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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 April 2014 (10.04.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/055448 A1

(51) **International Patent Classification**:
G06F 15/16 (2006.01) *G06F 9/06* (2006.01)

(21) **International Application Number**:
PCT/US2013/062733

(22) **International Filing Date**:
30 September 2013 (30.09.2013)

(25) **Filing Language**: English

(26) **Publication Language**: English

(30) **Priority Data**:
61/708,794 2 October 2012 (02.10.2012) US

(71) **Applicant**: **NEXTBIT, INC.** [US/US]; 290 King Street, Unit #9, San Francisco, California 94107 (US).

(72) **Inventors**: **CHAN, Michael A.**; 170 King St., #602, San Francisco, California 94107 (US). **MOSS, Tom**; 97 Pepper Drive, Los Altos, California 94022 (US). **QUAN, Justin**; 310 Valencia St., San Francisco, California 94103 (US).

(74) **Agents**: **COLEMAN, Brian R.** et al.; Perkins Coie LLP, P.O. Box 1208, Seattle, Washington 98111-1208 (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, 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, 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, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) **Title**: CUSTOMIZING OPERATING SYSTEM BASED ON DETECTED CARRIER

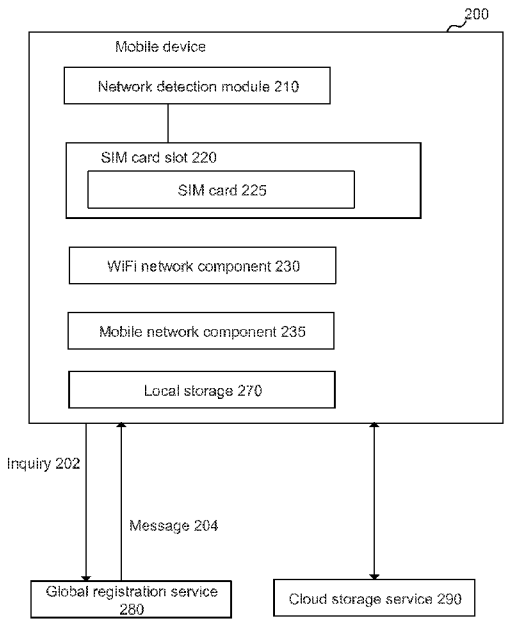

FIG. 2

(57) **Abstract**: Technology disclosed herein includes a method for loading a carrier specific OS onto a computing device depending on what network the computing device is connected to. The computing device detects an identity of a network to which a computing device is connected or is to be connected during a network identification process executed on the computing device. The network can be identified, e.g., by examining a subscriber identification module (SIM) card electronically connected to the computing device. The device then sends a request including the identity of the network to a remote registration service. In turn the device receives an instruction from the remote registration service identifying a distribution of an operating system (OS) specific for the network. After retrieving the OS distribution, the device loads the distribution of the operating system on the computing device.

WO 2014/055448 A1

Published:

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

CUSTOMIZING OPERATING SYSTEM BASED ON DETECTED CARRIER

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims to the benefit of U.S. Provisional Patent Application No. 61/708,794, entitled "CLOUD COMPUTING INTEGRATED OPERATING SYSTEM", which was filed on October 2, 2012, which is incorporated by reference herein in its entirety.

FIELD OF THE INVENTION

[0002] At least one embodiment of the present invention pertains to cloud computing, and more particularly, to automatically loading operating system based on network carrier using cloud storage.

BACKGROUND

[0003] Wireless devices, e.g., mobile phones, tablets, computers, mobile hotspot devices, etc., are manufactured for use on one or more telecommunication carrier's networks. Sometime, particular carriers apply different requirements which devices must meet in order to operate on the carrier's network. Typically manufactures and vendors of the devices modify the hardware and the software (including, e.g., operating systems) of the devices to meet carrier-specific requirements.

[0004] Users of such devices may need or desire to use the same device in communication networks of different telecommunication carriers. For instance, a user can use a mobile phone with a first carrier in one country, and needs to use the same mobile phone with a second carrier in another country when he travels abroad.

SUMMARY

[0005] Technology introduced here provides a mechanism for loading a carrier specific OS onto a computing device depending on what network the computing device is connected to. In accordance with the technology introduced here, the computing device detects an identity of a network to which a computing device is connected or is to be connected, during a network identification process executed on the computing device. There are multiple ways a network can be identified, e.g., by examining a subscriber identification module (SIM) card electronically connected to the computing device. The device then sends a request including the identity of the network to a remote registration service. In turn the device receives an instruction from the remote registration service identifying a distribution of an operating system (OS) specific for the network. Once the OS distribution is retrieved, the device loads the distribution of the operating system on the computing device.

[0006] Such a mechanism enables a user to start using a device without the need of manually setting up the device first. For instance, when a user receives a new mobile phone or mobile device, the user only needs to insert his SIM card into the device. The device can automatically detect with which network the SIM card works (e.g., which wireless carrier for the network) and correspondingly load an operating system customized for that network. When the mobile device finishes booting up, the user has a new device with a running operating system customized for that network carrier, or even further customized for that user.

[0007] Other aspects of the technology introduced here will be apparent from the accompanying figures and from the detailed description which follows.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] These and other objects, features and characteristics of the present invention will become more apparent to those skilled in the art from a study of the following detailed description in conjunction with the appended claims and drawings, all of which form a part of this specification. In the drawings:

[0009] FIG. 1 illustrates an example system for mobile devices retrieving data from a cloud storage service.

[0010] FIG. 2 illustrates an example of a mobile device capable of switching operating system based on the telecommunication carrier.

[0011] FIG. 3 illustrates an example of a carrier environment with which such mobile devices can switch operating systems based on the network.

[0012] FIG. 4 illustrates an example of a message sequence chart for a mobile device switching between telecommunication networks.

[0013] FIG. 5 illustrates an example of an operating system loading process based on the identity of the network.

[0014] FIG. 6 is a high-level block diagram showing an example of the architecture of a computer device, which may represent any electronic device or any server within a cloud storage service as described herein.

DETAILED DESCRIPTION

[0015] References in this specification to "an embodiment," "one embodiment," or the like, mean that the particular feature, structure, or characteristic being described is included in at least one embodiment of the present invention. Occurrences of such phrases in this specification do not all necessarily refer to the same embodiment, however.

