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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 March 2018 (22.03.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/052256 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)

(21) International Application Number:
PCT/KR2017/010135

(22) International Filing Date:
15 September 2017 (15.09.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
15/268,511 16 September 2016 (16.09.2016) US

(71) Applicant: **SAMSUNG ELECTRONICS CO., LTD.** [KR/KR]; 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 16677 (KR).

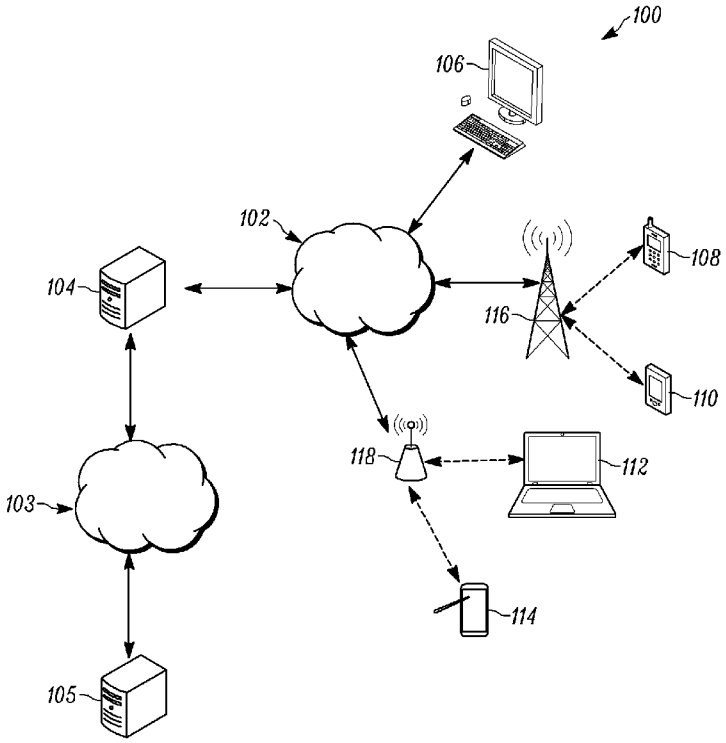
(72) Inventors: **SONASATH, Moiz K**; 665 Clyde Ave., Mountain View, California 94043 (US). **VERMA, Sanjeev**; 665 Clyde Ave., Mountain View, California 94043 (US).

(74) Agent: **LEE, Keon-Joo** et al.; Mihwa Bldg., 16 Daehak-ro 9-gil, Chongro-gu, Seoul 03079 (KR).

(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, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

(54) Title: METHOD OF PROVIDING SECURE ACCESS TO HOTEL IOT SERVICES THROUGH MOBILE DEVICES



(57) Abstract: A system and method for secure access to internet of things (IoT) devices using a mobile device. The mobile device includes a memory configured to store a private value thereon. The mobile device also includes a processor. The processor is configured establish a secure connection with the between the mobile device and a trusted server using the private value, receive a token from the a third party server via the trusted server, transmit the token to a provisioning server via the trusted server, receive an IoT profile from the provisioning server via the trusted server, and configure an IoT gateway based on the IoT profile.

WO 2018/052256 A1

[Continued on next page]

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))*

Description

Title of Invention: METHOD OF PROVIDING SECURE ACCESS TO HOTEL IOT SERVICES THROUGH MOBILE DEVICES

Technical Field

[1] This disclosure relates generally to Internet of Things (IoT). More specifically, this disclosure relates to secure access to IoT devices using a mobile device.

Background Art

[2] The Internet, which is a human centered connectivity network where humans generate and consume information, is now evolving to the Internet of Things (IoT) where distributed entities, such as things, exchange and process information without human intervention. The Internet of Everything (IoE), which is a combination of the IoT technology and the Big Data processing technology through connection with a cloud server, has emerged. As technology elements, such as "sensing technology", "wired/wireless communication and network infrastructure", "service interface technology", and "Security technology" have been demanded for IoT implementation, a sensor network, a Machine-to-Machine (M2M) communication, Machine Type Communication (MTC), and so forth have been recently researched.

[3] Such an IoT environment may provide intelligent Internet technology services that create a new value to human life by collecting and analyzing data generated among connected things. IoT may be applied to a variety of fields including smart home, smart building, smart city, smart car or connected cars, smart grid, health care, smart appliances and advanced medical services through convergence and combination between existing Information Technology (IT) and various industrial applications.

Disclosure of Invention

Technical Problem

[4] The present disclosure relates to a sensor network, Machine Type Communication (MTC), Machine-to-Machine (M2M) communication, and technology for Internet of Things (IoT). The present disclosure may be applied to intelligent services based on the above technologies, such as smart home, smart building, smart city, smart car, connected car, health care, digital education, smart retail, security and safety services.

Solution to Problem

[5] In a first embodiment, a mobile device includes a memory configured to store a private value thereon and a processor coupled to the memory. The processor is configured to establish a secure connection between the mobile device and a the trusted server, receive a token from the third party server via the trusted server, transmit the token to a provisioning server via the trusted server, and receive an

Internet of Things (IoT) profile from the provisioning server via the trusted server.

[6] In a second embodiment, a method for controlling an Internet of Things (IoT) gateway using a mobile device includes establishing a secure connection between the mobile device and a trusted server using a private value stored in the mobile device. The method also includes receiving a token at the mobile device from the third party server via the trusted server. The token is transmitted from the mobile device to a provisioning via the trusted server and the mobile device receives an IoT profile from the provisioning server via the trusted server. The method also includes configuring the IoT gateway based on the IoT profile.

[7] In a third embodiment, a trusted server includes a memory and a. The processor is configured to establish a secure connection with a mobile device using a private value received from the mobile device, receive a token from a third party server and transmit the token to the mobile device, transmit the token to a provisioning server, receive an Internet of Things (IoT) profile from the provisioning server, and provide the IoT profile to the mobile device.

[8] Other technical features may be readily apparent to one skilled in the art from the following figures, descriptions, and claims.

Brief Description of Drawings

[9] For a more complete understanding of this disclosure, reference is now made to the following description, taken in conjunction with the accompanying drawings, in which:

[10] FIG. 1 illustrates an example computing system according to this disclosure;

[11] FIGS. 2 and 3 illustrate example devices in a computing system according to this disclosure;

[12] FIG. 4 illustrates an example client device according to this disclosure;

[13] FIG. 5 illustrates an example system for gaining secure access to one or more third party IoT services according to this disclosure;

[14] FIG. 6 illustrates a flowchart for obtaining a reservation token according to this disclosure;

[15] FIG. 7 illustrates an example system for obtaining a reservation token according to this disclosure;

[16] FIG. 8 illustrates a flowchart for accessing a hotel IoT system according to this disclosure; and

[17] FIG. 9 illustrates an example system for accessing a hotel IoT system according to this disclosure.

Mode for the Invention

[18] Before undertaking the DETAILED DESCRIPTION below, it may be advantageous to set forth definitions of certain words and phrases used throughout this patent

document. The term "couple" and its derivatives refer to any direct or indirect communication between two or more elements, whether or not those elements are in physical contact with one another. The terms "transmit," "receive," and "communicate," as well as derivatives thereof, encompass both direct and indirect communication. The terms "include" and "comprise," as well as derivatives thereof, mean inclusion without limitation. The term "or" is inclusive, meaning and/or. The phrase "associated with," as well as derivatives thereof, means to include, be included within, interconnect with, contain, be contained within, connect to or with, couple to or with, be communicable with, cooperate with, interleave, juxtapose, be proximate to, be bound to or with, have, have a property of, have a relationship to or with, or the like. The term "controller" means any device, system or part thereof that controls at least one operation. Such a controller may be implemented in hardware or a combination of hardware and software and/or firmware. The functionality associated with any particular controller may be centralized or distributed, whether locally or remotely. The phrase "at least one of," when used with a list of items, means that different combinations of one or more of the listed items may be used, and only one item in the list may be needed. For example, "at least one of: A, B, and C" includes any of the following combinations: A, B, C, A and B, A and C, B and C, and A and B and C.

