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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 September 2017 (08.09.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/151161 A1

(51) International Patent Classification:
G06F 11/30 (2006.01) *G06F 15/16* (2006.01)

(21) International Application Number:
PCT/US2016/030200

(22) International Filing Date:
29 April 2016 (29.04.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201641007754 4 March 2016 (04.03.2016) IN

(71) Applicant: **HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP** [US/US]; 11445 Compaq Center Drive W., Houston, Texas 77070 (US).

(72) Inventors: **SHIVANNA, Suhas**; Sy.No.192, Whitefield Road, Mahadevapura Post, Bangalore 560048 (IN). **SALEEM, Mohammed**; Sy.No.192, Whitefield Road, Mahadevapura Post, Bangalore IN (IN). **VARADARAJAN SAHASRANAMAM, Srinivasan**; Sy.No.192, Whitefield Road, Mahadevapura Post, Bangalore 560048 (IN). **SHENOY, Ananth Yelthimar**; Sy.No.192, Whitefield Road, Mahadevapura Post, Bangalore 560048 (IN). **RAJAGOPALAN, Srinivasa Ragavan**; Sy.No.192, Whitefield Road, Mahadevapura Post, Bangalore 560048 (IN).

(74) Agent: **SURESH, Anup A.**; 3000 Hanover St, Palo Alto, California 94304 (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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[Continued on next page]

(54) Title: DETECTING ANOMALIES OF DEVICES

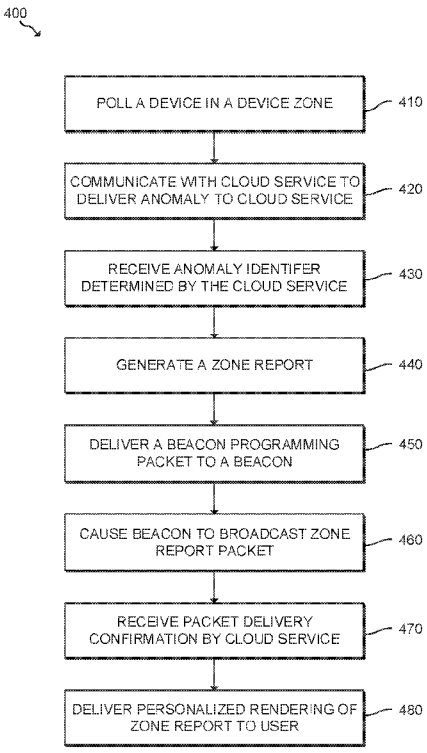

FIG. 4

(57) Abstract: Some examples relate to detecting anomalies of devices. The examples disclosed herein enable polling a device in a zone covered by the computing 5 device. In response to detecting an anomaly of the device in the zone, examples herein enable configuring a beacon to generate a zone report packet. The zone report packet may include a location of the device in the zone, an anomaly identifier determined by analyzing a detected symptom associated with the anomaly, and instructions for a particular user 10 type. Examples enable causing the beacon to broadcast the zone report packet to be received by a user device associated with a user of the particular user type.

WO 2017/151161 A1

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

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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

BACKGROUND

[0001] Computing devices may be organized and stored together in various ways. Vast numbers of devices may be housed together, such as in a datacenter. Data centers often contain large fleets of computing equipment, which are often organized in racks and related infrastructures. A typical data center typically houses thousands of computers and related hardware such as networking gear. Managers of the datacenter may monitor the status and health of the devices by keeping track of the devices.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] The following detailed description references the drawings, wherein:

[0003] FIG. 1 is a block diagram depicting an example computing device for detecting anomalies of devices;

[0004] FIG. 2 is a block diagram depicting an example environment in which various examples may be implemented as a system for detecting anomalies of devices;

[0005] FIG. 3 is a block diagram depicting an example system for detecting anomalies of devices;

[0006] FIG. 4 is a block diagram depicting an example method for detecting computing device anomalies; and

[0007] FIG. 5 is a schematic diagram of an example environment having devices being monitored by example systems for detecting anomalies of devices.

DETAILED DESCRIPTION

[0008] With the rapid growth in the use of computers to host business applications, websites, cloud, etc., the need for larger data centers to house computing hardware has also grown rapidly. A data center or server farm is a facility to house computer systems and related equipment (e.g., storage, networking switches, routers, etc.). For example, a business or organization may house all or some of its computer servers (i.e., hosts) at a set of physical locations in order to manage these systems effectively. The computer systems in a data center may be connected to clients via the Internet, Wide Area Network, Local Area Network, or other medium. Servers often host critical applications of a business, which may depend on the continuous operation and reliability of the servers. Management of the health and status of computing servers and other devices can be critical in responding to events that require manual intervention and in maintaining reliability of computing resources.