[0016] FIG. 1 illustrates an example system for mobile devices retrieving data from a cloud storage service. The system includes a cloud storage service 110 configured to store data for mobile devices. In one embodiment, the cloud storage service 110 can be a storage cluster having computer nodes interconnected with each other by a network. The storage cluster can communicate with other mobile devices (e.g., mobile devices 130 or 140) via the Internet. The cloud storage service 110 can contain storage nodes 112. Each of the storage nodes 112 contains one or more processors 114 and storage devices 116. The storage devices can include optical disk storage, RAM, ROM, EEPROM, flash memory, phase change memory, magnetic cassettes, magnetic tapes, magnetic disk storage or any other computer storage medium which can be used to store the desired information.

[0017] A cloud communication interface 120 can also be included to receive data to be stored in the cloud storage service. The cloud communication interface 120 can include network communication hardware and network connection logic to receive the information from electronic devices. The network can be a local area network (LAN), wide area network (WAN) or the Internet. The cloud communication interface 120 may include a queuing mechanism to organize the received synchronization data to be stored in the cloud storage service 110. The cloud communication interface 120 can communicate with the cloud storage service 110 to send requests to the cloud storage service 110 for storing application state data and retrieving data.

[0018] A mobile device 130 includes an operating system 132 to manage the hardware resources of the mobile device 130. The mobile device 130 includes at least one local storage device 138 to store the operating system data, application data, and user data. The mobile device 130 can retrieve data from the cloud storage service 110 via the cloud communication interface 120. The mobile device 130 or 140 can be a desktop computer, a laptop computer, a tablet computer, an automobile computer, a game console, a smart phone, a personal digital assistant, a

mobile hotspot device, or other electronic devices capable of running computer applications, as contemplated by a person having ordinary skill in the art.

[0019] The computer applications 134 stored in the mobile device 130 can include applications for general productivity and information retrieval, including email, calendar, contacts, and stock market and weather information. The computer applications 134 can also include applications in other categories, such as mobile games, factory automation, GPS and location-based services, banking, order-tracking, ticket purchases or any other categories as contemplated by a person having ordinary skill in the art.

[0020] The mobile device 130 or 140 can download data from the cloud storage service to update or change the operating system 132 or 142 on the mobile device 130 or 140. The mobile device 130 or 140 can download the data using its data communication module 136 or 146. The update or change of the operating system can be triggered by various events. For instance, when the mobile device 130 detects that it has connected to a network service of a different mobile network carrier, the mobile device 130 can request data from the cloud storage service 110 for an operating system designed for the mobile device 130 running on the mobile network carrier.

[0021] FIG. 2 illustrates an example of a mobile device capable of switching operating system based on the telecommunication carrier. The mobile device 200 includes a network detection module 210. The network detection module 210 is capable of detecting the network(s) that the mobile device 200 is connected to or can be connected to. For instance, the network detection module 210 can detect whether the mobile device 200 is connected to a home WiFi network, a work WiFi network, or a public WiFi network (e.g. airport WiFi network). For example, the network detection module 210 may determine whether it's connected to a home WiFi network based on the SSID (service set identifier) of the WiFi network or the MAC (media access control) address of the WiFi network gateway.

[0022] The network detection module 210 can also detect the mobile network carrier of the mobile network that the mobile device 200 is connected to. For instance, the network detection module 210 is able to detect whether it is connected to an AT&T or T-Mobile mobile network by communicating with a SIM (subscriber identity module) card 225 inserted in a SIM card slot 220 in the mobile device 200. In the illustrated embodiment, the network detection module 210 can request and

retrieve an IMSI (international mobile subscriber identity) number or ICCID (Integrated Circuit Card Identifier) number from the SIM card, and use the IMSI number or ICCID number to determine the mobile network that the SIM card is designed to work with.

[0023] The network detection module 210 may further perform its network detection functionality when the mobile device 200 boots up and before an operating system launches on the mobile device 200. In some embodiments, the instructions for the network detection can be stored in a firmware or in a Basic Input/Output System (BIOS) of the mobile device 200. The network detection module 210 can also perform its network detection functionality during any operation stages of the mobile device 200.

[0024] Once the network detection module 210 detects the identity of the WiFi or mobile network that the mobile device 200 is connected to, the mobile device 200 contacts and sends an inquiry 202 to a global registration service 280 in order to determine the type and distribution of the operating system that the mobile device 210 should run. The global registration service 280 can be implemented on a web server or on a cloud computing service. The inquiry 202 can include the identity of the connected network, an identity of the mobile device 200, or even an identity of the user using the mobile device 200. The global registration service 280 determines a suggestion of a distribution of an operating system based on the information included in the inquiry, and sends a message 204 containing an identity of the suggested distribution of the operating system back to the mobile device 210. The suggested distribution of the operating system can be a version of the operating system customized for the connected network. The inquiry 202 can be sent out via a WiFi network component 230 or a mobile network component 235 that has been connected to a WiFi or mobile network. Likewise, the message 204 can be received via the WiFi network component 230 or the mobile network component 235.

[0025] The message 204 sent by the global registration service 280 can include a location link indicating where to retrieve the data of the suggested distribution of the operating system. For instance, the location link may include a network address of a web server or a cloud storage service 290 that stores in the suggested distribution of the operating system. The mobile device 200 is able to download the suggested distribution of the operating system from the cloud storage service 290 located by the location link in the message 204. The cloud storage

service 290 can be implemented along with the global registration service 280 within a common cloud computing service. The cloud storage service 290 can also be implemented in a cloud computing service separated from the global registration service 280, as illustrated in FIG. 2.

[0026] In some embodiments, a copy of the suggested distribution of the operating system can be stored in a local storage 270 of the mobile device 200. In some embodiments, a copy of the suggested distribution of the operating system can be stored in a web server within the connected mobile network of the mobile network carrier.

[0027] The suggested distribution of the operating system can be distributed to the mobile device 200 as an over-the-air update. The mobile device 200 can receive the suggested distribution of the operating system as a full image of the operating system, or as an incremental copy of the operating system including changes on the operating system or changes to the framework or applications in the operating system. In some embodiments, the installation of the OS distribution is mandatory instead of optional. The user cannot refuse, defer, or alter the update using the OS distribution. After the installation of the OS distribution, the mobile device 200 may need to reboot for the update to take effect.

[0028] In some embodiments, the suggested OS distribution includes updates that do not require the mobile device 200 to reboot. For instance, the suggested OS distribution can include asset changes, e.g. changes to the visuals of icons and taskbar or pre-load of applications. For these changes, the mobile device 200 can directly apply the updates without the need to reboot.

[0029] If there is any data duplication between the current operating system on the mobile device 200 and the suggested OS distribution. The mobile device 200 does not need to retrieve the entire suggested OS distribution. The mobile device 200 may retrieve only the difference between the current operating system on the mobile device 200 and the suggested OS distribution.