[19] Moreover, various functions described below can be implemented or supported by one or more computer programs, each of which is formed from computer readable program code and embodied in a computer readable medium. The terms "application" and "program" refer to one or more computer programs, software components, sets of instructions, procedures, functions, objects, classes, instances, related data, or a portion thereof adapted for implementation in a suitable computer readable program code. The phrase "computer readable program code" includes any type of computer code, including source code, object code, and executable code. The phrase "computer readable medium" includes any type of medium capable of being accessed by a computer, such as read only memory (ROM), random access memory (RAM), a hard disk drive, a compact disc (CD), a digital video disc (DVD), or any other type of memory. A "non-transitory" computer readable medium excludes wired, wireless, optical, or other communication links that transport transitory electrical or other signals. A non-transitory computer readable medium includes media where data can be permanently stored and media where data can be stored and later overwritten, such as a rewritable optical disc or an erasable memory device.

[20] Definitions for other certain words and phrases are provided throughout this patent document. Those of ordinary skill in the art should understand that in many if not most instances, such definitions apply to prior as well as future uses of such defined words and phrases.

[21] FIGS. 1 through 9, discussed below, and the various embodiments used to describe the principles of the present disclosure in this patent document are by way of illustration only and should not be construed in any way to limit the scope of the disclosure. Those skilled in the art will understand that the principles of this disclosure may be implemented in any suitably arranged device or system.

[22] One or more embodiments described herein provide secure access to IoT devices of a third party (e.g., hotel, corporation, etc.). In one embodiment, a user may use a third party app on a mobile device to perform a task (e.g., make an on-line reservation) using a third party server via a trusted server. The mobile device includes a pre-configured key that is set at manufacturing time, and the preconfigured key is used to securely communicate between the mobile device and the trusted server. The third party server securely communicates with the mobile device via the trusted server. A time-bound token is securely communicated to the mobile device via the trusted server and stored in a secure area of the mobile device. At a certain later time when the time-bound token is presented to the third party server, the third party server generates a provisioning IoT profile that is based on user preferences, credentials, and/or access data. The provisioning IoT profile is securely transmitted from the third party server to the mobile device via the trusted server and stored in the secure area of the mobile device. The provisioning IoT profile gives the mobile device access to an IoT controller to control a plurality of IoT devices of the third party. The third party server configures the IoT controller so that the mobile device can control the IoT devices and also pre-configure the IoT devices based on the provisioning IoT profile.

[23] FIG. 1 illustrates an example computing system 100 according to this disclosure. The embodiment of the computing system 100 shown in FIG. 1 is for illustration only. Other embodiments of the computing system 100 could be used without departing from the scope of this disclosure.

[24] As shown in FIG. 1, the system 100 includes a network 102 and network 103, which facilitates communication between various components in the system 100. For example, the network 102, 103 may communicate Internet Protocol (IP) packets, frame relay frames, Asynchronous Transfer Mode (ATM) cells, or other information between network addresses. The network 102 may include one or more local area networks (LANs), metropolitan area networks (MANs), wide area networks (WANs), all or a portion of a global network such as the Internet, or any other communication system or systems at one or more locations.

[25] The network 102 facilitates communications between at least one trusted server 104 and various client devices 106-114. The network 103 facilitates communications between the least one trusted server 104 and a third party server 105. Each server 104, 105 includes any suitable computing or processing device that can provide computing

services for one or more client devices. Each server 104, 105 could, for example, include one or more processing devices, one or more memories storing instructions and data, and one or more network interfaces facilitating communication over the network 102.

[26] The server 104 is a trusted service manager (TSM) that plays a role in a near field communication (NFC) ecosystem. It acts as a neutral broker that sets up business agreements and technical connections with mobile network operators, phone manufacturers, or other entities controlling the secure element on mobile phones. The TSM enables service providers to distribute and manage their contactless applications remotely by allowing access to a secure element in NFC-enabled handsets.

[27] Each client device 106-114 represents any suitable computing or processing device that interacts with at least one server or other computing device(s) over the network 102. In this example, the client devices 106-114 include a desktop computer 106, a mobile telephone or smartphone 108, a personal digital assistant (PDA) 110, a laptop computer 112, and a tablet computer 114. However, any other or additional client devices could be used in the computing system 100.

[28] In this example, some client devices 108-114 communicate indirectly with the network 102. For example, the client devices 108-110 communicate via one or more base stations 116, such as cellular base stations or eNodeBs. Also, the client devices 112-114 communicate via one or more wireless access points 118, such as IEEE 802.11 wireless access points. Note that these are for illustration only and that each client device could communicate directly with the network 102 or indirectly with the network 102 via any suitable intermediate device(s) or network(s).

[29] As described in more detail below, each client device may communicate securely with the third party server 105 via the trusted server 104.

[30] Although FIG. 1 illustrates one example of a computing system 100, various changes may be made to FIG. 1. For example, the system 100 could include any number of each component in any suitable arrangement. In general, computing and communication systems come in a wide variety of configurations, and FIG. 1 does not limit the scope of this disclosure to any particular configuration. While FIG. 1 illustrates one operational environment in which various features disclosed in this patent document can be used, these features could be used in any other suitable system.

[31] FIGURES 2 and 3 illustrate example devices in a computing system according to this disclosure. In particular, FIG. 2 illustrates an example server 200, and FIG. 3 illustrates an example client device 300. The server 200 could represent the server 104 or server 105 in FIG. 1, and the client device 300 could represent one or more of the client devices 106-114 in FIG. 1.

[32] As shown in FIG. 2, the server 200 includes a bus system 205, which supports com-

munication between at least one processing device 210, at least one storage device 215, at least one communications unit 220, and at least one input/output (I/O) unit 225.

[33] The processing device 210 executes instructions that may be loaded into a memory 230. The processing device 210 may include any suitable number(s) and type(s) of processors or other devices in any suitable arrangement. Example types of processing devices 210 include microprocessors, microcontrollers, digital signal processors, field programmable gate arrays, application specific integrated circuits, and discreet circuitry.

[34] The memory 230 and a persistent storage 235 are examples of storage devices 215, which represent any structure(s) capable of storing and facilitating retrieval of information (such as data, program code, and/or other suitable information on a temporary or permanent basis). The memory 230 may represent a random access memory or any other suitable volatile or non-volatile storage device(s). The persistent storage 235 may contain one or more components or devices supporting longer-term storage of data, such as a ready only memory, hard drive, Flash memory, or optical disc.

[35] The communications unit 220 supports communications with other systems or devices. For example, the communications unit 220 could include a network interface card or a wireless transceiver facilitating communications over the network 102. The communications unit 220 may support communications through any suitable physical or wireless communication link(s).

[36] The I/O unit 225 allows for input and output of data. For example, the I/O unit 225 may provide a connection for user input through a keyboard, mouse, keypad, touchscreen, or other suitable input device. The I/O unit 225 may also send output to a display, printer, or other suitable output device.

[37] Note that while FIG. 2 is described as representing the server 104 or server 105 of FIG. 1, the same or similar structure could be used in one or more of the client devices 106-114. For example, a laptop or desktop computer could have the same or similar structure as that shown in FIG. 2.

[38] As shown in FIG. 3, the client device 300 includes an antenna 305, a radio frequency (RF) transceiver 310, transmit (TX) processing circuitry 315, a microphone 320, and receive (RX) processing circuitry 325. The client device 300 also includes a speaker 330, a main processor 340, an input/output (I/O) interface (IF) 345, a keypad 350, a display 355, and a memory 360. The memory 360 includes a basic operating system (OS) program 361 and one or more applications 362.