[0009] Examples disclosed herein provide for detecting anomalies of devices. The examples disclosed herein enable polling a device in a zone covered by the computing device. In response to detecting an anomaly of the device in the zone, examples herein enable configuring a beacon to generate a zone report packet. The zone report packet may include a location of the device in the zone, an anomaly identifier determined by analyzing a detected symptom associated with the anomaly, and instructions for a particular user type. Examples enable causing the beacon to broadcast the zone report packet to be received by a user device associated with a user of the particular user type. In this manner, examples may provide detecting anomalies of a device and reporting that anomaly to a particular user who may then take action on detected anomalies.

[0010] Referring now to the drawings, FIG. 1 is an example computing device 100 for detecting anomalies of devices. Computing device 100 may be an electronic device capable of performing the functions to be described herein. For example, computing device 100 may be a particular-purpose device, or it may be implemented as other devices such as servers, integrated or distributed devices, personal computing devices, all-in-one computing devices, tablet or other mobile computing device, mobile phones, electronic

book readers, network-enabled appliances, and/or other suitable electronic devices. As shown in FIG. 1, computing device 100 may include a processor 110 and a non-transitory machine-readable storage medium 120.

[0011] Processor 110 may be at least one central processing unit (CPU), microprocessor, and/or other hardware device suitable for retrieval and execution of instructions stored in machine-readable storage medium 120. Processor 110 may fetch, decode, and execute instructions 121, 122, 123, and/or other instructions. As an alternative or in addition to retrieving and executing instructions, processor 110 may include at least one electronic circuit comprising a number of electronic components for performing the functionality of at least one of instructions 121, 122, 123, and/or other instructions.

[0012] Machine-readable storage medium 120 may be any electronic, magnetic, optical, or other physical storage device that contains or stores executable instructions. In some implementations, machine-readable storage medium 120 may be a non-transitory storage medium, where the term "non-transitory" does not encompass transitory propagating signals. Machine-readable storage medium 120 may be implemented in a single device or distributed across devices. Likewise, processor 110 may represent any number of processors capable of executing instructions stored by machine-readable storage medium 120. Processor 110 may be integrated in a single device or distributed across devices. Further, machine-readable storage medium 120 may be fully or partially integrated in the same device as processor 110, or it may be separate but accessible to that device and processor 110.

[0013] In one example, the program instructions may be part of an installation package that, when installed, can be executed by processor 110. In this case, machine-readable storage medium 120 may be a portable medium such as a floppy disk, CD, DVD, or flash drive or a memory maintained by a server from which the installation package can be downloaded and installed. In another example, the program instructions may be part of an application or applications already installed. Here, machine-readable storage medium 120 may include a hard disk, optical disk, tapes, solid state drives, RAM, ROM, EEPROM, or the like.

[0014] Polling device in zone instructions 121, when executed by processor 110, may poll a device in a zone covered by the computing device 100. For example, polling device in zone instructions 121 may send a status request to the device in the zone and await a response. Alternatively, polling device in zone instructions 121 may be subscribed to status alerts from the device. In some examples, polling device in zone instructions 121 may poll the device in the zone by wireless communication. For example, the device and the computing device 100 may communicate via Wi-Fi, Bluetooth, cloud network, or other forms of wireless electronic communication. Alternatively, the device and the computing device 100 may be physically connected, either directly or through a network such as the internet.

[0015] The device may be in a zone, which may be an established geographic area. In some examples, a zone may cover a plurality of devices in an established geographic area. For example, a zone may be a datacenter or a particular area within a datacenter. Polling device in zone instructions 121 may be responsible for monitoring the plurality of devices in the zone by polling the devices in the zone.

[0016] The device in the zone may be any device that has a status or other information that may be polled by polling device in zone instructions 121. For example, the device may be a computing system in a datacenter. Other examples of devices may be storage devices, switches and networking equipment, as well as personal devices. In a specific example, the zone may cover all of the devices of a particular section of a datacenter. For example, the zone may cover all devices on a particular rack. Polling device in zone instructions 121 in such an example, monitors the health and status of the devices on that particular rack. Other examples of information that may be polled include power consumption, processor usage, memory capacity, device temperature, and various other data.

[0017] Beacon programming instructions 122, when executed by processor 110, may configure a beacon to generate a zone report packet. Beacon programming instructions 122 may do so in response to the computing device 100 detecting an anomaly of the device in the zone, through the execution of polling device in zone instructions 121. Beacon programming instructions 122 may configure a beacon by communicating configuration instructions to the beacon.