[0030] Besides detecting the identity of the WiFi or mobile network that the mobile device 200 is connected to, the network detection module 210 may further detect the identity of the subscriber's number that the mobile device 200 is currently using. For instance, the network detections module 210 can detect that the current subscriber's number belong to an account for a corporation. A configuration of the operating system customized for this corporation is automatically pushed to the

mobile device 200. The mobile device 200 can then automatically change the look and feel of user interfaces of the mobile device 200, based on the received configuration of the operating system for that corporation account.

[0031] The mobile device 200 illustrated in the FIG. 2 can work with multiple mobile network carriers or telecommunication carriers. FIG. 3 illustrates an example of a carrier environment with which such mobile devices can switch operating systems based on the network. Multiple mobile devices 302, 304, 306 can work with one or more of mobile network carriers, 310, 320, 330. For instance, mobile device 302 may be configured to operate with carriers 310 and 320. Mobile device 304 may be configured to operate with carrier 320. Mobile device 306 may be configured to work with carriers 310 and 330. The network detections modules of the mobile devices 302, 304, 306 detect the carriers to which the mobile devices are currently connected. Accordingly, certain suggested OS distribution can be distributed to the mobile devices 302, 304, 306 based on the carriers to which the mobile devices are currently connected and on the particular mobile devices.

[0032] FIG. 4 illustrates an example of a message sequence chart for a mobile device 406 switching between telecommunication networks (also referred to as mobile networks). The mobile device 406 establishes a connection 400 with a network 408 by exchanging handshake messages. The network 408 can be a WiFi network, a mobile phone network, or other type of communication networks. After the establishment of the connection, the mobile device 406 detects that it established another connection 402 with another network 410. This can happen in various situations. For instance, the mobile device 406 may find itself out of the network 408 because it is no longer able to connect to the network 408. Then the mobile device 406 actively locates the network 410 and initiates the handshake process. Alternatively, the mobile device 406 keeps the connection with the network 408 (e.g. a mobile phone network), and then detects another type of network 410 (e.g. a WiFi network). The mobile device initiates the connection to the network 410 in order to be connected with both networks 408 and 410 (e.g., a mobile phone network and a WiFi network).

[0033] The network detections module of the mobile device 406 detects that the mobile device established a new connection with the network 410. The mobile device 406 then reports its network connection status 404 to a cloud storage service 414 via the network 410. Alternatively, the mobile device 406 can also report to the

cloud storage service 414 via the network 408 if it still connects with the network 408. The network connection status 404 can include information identifying both the mobile device 406 and the network 210.

[0034] Once the cloud storage service 414 receives the network connection status 404, it determines a corresponding OS distribution based on the mobile device 406 and the new connection with the network 410. The cloud storage service 414 transmits the OS distribution 420 to the mobile device 406. Alternatively, the cloud storage service 414 can transmit a location of the OS distribution 420 to the mobile device 406. The mobile device 406 can retrieve the OS distribution 420 based on the received location.

[0035] The mobile device 406 loads the OS distribution 420 and starts running the operating system. If the OS distribution 420 is a collection of customized user interface tweaks and pre-loaded applications, the mobile device 406 can load the collection as updates to the currently running operating system without restarting the device or operating system. If the OS distribution 420 is an operating system different from the currently running operating system, the mobile device 406 may need to restart (e.g., reboot) the device and then load the OS distribution 420.

[0036] FIG. 5 illustrates an example of an operating system (OS) loading process 500 based on the identity of the network. The OS loading process 500 starts at step 510, where a computing device starts executing a network identification process. The network identification process can include a device booting process or a network connection process. For instance, the computing device can start booting itself or start connecting a network at step 510. The network identification process can be triggered by various events, e.g., the computing device changing its location, the computing device booting up, a subscriber module of the computing device being replaced or inserted, or a previously scheduled network detecting event. The subscriber module can be a subscriber identification module (SIM) card.

[0037] At step 520 of the OS loading process 500, the computing device detects an identity of a network to which the computing device is connected or is to be connected, during the network identification process. The detection of the network can be achieved by examining the subscriber module (e.g. SIM card) electronically connected to the computing device. Alternatively, the detection of the network can be achieved by identifying a radio frequency of the network, or by

identifying a service set identification (SSID) of the network or a media access control (MAC) address of a gateway of the network.

[0038] Once the network is identified, at step 530, the computing device sends a request including the identity of the network to a remote registration service.

[0039] At step 540, the computing device receives an instruction from the remote registration service identifying a distribution of an operating system specific for the network. The instruction from the remote registration service responds to the request that the computer device sends. The instruction can include the location of the distribution of the operating system specific for the network. The distribution of the operating system can be customized based on the identity of the network. Alternatively, the distribution of the operating system can be customized based on both the identity of the network and an identity of a user of the computing device. For instance, the identity of the user can be associated with a corporate account for the user based on the subscriber number of the computing device, the user identity, or the network connected to the computing device.

[0040] Based on the received instruction, at step 550, the computing device requests and retrieves the distribution of the operating system, or a difference between the distribution of the operating system and an operating system currently installed on the computing device, from a cloud storage service. In some embodiments, the cloud storage service can share a common cloud service or a common cloud server with the remote registration service. In some alternative embodiments, the cloud storage service can be a dedicated server within the connected network, such as a wireless carrier's network.

[0041] After retrieving the OS distribution or the portion of the OS distribution that is different from the currently running OS, at step 560, the computing device loads the distribution of the operating system on the computing device. Such a loading can be a full over-the-air (OTA) update to the operating system that requires a reboot of the computing device. Alternatively, the loading can be an update of OS features (e.g. icons, user interfaces, pre-loaded apps) that does not require a reboot of the computing device.

[0042] At step 570, the computing device determines whether the loading requires a device reboot. If the loading requires a device reboot, the computing device reboots the computing device at step 574 and starts the loaded customized OS distribution at 578. If the loading does not require a device reboot, at step 580,

the computing device loads the distribution of the operating system on the computing device by applying customized features of the distribution to an operating system currently running on the computing device without restarting the computing device. The customized features can include pre-loaded applications or user interface designs. If the user identity is associated with a corporate account, the computing device can apply user interface settings or load pre-loaded applications specific for the corporate account onto the computing device.