[39] The RF transceiver 310 receives, from the antenna 305, an incoming RF signal transmitted by another component in a system. The RF transceiver 310 down-converts the incoming RF signal to generate an intermediate frequency (IF) or baseband signal.

The IF or baseband signal is sent to the RX processing circuitry 325, which generates a processed baseband signal by filtering, decoding, and/or digitizing the baseband or IF signal. The RX processing circuitry 325 transmits the processed baseband signal to the speaker 330 (such as for voice data) or to the main processor 340 for further processing (such as for web browsing data).

[40] The TX processing circuitry 315 receives analog or digital voice data from the microphone 320 or other outgoing baseband data (such as web data, e-mail, or interactive video game data) from the main processor 340. The TX processing circuitry 315 encodes, multiplexes, and/or digitizes the outgoing baseband data to generate a processed baseband or IF signal. The RF transceiver 310 receives the outgoing processed baseband or IF signal from the TX processing circuitry 315 and up-converts the baseband or IF signal to an RF signal that is transmitted via the antenna 305.

[41] The main processor 340 can include one or more processors or other processing devices and execute the basic OS program 361 stored in the memory 360 in order to control the overall operation of the client device 300. For example, the main processor 340 could control the reception of forward channel signals and the transmission of reverse channel signals by the RF transceiver 310, the RX processing circuitry 325, and the TX processing circuitry 315 in accordance with well-known principles. In some embodiments, the main processor 340 includes at least one microprocessor or microcontroller.

[42] The main processor 340 is also capable of executing other processes and programs resident in the memory 360. The main processor 340 can move data into or out of the memory 360 as required by an executing process. In some embodiments, the main processor 340 is configured to execute the applications 362 based on the OS program 361 or in response to signals received from external devices or an operator. The main processor 340 is also coupled to the I/O interface 345, which provides the client device 300 with the ability to connect to other devices such as laptop computers and handheld computers. The I/O interface 345 is the communication path between these accessories and the main processor 340.

[43] The main processor 340 is also coupled to the keypad 350 and the display 355. The operator of the client device 300 can use the keypad 350 to enter data into the client device 300. The display 355 may be a liquid crystal display or other display capable of rendering text and/or at least limited graphics, such as from web sites.

[44] The memory 360 is coupled to the main processor 340. Part of the memory 360 could include a random access memory (RAM), and another part of the memory 360 could include a Flash memory or other read-only memory (ROM).

[45] As described in more detail below, memory 360 includes a secure area in which a private value such as a private key may be stored therein. The secure area also stores a

reservation token provided by the third party server 105 as well as an Internet of Things (IoT) profile to access an IoT controller in order to control one or more IoT devices.

[46] Although FIGURES 2 and 3 illustrate examples of devices in a computing system, various changes may be made to FIGURES 2 and 3. For example, various components in FIGURES 2 and 3 could be combined, further subdivided, or omitted and additional components could be added according to particular needs. As a particular example, the main processor 340 could be divided into multiple processors, such as one or more central processing units (CPUs) and one or more graphics processing units (GPUs). Also, while FIG. 3 illustrates the client device 300 configured as a mobile telephone or smartphone, client devices could be configured to operate as other types of mobile or stationary devices. In addition, as with computing and communication networks, client devices and servers can come in a wide variety of configurations, and FIGURES 2 and 3 do not limit this disclosure to any particular client device or server.

[47] FIG. 4 illustrates an example client device according to this disclosure. As shown in FIG. 4, the client device or mobile device 400 includes a secure area 410 included in a memory (not shown). The secure area 410 includes an ecosystem provider software agent 412. The ecosystem provider software agent 412 may be software provided by a travel portal (e.g., Expedia®, Travelocity®, Hotels.com®, etc.) as a mobile application and stored in the secure area 410. The ecosystem provider software agent 412 may work in conjunction with one or more agent applications 414, 416. Agent applications 414, 416 may be provided by a hotel chain (e.g., Hilton®, Sheraton®, Holiday Inn®, etc.) or a company (Apple®, Google®, etc.) and stored in secure area 410.

[48] Secure area 410 also stores secure data 418 as will be discussed below and a primary key 420. Primary key 420 is either preconfigured at manufacturing time or can be configured or flashed into the device's secure area using software (e.g., after proper user identification through documents/biometric data etc. at a specific location). The primary key 420 enables a security association between the mobile device 400 and the TSM, such as trusted server 104, thereby allowing the mobile device to securely communicate with the TSM and in turn allowing, e.g., hotels, to communicate securely with the mobile device through the usage of the TSM. The primary key 420 can be of any type and length (e.g., 64, 128, 256, 512 bytes) and can also include a user's biometric data (e.g., image recognition output or finger print) as part of the key. The primary key can be used to communicate securely between two mobile devices. The primary key can be shared among mobile devices so that, for example, members of a family have access to a hotel room or access to a family car.

[49] FIG. 5 illustrates an example system for gaining secure access to one or more third party IoT services according to this disclosure. As shown in FIG. 5, a mobile device

400 establishes a secure communication path with a trusted server 502 by sending a private key to the trusted server 502. The trusted server 502 is similar to trusted server 104 as shown in FIG. 1. Once the secure communication path is established, the mobile device may communicate with a third party ecosystem 504 via the trusted server 502 using the ecosystem provider software agent 412. The third party ecosystem may be travel portal or a company portal. A user profile 506 may also be stored in the third party ecosystem 504 using the mobile device 400 or any of client devices 106-114 as shown in FIG. 1. The mobile device also communicates with one or more third party servers 508-514 via the trusted server 502 using one of the agent application 414, 416. Third party servers 518-514 are similar to third party server 105 of FIG. 1. As will be discussed below, one or more of the third party servers 508-514 provides one or more time/location bound tokens that the mobile device may use to access IoT services 516.

[50] FIGURES 6-9 will be used to describe a process for making a hotel reservation and checking into a hotel to use IoT services provided by the hotel. However, the embodiments described herein are not limited to using IoT services in a hotel and may be used in conjunction with any location that provides IoT services such as a hotel, company, sporting event, connected car, hospital, factory, shopping mall or stores, prisons, schools, theme parks.

[51] FIG. 6 illustrates a flowchart for obtaining a reservation token according to this disclosure and FIG. 7 illustrates an example system for obtaining a reservation token according to this disclosure.

[52] As shown in FIGURES 6 and 7, in process 600, a mobile device 400 establishes a secure communication path with the trusted server 502. Once the secure communication path is established, the mobile device 400 communicates with a third party ecosystem 504 such as Expedia® or Hotels.com® to select a hotel in process 602. The hotel may be selected by the user or based on a user profile 506 provided by the user in advance and stored on the mobile device 400 or with the third party ecosystem 504. Once the hotel is selected, the user uses his or her credentials (e.g., user name, password, credit card information, biometric data etc.) to login to the hotel website and fill out a reservation form 704 and submits the reservation form in process 604 to the third party server 702 belonging to the selected hotel. The third party server 702 then transmits a time/location reservation token 706 to the mobile device 400 via the trusted server 502 and the mobile device 400 receives the time/location reservation token 706 in process 606. The time/location reservation token 706 is generated by the hotel and sent to the mobile device 400 and stored as secure data 418 in the secure area 410 after a successful reservation in process 608. The time/location reservation token 706 is active during the active reservation period for a specific location. As will be described

below, upon check-in, this time/location reservation token 706 (from the mobile device 400) is sent to a hotel provisioning server via the TSM for verification.

[53] FIG. 8 illustrates a flowchart for accessing a hotel IoT system according to this disclosure and FIG. 9 illustrates an example system for accessing a hotel IoT system according to this disclosure.

[54] As shown in FIGURES 8 and 9, in process 800, the mobile device presents the time/location reservation token 706 to a hotel kiosk 902 using a near field communication (NFC) method such as Wi-Fi®, Bluetooth®, radio frequency signals, etc. The hotel kiosk 902 forwards the reservation token to 706 to a hotel provisioning server 904 in process 802. The hotel provisioning server 904 retrieves user preferences stored in the user profile 506 from the third party ecosystem 504 in process 804 and generates an IoT profile in process 806. The IoT profile includes configuration data, access keys, and authorization data that are generated based on the user preferences, credentials, and reservation data.

