



- (51) **International Patent Classification:**  
*H04L 9/32* (2006.01)      *H04L 12/16* (2006.01)
- (21) **International Application Number:**  
PCT/US2013/031386
- (22) **International Filing Date:**  
14 March 2013 (14.03.2013)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant (for all designated States except US):** **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, California 95054 (US).
- (72) **Inventors; and**
- (71) **Applicants (for US only):** **SATAPATHY, Jiphun C.** [IN/US]; 14910 NW Marguerite Ln., Portland, Oregon 97229 (US). **MIRASHRAFI, Mojtaba** [US/US]; 15007 NW Germantown Road, Portland, Oregon 97231 (US). **PRAKASH, Gyan** [IN/US]; 1563 NW 209th Ave., Beaverton, Oregon 97006 (US). **HAZRA, Mousumi M.** [US/US]; 16635 SW Ivy Glenn St., Beaverton, Oregon 97007 (US).
- (74) **Agent:** **DESANTIS, LuAnne**; Garrett IP, LLC, c/o CPA Global, PO Box 52050, Minneapolis, Minnesota 55402 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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, 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, ML, MR, NE, SN, TD, TG).

**Published:**

- with international search report (Art. 21(3))

(54) **Title:** SYSTEMS, METHODS, AND COMPUTER PROGRAM PRODUCTS FOR PROVIDING A UNIVERSAL PERSISTENCE CLOUD SERVICE

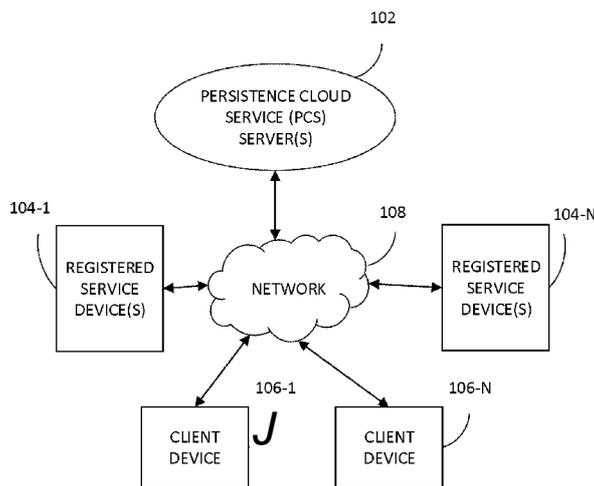


FIG. 1

(57) **Abstract:** Methods, systems, and computer program products that relate to managing persistence information of client devices for services registered with a persistence cloud service. A method from the perspective of a computing device associated with a registered service may include receiving, from a client device, a device identifier that identifies the client device to the registered service. The method further may include requesting, from a persistence cloud server associated with the persistence cloud service, persistence information associated with the device identifier. The method may also include receiving the persistence information, determining a level of service to provide to the client device based on the persistence information, and providing the level of service to the client device. The computing device may, for example, be a server associated with the registered service, or may, for example, be a router.

WO 2014/142883 A1

## SYSTEMS, METHODS, AND COMPUTER PROGRAM PRODUCTS FOR PROVIDING A UNIVERSAL PERSISTENCE CLOUD SERVICE

### TECHNICAL FIELD

5           Embodiments described herein generally relate to managing information as a cloud service over a network.

### BACKGROUND

Client devices, such as personal computers, tablets, smartphones, cameras, e-readers, gaming consoles, and the like, that may use a cloud-based service are typically a part of a client-  
10 server model to provide the end-to-end experience. In this model, a client side component communicates with a server side component to provide the service. The persistence of the client device information can be stored at the server, at the client device, or at both the server and the client device. To ensure that the device information is identical at both the server and the client device, the server and the client device need to periodically communicate, typically via software  
15 components at each end. Client devices may be used as dummy consoles to experience services because all of the information can be stored at the server end or in the cloud. This model is convenient in that a user can use any device to consume a service with proper authentication. In this model, the information retained at the servers is specific to a particular service's usage and is controlled and maintained separately by each service provider.

20

### BRIEF DESCRIPTION OF THE DRAWINGS/FIGURES

FIGs. 1 and 2 each illustrate an exemplary block diagram of the system described herein, according to embodiments described herein.

FIG. 3 is a sequence diagram illustrating an exemplary process flow for registering a  
25 client device with the persistence cloud service described herein, according to an embodiment.

- 2 -

FIG. 4 illustrates an exemplary record of data associated with persistence information for a particular device, according to an embodiment.

FIG. 5 is a sequence diagram illustrating an exemplary process flow for providing client device persistence information from the persistence cloud service described herein, according to an embodiment.

FIG. 6 is a sequence diagram illustrating an exemplary process flow for providing client device persistence information to a router device from the persistence cloud service described herein, according to an embodiment.

FIG. 7 is a flow chart illustrating an exemplary process flow of the system described herein, from the perspective of a service registered with the persistence cloud service, according to an embodiment.

FIG. 8 is a flow chart illustrating an exemplary process flow for registering a client device with the persistence cloud service described herein, from the perspective of a service registered with the persistence cloud service, according to an embodiment.

FIG. 9 is a flow chart illustrating an exemplary process flow for updating the persistence cloud service described herein, from the perspective of a service registered with the persistence cloud service, according to an embodiment.

FIG. 10 is a flow chart illustrating an exemplary process flow of the system described herein, from the perspective of a persistence cloud service server, according to an embodiment.

FIG. 11 is a flow chart illustrating an exemplary process flow for registering a client device with the persistence cloud service described herein, from the perspective of a persistence cloud service server, according to an embodiment.

FIG. 12 is a block diagram of an example persistence cloud server, according to an embodiment.

FIG. 13 is a block diagram of an example registered service device, according to an embodiment.

FIG. 14 is a block diagram of an example client device, according to an embodiment.

In the drawings, the leftmost digit(s) of a reference number may identify the drawing in which the reference number first appears.

30

## DETAILED DESCRIPTION

As discussed above, client devices that may use a cloud-based service are typically a part of a client-server model to provide the end-to-end experience. In this model, a client side

- 3 -

component communicates with a server side component to provide the service. The persistence of the client device information can be stored at the server, at the client device, or at both the server and the client device. To ensure that the device information is identical at both the server and the client device, the server and the client device need to periodically communicate, typically via software components at each end. One downside to this model of information persistence is that, if the client side software component is removed from the client device, the communication between the client and the server is interrupted and it becomes difficult to maintain information persistence at the client side.

The above may not be a concern if the client devices are used as dummy consoles to experience services because all of the information can be stored at the server end or in the cloud. This model is convenient in that a user can use any device to consume a service with proper authentication. However, in this model, the information retained at the servers is specific to a particular service's usage and is controlled and maintained separately by each service provider.

Currently, there is no single cloud persistence service that can provide a mechanism to maintain universal device information and provide device-specific information to any service that may need it. For example, there is currently no single cloud persistence service that can obtain information from one service indicating that there may be a particular activity or state associated with a particular device (e.g., peculiar or suspicious activity, a state of being lost or stolen, etc.) and be able to alert other services so that those other services can proceed as appropriate for usage of their services by that particular device.

Disclosed herein are methods, systems, and computer program products that solve the technical problem of how to manage device persistence information in a universally centralized manner for sharing with registered services.

Embodiments are now described with reference to the figures, where like reference numbers may indicate identical or functionally similar elements. While specific configurations and arrangements are discussed, it should be understood that this is done for illustrative purposes only. A person skilled in the relevant art will recognize that other configurations and arrangements can be used without departing from the spirit and scope of the description. It will be apparent to a person skilled in the relevant art that this can also be employed in a variety of other systems and applications other than what is described herein.

FIG. 1 illustrates an exemplary block diagram 100 of a persistence cloud service (PCS) system, according to an embodiment. The PCS system may include a PCS server 102, one or more registered service devices 104-1 to 104-N (collectively, 104), and one or more client devices (e.g., user devices) 106-1 to 106-N (collectively, 106), in communication via a network

- 4 -

108. The persistence cloud service may be implemented in software and/or hardware executed or controlled by a controller of the PCS server 102. While only one PCS server is illustrated for clarity and ease of discussion, it should be appreciated that the persistence cloud service may be hosted by multiple distributed server computers for redundancy and/or load sharing, for example.

5 The registered service devices 104 may be computing devices that may include, for example, web-based service servers that allow users to log in to consume those services. Such web-based services may include, but are not to be limited to, for example, banking services, social networking services, gaming services, shopping services, anti-theft services, anti-virus services, data backup services, data storage services, etc., some of which are shown as registered  
10 service devices 204 in FIG. 2. The registered service devices 104/204 may also include routers used for routing network traffic, as discussed in further detail herein.

The client devices 106 may be computing devices that may include, but are not to be limited to, for example, personal computers (PCs), laptop computers, ultra-laptop computers, tablets, touch pads, portable computers, handheld computers, palmtop computers, personal  
15 digital assistants (PDAs), e-readers, cellular telephones, combination cellular telephone/PDAs, televisions, smart devices (e.g., smart phones, smart tablets or smart televisions), mobile internet devices (MIDs), messaging devices, data communication devices, media playing devices, cameras, gaming consoles, etc. The client devices 106 may include controllers and other components that execute software and/or control hardware in order to consume services provided  
20 by registered service devices 104, for example, over a network. For example, the client devices 106 may include one or more software clients for accessing web-based services provided by one or more of the registered service devices 104. The client devices 106 may also, or instead, include a web interface running in a browser from which the client device can access such web-based services.

25 The network 108 may be any wired or wireless network, such as a Wide Area Network (WAN), a Local Area Network (LAN), and/or the like. As an example, the network 108 may be a distributed public network, such as the Internet, where the PCS server 102, the registered services 104, and the client devices 106 are connected to the network via wired or wireless connections.

30 According to an embodiment, service providers of the services that wish to subscribe to the persistence cloud service may register with the persistence cloud service in advance so that the persistence cloud service will be aware of what services (and, for example, what addresses of those services) to which device persistence information should be provided and also what services from which to expect device persistence information updates, as will be described in

- 5 -

further detail below. The registered service devices 104 may each require an application program interface (API) in order to communicate with the PCS server 102. Data communication between registered service devices 104 and the PCS server 102 may be executed in any manner as would be appreciated by those skilled in the art (e.g., standard server to server communications may be used). Registering of client devices that use such registered services will now be discussed.

FIG. 3 is a sequence diagram 300 illustrating an exemplary process flow for registering a client device with the persistence cloud service described herein, according to an embodiment. A user of client device 306 may log into (320) a registered service (e.g., a banking service or a social networking service) hosted by registered service device 304 via, for example, client software running on client device 306 or a web-based client running in a browser on client device 306. Registered service device 304 may request a client device ID from client device 306 (322), and client device 306 may provide the client device ID to the registered service device 304 (324). Alternatively, the client device ID may have been included during login 320. The registered service device 304 may check to see if the device associated with the provided client device ID had previously opted into the persistence cloud service with respect to its associated registered service (326). If the client device associated with the client device ID had not previously opted into the persistence cloud service, the registered service device 304 may send a request to the client device 306 asking the user of client device 306 whether he or she wants to register client device 306 with the persistence cloud service with respect to this particular registered service (328). Client device 306 may send an opt-in decision to the registered service device 304 (330). If the decision was to opt in to the persistence cloud service, the registered service device 304 may provide client device data (e.g., registration data) associated with the client device ID to PCS server 302 (332), and may also store associated client device and/or registration data itself such that it will know that the device associated with that client device ID has already been registered with the persistence cloud service. The PCS server 302 may send confirmation of receipt of the client device opt-in data to the registered service device 304 (334). The registered service device 304 may send confirmation of the opt-in to the client device 306 (336).