[0043] FIG. 6 is a high-level block diagram showing an example of the architecture of a computer, which may represent any electronic device or any server within a cloud storage service as described herein. The server 600 includes one or more processors 610 and memory 620 coupled to an interconnect 630. The interconnect 630 shown in FIG. 6 is an abstraction that represents any one or more separate physical buses, point to point connections, or both connected by appropriate bridges, adapters, or controllers. The interconnect 630, therefore, may include, for example, a system bus, a Peripheral Component Interconnect (PCI) bus or PCI-Express bus, a HyperTransport or industry standard architecture (ISA) bus, a small computer system interface (SCSI) bus, a universal serial bus (USB), IIC (I2C) bus, or an Institute of Electrical and Electronics Engineers (IEEE) standard 1394 bus, also called “Firewire”.

[0044] The processor(s) 610 is/are the central processing unit (CPU) of the server 600 and, thus, control the overall operation of the server 600. In certain embodiments, the processor(s) 610 accomplish this by executing software or firmware stored in memory 620. The processor(s) 610 may be, or may include, one or more programmable general-purpose or special-purpose microprocessors, digital signal processors (DSPs), programmable controllers, application specific integrated circuits (ASICs), programmable logic devices (PLDs), trusted platform modules (TPMs), or the like, or a combination of such devices.

[0045] The memory 620 is or includes the main memory of the server 600. The memory 620 represents any form of random access memory (RAM), read-only memory (ROM), flash memory, or the like, or a combination of such devices. In use, the memory 620 may contain a code 670 containing instructions according to the techniques disclosed herein.

[0046] Also connected to the processor(s) 610 through the interconnect 630 are a network adapter 640 and a storage adapter 650. The network adapter 640

provides the server 600 with the ability to communicate with remote devices, over a network and may be, for example, an Ethernet adapter or Fibre Channel adapter. The network adapter 640 may also provide the server 600 with the ability to communicate with other computers. The storage adapter 650 allows the server 600 to access a persistent storage, and may be, for example, a Fibre Channel adapter or SCSI adapter.

[0047] The code 670 stored in memory 620 may be implemented as software and/or firmware to program the processor(s) 610 to carry out actions described above. In certain embodiments, such software or firmware may be initially provided to the server 600 by downloading it from a remote system through the server 600 (e.g., via network adapter 640).

[0048] The techniques introduced herein can be implemented by, for example, programmable circuitry (e.g., one or more microprocessors) programmed with software and/or firmware, or entirely in special-purpose hardwired circuitry, or in a combination of such forms. Special-purpose hardwired circuitry may be in the form of, for example, one or more application-specific integrated circuits (ASICs), programmable logic devices (PLDs), field-programmable gate arrays (FPGAs), etc.

[0049] Software or firmware for use in implementing the techniques introduced here may be stored on a machine-readable storage medium and may be executed by one or more general-purpose or special-purpose programmable microprocessors. A "machine-readable storage medium", as the term is used herein, includes any mechanism that can store information in a form accessible by a machine (a machine may be, for example, a computer, network device, cellular phone, personal digital assistant (PDA), manufacturing tool, any device with one or more processors, etc.). For example, a machine-accessible storage medium includes recordable/non-recordable media (e.g., read-only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; etc.), etc.

[0050] The term "logic", as used herein, can include, for example, programmable circuitry programmed with specific software and/or firmware, special-purpose hardwired circuitry, or a combination thereof.

[0051] In addition to the above mentioned examples, various other modifications and alterations of the invention may be made without departing from the invention. Accordingly, the above disclosure is not to be considered as limiting

and the appended claims are to be interpreted as encompassing the true spirit and the entire scope of the invention.

CLAIMS

What is claimed is:

1. A computer-implemented method comprising:

detecting an identity of a network to which a computing device is connected or is to be connected, during a network identification process executed on the computing device;

sending a request including the identity of the network to a remote registration service;

receiving an instruction from the remote registration service identifying a distribution of an operating system specific for the network; and

loading the distribution of the operating system on the computing device.

2. The computer-implemented method of claim 1, wherein the network identification process is a device booting process or a network connection process.

3. The computer-implemented method of claim 1, wherein the network identification process is triggered by an event of the computing device changing its location, an event of the computing device booting up, an event of a subscriber module of the computing device being replaced, or a scheduled network detecting event.

4. The computer-implemented method of claim 1, wherein the detecting comprises:

detecting an identity of a network to which a computing device is connected or is to be connected, during a booting process executed on the computing device, by examining a subscriber module electronically connected to the computing device.

5. The computer-implemented method of claim 4, wherein the subscriber module is a subscriber identification module (SIM) card.

6. The computer-implemented method of claim 1, wherein the detecting comprises:

detecting an identity of a network to which a computing device is connected or is to be connected, during a booting process executed on the computing device, by identifying a radio frequency of the network.

7. The computer-implemented method of claim 1, wherein the detecting comprises:

detecting an identity of a network to which a computing device is connected or is to be connected, during a booting process executed on the computing device, by identifying a service set identification (SSID) of the network or a media access control (MAC) address of a gateway of the network.

8. The computer-implemented method of claim 1, further comprising:

retrieving the distribution of the operating system, or a difference between the distribution of the operating system and an operating system currently installed on the computing device, from a cloud storage service.

9. The computer-implemented method of claim 1, wherein the instruction from the remote registration service includes a location where the distribution of the operating system is stored.

10. The computer-implemented method of claim 1, wherein the distribution of the operating system is customized based on the identity of the network.

11. The computer-implemented method of claim 1, wherein the distribution of the operating system is customized based on the identity of the network and an identity of a user of the computing device.

12. The computer-implemented method of claim 1, wherein the loading comprises:

loading the distribution of the operating system on the computing device by restarting the computing device.

13. The computer-implemented method of claim 1, wherein the loading comprises:

loading the distribution of the operating system on the computing device by applying customized features of the distribution to an operating system currently running on the computing device without restarting the computing device.

14. The computer-implemented method of claim 13, wherein the customized features include pre-loaded applications or user interface designs.

15. The computer-implemented method of claim 1, further comprising:

identifying a corporate account for the user based on the a subscriber number of the computing device, a user identity, or the network connected to the computing device; and

applying user interface settings or loading pre-loaded applications specific for the corporate account onto the computing device.

16. An electronic device comprising:

a processor;

a network component configured to communicate with a remote registration service; and

a memory component storing instructions which, when executed by the processor, cause the electronic device to perform a process including:

detecting an identity of a network to which an electronic device is connected or is to be connected, during a device booting process executed on the electronic device;

sending a request including the identity of the network to the remote registration service;

receiving an instruction from the remote registration service identifying a distribution of an operating system specific for the network; and

loading the distribution of the operating system on the electronic device during the device booting process.

17. The electronic device of claim 16, further comprising:

a circuitry configured to electronically connect to a subscriber identification module (SIM) card such that the identity of the network can be detected by examining the subscriber module.