[55] In process 808, the hotel provisioning server 904 transfers an IOT profile to the mobile device 400 via the trusted server (not shown) that includes a time/location bound access key and authorization token 906 (hereinafter "authorization token 906"). The authorization token 906 is stored as secure data 418 in the secure area 410. The authorization token 906 enables the mobile device to securely communicate with an IoT gateway 910 of the hotel thereby enabling the mobile device 400 to control a plurality of IoT devices 912a-912j and access other hotel services. In process 810, the IoT profile (e.g., user preferences, credentials, and/or authorization 908) is also transmitted by the hotel provisioning server 904 to the IoT gateway 910 to enable the user to use the plurality of IoT device 912a-912j connected to the IoT gateway 910. In process 812, the mobile device 400 accesses the IoT gateway by providing the authorization token 906 to the IoT gateway 910 using NFC methods to establish a secure communication path between the mobile device 400 and the IoT gateway 910. This permits the mobile device to control the various IoT devices 912a-912j connected to the IoT gateway such as, but not limited to, help or room service device 912a, a door contact, 912b, a door camera 912c, an electronic doorplate 912d, a networking radiofrequency lock 912e, a thermostat 912f, lighting controller 912g, electronic curtain 912h, bathroom fixtures (e.g., fan, mirror, lights) 912i, and identity recognition power switches (e.g., bar, check out, lights, etc.) 912j.

[56] Although the figures illustrate different examples of devices, various changes may be made to the figures. For example, the user equipment can include any number of each component in any suitable arrangement. In general, the figures do not limit the scope of this disclosure to any particular configuration(s). Moreover, while figures illustrate operational environments in which various user equipment features disclosed in this

patent document can be used, these features can be used in any other suitable system.

[57] None of the description in this application should be read as implying that any particular element, step, or function is an essential element that must be included in the claim scope. The scope of patented subject matter is defined only by the claims. Moreover, none of the claims is intended to invoke 35 U.S.C. § 112(f) unless the exact words "means for" are followed by a participle. Use of any other term, including without limitation "mechanism," "module," "device," "unit," "component," "element," "member," "apparatus," "machine," "system," "processor," or "controller," within a claim is understood by the applicants to refer to structures known to those skilled in the relevant art and is not intended to invoke 35 U.S.C. § 112(f).

[58] Although the present disclosure has been described with an exemplary embodiment, various changes and modifications may be suggested to one skilled in the art. It is intended that the present disclosure encompass such changes and modifications as fall within the scope of the appended claims.

Claims

[Claim 1] A mobile device, comprising:
a memory configured to store a private value thereon; and
a processor coupled to the memory, the processor is configured to:
establish a secure connection between the mobile device and a trusted server using the private value;
receive a token from a third party server via the trusted server;
transmit the token to a provisioning server via the trusted server; and
receive an internet of things (IoT) profile from the provisioning server via the trusted server.

[Claim 2] The mobile device of claim 1, wherein the private value is stored in the memory at a manufacturing time or flashed onto the memory.

[Claim 3] The mobile device of claim 1, wherein the processor is configured to:
transmit a reservation form to the third party server via the trusted server.

[Claim 4] The mobile device of claim 1, wherein the IoT profile is configured to provide the mobile device with access to an IoT gateway configured to control a plurality of IoT devices.

[Claim 5] A method for controlling an internet of things (IoT) gateway using a mobile device, the method comprising:
establishing a secure connection between the mobile device and a trusted server using a private value stored in the mobile device;
receiving a token at the mobile device from a third party server via the trusted server;
transmitting the token from the mobile device to a provisioning via the trusted server;
receiving an IoT profile at the mobile device from the provisioning server via the trusted server; and
configuring the IoT gateway based on the IoT profile.

[Claim 6] The method of claim 5, wherein the private value is stored in a memory of the mobile device at a manufacturing time.

[Claim 7] The method of claim 5, wherein the private value is flashed onto a memory of the mobile device.

[Claim 8] The mobile device of claim 1 or the method of claim 5, wherein the private value includes biometric data.

[Claim 9] The mobile device of claim 1 or the method of claim 5, wherein the token includes at least one of a time or location.

[Claim 10] The mobile device of claim 1 or the method of claim 5, wherein the IoT profile is based on at least one of user preferences, user credentials, or reservation data.

[Claim 11] The mobile device of claim 1 or the method of claim 5, wherein the IoT profile includes a time/location bound access key and authorization token.

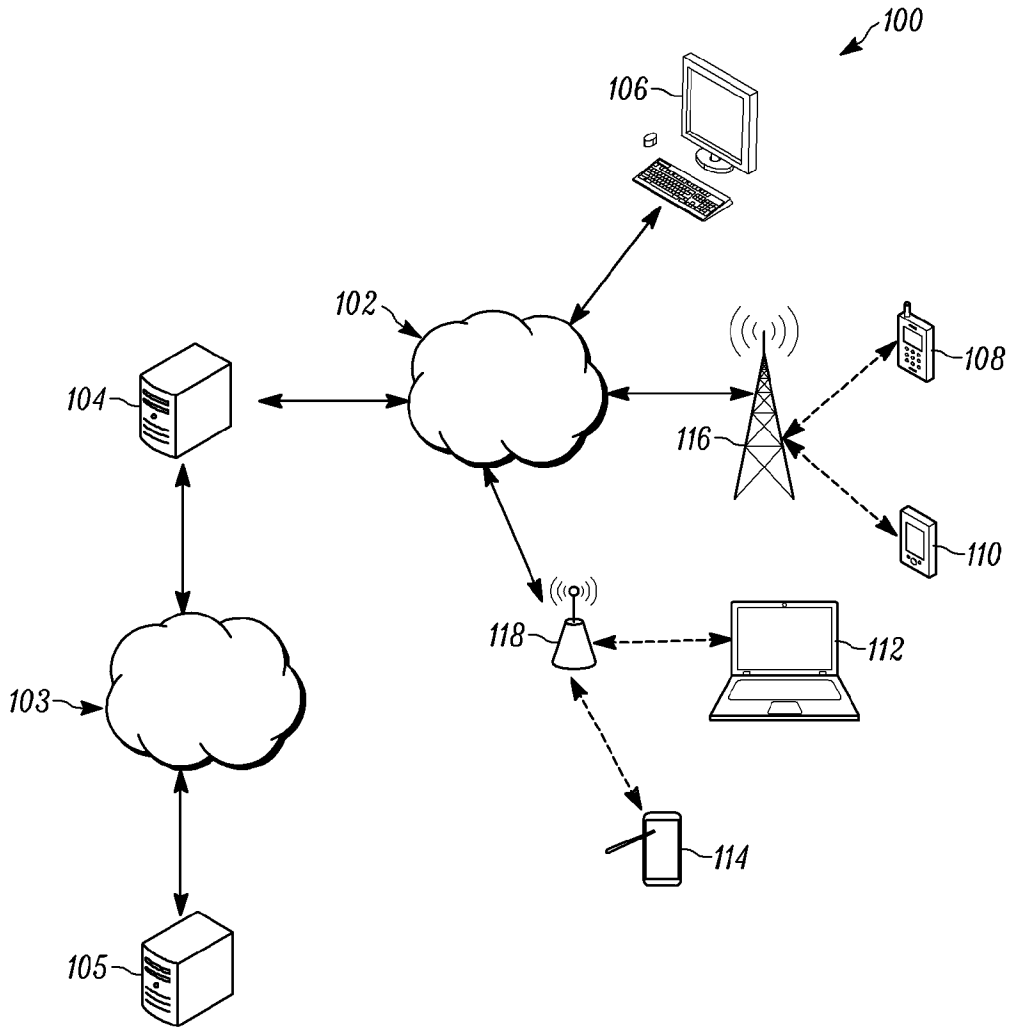
[Claim 12] The method of claim 5, wherein the IoT gateway is configured to control a plurality of IoT devices.

