indicating the access credential comprises a text message that includes the alphanumeric code.

18. A non-transitory computer-readable storage device encoded with computer program instructions that, when executed by one or more computers, cause the one or more computers to perform operations comprising:

generating, by a server system, an access credential that specifies a time period that the access credential provides access to a property;

transmitting, by the server system and to a computing device of a user, data indicating the access credential;

receiving, by the server system and from the computing device of the user, access data indicating a submitted access credential;

determining that the submitted access credential is valid based on the received access data; and

in responses to determining that the submitted access credential is valid, providing access to a user interface on the computing device, the user interface enabling the user to access the property for the period of time specified by the access credential.

19. The non-transitory computer-readable storage device of claim 18, wherein the access credential is valid during the time period once the access credential has been used to provide access to the property.

20. The non-transitory computer-readable storage device of claim 18, wherein:
the access credential is an alphanumeric code; and
data indicating the access credential comprises a text message that includes the alphanumeric code.

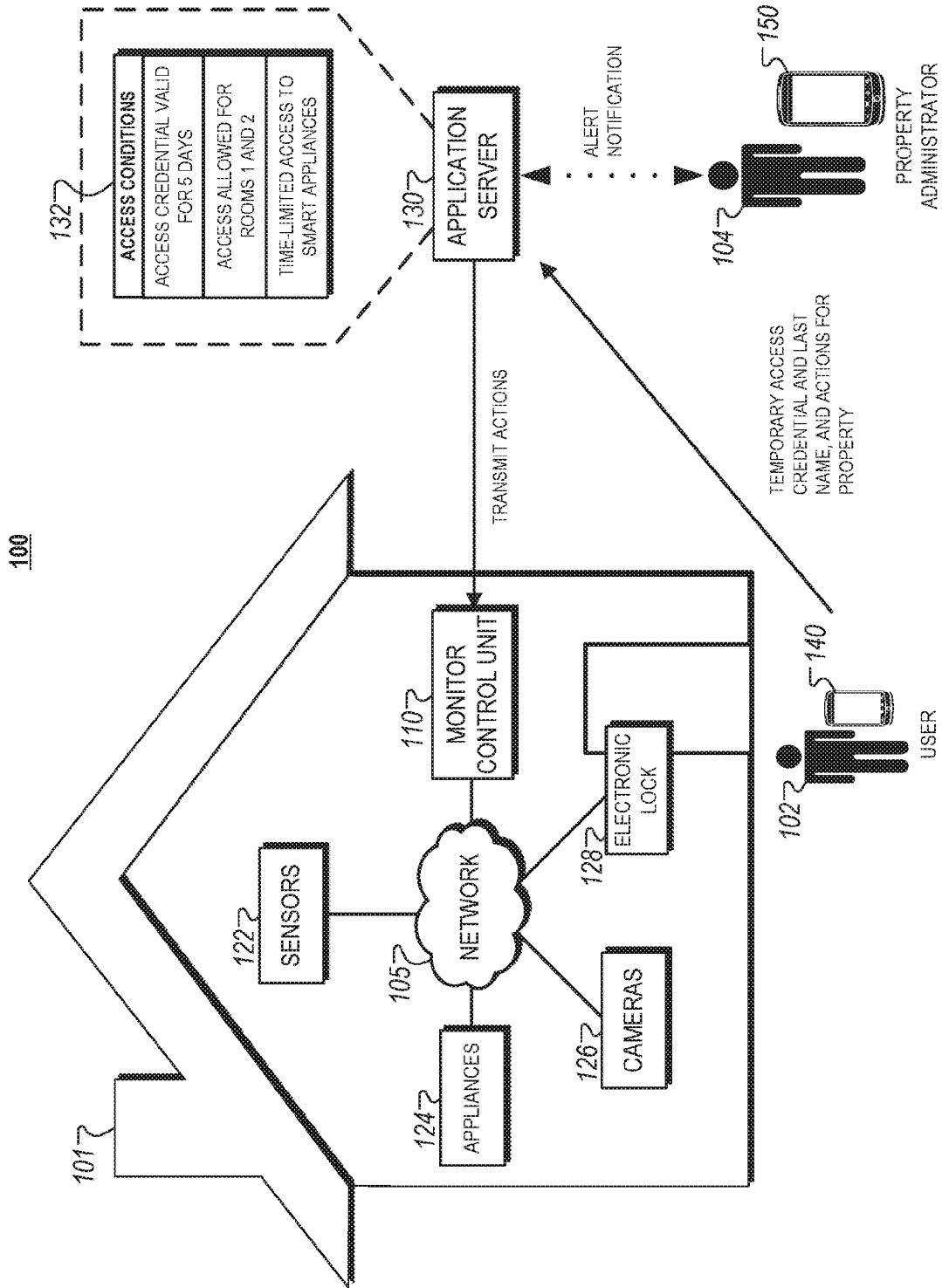


FIG. 1

2/9

200

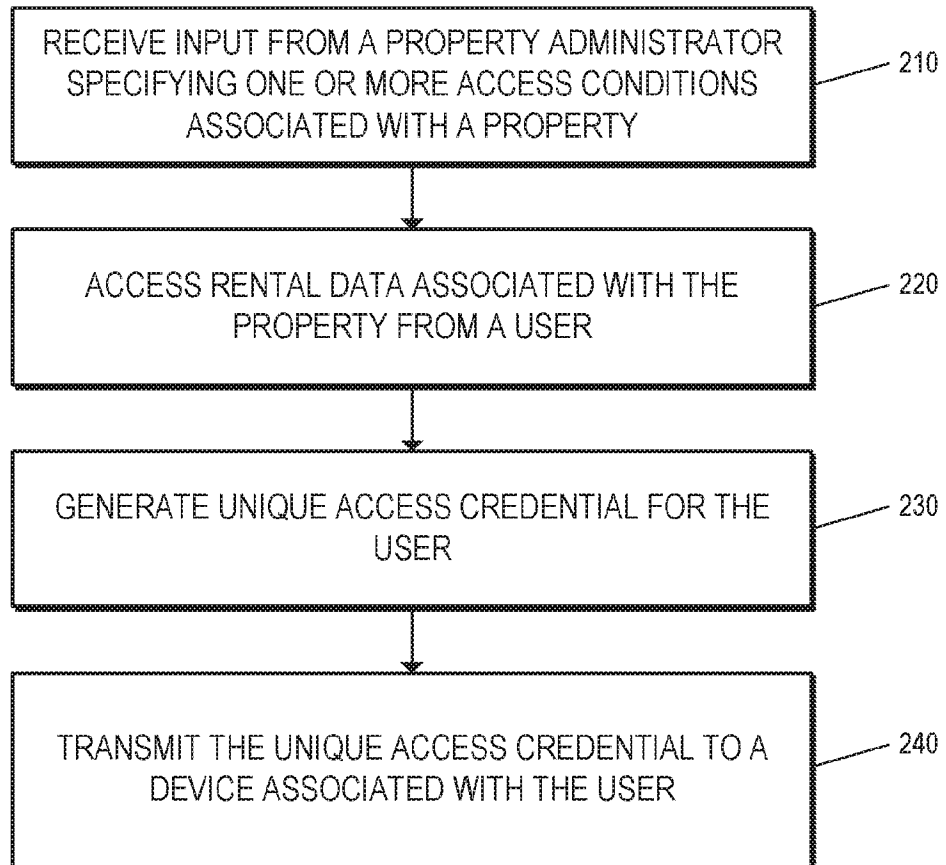


FIG. 2