18. The electronic device of claim 16, wherein the detecting comprises:

detecting an identity of a network to which a computing device is connected or is to be connected, during a device booting process executed on the computing device.

19. The electronic device of claim 16, further comprising:

a data retrieving component configured to retrieve the distribution of the operating system.

20. The electronic device of claim 16, further comprising:

a data retrieving component configured to retrieve a difference between the distribution of the operating system and an operating system currently running on the electronic device.

21. A method, comprising:

identifying a subscriber module being inserted into an electronic device;

retrieving an operating system from a cloud storage system, wherein the operating system is customized based on an identity of the subscriber module; and

executing the operating system on the electronic device so that the operating system replaces an original operating system on the electronic device.

22. The method of claim 21, wherein the subscriber module contains identity information of a subscriber of a network.

23. The method of claim 21, wherein the subscriber module includes subscriber information being used to identify a network for the subscriber module and the operating system is customized for the network.

24. The method of claim 21, further comprising:

determining an identity of a user of the subscriber module based on the information in subscriber module; and

sending a request including the identity of the user to a registration server, wherein the registration server determines an operating system for the user.

25. The method of claim 21, further comprising:

determining an identity of an organization owning the subscriber module based on information in the subscriber module; and

sending a request including the identity of the organization to a registration server, wherein the registration server determines an operating system for the organization.

26. An apparatus comprising:

means for determining a subscriber identity based on a subscriber module electronically connected to an electronic device;

means for sending a request including the subscriber identity;

means for retrieving an operating system for the electronic device customized based on the subscriber identity from a cloud storage; and

means for running the operating system on the electronic device.

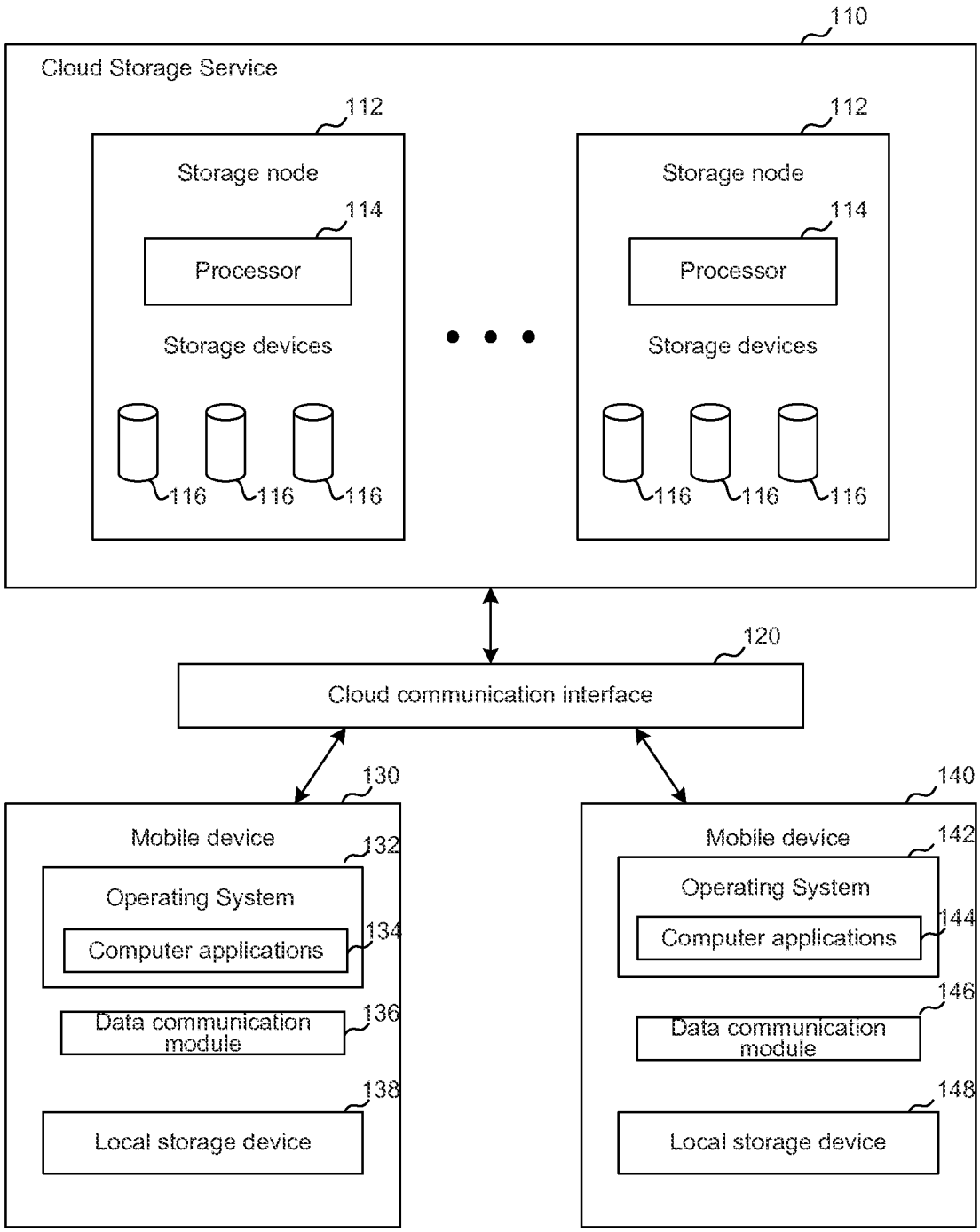
110
Cloud Storage Service
112
Storage node
114
Processor
Storage devices
116
116
116
112
Storage node
114
Processor
Storage devices
116
116
116
120
Cloud communication interface
130
Mobile device
132
Operating System
134
Computer applications
136
Data communication module
138
Local storage device
140
Mobile device
142
Operating System
144
Computer applications
146
Data communication module
148
Local storage device