According to an embodiment, the client device registration data provided to the PCS server 302 by the registered service device 304 may include, for example, the client device ID, client device status information, an affiliate ID, and an affiliate policy. The client device ID may, for example, be (or be based on or derived from) a unique hardware identifier of the client device 306, such as the Media Access Control (MAC) address of the client device 306, or any

- 6 -

other identifier for the client device 306. Client device status information may be any information that would appropriately indicate a status of the client device 306 with respect to the particular registered service providing the information. For example, the client device status information may likely be some type of "normal" indication upon initial registration of the client device 306. The affiliate ID may be a unique identifier for the registered service that is sending the information. The affiliate policy may include a policy to be followed by the persistence cloud service based on a current client device status. For example, the affiliate policy may include instructions pertaining to how the persistence cloud service should update the client device status at the PCS server 302 based on a later client device update from the registered service device 304. The affiliate policy may also include instructions pertaining to what information to include as the client device persistence information provided to the registered service device 304 based on the current client device status at the PCS server 302.

FIG. 4 illustrates an exemplary record of data 400 associated with persistence information for a particular client device, according to an embodiment. This exemplary record of data may be stored at the PCS server 102/302, for example, for each registered client device 106/306. The record of data 400 may include a client device ID 440 (e.g., a MAC address of the client device 106/306), client device information 442, and affiliate IDs 444-1 to 444-N and affiliate policies 446-1 to 446-N of the registered services with which the client device 106/306 has been registered for use with the persistence cloud service.

The client device information (or persistence information) 442 may be any information indicating a current status of the client device 106/306. For example, client device information 442 may include, but is not to be limited to, an indication that the client device is in a normal state, an indication that the client device has been lost or stolen, an indication that activity (e.g., login activity) at the client device is suspicious, an indication that usage of the client device should follow a defined set of policies, and/or an indication of a location of the client device. Other client device information or statuses may also be contemplated. The client device information 442 maintained by the PCS server 102/302 may be dependent upon updates that the PCS server 102/302 receives from the registered service devices 104/304 for a particular client device. The updates may depend upon the particular service provided by a registered service, as discussed in more detail below.

FIG. 5 is a sequence diagram 500 illustrating an exemplary process flow for providing client device persistence information from the persistence cloud service described herein, according to an embodiment. The initial login sequence shown in FIG. 5 is similar to that shown in FIG. 3. If, however, it is determined that client device 506 is already registered for the

- 7 -

persistence cloud service with respect to the registered service associated with registered service device 504-1, registered service device 504-1 may send updated client device information with respect to client device 506 to the PCS server 502 and/or may request current client device information with respect to client device 506 from PCS server 502 (550). For example, if the  
5 login into the registered service is normal, then the registered service device 504-1 may indicate that to PCS server 502 and request current client device information from PCS server 502 in order to determine how to proceed with its service at the client device 506. If, however, the login procedure took multiple incorrect passwords before a correct password was achieved (if at all), the registered service device 504-1 may indicate to the PCS server 502 that there was  
10 "suspicious activity" at client device 506. In its update or request for current client device information, the registered service device 504-1 may include its affiliate ID to identify the registered service device 504-1 to the PCS service. In an embodiment, the PCS server 502 may verify, based on the provided affiliate ID, that the service associated with the registered service device 504-1 is indeed registered with the persistence cloud service. The PCS server 502 may  
15 update the client device information in its data record for client device 506 based on the update provided by the registered service device 504-1 (552). The PCS server 502 may send current client device information to the registered service device 504-1 (554). For example, if another registered service device 504-2 had previously sent an update to the PCS server 502 that indicated, for example, that the client device 506 has had suspicious login activity, or had been  
20 reported as lost or stolen, or had been reported as having some other type of warning or non-normal status (555), the current client device information sent by PCS server 502 to registered service device 504-1 would indicate that information. Otherwise, the current client device information sent by PCS server 502 would indicate that the current client device status is normal.

Registered service device 504-1 may determine a level of service to be provided to client  
25 device 506 that is based on the current client device information provided by the PCS server 502 (556). Registered service device 504-1 may send an indication of the determined level of service to client device 506 (558). According to an embodiment, the level of service may include, but is not to be limited to, allowing full access to the registered service, denying access to the registered service, providing limited access to the registered service, and/or invoking further  
30 security actions. Other levels of service may also be contemplated. For example, if the current client device information indicates that there has been recent "suspicious activity" at client device 506, the registered service may invoke further security actions at client device 506 first, then may decide what level of access to provide (e.g., full, limited, or none) at client device 506. Invoking further security actions may include, but not be limited to, for example, executing

- 8 -

further authentication checks, locking accounts associated with the registered service, locking client device 506, and/or deleting data from client device 506. Other further security actions may also be contemplated. In another example, if the current device information indicates that client device 506 has been reported lost or stolen, the registered service may immediately limit or deny access to the registered service at the client device 506. Limiting access to the registered service may include, but not be limited to, for example, limiting types of actions that can be conducted, limiting quantities involved in actions that can be conducted, and/or limiting a local area in which actions can be conducted. Other types of limiting access may also be contemplated. Following the banking service example, limiting types of actions that can be conducted may include, for example, allowing deposits but not withdrawals; limiting quantities may include, for example, allowing only small denomination transactions and/or limiting the number of transactions; and limiting a local area in which actions can be conducted may include, for example, allowing transactions only if the device is located within a defined radius of the rightful user's local bank.

FIG. 6 is a sequence diagram illustrating an exemplary process flow 600 for providing client device persistence information to a router device from the persistence cloud service described herein, according to an embodiment. A router is a device that determines the next network point to which a data packet should be forwarded. A registered service device, such as registered service device 504 discussed above, may be a router. When a client device 606 accesses a registered router 604 in order to access a network, a client device ID of the client device 606 may be sent to registered router 604 (634). Registered router 604 may send a request to the PCS server 602 for current client device information (650). In its request, router 604 may provide a router identifier that identifies the router to the PCS service. PCS server 602 may send the current client device information to registered router 604 (654). The current client device information may include a device status assigned to the device, such as, for example, an indication that the client device is in a normal state, an indication that the client device has been lost or stolen, an indication that activity at the client device is suspicious, an indication that usage of the client device should follow a defined set of policies, and/or an indication of a location of the client device, etc. Other current client device information or statuses may also be contemplated. Registered router 604 may determine a level of service to provide to client device 606 based on the received current device information (656). Registered router 604 may provide the determined level of service to client device 606 (658). The levels of service that the router may provide may include, for example, allowing full network access, denying network access,

- 9 -

providing limited network access, and/or invoking further security actions, etc. Other levels of service may also be contemplated.

FIG. 7 is a flow chart illustrating an exemplary process flow 700 of the system described herein, from the perspective of a service registered with the persistence cloud service, according to an embodiment. At 702, a registered service device receives, from a client device, a device identifier that identifies the client device to the registered service. This may be received, for example, when a user at a client device logs into the registered service, or may alternatively be requested by the registered service device after login. At 704, the registered service device requests, from a server associated with a persistence cloud service, current client device persistence information associated with the device identifier. At 706, the registered service device receives the current client device persistence information from the PCS server. As discussed above, the client device information, or persistence information, may be any information indicating a current status of the client device. At 708, the registered service device may determine a level of service to provide to the client device based on the persistence information. At 710, the registered service device may provide the determined level of service to the client device. As discussed above, the levels of service may include, for example, allowing full access to the registered service, denying access to the registered service, providing limited access to the registered service, and/or invoking further security actions, etc.

FIG. 8 is a flow chart illustrating an exemplary process flow 800 for registering a client device with the persistence cloud service described herein, from the perspective of a service registered with the persistence cloud service, according to an embodiment. Upon login to a registered service via a client device, the registered service device may, at 802, determine whether the client device is registered with the persistence cloud service with respect to the registered service. At 804, in response to determining that the client device is not registered with the persistence cloud service, the registered service device may send a request to the client device inquiring whether to register the client device with the persistence cloud service. At 806, in response to determining that the client device is to be registered with the persistence cloud service, the registered service device may send registration information associated with the client device to the PCS server. As discussed above, the registration information may include, for example, a client device ID of the client device, client device status information, an affiliate ID that identifies the registered service, and an associated affiliate policy.

FIG. 9 is a flow chart illustrating an exemplary process flow 900 for updating the persistence cloud service described herein, from the perspective of a service registered with the persistence cloud service, according to an embodiment. During login to a registered service via a

- 10 -

client device, the registered service device may, at 902, receive, from the client device, login information of the user of the client device. At 904, the registered service device may provide a client device state change notification or update to the PCS server based on the login information. As discussed above, the client device state change update may include any  
5 information that would appropriately indicate a status of the client device with respect to the particular registered service providing the information. For example, the client device state change update may indicate, for example, that the client device is in a normal state, that the client device has been lost or stolen, that activity (e.g., login activity) at the client device is suspicious, that usage of the client device should follow a defined set of policies, and/or an indication of a  
10 location of the client device, etc.

FIG. 10 is a flow chart illustrating an exemplary process flow 1000 of the system described herein, from the perspective of a PCS server, according to an embodiment. At 1002, the PCS server may receive, from a first computing device associated with a first service registered with the persistence cloud service, a client device update for a client device registered  
15 with the persistence cloud service. At 1004, the PCS server may update client device persistence information associated with the client device based on the client device update. At 1006, the PCS server may receive from a second computing device associated with a second service registered with the persistence cloud service, a request for the client device persistence information. At 1008, the PCS server may provide the client device persistence information to  
20 the second computing device.

FIG. 11 is a flow chart illustrating an exemplary process flow 1100 for registering a client device with the persistence cloud service described herein, from the perspective of a PCS server, according to an embodiment. At 1102, the PCS server may receive, from a computing device associated with a service registered with the persistence cloud service, registration  
25 information for a client device. At 1104, the PCS server may store the registration information.

FIG. 12 is a block diagram of an example PCS server 1202, according to an embodiment. The PCS server 1202 may represent, for example, the PCS server 102, 302, 502, or 602 of FIGs. 1, 3, 5, or 6, respectively. As illustrated, the PCS server 1202 may include a processor or controller 1260 connected to memory 1262, one or more secondary storage devices 1264, and a  
30 communication interface 1266 by a bus 1268 or similar mechanism. The PCS server 1202 may optionally include user interface components 1270 for use by a system administrator, for example, that may include, for example, a touchscreen, a display, one or more user input components (e.g., a keyboard, a mouse, etc.), a speaker, or the like, or any combination thereof. Note, however, that while not shown, PCS server 1202 may include additional components. The

- 11 -

processor 1260 may be a microprocessor, digital ASIC, FPGA, or similar hardware device. In an embodiment, the processor 1260 may be a microprocessor, and software may be stored or loaded into the memory 1262 for execution by the processor 1260 to provide the functions described herein. The one or more secondary storage devices 1264 may be, for example, one or more hard drives or the like, and may store logic 1272 to be executed by the processor 1260. The communication interface 1266 may be implemented in hardware or a combination of hardware and software. The communication interface 1266 may provide a wired or wireless network interface to a network, such as the network 108 shown in FIG. 1.