[Claim 13] The method of claim 12, further comprising configuring the plurality of IoT devices based on the IoT profile.

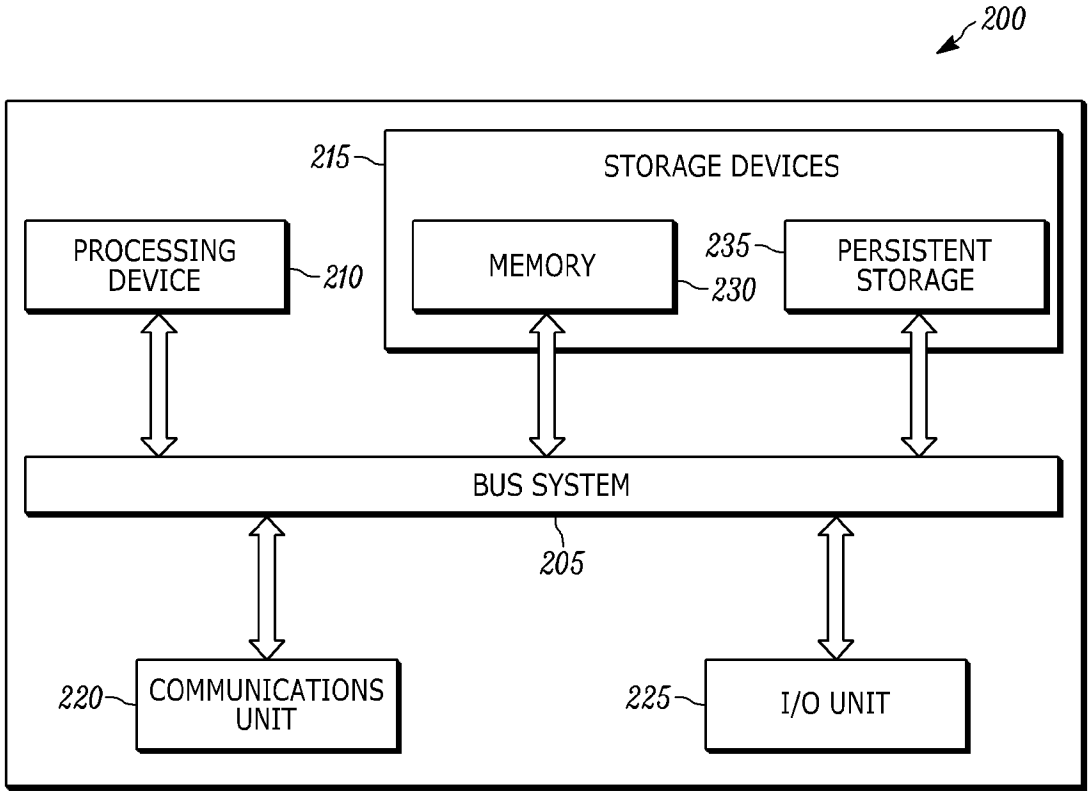
[Claim 14] A trusted server comprising:
a memory; and
a processor coupled to the memory, the processor is configured to:
establish a secure connection with a mobile device using a private value received from the mobile device;
receive a token from a third party server and transmit the token to the mobile device;
transmit the token to a provisioning server;
receive an internet of things (IoT) profile from the provisioning server; and
provide the IoT profile to the mobile device.

[Claim 15] The trusted server of claim 14, wherein the processor is further configured to:
receive a reservation form from the mobile device and transmit the reservation form to the third party server.

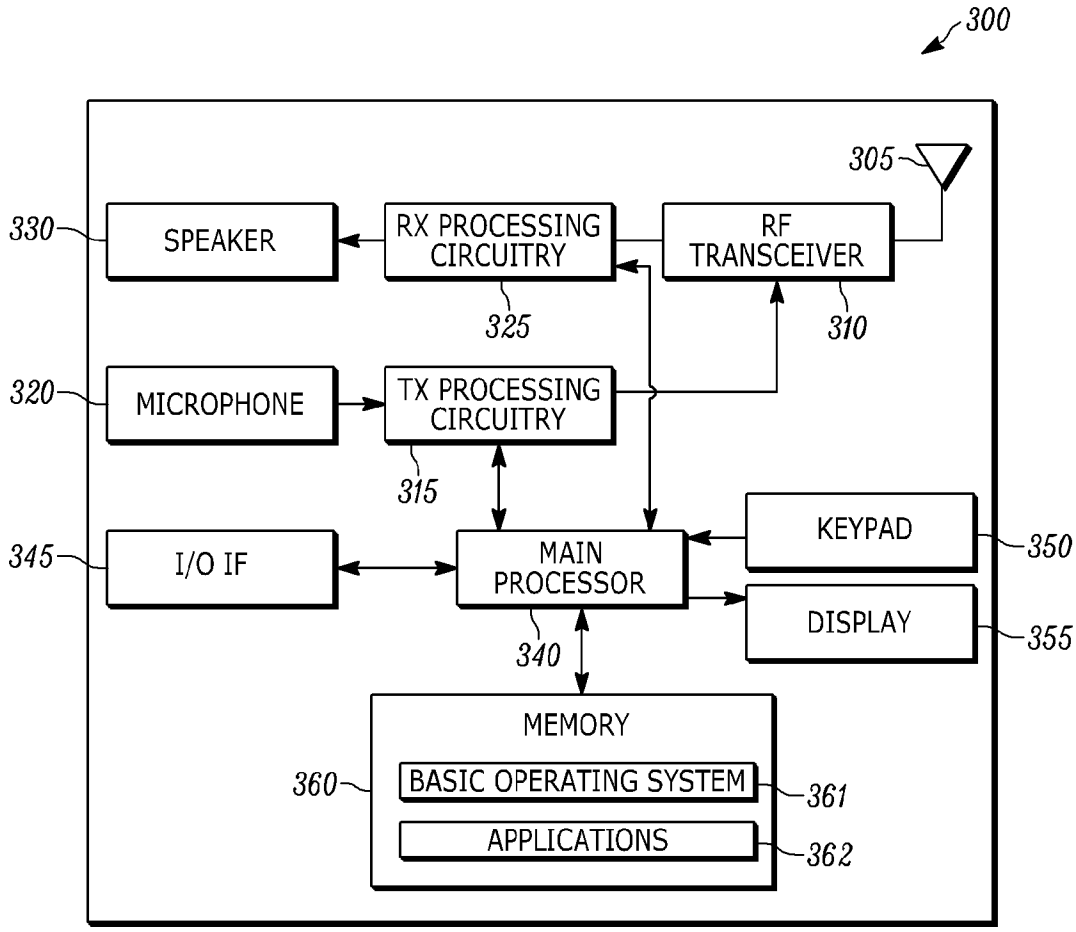
[Fig. 1]