FIG. 1

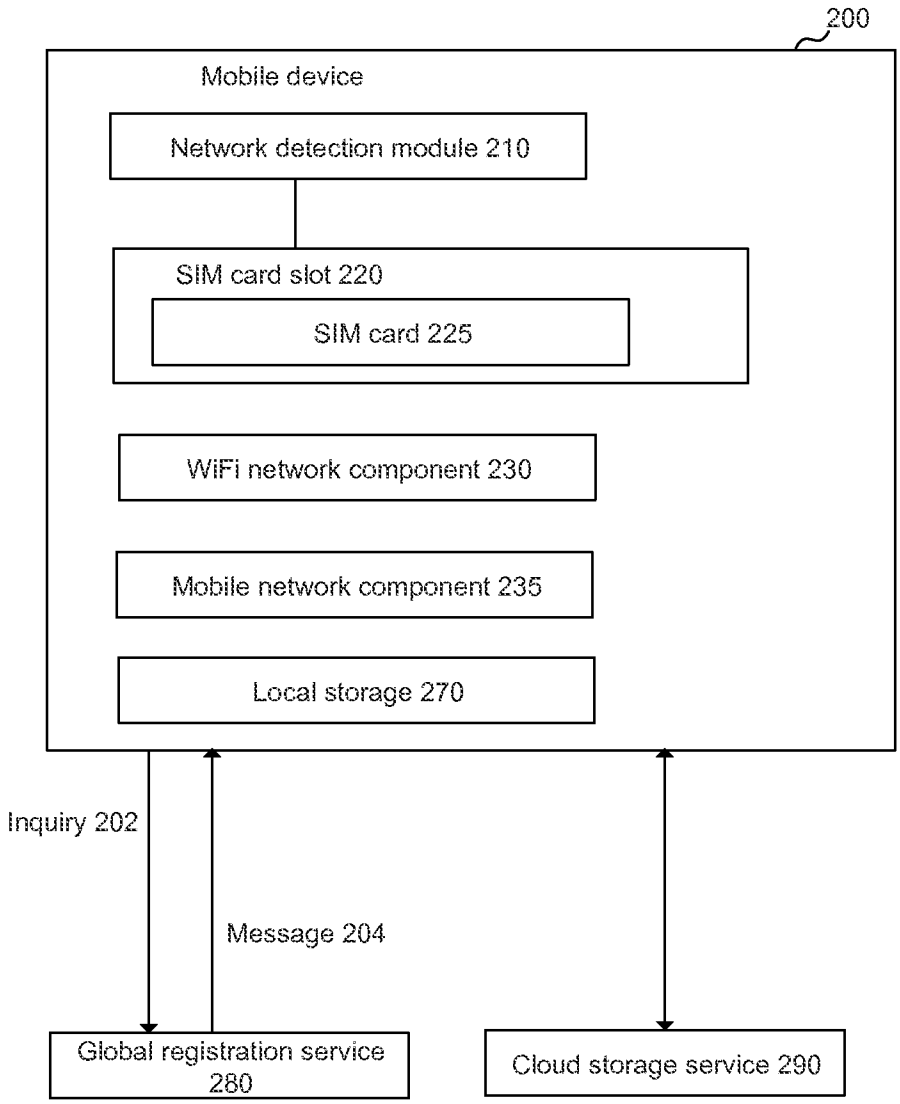
200
Mobile device
Network detection module 210
SIM card slot 220
SIM card 225
WiFi network component 230
Mobile network component 235
Local storage 270
Inquiry 202
Message 204
Global registration service 280
Cloud storage service 290

FIG. 2

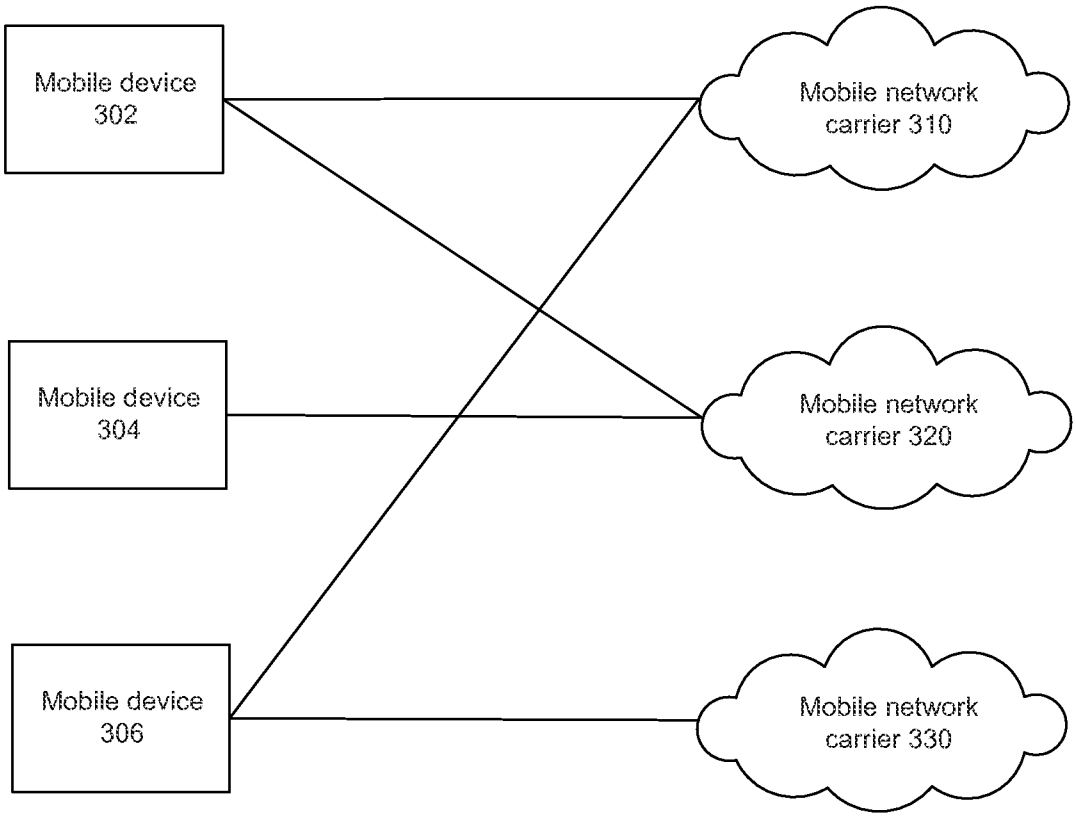
Mobile device 302
Mobile device 304
Mobile device 306
Mobile network carrier 310
Mobile network carrier 320
Mobile network carrier 330