3/9

300

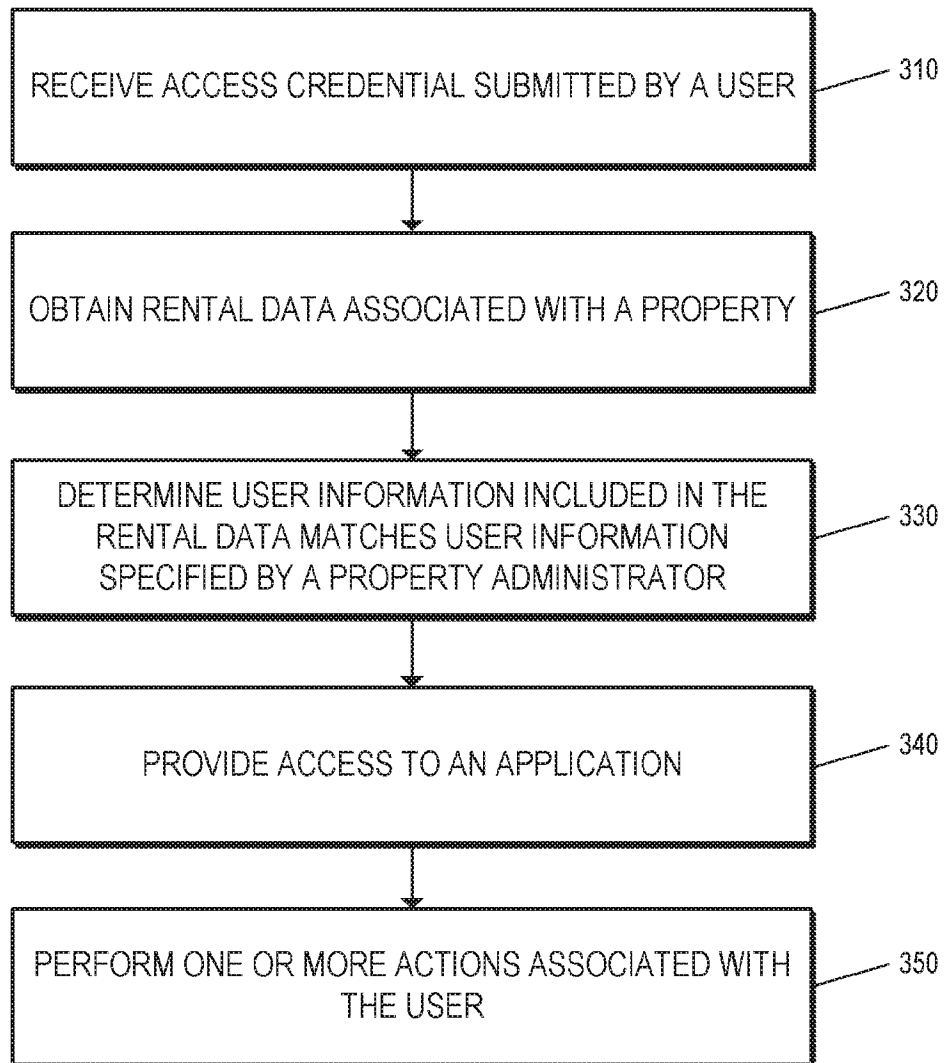


FIG. 3

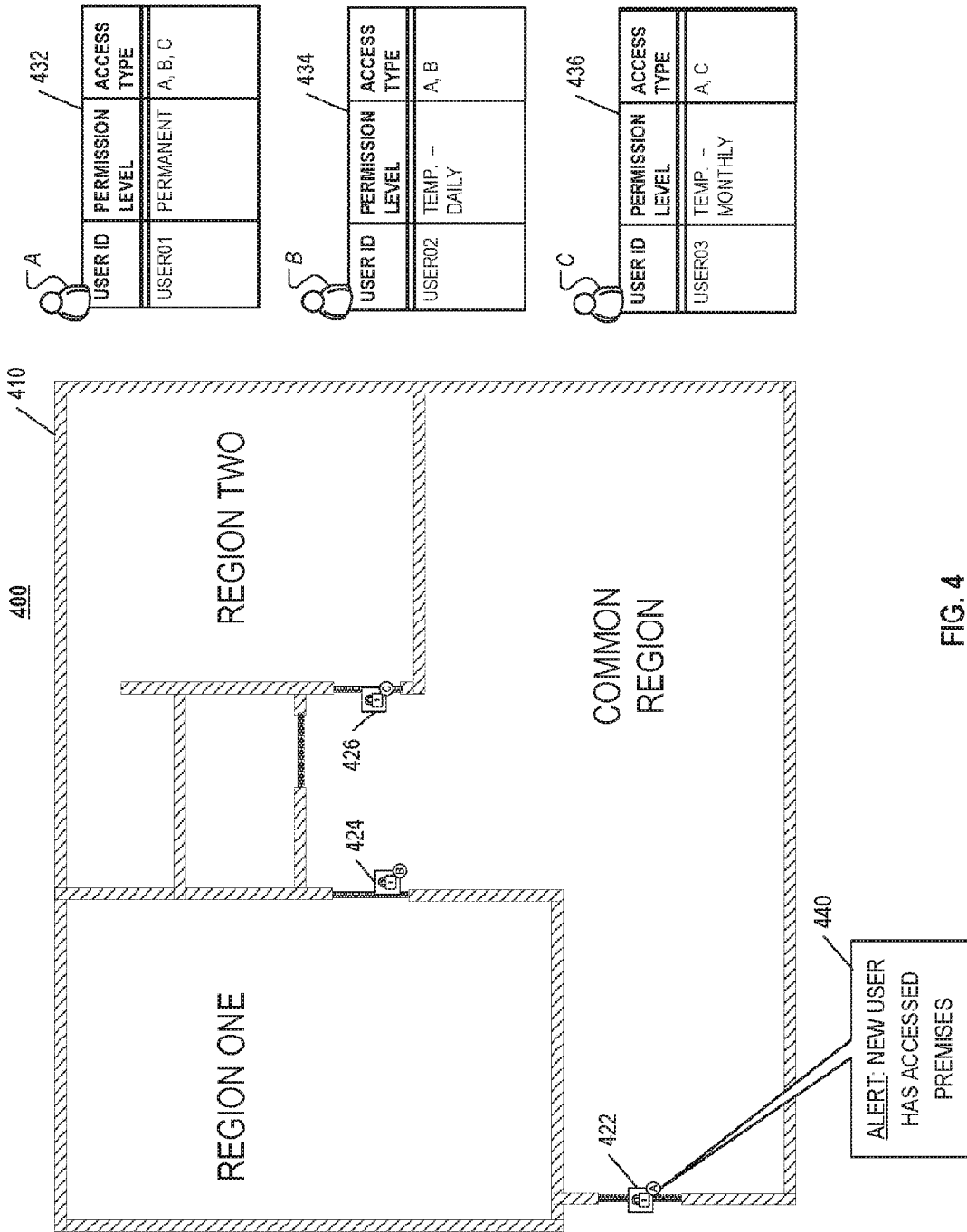


FIG. 4

5/9

500A

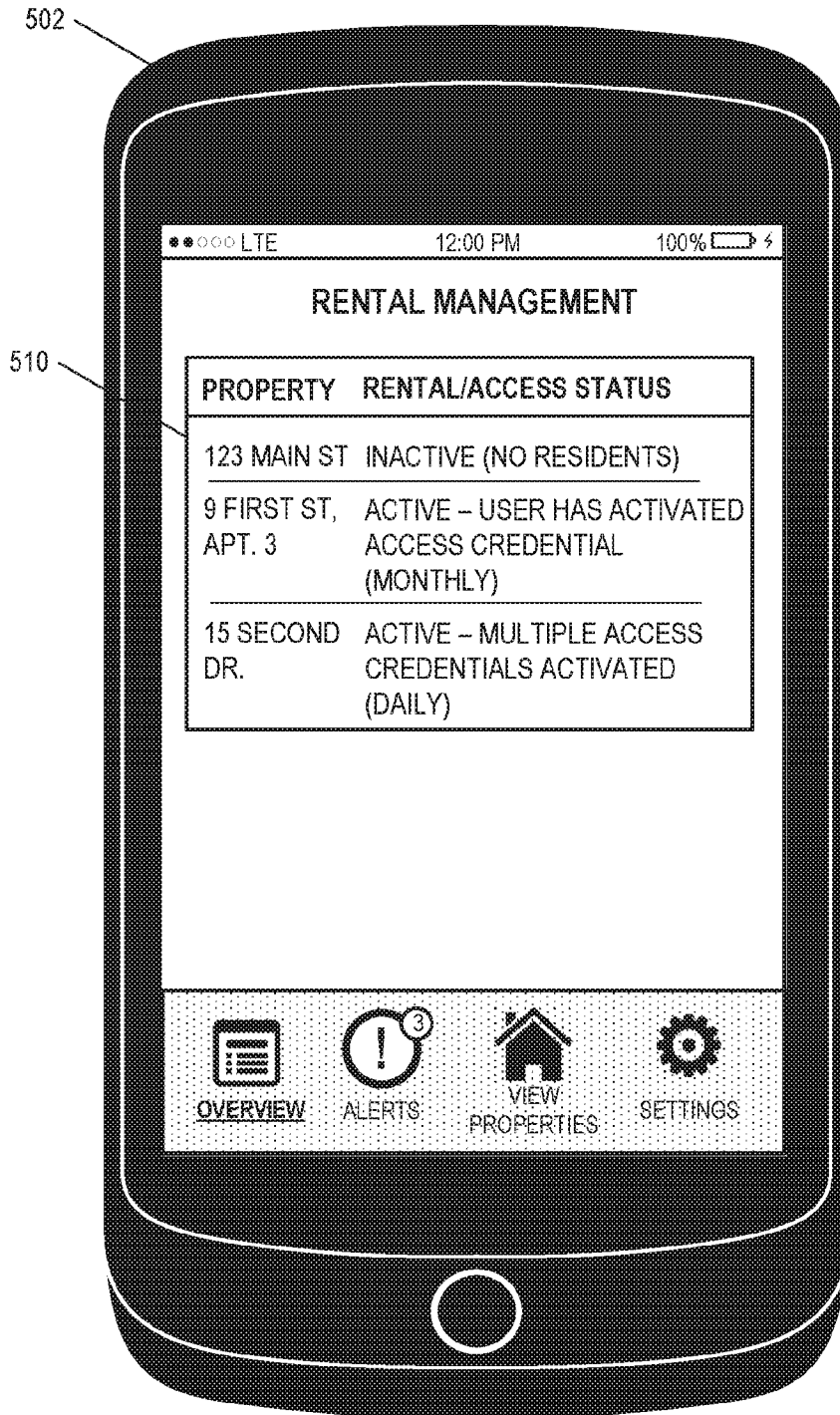


FIG. 5A

6/9

500B

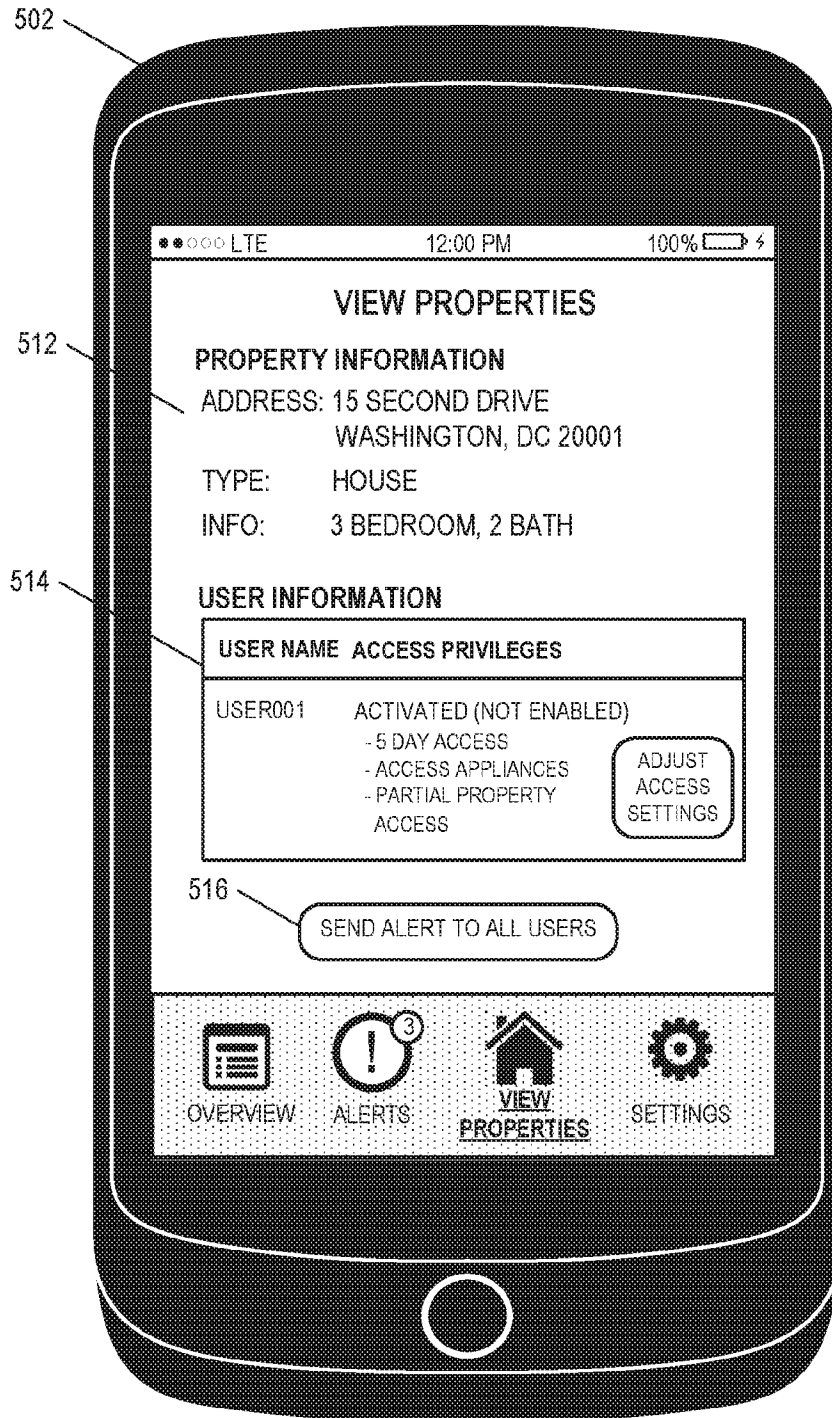


FIG. 5B

7/9

600A

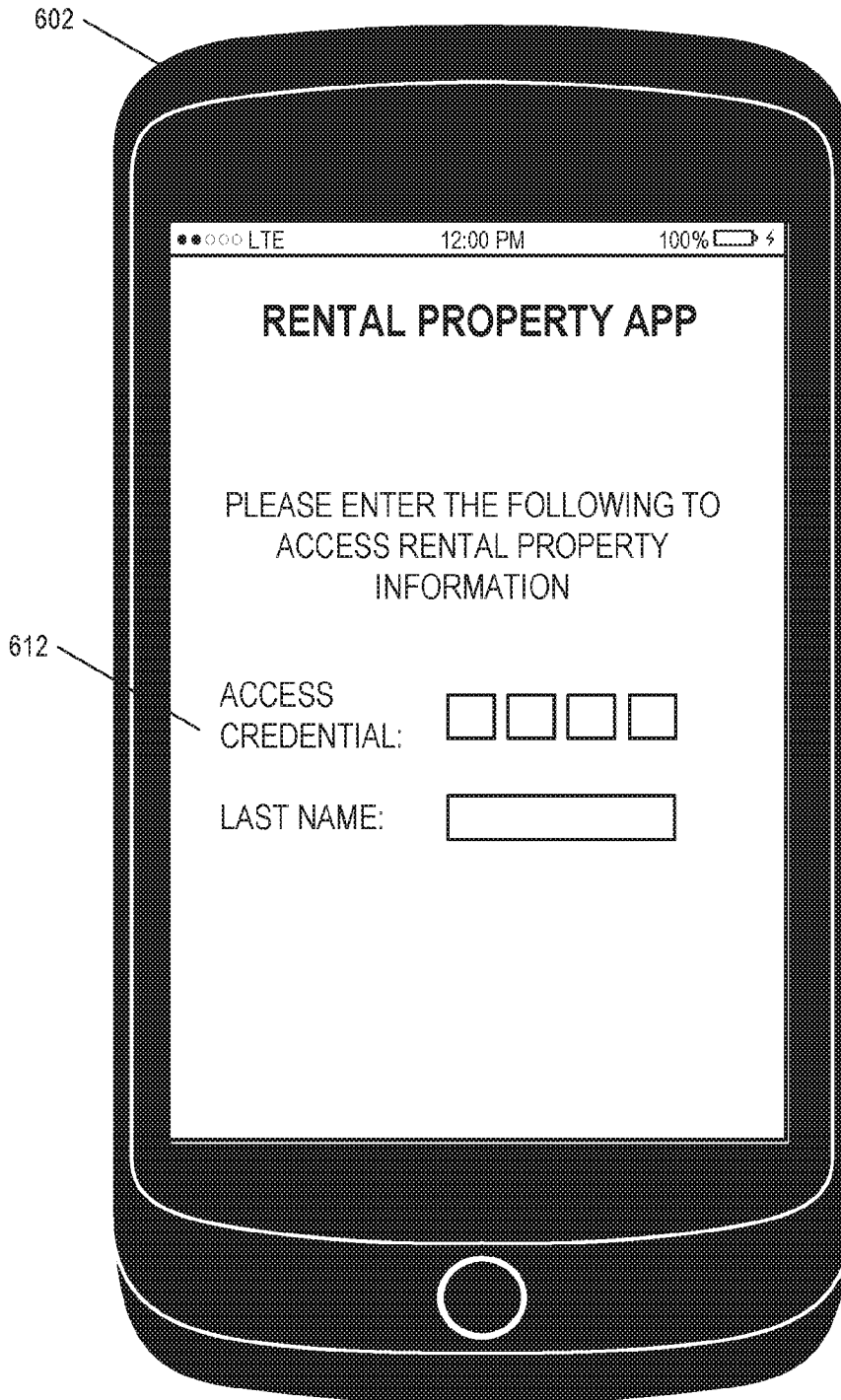


FIG. 6A

8/9

600B

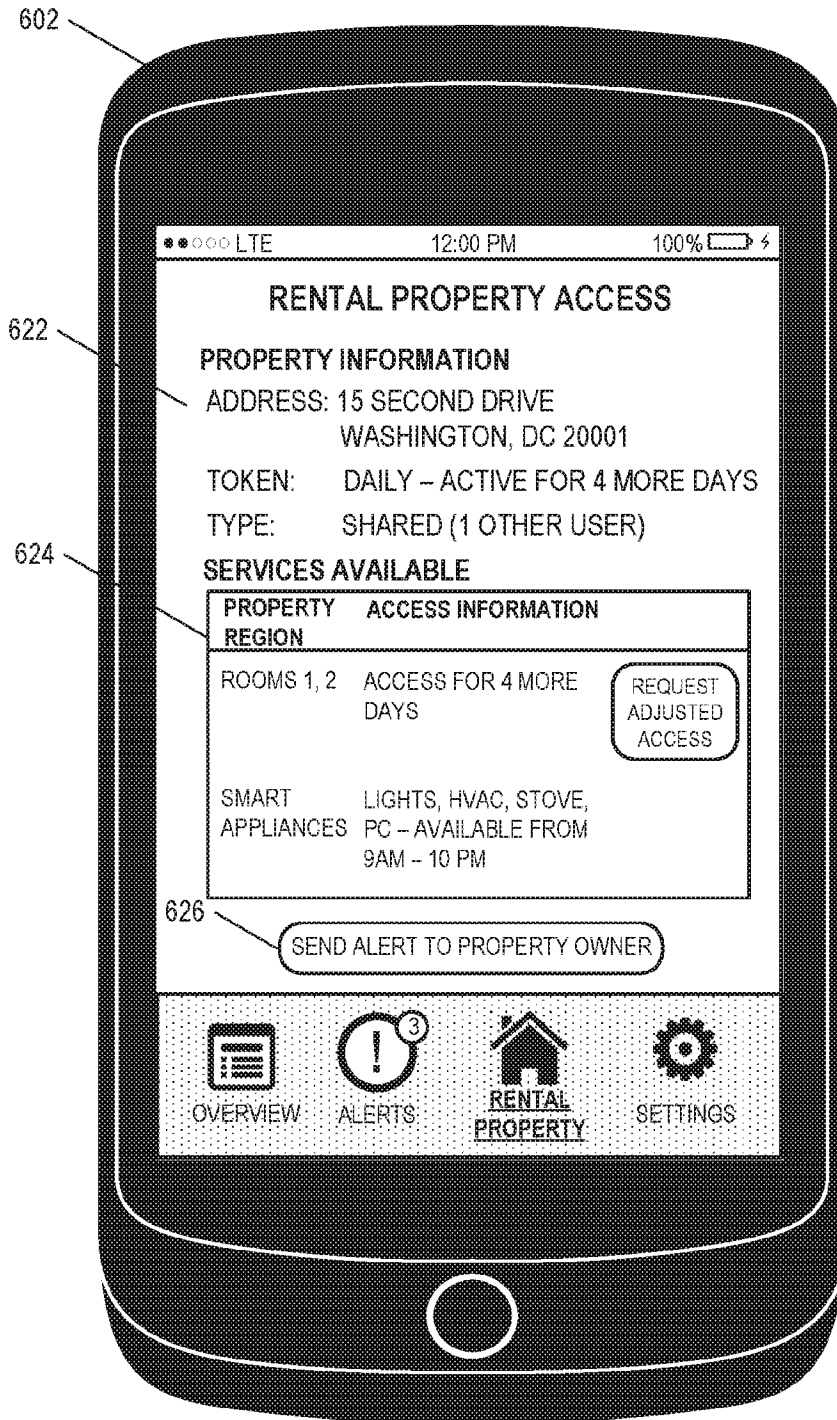


FIG. 6B

9/9

700

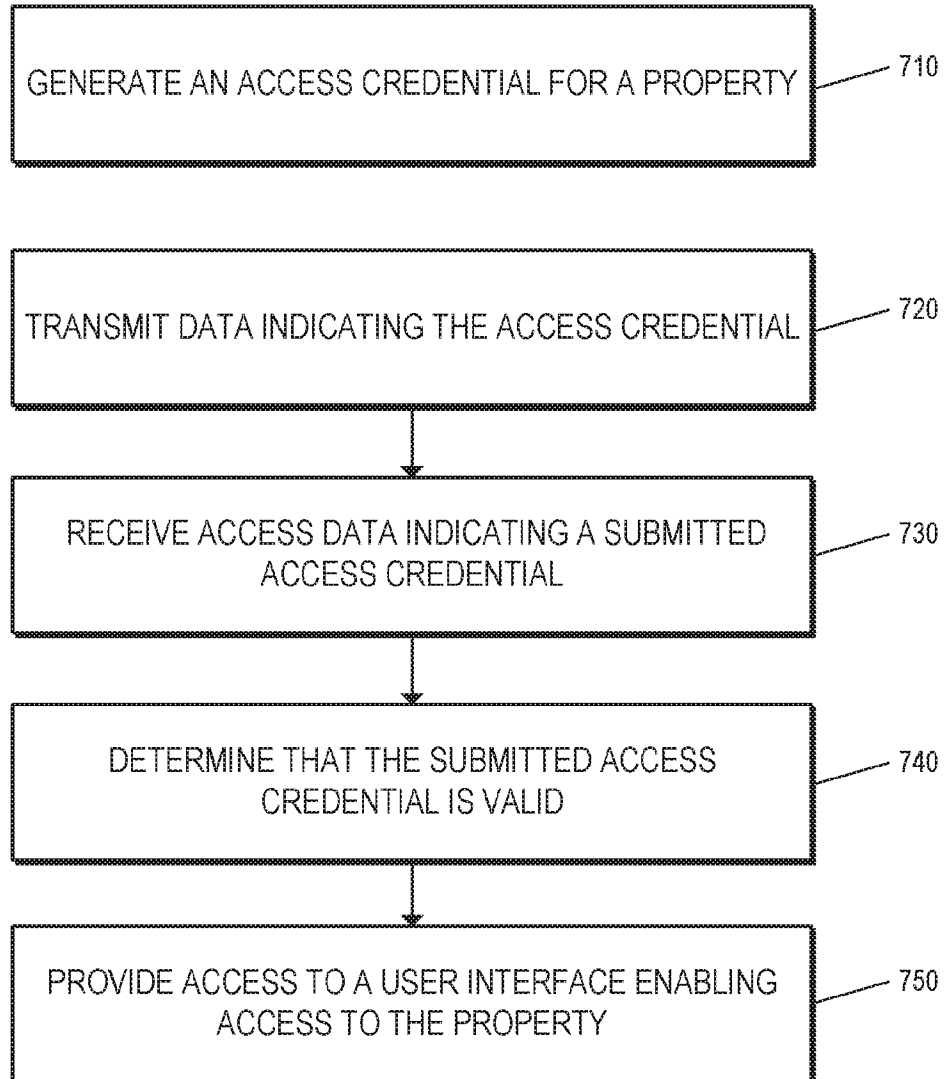


FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 17/40304

A. CLASSIFICATION OF SUBJECT MATTER IPC(8) - G06Q 10/00 (2017.01) CPC - G06Q 30/0645, G06Q 40/06, G06Q 50/16, G06Q 40/025, G06Q 40/00, G06Q 30/06, G06Q 30/0601, G06Q 30/02, G06Q 50/163, G06Q 10/06, G06Q 10/0631		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) See Search History Document		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched See Search History Document		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) See Search History Document		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X -- Y	US 2016/0080390 A1 (StoryCloud, Inc.) 17 March 2016 (17.03.2006), entire document especially Fig. 1,11; para [0030]-[0033], [0047]-[0059], [0075]-[0091], [0093]	1-12, 14-20 ----- 13
Y	US 2014/0129113 A1 (Ford Global Technologies, LLC) 08 May 2014 (08.05.2014), entire document especially para [0046], [0047], [0076], [0081]	13
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 25 August 2017 (25.08.2017)		Date of mailing of the international search report 15 SEP 2017
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300		Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774