100
106
102
104
108
116
110
118
112
103
114
105

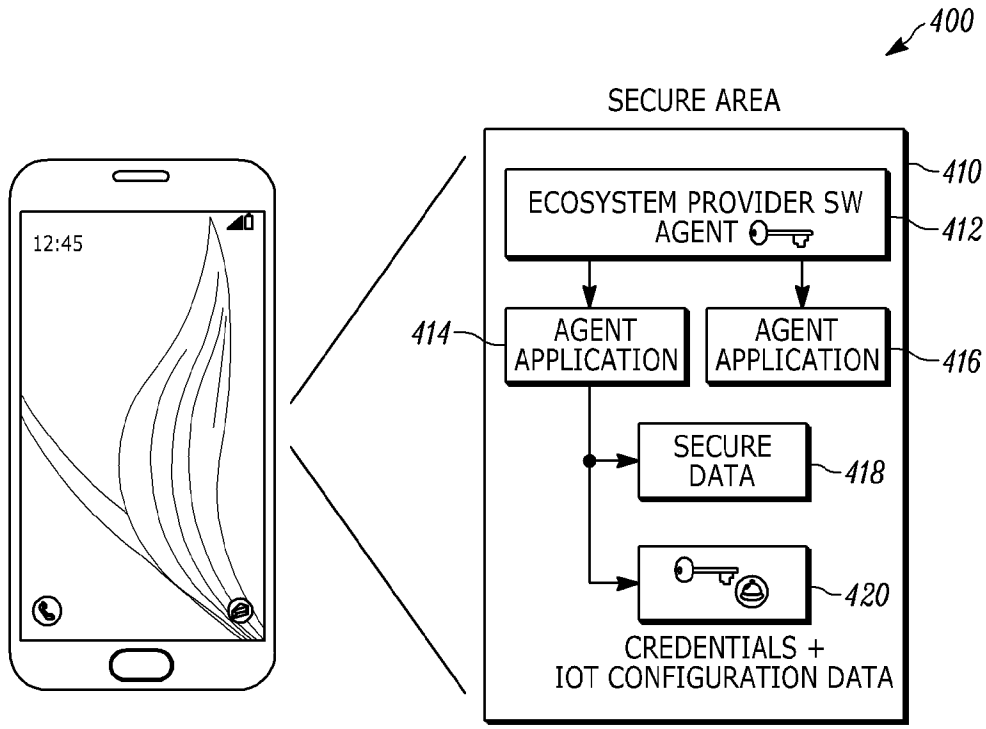
[Fig. 2]


200
215
STORAGE DEVICES
PROCESSING DEVICE
210
MEMORY
230
235
PERSISTENT STORAGE
BUS SYSTEM
205
220
COMMUNICATIONS UNIT
225
I/O UNIT

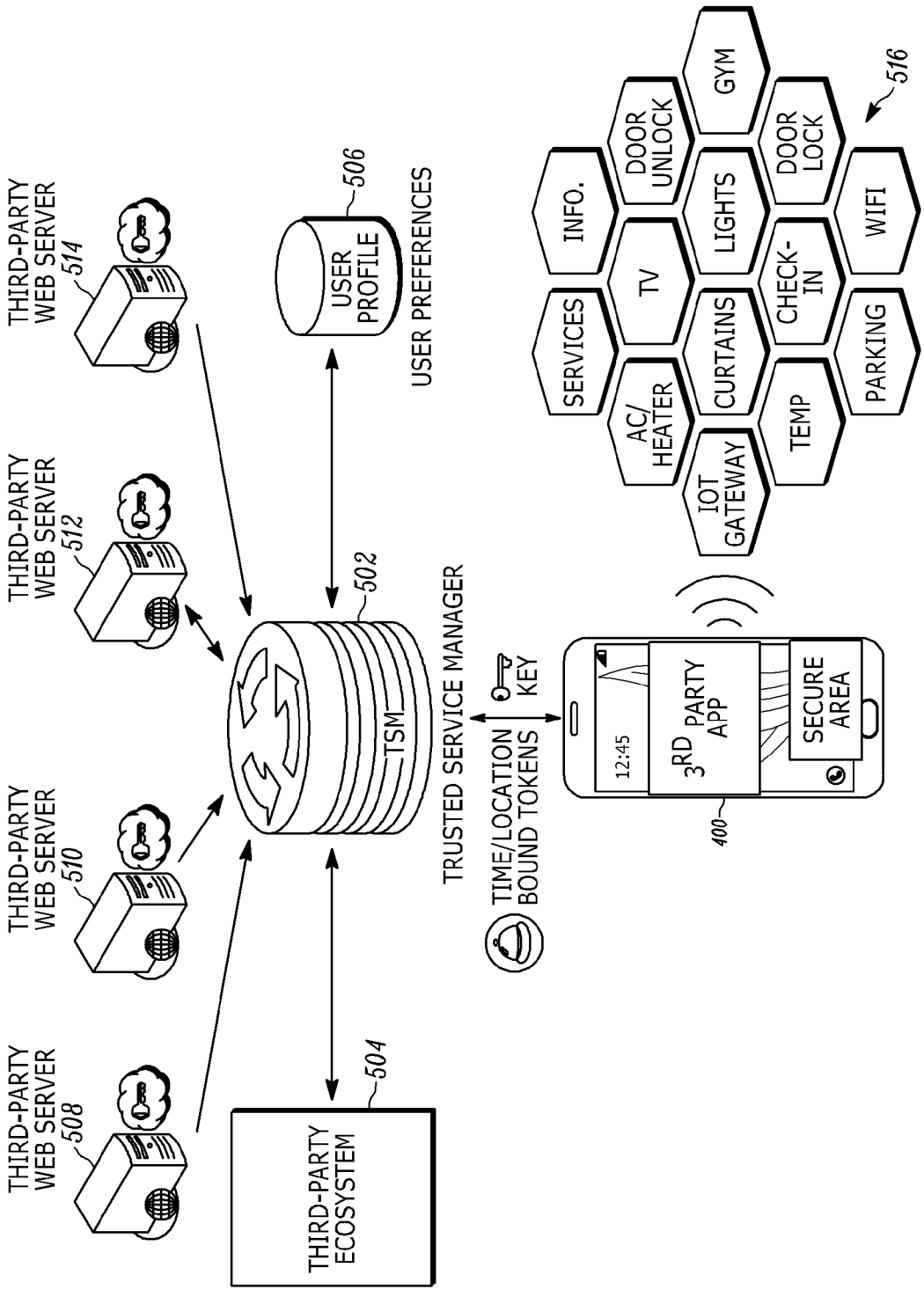
[Fig. 3]


300
305
330
SPEAKER
RX PROCESSING CIRCUITRY
RF TRANSCEIVER
325
310
320
MICROPHONE
TX PROCESSING CIRCUITRY
315
345
I/O IF
MAIN PROCESSOR
KEYPAD
350
DISPLAY
355
340
MEMORY
360
BASIC OPERATING SYSTEM
361
APPLICATIONS
362

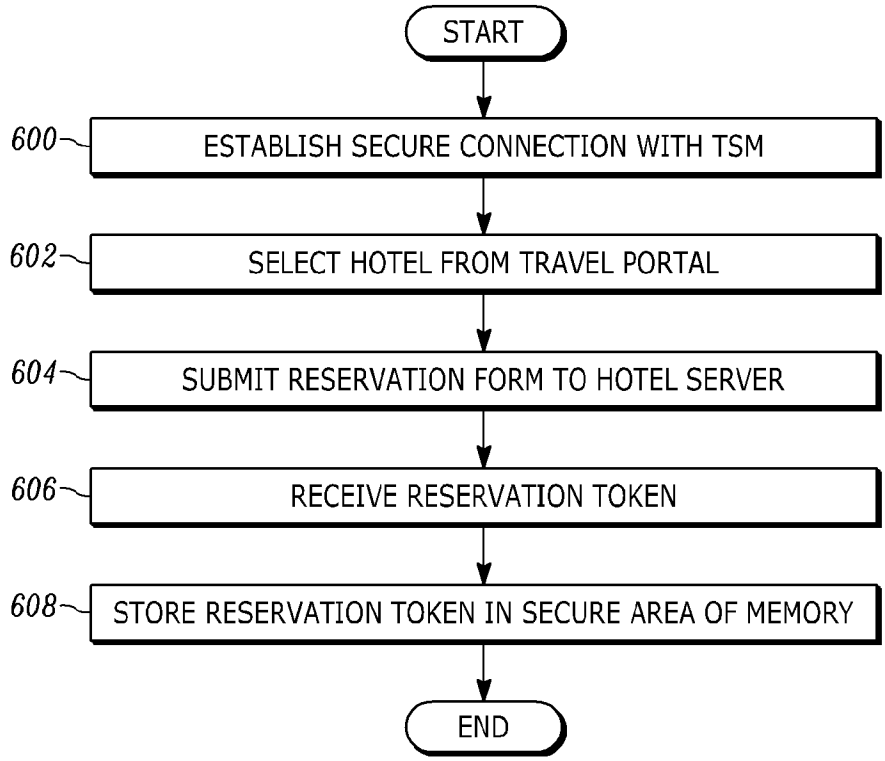
[Fig. 4]