FIG. 3

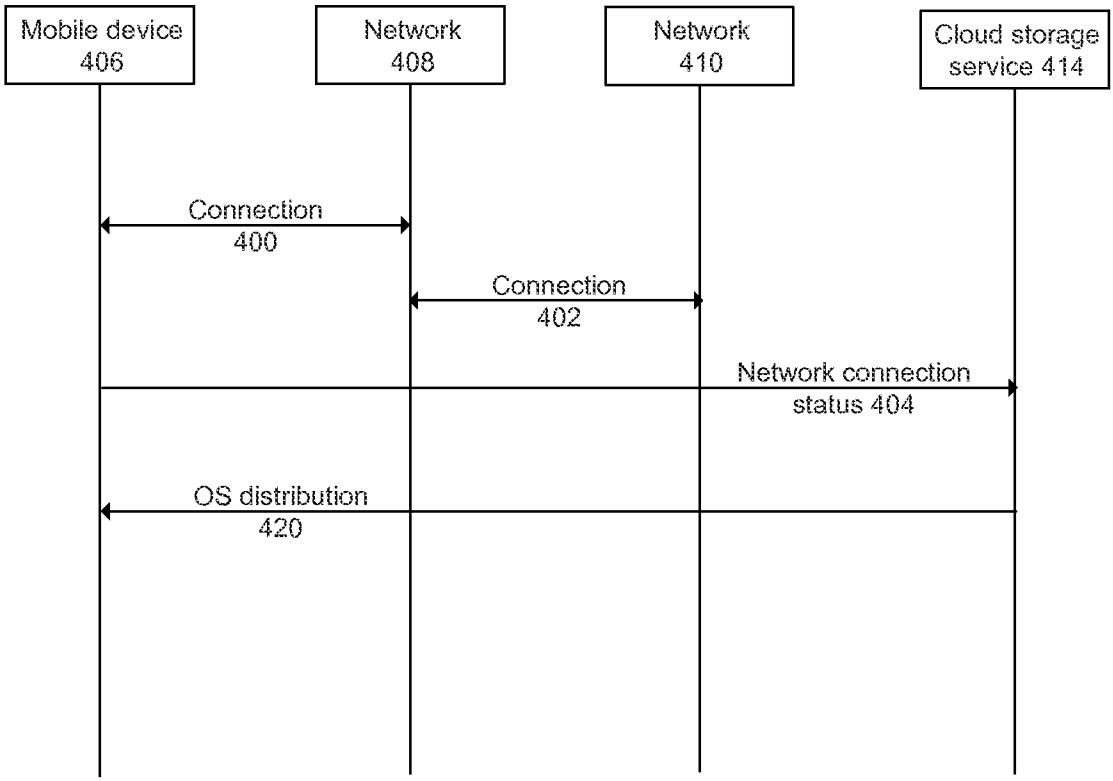
Mobile device
406
Network
408
Network
410
Cloud storage
service 414
Connection
400
Connection
402
Network connection
status 404
OS distribution
420

FIG. 4

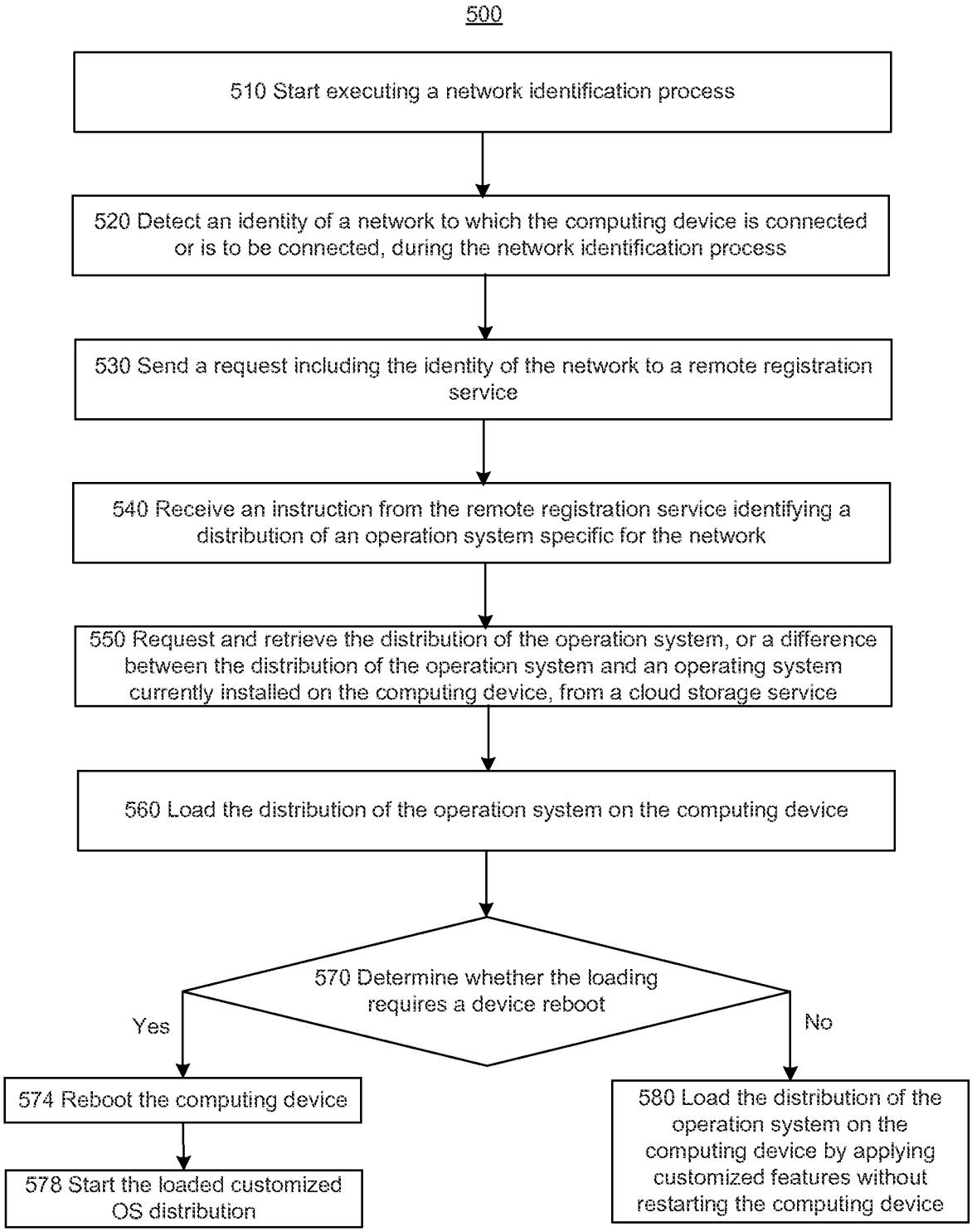
500
510 Start executing a network identification process
520 Detect an identity of a network to which the computing device is connected or is to be connected, during the network identification process
530 Send a request including the identity of the network to a remote registration service
540 Receive an instruction from the remote registration service identifying a distribution of an operation system specific for the network
550 Request and retrieve the distribution of the operation system, or a difference between the distribution of the operation system and an operating system currently installed on the computing device, from a cloud storage service
560 Load the distribution of the operation system on the computing device
570 Determine whether the loading requires a device reboot
Yes
No
574 Reboot the computing device
578 Start the loaded customized OS distribution
580 Load the distribution of the operation system on the computing device by applying customized features without restarting the computing device