FIG. 13 is a block diagram of an example registered service device 1304, according to an embodiment. The registered service device 1304 may represent, for example, any of the registered service devices 104, 204, 304, 504, or 604 of FIGs. 1, 2, 3, 5, or 6, respectively. As illustrated, the registered service device 1304 may include a processor or controller 1360 connected to memory 1362, one or more secondary storage devices 1364, and a communication interface 1366 by a bus 1368 or similar mechanism. The registered service device 1304 may optionally include user interface components 1370 for use by a system administrator, for example, that may include, for example, a touchscreen, a display, one or more user input components (e.g., a keyboard, a mouse, etc.), a speaker, or the like, or any combination thereof. Note, however, that while not shown, registered service device 1304 may include additional components. The processor 1360 may be a microprocessor, digital ASIC, FPGA, or similar hardware device. In an embodiment, the processor 1360 may be a microprocessor, and software may be stored or loaded into the memory 1362 for execution by the processor 1360 to provide the functions described herein. The one or more secondary storage devices 1364 may be, for example, one or more hard drives or the like, and may store logic 1372 to be executed by the processor 1360. The communication interface 1366 may be implemented in hardware or a combination of hardware and software. The communication interface 1366 may provide a wired or wireless network interface to a network, such as the network 108 shown in FIG. 1.

FIG. 14 is a block diagram of an example client device 1406, according to an embodiment. The client device 1406 may represent, for example, the client device 106, 306, 506, or 606 of FIGs. 1, 3, 5, or 6, respectively. As illustrated, the client device 1406 may include a processor or controller 1460 connected to memory 1462, one or more secondary storage devices 1464, and a communication interface 1466 by a bus 1468 or similar mechanism. The client device 1406 may also include user interface components 1470 for use by a user of the client device, for example, that may include, for example, a touchscreen, a display, one or more user input components (e.g., a keyboard, a mouse, etc.), a speaker, or the like, or any

- 12 -

combination thereof. Note, however, that while not shown, client device 1406 may include additional components. The processor 1460 may be a microprocessor, digital ASIC, FPGA, or similar hardware device. In an embodiment, the processor 1460 may be a microprocessor, and software may be stored or loaded into the memory 1462 for execution by the processor 1460 to provide the functions described herein. The one or more secondary storage devices 1464 may be, for example, one or more hard drives or the like, and may store logic 1472 to be executed by the processor 1460. The communication interface 1466 may be implemented in hardware or a combination of hardware and software. The communication interface 1466 may provide a wired or wireless network interface to a network, such as the network 108 shown in FIG. 1.

Methods and systems are disclosed herein with the aid of functional building blocks illustrating functions, features, and relationships thereof. At least some of the boundaries of these functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternate boundaries may be defined so long as the specified functions and relationships thereof are appropriately performed. While various embodiments are disclosed herein, it should be understood that they are presented as examples. The scope of the claims should not be limited by any of the example embodiments disclosed herein.

As discussed above, one or more features disclosed herein may be implemented in hardware, software, firmware, and combinations thereof, including discrete and integrated circuit logic, application specific integrated circuit (ASIC) logic, and microcontrollers, and may be implemented as part of a domain-specific integrated circuit package, or a combination of integrated circuit packages. The terms software and firmware, as used herein, refer to a computer program product including at least one computer readable medium having computer program logic, such as computer-executable instructions, stored therein to cause a computer system to perform one or more features and/or combinations of features disclosed herein. The computer readable medium may be transitory or non-transitory. An example of a transitory computer readable medium may be a digital signal transmitted over a radio frequency or over an electrical conductor, through a local or wide area network, or through a network such as the Internet. An example of a non-transitory computer readable medium may be a compact disk, a flash memory, or other data storage device.

As used in this application and in the claims, a list of items joined by the term "one or more of" can mean any combination of the listed terms. For example, the phrases "one or more of A, B or C" can mean A; B; C; A and B; A and C; B and C; or A, B and C."

- 13 -

The following examples pertain to further embodiments.

Example 1 may include a computing device associated with a service registered with a persistence cloud service, comprising a processor and a memory in communication with the processor, the memory having stored therein a plurality of processing instructions adapted to  
5 direct the processor to: receive, from a client device, a device identifier that identifies the client device to the registered service; request, from a persistence cloud server associated with the persistence cloud service, persistence information associated with the device identifier; receive the persistence information; determine a level of service to provide to the client device based on the persistence information; and provide the level of service to the client device.

10 Example 2 may include the subject matter of Example 1, wherein providing the level of service comprises providing a level of service indication to the client device, the level of service indication indicating how a client application associated with the registered service is to proceed at the client device.

Example 3 may include the subject matter of any one of Examples 1-2, wherein the  
15 processing instructions are further adapted to direct the processor to: determine whether the client device is registered with the persistence cloud service; in response to determining that the client device is not registered with the persistence cloud service, send a request to the client device inquiring whether to register the client device with the persistence cloud service; and in response to determining that the client device is to be registered with the persistence cloud  
20 service, send registration information associated with the client device to the persistence cloud server.

Example 4 may include the subject matter of Example 3, wherein the registration information includes the device identifier, a service identifier that identifies the registered service, and a policy of the registered service to be followed by the persistence cloud service  
25 based on the persistence information associated with the client device.

Example 5 may include the subject matter of any one of Examples 1-4, wherein the device identifier is based on a Media Access Control (MAC) address of the client device.

Example 6 may include the subject matter of any one of Examples 1-5, wherein the persistence information includes a device status assigned to the client device.

30 Example 7 may include the subject matter of Example 6, wherein the device status includes one or more of: an indication that the client device is in a normal state, an indication that the client device has been lost or stolen, an indication that activity at the client device is suspicious, an indication that usage of the client device should follow a defined set of policies, and an indication of a location of the client device.

- 14 -

Example 8 may include the subject matter of any one of Examples 1-7, wherein the requesting of persistence information includes providing, to the persistence cloud server, a service identifier that identifies the registered service.

5 Example 9 may include the subject matter of any one of Examples 1-8, wherein the level of service includes one or more of: allowing full access to the registered service, denying access to the registered service, providing limited access to the registered service, and invoking further security actions.

10 Example 10 may include the subject matter of Example 9, wherein the providing limited access to the registered service includes one or more of: limiting types of actions that can be conducted, limiting quantities involved in actions that can be conducted, and limiting a local area in which actions can be conducted.

15 Example 11 may include the subject matter of any one of Examples 9-10, wherein the invoking further security actions includes one or more of: executing further authentication checks, locking accounts associated with the registered service, locking the client device, and deleting data from the client device.

Example 12 may include the subject matter of any one of Examples 1-11, wherein the processing instructions are further adapted to direct the processor to: receive, from the client device, login information of the user of the client device; and provide a device state change notification to the persistence cloud server based on the login information.

20 Example 13 may include an apparatus associated with a service registered with a persistence cloud service comprising means for receiving, from a client device, a device identifier that identifies the client device to the registered service; means for requesting, from a persistence cloud server associated with the persistence cloud service, persistence information associated with the device identifier; means for receiving the persistence information; means for  
25 determining a level of service to provide to the client device based on the persistence information; and means for providing the level of service to the client device.

30 Example 14 may include a router registered with a persistence cloud service, comprising a processor and a memory in communication with the processor, the memory having stored therein a plurality of processing instructions adapted to direct the processor to: receive, from a client device, a device identifier that identifies the client device; request, from a persistence cloud server associated with the persistence cloud service, persistence information associated with the device identifier; receive the persistence information; determine a level of service to provide based on the persistence information; and provide the level of service to the client device.

- 15 -

Example 15 may include the subject matter of Example 14, wherein the persistence information includes a device status assigned to the client device.

Example 16 may include the subject matter of Example 15, wherein the device status includes one or more of: an indication that the client device is in a normal state, an indication  
5 that the client device has been lost or stolen, an indication that activity at the client device is suspicious, an indication that usage of the client device should follow a defined set of policies, and an indication of a location of the client device.

Example 17 may include the subject matter of any one of Examples 14-16, wherein the requesting of persistence information includes providing, to the persistence cloud server, a router  
10 identifier that identifies the registered router.

Example 18 may include the subject matter of any one of Examples 14-17, wherein the level of service includes one or more of: allowing full network access, denying network access, providing limited network access, and invoking further security actions.

Example 19 may include a method of providing a service to a client device comprising:  
15 receiving, from a client device, a device identifier that identifies the client device; requesting, from a persistence cloud server associated with a persistence cloud service, persistence information associated with the device identifier; receiving the persistence information; determining a level of service to provide to the client device based on the persistence information; and providing the level of service to the client device.

Example 20 may include the subject matter of Example 19, wherein providing the level  
20 of service comprises providing an indication of the level of service to the client device, the level of service indication indicating how a client application associated with a service registered with the persistence cloud service is to proceed at the client device.

In Example 21, the subject matter of any one of Examples 19-20 may optionally include  
25 determining whether the client device is registered with the persistence cloud service; in response to determining that the client device is not registered with the persistence cloud service, sending a request to the client device inquiring whether to register the client device with the persistence cloud service; and in response to determining that the client device is to be registered with the persistence cloud service, sending registration information associated with the client  
30 device to the persistence cloud server.

In Example 22, the subject matter of any one of Examples 19-21 may optionally include receiving, from the client device, login information of the user of the client device; and providing a device state change notification to the persistence cloud server based on the login information.

- 16 -

Example 23 may include a non-transitory computer-readable medium storing control logic to instruct a processor of a computing device to: receive, from a client device, a device identifier that identifies the client device; request, from a persistence cloud server associated with a persistence cloud service, persistence information associated with the device identifier;  
5 receive the persistence information; determine a level of service to provide to the client device based on the persistence information; and provide the level of service to the client device.

Example 24 may include the subject matter of Example 23, wherein the providing of the level of service comprises providing an indication of the level of service to the client device, the level of service indication indicating how a client application associated with a service registered  
10 with the persistence cloud service is to proceed at the client device.

Example 25 may include the subject matter of any one of Examples 23-24, wherein the control logic is implemented to further instruct the processor to: determine whether the client device is registered with the persistence cloud service; in response to determining that the client device is not registered with the persistence cloud service, send a request to the client device  
15 inquiring whether to register the client device with the persistence cloud service; and in response to determining that the client device is to be registered with the persistence cloud service, send registration information associated with the client device to the persistence cloud server.

Example 26 may include the subject matter of any one of Examples 23-25, wherein the control logic is implemented to further instruct the processor to: receive, from the client device,  
20 login information of the user of the client device; and provide a device state change notification to the persistence cloud server based on the login information.

Example 27 may include a persistence cloud server associated with a persistence cloud service, comprising a processor and memory in communication with the processor, the memory having stored therein a plurality of processing instructions adapted to direct the processor to:  
25 receive, from a first computing device associated with a first service registered with the persistence cloud service, a client device update for a client device registered with the persistence cloud service; update client device persistence information associated with the client device based on the client device update; receive from a second computing device associated with a second service registered with the persistence cloud service, a request for the client device  
30 persistence information; and provide the client device persistence information to the second computing device.

Example 28 may include the subject matter of Example 27, wherein the second computing device is a router.

- 17 -

Example 29 may include the subject matter of Example 27, wherein the receiving the request for the client device persistence information includes receiving a service identifier that identifies the second registered service.

5 Example 30 may include the subject matter of Example 29, wherein the processing instructions are further adapted to direct the processor to verify, based on the received service identifier, that the second registered service is registered with the persistence cloud service.

Example 31 may include the subject matter of any one of Examples 27-30, wherein the client device persistence information includes a client device status assigned to the client device.

10 Example 32 may include the subject matter of Example 31, wherein the client device status includes one or more of: an indication that the client device is in a normal state, an indication that the client device has been lost or stolen, an indication that activity at the client device is suspicious, an indication that usage of the client device should follow a defined set of policies, and an indication of a location of the client device.