400
SECURE AREA
12:45
410
ECOSYSTEM PROVIDER SW AGENT
412
414
AGENT APPLICATION
AGENT APPLICATION
416
SECURE DATA
418
420
CREDENTIALS + IOT CONFIGURATION DATA

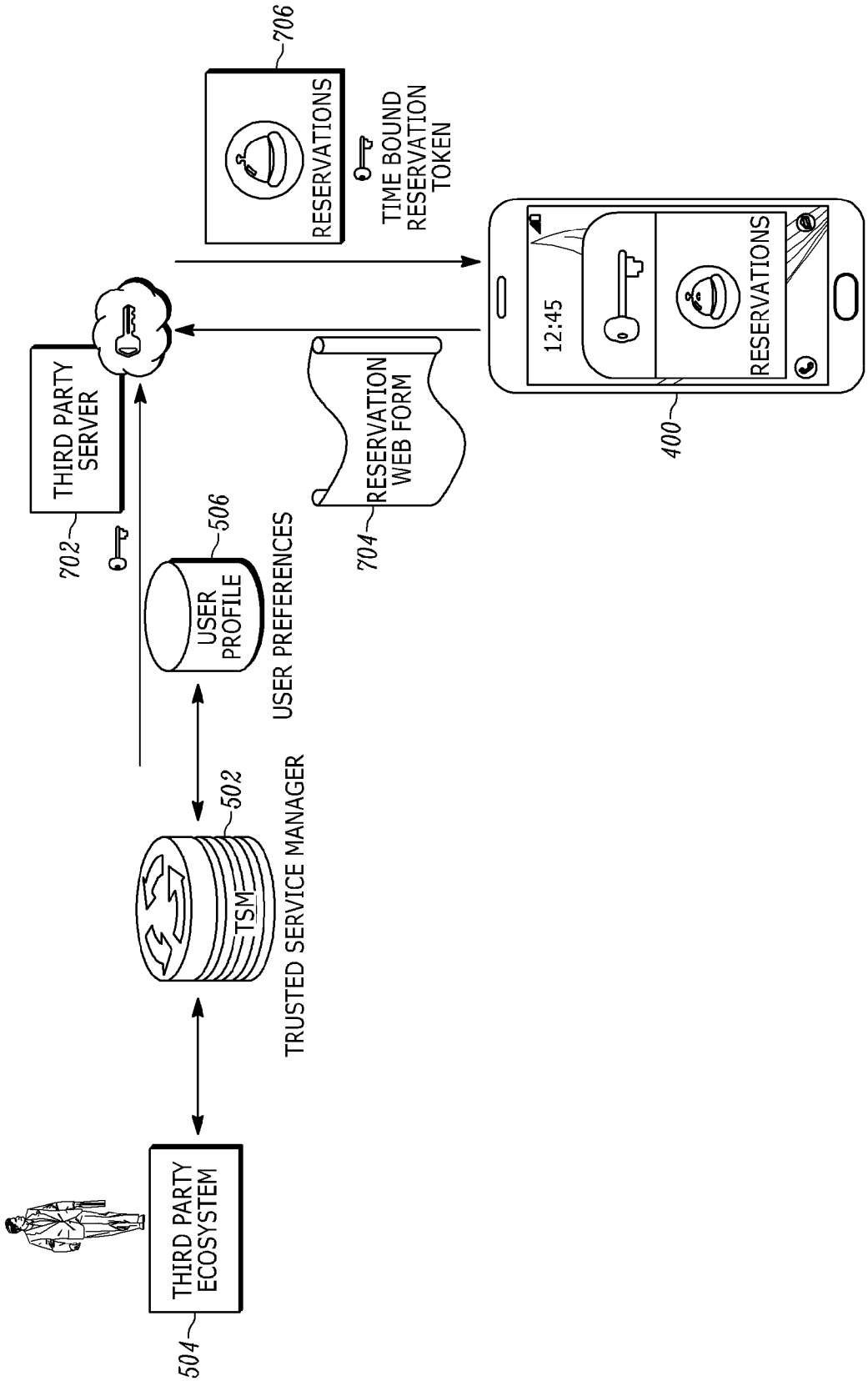
[Fig. 5]


THIRD-PARTY WEB SERVER 514
THIRD-PARTY WEB SERVER 512
THIRD-PARTY WEB SERVER 510
THIRD-PARTY WEB SERVER 508
506
USER PROFILE
USER PREFERENCES
502
TSM
TRUSTED SERVICE MANAGER
TIME/LOCATION BOUND TOKENS
KEY
504
THIRD-PARTY ECOSYSTEM
516
GYM
DOOR UNLOCK
DOOR LOCK
INFO.
LIGHTS
WIFI
SERVICES
TV
CHECK-IN
CURTAINS
PARKING
AC/ HEATER
TEMP
IOT GATEWAY
12:45
3RD PARTY APP
SECURE AREA
400

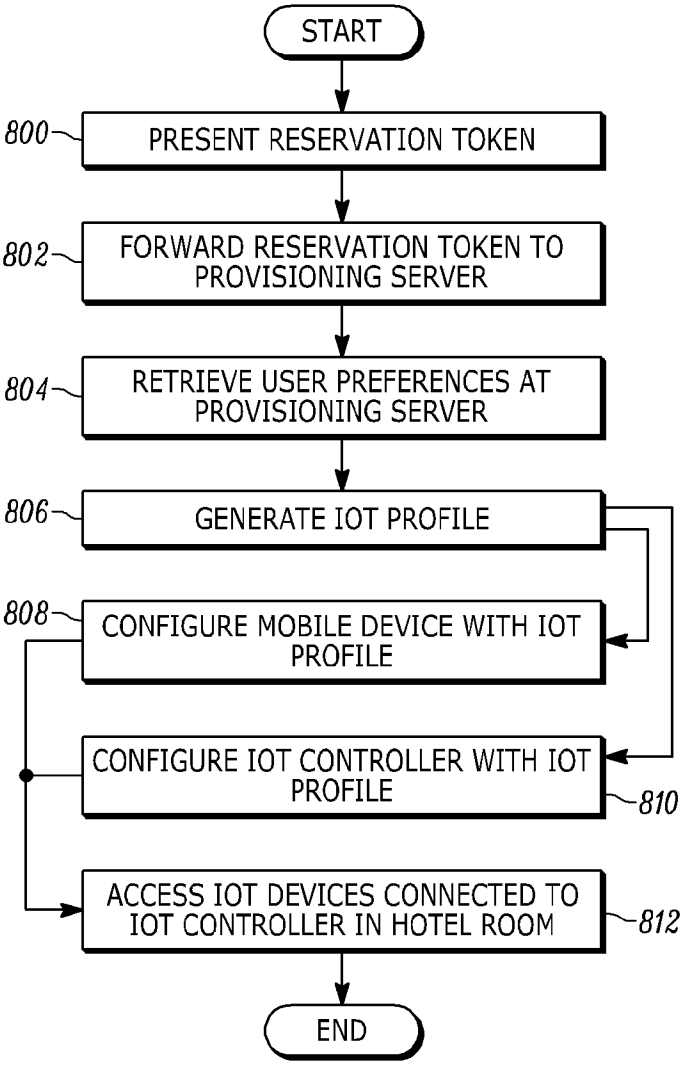
[Fig. 6]