FIG. 5

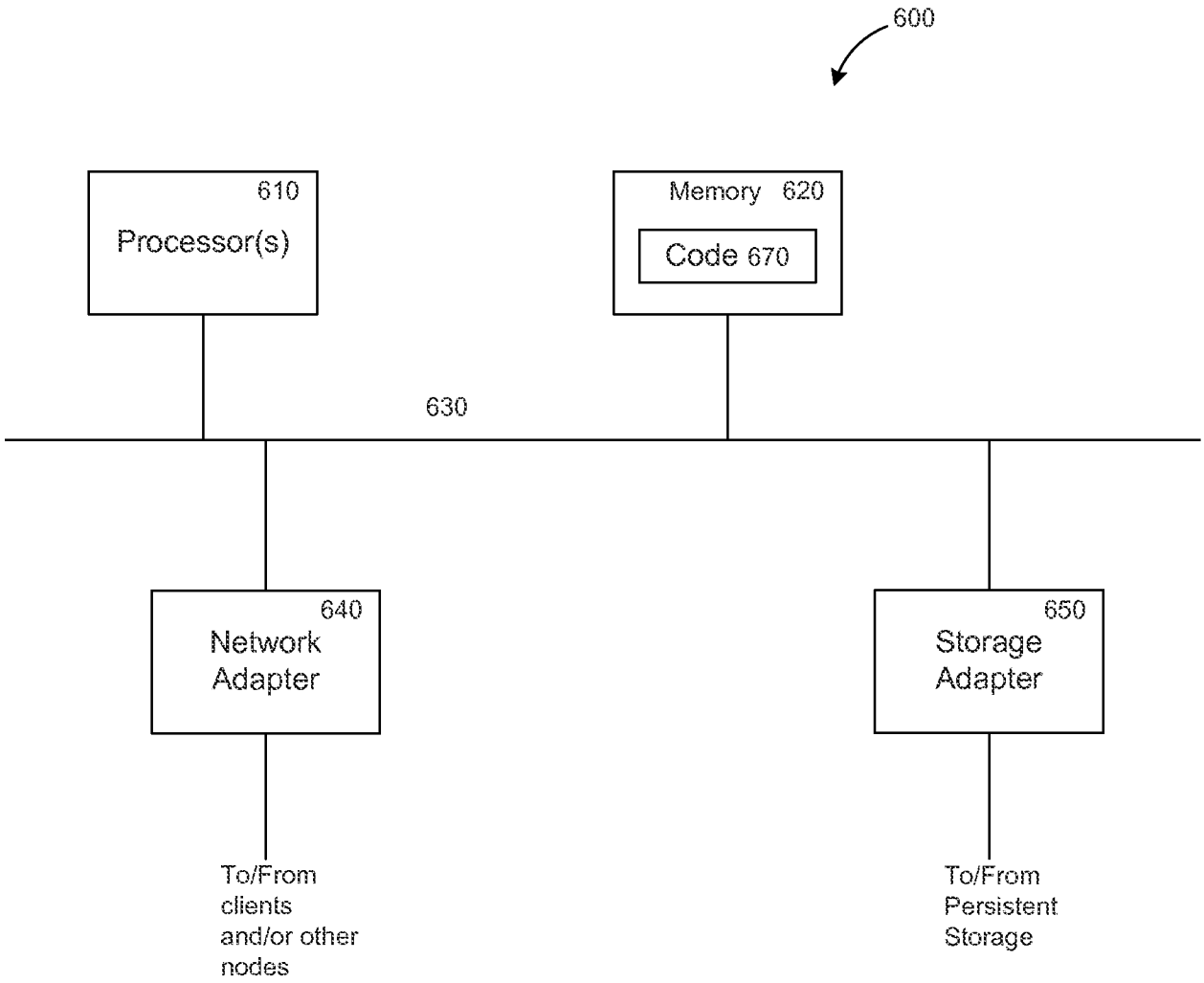
600
610
Processor(s)
Memory 620
Code 670
630
640
Network Adapter
650
Storage Adapter
To/From clients and/or other nodes
To/From Persistent Storage

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/062733

A. CLASSIFICATION OF SUBJECT MATTER

G06F 15/16(2006.01)i, G06F 9/06(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)
G06F 15/16; G06F 15/173; G06F 12/00; H04L 29/06; H04L 12/28; H04L 12/56; G06F 13/00; G06F 9/06

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:distributed network, subscriber, remote, registratio, distribution

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2008-0077966 A (MICROSOFT CORP.) 26 August 2008 See abstract; paragraphs [20]-[25], [27]-[29], [40], [48]; claims 1-9 and figures 1-4.	1-26
A	JP 2002-530014 A (Telefonaktiebolaget L M Ericsson) 10 September 2002 See paragraphs [11]-[13], [44]; claims 10-22 and figures 2-7.	1-26
A	JP 2003-196135 A (MITSUBISHI ELECTRIC CORP) 11 July 2003 See paragraphs [23],[31]; claims 1-15 and figure 1.	1-26
A	EP 2001194 A2 (KING`S COLLEGE LONDON) 10 December 2008 See paragraphs [14]-[33], [40]; claims 1-3 and figures 2-5.	1-26

☐ 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
30 December 2013 (30.12.2013)	**31 December 2013 (31.12.2013)**

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
HONG, Kyoung Ah
Telephone No. +82-42-481-5668

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2013/062733

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR 10-2008-0077966 A	26/08/2008	AU 2006-320927 A1	07/06/2007
		AU 2006-320927 B2	17/03/2011
		CA 2624273 A1	07/06/2007
		CN 101322114 A	10/12/2008
		EP 1955181 A1	13/08/2008
		JP 04-801169 B2	26/10/2011
		JP 2009-518883 A	07/05/2009
		US 2007-0130304 A1	07/06/2007
		US 7606937 B2	20/10/2009
		WO 2007-064415 A1	07/06/2007
JP 2002-530014 A	10/09/2002	AU 2000-15913 A1	29/05/2000
		CN 1154322 C0	16/06/2004
		CN 1332924 A0	23/01/2002
		EP 1129558 A1	05/09/2001
		US 6304913 B1	16/10/2001
		WO 00-28713 A1	18/05/2000
JP 2003-196135 A	11/07/2003	JP 4113354 B2	09/07/2008
EP 2001194 A2	10/12/2008	EP 2001194 A3	19/12/2012
		GB 2449923 A	10/12/2008
		US 2008-0304458 A1	11/12/2008