15 Example 33 may include the subject matter of any one of Examples 31-32, wherein the processing instructions are further adapted to direct the processor to: receive, from the second computing device, registration information for the client device, the registration information including a device identifier that identifies the client device, a service identifier that identifies the second registered service, and a policy set of the second registered service to be followed by the persistence cloud service based on the client device status; and store the registration information.

20 Example 34 may include the subject matter of Example 33, wherein the device identifier is based on a Media Access Control (MAC) address of the client device.

25 Example 35 may include the subject matter of any one of Examples 33-34, wherein the policy set includes one or both of: instructions pertaining to how the persistence cloud server should update the client device status based on a subsequent client device update from the second server, and instructions pertaining to what information to include as the client device persistence information provided to the second server based on the client device status.

30 Example 36 may include an apparatus associated with a persistence cloud service comprising means for receiving, from a first computing device associated with a first service registered with the persistence cloud service, a client device update for a client device registered with the persistence cloud service; means for updating client device persistence information associated with the client device based on the client device update; means for receiving from a second computing device associated with a second service registered with the persistence cloud service, a request for the client device persistence information; and means for providing the client device persistence information to the second computing device.

- 18 -

Example 37 may include a method of providing a persistence cloud service to registered services, comprising receiving, from a first computing device associated with a first service registered with the persistence cloud service, a client device update for a client device registered with the persistence cloud service; updating client device persistence information associated with the client device based on the client device update; receiving, from a second computing device associated with a second service registered with the persistence cloud service, a request for the client device persistence information; and providing the client device persistence information to the second computing device.

In Example 38, the subject matter of Example 37 may optionally include receiving, from the second computing device, registration information for the client device, the registration information including a device identifier that identifies the client device, a service identifier that identifies the second registered service, and a policy set of the second registered service to be followed by the persistence cloud service based on the client device persistence information; and storing the registration information.

Example 39 may include a non-transitory computer-readable medium storing control logic to instruct a processor of a computing device to: receive, from a first computing device associated with a first service registered with a persistence cloud service, a client device update for a client device registered with the persistence cloud service; update client device persistence information associated with the client device based on the client device update; receive, from a second computing device associated with a second service registered with the persistence cloud service, a request for the client device persistence information; and provide the client device persistence information to the second computing device.

Example 40 may include the subject matter of claim 39, wherein the control logic is implemented to further instruct the processor to: receive, from the second computing device, registration information for the client device, the registration information including a device identifier that identifies the client device, a service identifier that identifies the second registered service, and a policy set of the second registered service to be followed by the persistence cloud service based on the client device persistence information; and store the registration information.

Example 41 may include at least one machine readable medium comprising a plurality of instructions that in response to being executed on a computing device, cause the computing device to carry out the method of any one of Examples 18-21.

Example 42 may include a computer system to perform the method of any one of Examples 19-22.

- 19 -

Example 43 may include an apparatus configured to perform the method of any one of Examples 19-22.

Example 44 may include a machine to perform the method of any one of Examples 19-22.

5 Example 45 may include an apparatus comprising means for performing the method of any one of Examples 19-22.

Example 46 may include at least one machine readable medium comprising a plurality of instructions that in response to being executed on a computing device, cause the computing device to carry out the method of any one of Examples 19-22.

10 Example 47 may include a computer system to perform the method of any of Examples 37-38.

Example 48 may include an apparatus configured to perform the method of any one of Examples 37-38.

Example 49 may include a machine to perform the method of any of Examples 37-38.

15 Example 50 may include an apparatus comprising means for performing the method of any one of Examples 37-38.

The systems, methods, and computer program products described herein have an advantage of providing a universally centralized alert system that may provide immediate  
20 seamless protection for both client device users and virtually any services consumed by those users against improper use of those client devices. The more services registered with the persistence cloud service, the better the protection provided, as any registered service could report suspicious device activity to the system to be shared with the other registered services. Ideally, the services registered with the persistence cloud service may include some type of anti-  
25 theft service that could inform other services of the loss or theft of a device prior to the next use of their services by that device. Use of this system may even be useful in locating a lost or stolen client device and/or its perpetrator, as usage of the client device could potentially be tracked by the persistence cloud service. In this scenario, the more services registered with the persistence cloud service, the more thorough the tracking of the device. Another service that would be  
30 useful if registered with the persistence cloud service is a data backup service. If, for example, a client device has been reported as lost or stolen, a registered data backup service that may be associated with the client device may potentially be triggered to perform an unscheduled backup of the device, if the device is detected, such that data is backed up prior to a perpetrator attempting to wipe the device clean.

- 20 -

Another advantage of the PCS system is in its enterprise usages. A company may keep track of the user devices that it issues to its employees by, for example, the MAC address of each device or some other hardware identification. In the affiliate policy provided to the persistence cloud service for each of its devices, specific instructions can be provided as to what should  
5 happen to each device given any potential breach of security reported by the system. For example, if the device has been reported as lost or stolen, a data backup and/or data wipe of the device may be triggered to minimize any data loss or breach. In another example, the policy may provide instructions as to what level of access a specific device should have. If an employee of the company is a manager or a systems administrator or one having some key role  
10 in the company, that person's device may be allowed more extensive access to the company's systems and settings than other employees. Many other advantages and uses are also contemplated.

## WHAT IS CLAIMED IS:

1. A computing device associated with a service registered with a persistence cloud service, comprising:
  - 5 a processor; and
  - a memory in communication with the processor, the memory having stored therein a plurality of processing instructions adapted to direct the processor to:
    - receive, from a client device, a device identifier that identifies the client device to the registered service;
    - 10 request, from a persistence cloud server associated with the persistence cloud service, persistence information associated with the device identifier;
    - receive the persistence information;
    - determine a level of service to provide to the client device based on the persistence information; and
    - 15 provide the level of service to the client device.
2. The computing device of claim 1, wherein providing the level of service comprises providing a level of service indication to the client device, the level of service indication indicating how a client application associated with the registered service is to proceed at the  
20 client device.
3. The computing device of claim 1, wherein the processing instructions are further adapted to direct the processor to:
  - determine whether the client device is registered with the persistence cloud service;
  - 25 in response to determining that the client device is not registered with the persistence cloud service, send a request to the client device inquiring whether to register the client device with the persistence cloud service; and
  - in response to determining that the client device is to be registered with the persistence cloud service, send registration information associated with the client device to the persistence  
30 cloud server.
4. The computing device of claim 3, wherein the registration information includes the device identifier, a service identifier that identifies the registered service, and a policy of the

- 22 -

registered service to be followed by the persistence cloud service based on the persistence information associated with the client device.

5. The computing device of claim 1, wherein the persistence information includes a device status assigned to the client device.

6. The computing device of claim 5, wherein the device status includes one or more of: an indication that the client device is in a normal state, an indication that the client device has been lost or stolen, an indication that activity at the client device is suspicious, an indication that usage of the client device should follow a defined set of policies, and an indication of a location of the client device.

7. The computing device of claim 1, wherein the requesting of persistence information includes providing, to the persistence cloud server, a service identifier that identifies the registered service.

8. The computing device of claim 1, wherein the level of service includes one or more of: allowing full access to the registered service, denying access to the registered service, providing limited access to the registered service, and invoking further security actions.

9. The computing device of claim 8, wherein the providing limited access to the registered service includes one or more of: limiting types of actions that can be conducted, limiting quantities involved in actions that can be conducted, and limiting a local area in which actions can be conducted.

10. The computing device of claim 8, wherein the invoking further security actions includes one or more of: executing further authentication checks, locking accounts associated with the registered service, locking the client device, and deleting data from the client device.

11. The computing device of claim 1, wherein the processing instructions are further adapted to direct the processor to:  
receive, from the client device, login information of the user of the client device; and  
provide a device state change notification to the persistence cloud server based on the login information.

12. An apparatus associated with a service registered with a persistence cloud service, comprising:

means for receiving, from a client device, a device identifier that identifies the client device to the registered service;

means for requesting, from a persistence cloud server associated with the persistence cloud service, persistence information associated with the device identifier;

means for receiving the persistence information;

means for determining a level of service to provide to the client device based on the persistence information; and

means for providing the level of service to the client device.

13. A method of providing a service to a client device, comprising:

receiving, from the client device, a device identifier that identifies the client device;

requesting, from a persistence cloud server associated with a persistence cloud service, persistence information associated with the device identifier;

receiving the persistence information;

determining a level of service to provide to the client device based on the persistence information; and

providing the level of service to the client device.

14. A computer-readable medium storing control logic to instruct a processor of a computing device to:

receive, from a client device, a device identifier that identifies the client device;

request, from a persistence cloud server associated with a persistence cloud service, persistence information associated with the device identifier;

receive the persistence information;

determine a level of service to provide to the client device based on the persistence information; and

provide the level of service to the client device.

- 24 -

15. A persistence cloud server associated with a persistence cloud service, comprising:  
a processor;

a memory in communication with the processor, the memory having stored therein a plurality of processing instructions adapted to direct the processor to:

5 receive, from a first computing device associated with a first service registered with the persistence cloud service, a client device update for a client device registered with the persistence cloud service;

update client device persistence information associated with the client device based on the client device update;

10 receive from a second computing device associated with a second service registered with the persistence cloud service, a request for the client device persistence information; and

provide the client device persistence information to the second computing device.

15 16. The persistence cloud server of claim 15, wherein the second computing device is a router.

17. The persistence cloud server of claim 15, wherein the receiving the request for the client device persistence information includes receiving a service identifier that identifies the second  
20 registered service.

18. The persistence cloud server of claim 17, wherein the processing instructions are further adapted to direct the processor to:

25 verify, based on the received service identifier, that the second registered service is registered with the persistence cloud service.

19. The persistence cloud server of claim 15, wherein the client device persistence information includes a client device status assigned to the client device.

30 20. The persistence cloud server of claim 19, wherein the client device status includes one or more of: an indication that the client device is in a normal state, an indication that the client device has been lost or stolen, an indication that activity at the client device is suspicious, an indication that usage of the client device should follow a defined set of policies, and an indication of a location of the client device.

- 25 -

21. The persistence cloud server of claim 19, wherein the processing instructions are further adapted to direct the processor to:

receive, from the second computing device, registration information for the client device,  
5 the registration information including a device identifier that identifies the client device, a service identifier that identifies the second registered service, and a policy set of the second registered service to be followed by the persistence cloud service based on the client device status; and

store the registration information.

10

22. The persistence cloud server of claim 21, wherein the policy set includes one or both of: instructions pertaining to how the persistence cloud server should update the client device status based on a subsequent client device update from the second server, and instructions pertaining to what information to include as the client device persistence information provided to the second  
15 server based on the client device status.

23. An apparatus associated with a persistence cloud service, comprising:

means for receiving, from a first computing device associated with a first service registered with the persistence cloud service, a client device update for a client device registered  
20 with the persistence cloud service;

means for updating client device persistence information associated with the client device based on the client device update;

means for receiving from a second computing device associated with a second service registered with the persistence cloud service, a request for the client device persistence  
25 information; and

means for providing the client device persistence information to the second computing device.

24. A method of providing a persistence cloud service to registered services, comprising:

30 receiving, from a first computing device associated with a first service registered with the persistence cloud service, a client device update for a client device registered with the persistence cloud service;

updating client device persistence information associated with the client device based on the client device update;

- 26 -

receiving, from a second computing device associated with a second service registered with the persistence cloud service, a request for the client device persistence information; and providing the client device persistence information to the second computing device.