START
600
ESTABLISH SECURE CONNECTION WITH TSM
602
SELECT HOTEL FROM TRAVEL PORTAL
604
SUBMIT RESERVATION FORM TO HOTEL SERVER
606
RECEIVE RESERVATION TOKEN
608
STORE RESERVATION TOKEN IN SECURE AREA OF MEMORY
END

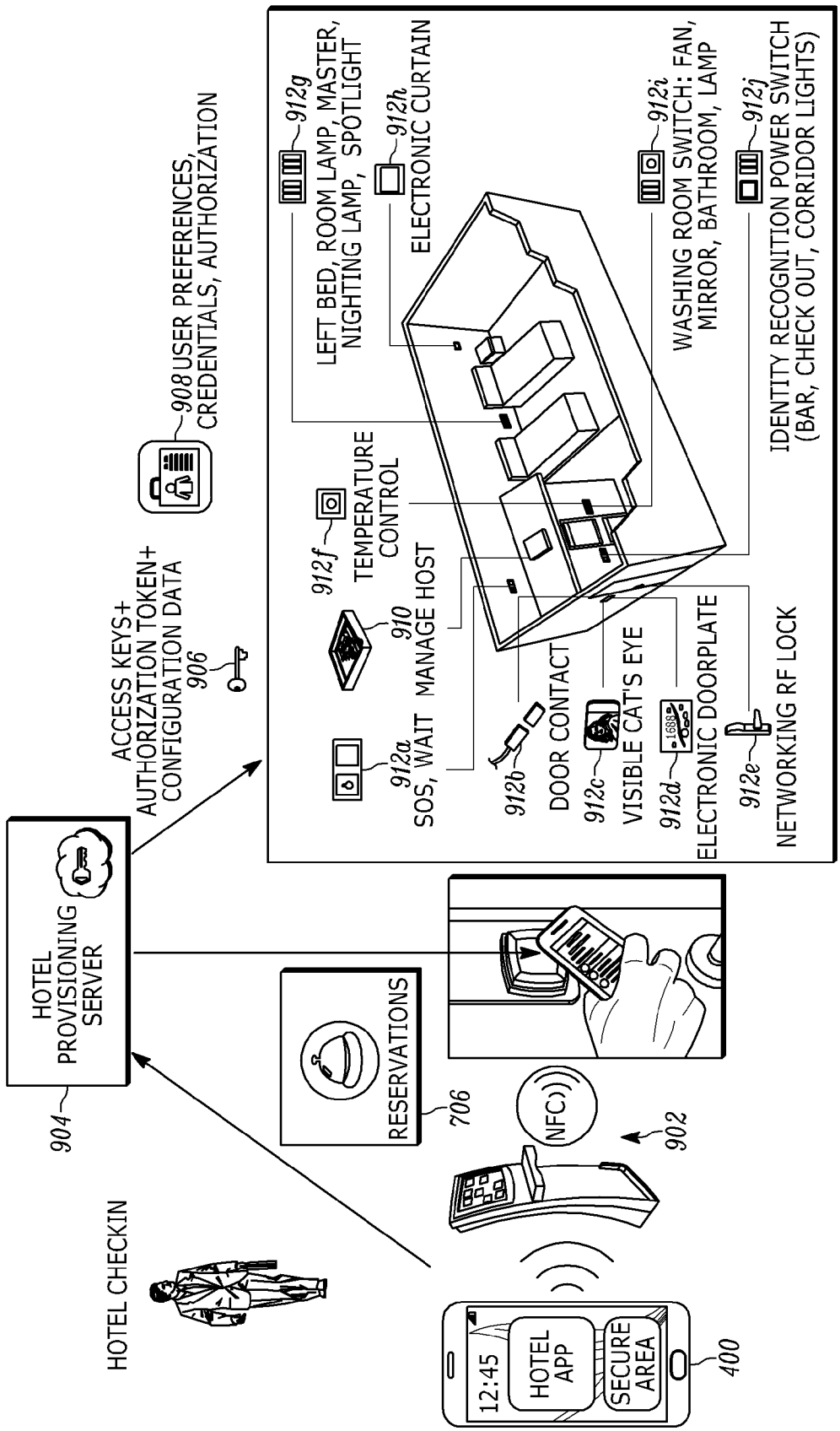
[Fig. 7]


706
RESERVATIONS
TIME BOUND RESERVATION TOKEN
12:45
RESERVATIONS
400
THIRD PARTY SERVER
702
RESERVATION WEB FORM
704
506
USER PROFILE
USER PREFERENCES
502
TSM
TRUSTED SERVICE MANAGER
THIRD PARTY ECOSYSTEM
504

[Fig. 8]


START
800
PRESENT RESERVATION TOKEN
802
FORWARD RESERVATION TOKEN TO PROVISIONING SERVER
804
RETRIEVE USER PREFERENCES AT PROVISIONING SERVER
806
GENERATE IOT PROFILE
808
CONFIGURE MOBILE DEVICE WITH IOT PROFILE
CONFIGURE IOT CONTROLLER WITH IOT PROFILE
810
ACCESS IOT DEVICES CONNECTED TO IOT CONTROLLER IN HOTEL ROOM
812
END

[Fig. 9]


HOTEL CHECKIN
HOTEL PROVISIONING SERVER
904
ACCESS KEYS+ AUTHORIZATION TOKEN+ CONFIGURATION DATA
906
908 USER PREFERENCES, CREDENTIALS, AUTHORIZATION
RESERVATIONS
706
NFC
902
12:45
HOTEL APP
SECURE AREA
400
912a SOS, WAIT
912b DOOR CONTACT
912c VISIBLE CAT'S EYE
912d ELECTRONIC DOORPLATE
912e NETWORKING RF LOCK
912f TEMPERATURE CONTROL
910 MANAGE HOST
912g LEFT BED, ROOM LAMP, MASTER, NIGHTING LAMP, SPOTLIGHT
912h ELECTRONIC CURTAIN
912i WASHING ROOM SWITCH: FAN, MIRROR, BATHROOM, LAMP
912j IDENTITY RECOGNITION POWER SWITCH (BAR, CHECK OUT, CORRIDOR LIGHTS)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2017/010135

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i, H04L 29/08(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L 29/06; H04L 29/08; H04W 12/06; G06Q 10/02; G06F 21/22

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: mobile device, private value, secure connection, third party server, trusted server, IoT, provisioning server

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2016-0227408 A1 (FINGI INC.) 04 August 2016 See paragraphs [0026]-[0050]; claim 5; and figures 1-2.	1-15
Y	WO 2011-162591 A1 (MIMOS BHD.) 29 December 2011 See page 10, line 23 - page 11, line 16; claims 1, 9; and figures 4-8.	1-15
Y	US 2016-0156614 A1 (HCL TECHNOLOGIES LIMITED) 02 June 2016 See paragraphs [0015]-[0038]; and figure 1.	1-15
A	EP 2709045 A1 (MARC COUSSEMENT et al.) 19 March 2014 See paragraphs [0136]-[0137]; and figure 2.	1-15
A	US 2015-0222621 A1 (TEXAS INSTRUMENTS INCORPORATED) 06 August 2015 See paragraphs [0021]-[0028]; and figures 2-4.	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 December 2017 (11.12.2017)	**11 December 2017 (11.12.2017)**

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

Authorized officer
KIM, Seong Woo
Telephone No. +82-42-481-3348

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2017/010135

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2016-0227408 A1	04/08/2016	US 2015-0170448 A1	18/06/2015
		WO 2014-007870 A1	09/01/2014
		WO 2014-143171 A1	18/09/2014
		WO 2015-038135 A1	19/03/2015
WO 2011-162591 A1	29/12/2011	None	
US 2016-0156614 A1	02/06/2016	None	
EP 2709045 A1	19/03/2014	None	
US 2015-0222621 A1	06/08/2015	US 9538311 B2	03/01/2017