5 25. A computer-readable medium storing control logic to instruct a processor of a computing device to:

receive, from a first computing device associated with a first service registered with a persistence cloud service, a client device update for a client device registered with the persistence cloud service;

10 update client device persistence information associated with the client device based on the client device update;

receive, from a second computing device associated with a second service registered with the persistence cloud service, a request for the client device persistence information; and provide the client device persistence information to the second computing device.

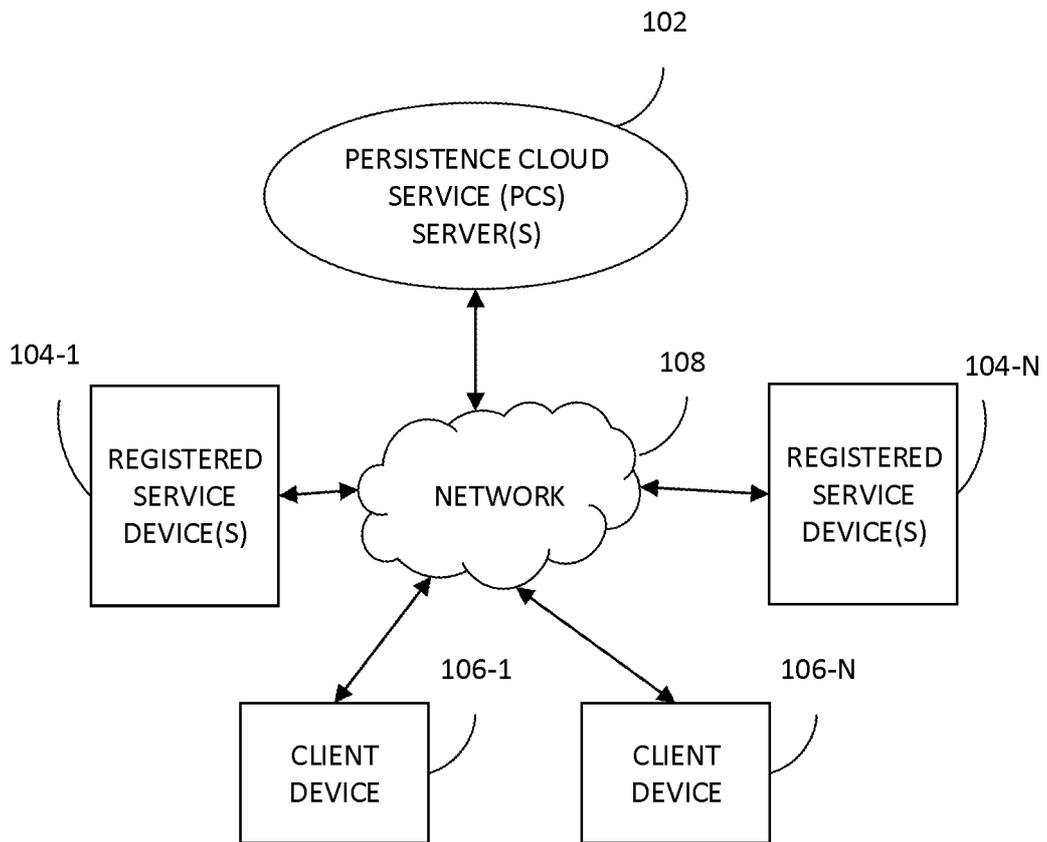


FIG. 1

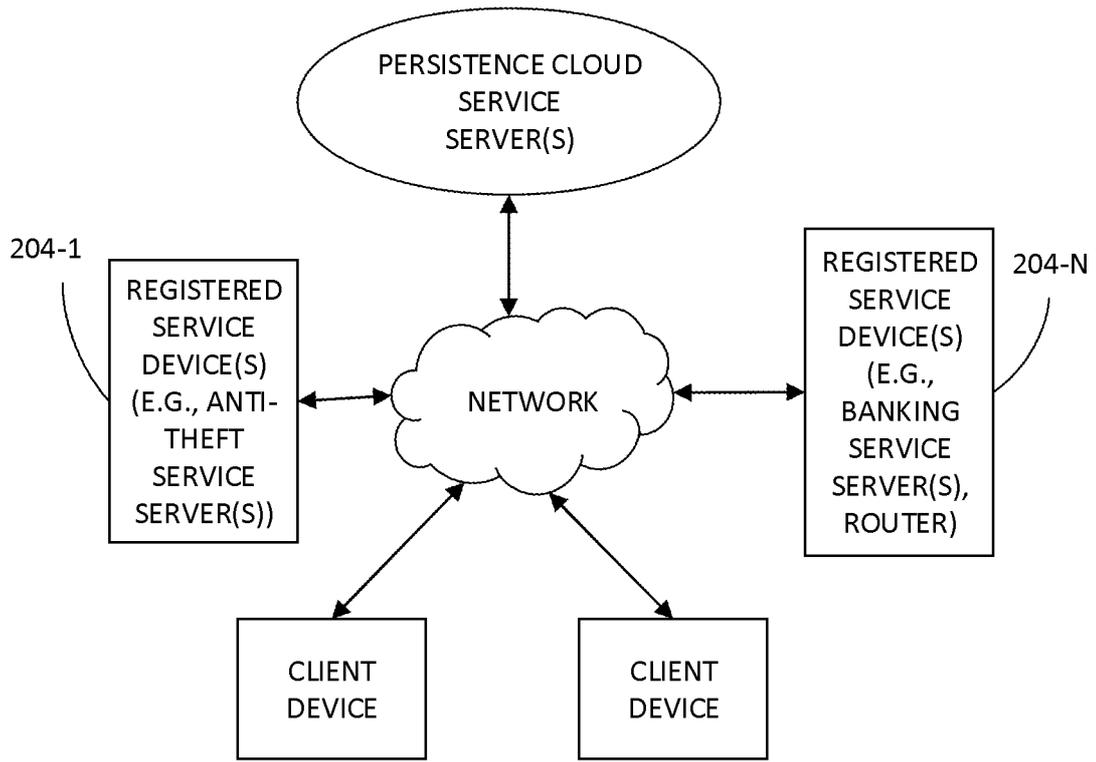


FIG. 2

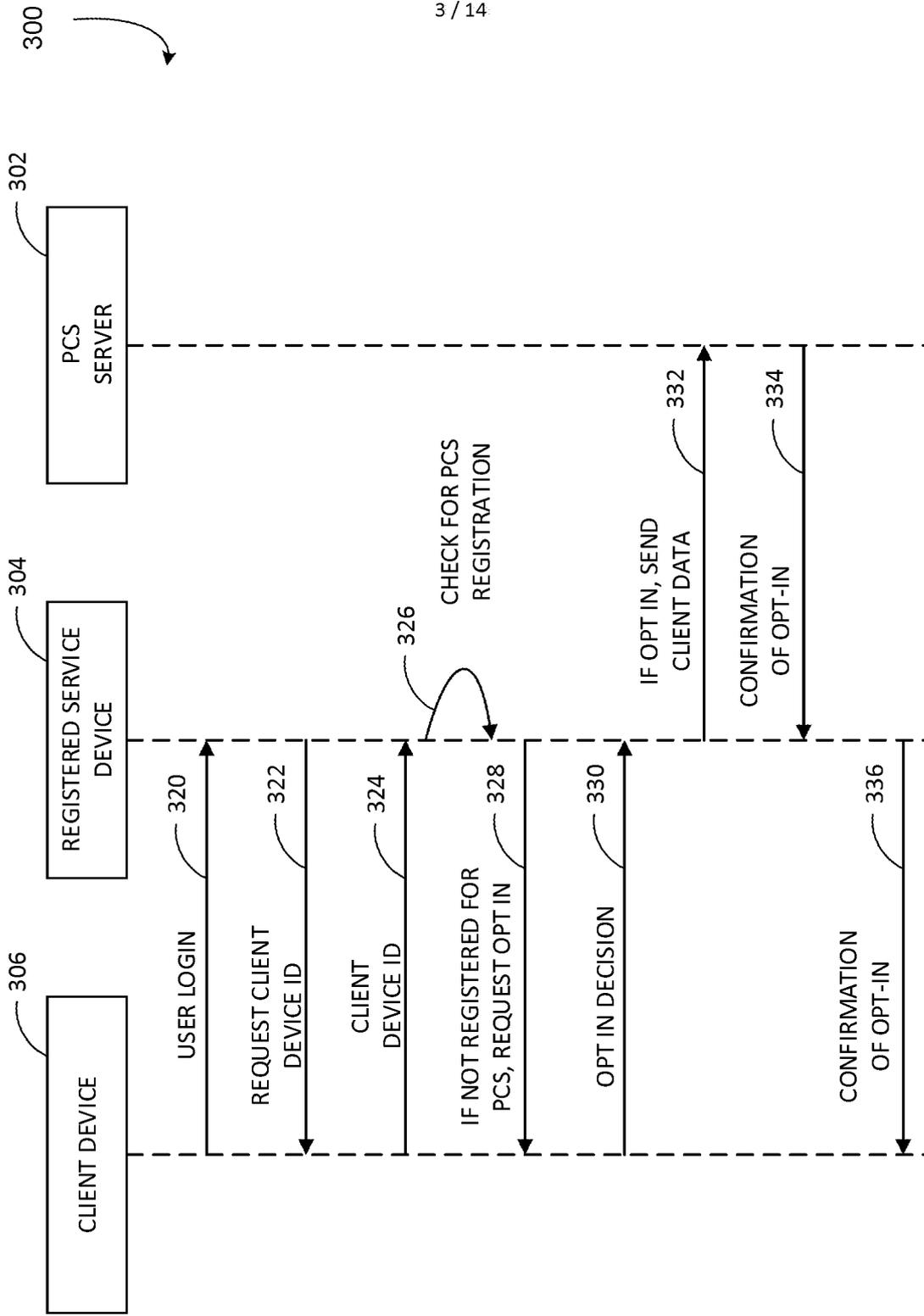


FIG. 3

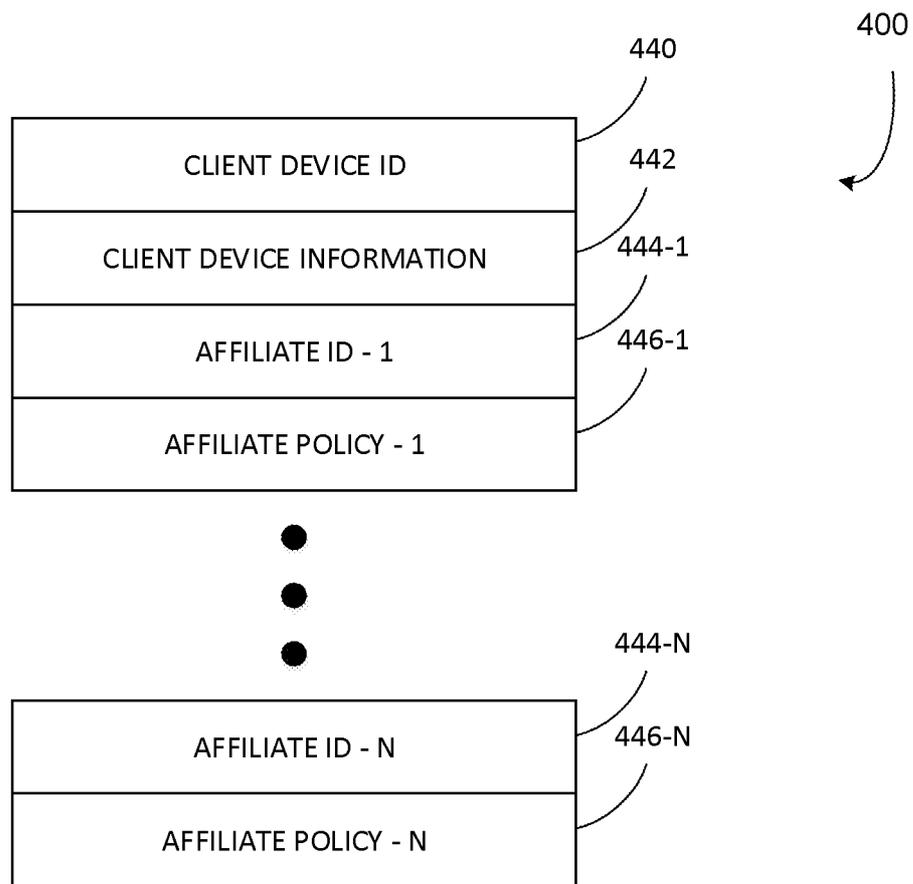


FIG. 4

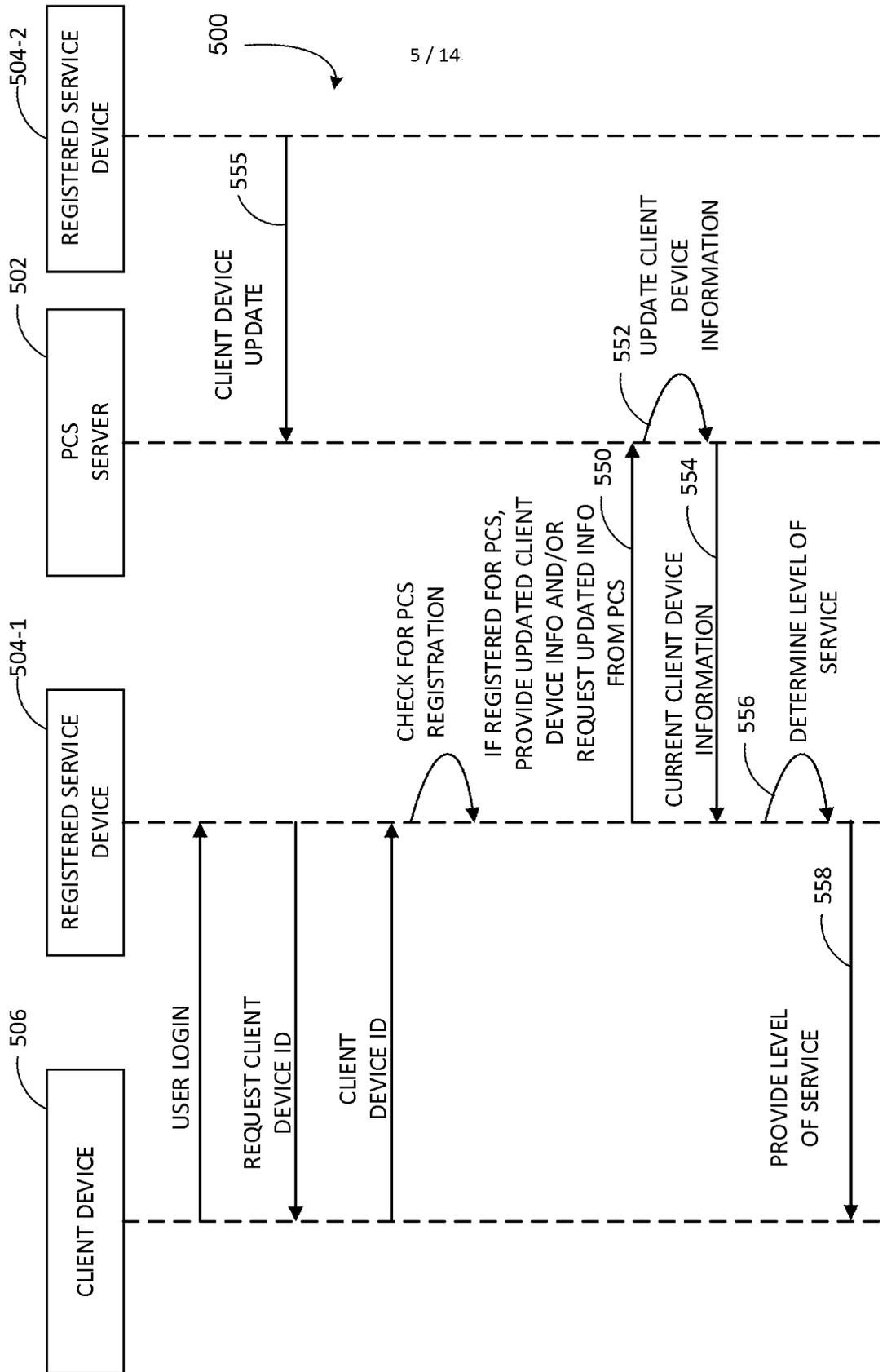


FIG. 5

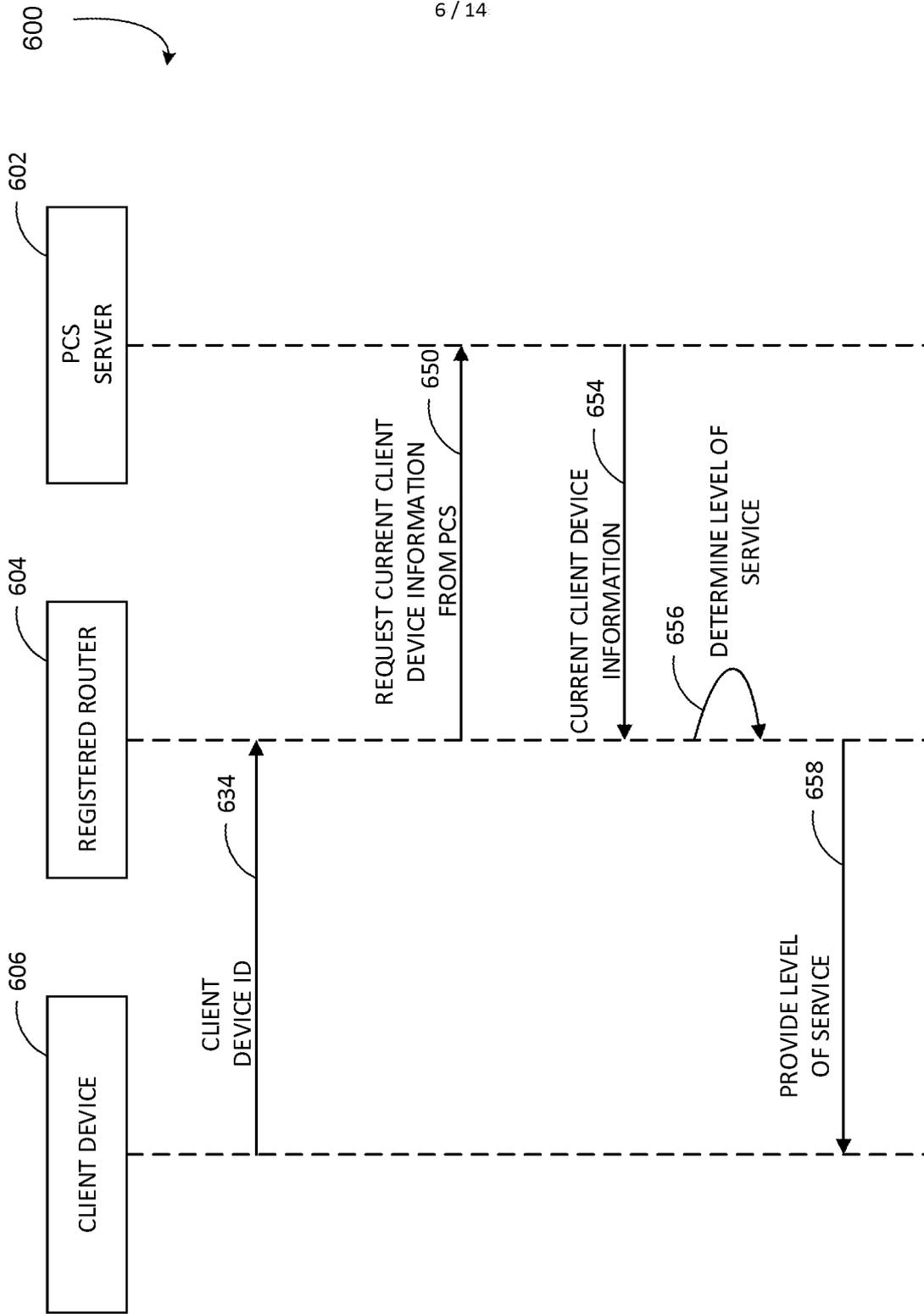


FIG. 6

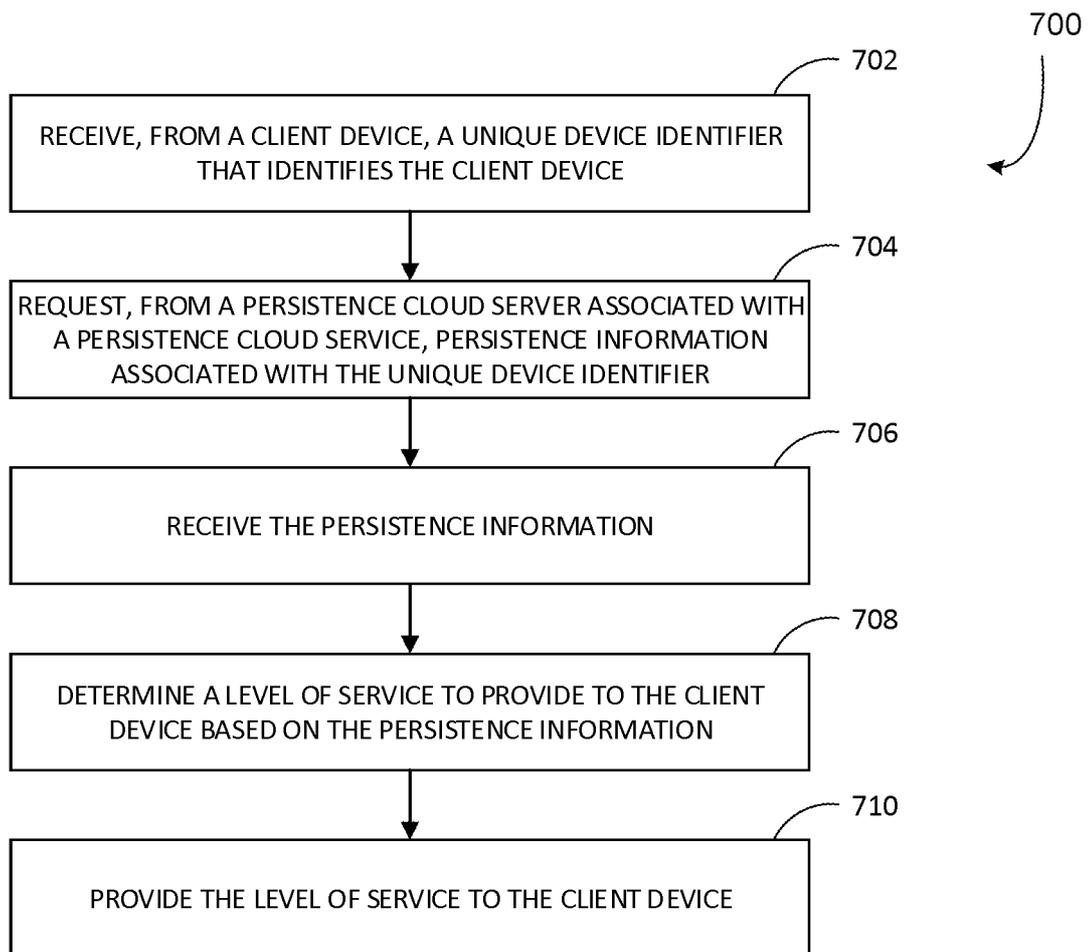
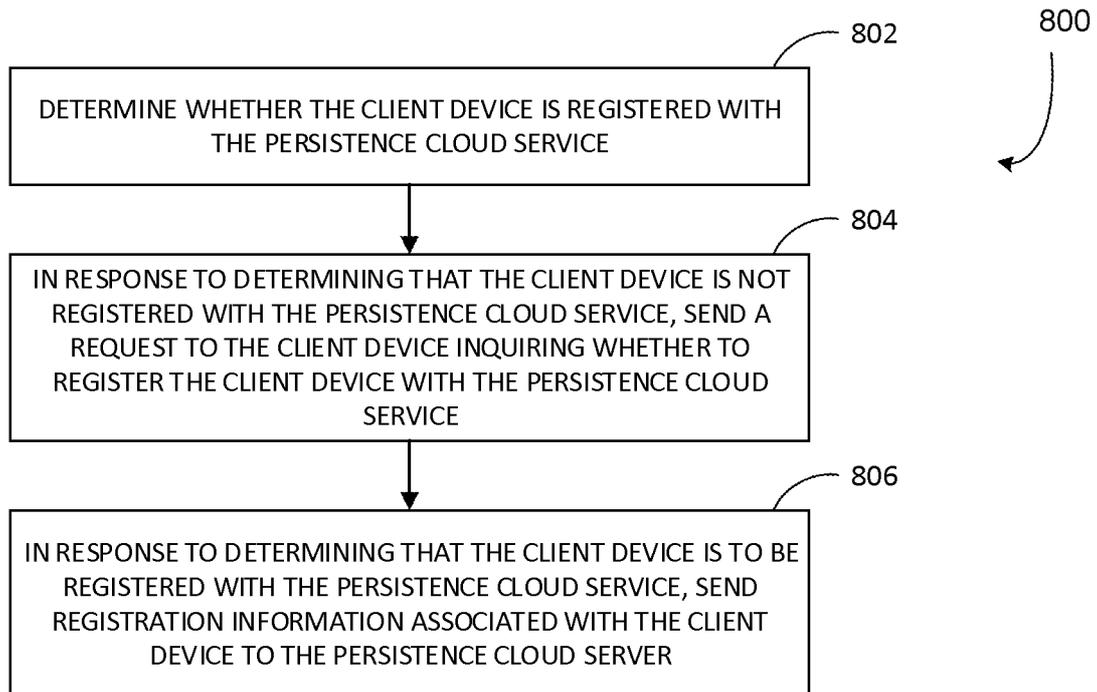


FIG. 7



**FIG. 8**

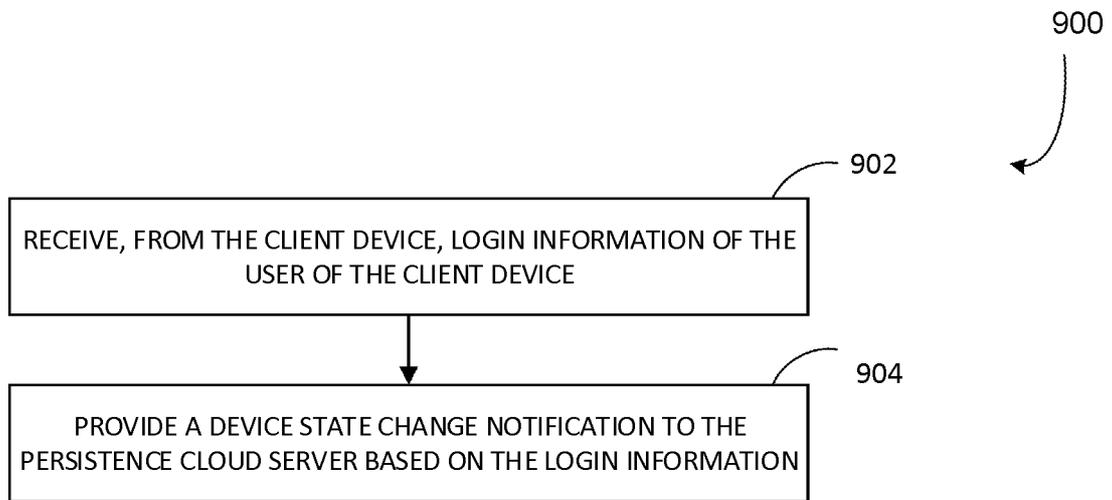


FIG. 9

10 / 14

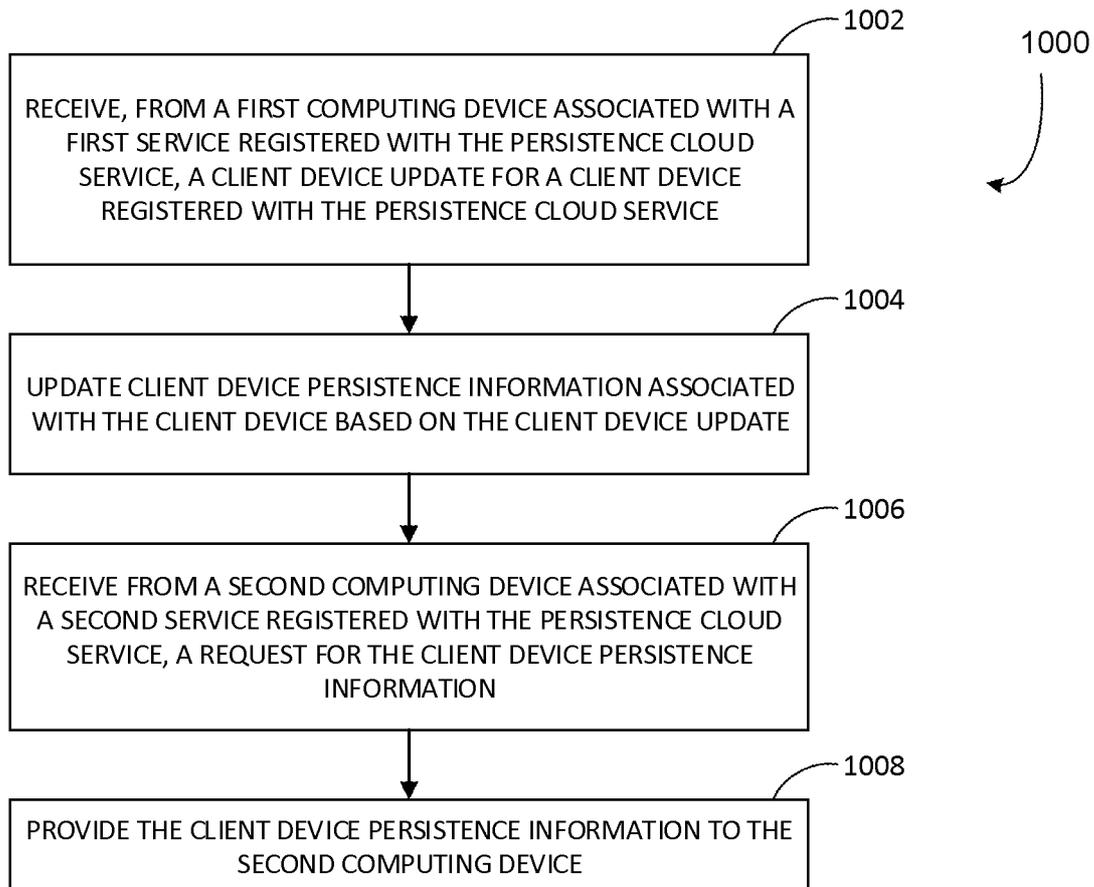


FIG. 10

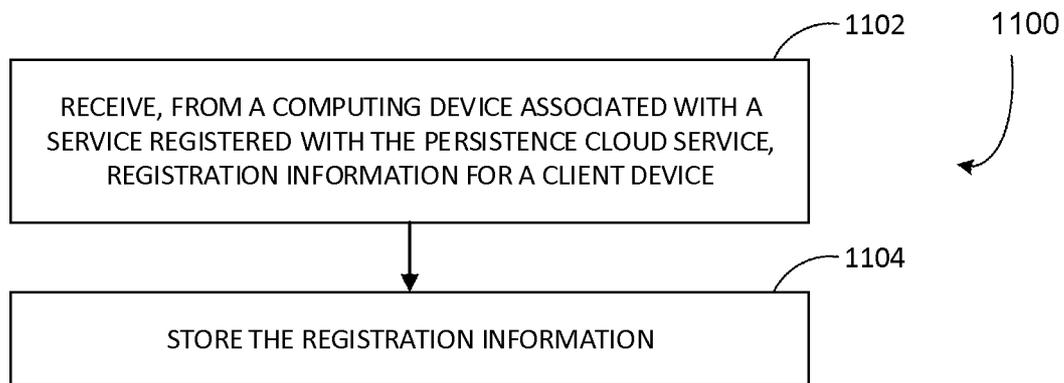


FIG. 11

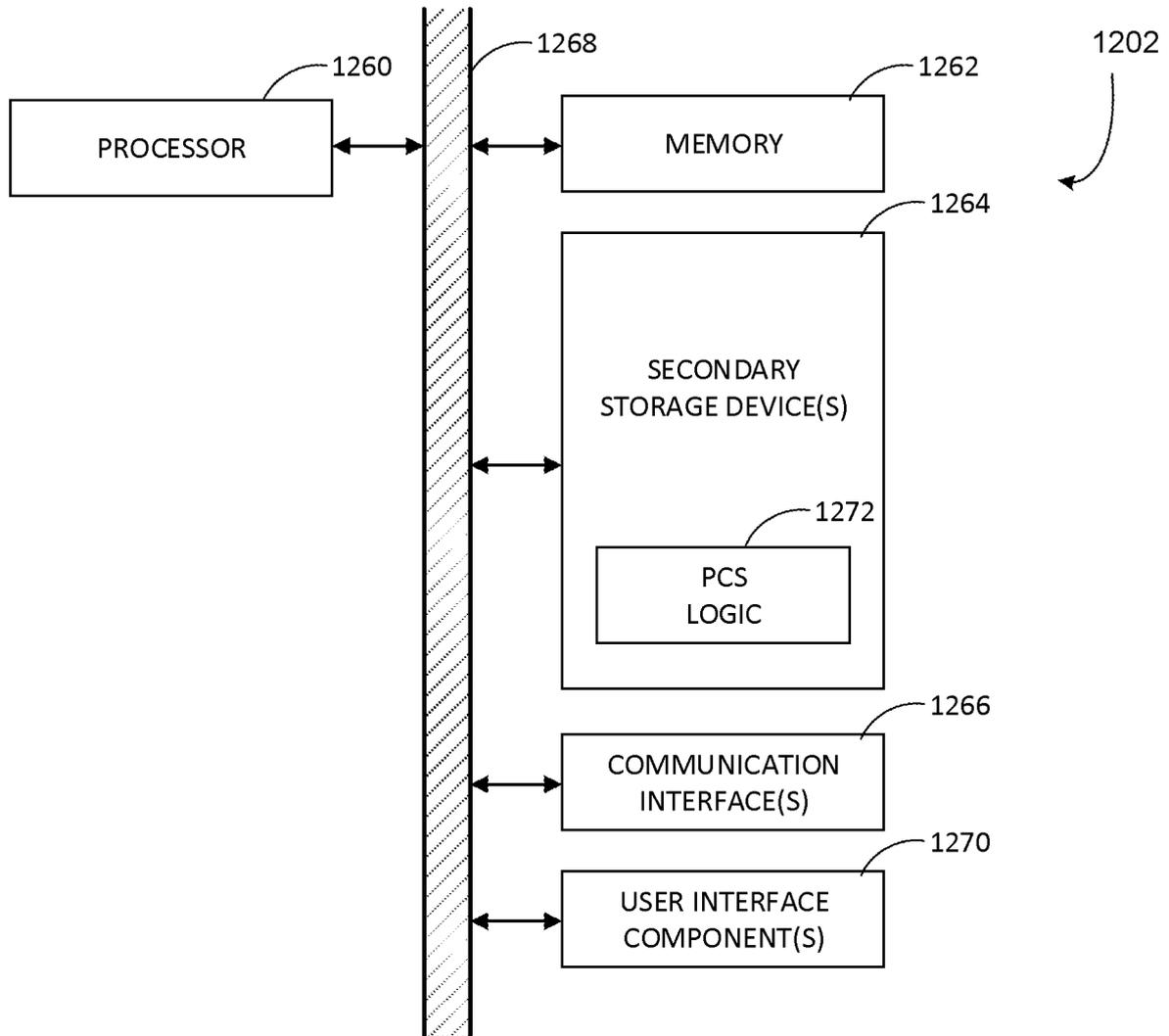


FIG. 12

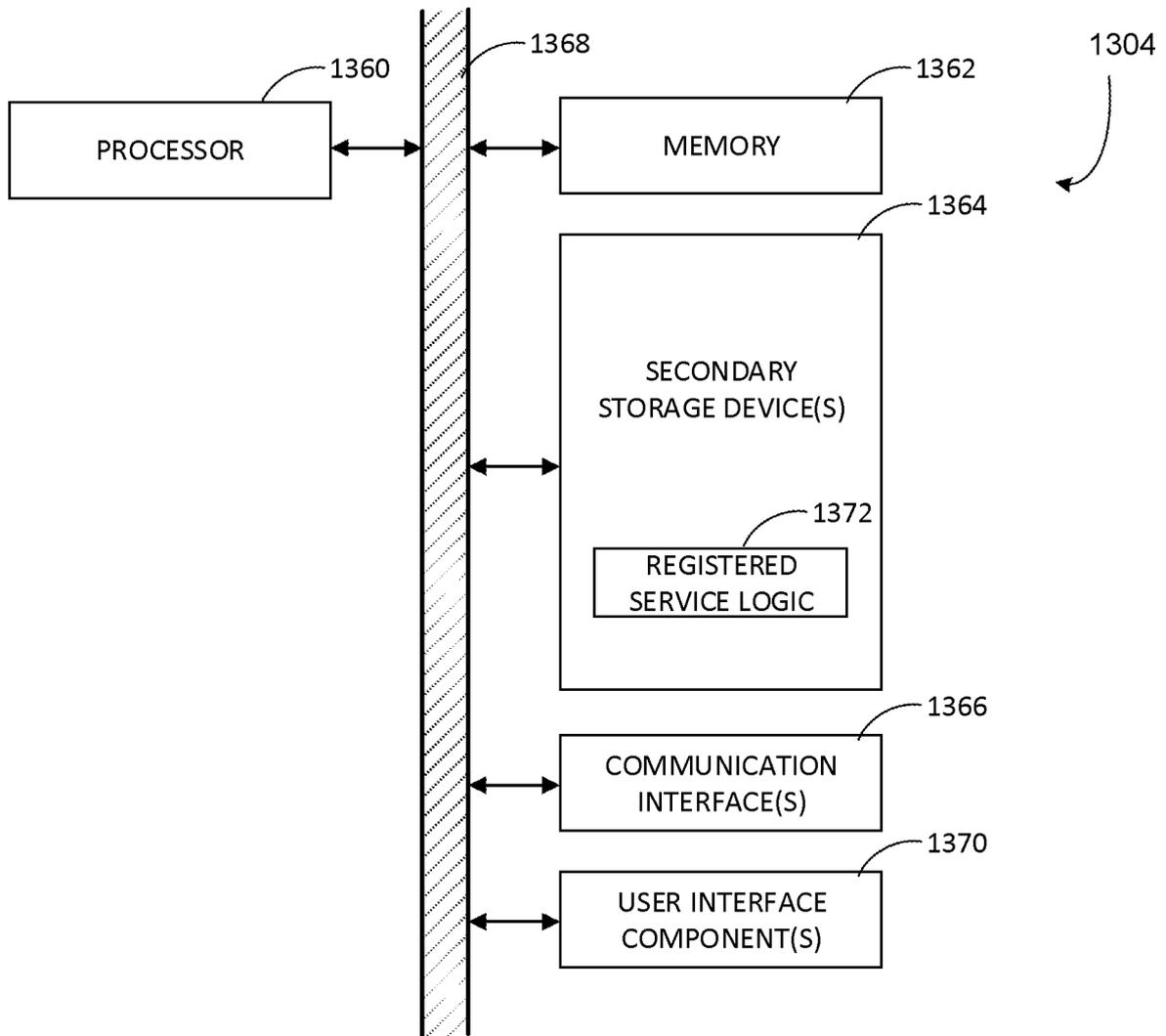


FIG. 13

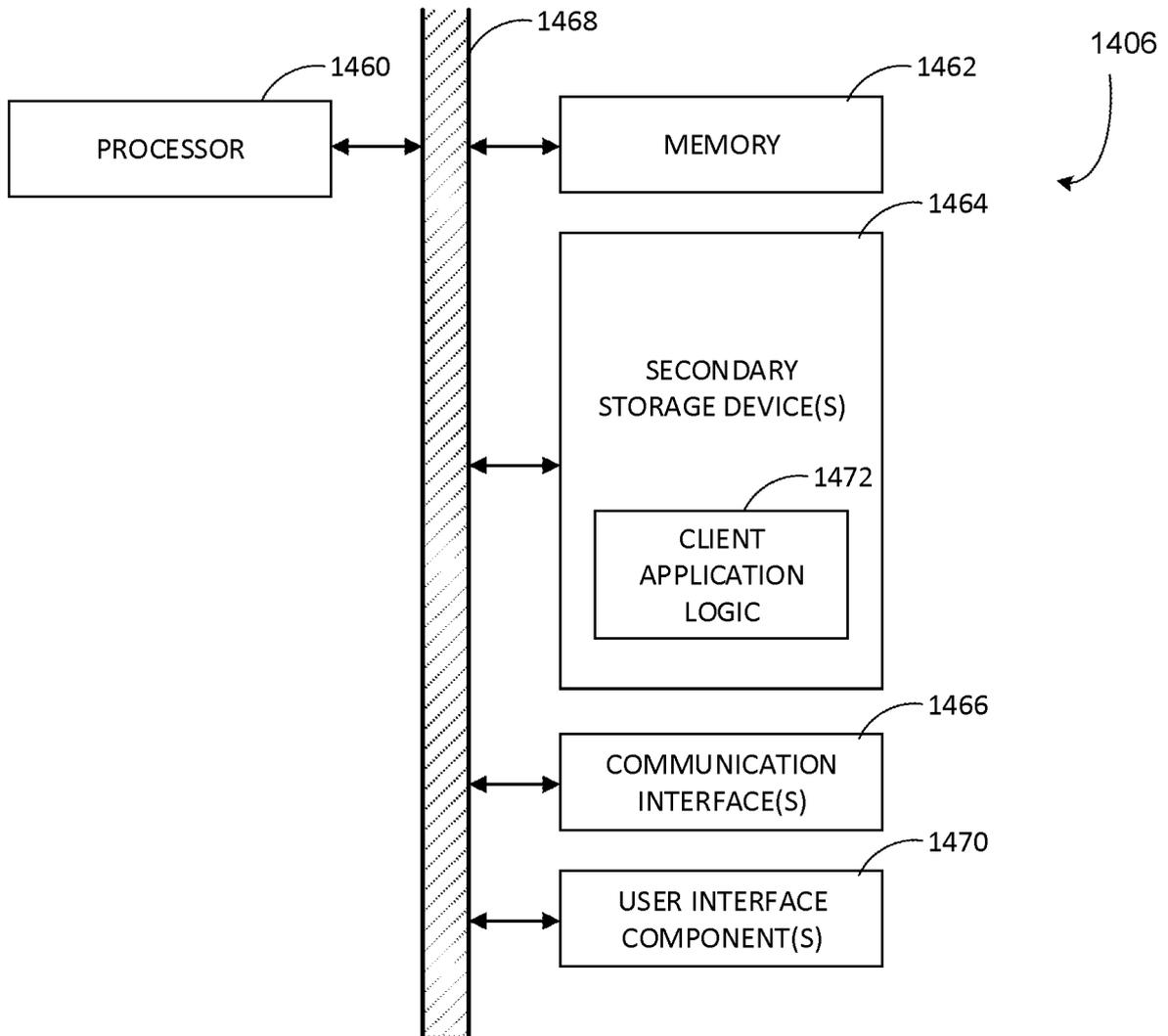


FIG. 14

**A. CLASSIFICATION OF SUBJECT MATTER****H04L 9/32(2006.01)i, H04L 12/16(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 9/32; G06F 15/16; H04W 68/00; G06F 11/14; H04W 12/06; G06Q 10/00; H04L 12/16Documentation 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 modelsElectronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
eKOMPASS(KIPO internal) & Keywords: cloud, server, service, identify, device information, level, security, affiliate**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012-0198268 A1 (RASHID QURESHI ) 02 August 2012 See paragraphs 21, 25, 27, 32, 34; and figure 1 .	1,2,7,12-14
A		3-5,6,8-11,15-25
A	US 2012-0203862 A1 (HAREL TAYEB et al.) 09 August 2012 See paragraphs 24, 29; and figure 3A.	1-25
A	US 2013-0052991 A1 (JORDAN NAFTOLIN) 28 February 2013 See paragraphs 35, 44; claim 9 ; and figure 5 .	1-25
A	US 2013-0060842 A1 (FRED CROSSMAN) 07 March 2013 See paragraphs 6 , 19; and figure 1 .	1-25
A	US 2012-0330711 A1 (NAVENDU JAIN et al.) 27 December 2012 See paragraphs 71, 77, 79; and figure 4 .	1-25

**I** 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

11 December 2013 (11.12.2013)

Date of mailing of the international search report

**12 December 2013 (12.12.2013)**

Name and mailing address of the ISA/KR



Korean Intellectual Property Office  
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City,  
302-701, Republic of Korea  
Facsimile No. +82-42-472-7140

Authorized officer

KANG, Hee Gok

Telephone No. +82-42-481-8264



**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No.

**PCT/US2013/031386**

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012-0198268 A1	02/08/2012	CN 102664909 A	12/09/2012
US 2012-0203862 A1	09/08/2012	WO 2012-107929 A2	16/08/2012
		WO 2012-107929 A3	26/10/2012
		WO 2012-107929 A9	03/01/2013
US 2013-0052991 A1	28/02/2013	None	
US 2013-0060842 A1	07/03/2013	None	
US 2012-0330711 A1	27/12/2012	WO 2013-003031 A2	03/01/2013
		WO 2013-003031 A3	11/04/2013