[0018] The beacon may be any device or component that may broadcast data packets. For example, a beacon may be able to broadcast packets wireless, such as via Bluetooth. As described in detail later, a beacon may be a separate device wirelessly connected to the computing device 100 or it may be a built-in connectivity engine of the computing device 100. The beacon may receive configuration instructions from beacon programming instructions 122 wirelessly or by a physical connection. The beacon may include antennas or other components for broadcasting communication packets.

[0019] A beacon may generate a zone report packet, which may include data to be communicated through a network. A zone report packet may include, among other information, a location of the device in the zone, an anomaly identifier determined by analyzing a detected symptom associated with the anomaly, and an instruction for a particular user type. For example, a zone report packet may contain universally unique identifiers, major codes, and minor codes to carry the various information. In some examples, the location of the device in the zone may be a relative position among the plurality of devices covered by the zone.

[0020] The anomaly identifier may be determined by analyzing a detected symptom associated with the anomaly. For example, when an anomaly is detected, computing device 100 may also receive metadata about the symptoms of the anomaly. For example, beacon programming instructions 122 may determine that the device is performing slowly, is unresponsive, or is overloaded. Each symptom may be associated with particular anomalies. After analyzing the symptoms, an identity of the anomaly may be determined and programmed to the zone report packet.

[0021] The instructions for a particular user type may be a set of instructions that may determine the information that is presented to a user of the particular user type. For example, different user types may be interested in different information about a particular anomaly. For instance, a datacenter maintenance engineer may be interested in viewing the details of a particular anomaly caused by a particular device, while a network administrator may be interested in viewing the overall performance metrics of the datacenter. The instructions for a particular user type may facilitate the communication of pertinent information to particular users.

[0022] Beacon broadcasting instructions 123, when executed by processor 110, may cause a beacon to broadcast the zone report packet generated in the execution of beacon programming instructions 122 to be received by a user device associated with a user of a particular user type. For example, the zone report packet may be broadcast within a particular range of the beacon. When a user device enters the range of the beacon, the zone report packet may be picked up by the user device, which may communicate the zone report packet to the user. How the user device may do so is explained herein in relation to later figures.

[0023] Furthermore, computing device 100 may include additional functionalities, some of which is further discussed herein in reference below to FIG. 2-5.

[0024] FIG. 2 is an example environment 200 in which various examples may be implemented as a computing device for detecting anomalies of devices 210. Environment 200 may include various components including a device zone 220 of a plurality of devices 225 (illustrated as 225A, 225B, 225C). Each device 225A, 225B, 225C may communicate with computing device 210. For example, computing device 210 may be subscribed to status alerts from devices 225A, 225B, 225C. Similarly, computing device 210 may continuously poll devices 225A, 225B, 225C for status updates. Devices 225A, 225B, 225C may be any type of device which may be monitored for anomalies by computing device 210. For example, the devices of device zone 220 may include servers, integrated or distributed computing devices, personal computing devices, all-in-one computing devices, tablet or other mobile computing device, mobile phones, electronic book readers, network-enabled appliances such as “Smart” televisions, and/or other suitable electronic devices. While each device is depicted as a single device, devices 225A, 225B, 225C may include any number of integrated or distributed computing systems.

[0025] Furthermore, environment 200 may include beacon 230 operably coupled to computing device 210. Beacon 230 may be a communications device that may broadcast computer communication. For example, beacon 230 may broadcast a data packet generated by computing device 210.

[0026] The various components (e.g., components 210, 230) depicted in FIG. 2 may be coupled to at least one other component via a network 250. Network 250 may comprise any infrastructure or combination of infrastructures that enable electronic communication

between the components. For example, network 250 may include at least one of the Internet, an intranet, a PAN (Personal Area Network), a LAN (Local Area Network), a WAN (Wide Area Network), a SAN (Storage Area Network), a MAN (Metropolitan Area Network), a wireless network, a cellular communications network, a Public Switched Telephone Network, and/or other network. According to various implementations, computing device 210 and the various components described herein may be implemented in hardware and/or a combination of hardware and programming that configures hardware. Furthermore, in FIG. 2 and other Figures described herein, different numbers of components or entities than depicted may be used.

[0027] A cloud service 260 may be connected to the other components of environment 200 by network 250. Cloud service 260 may receive information from the other components, perform functionalities, and send information to the other components. Cloud service 260 may include any resource that can be provided to environment 200 over network 250.

[0028] Computing device 210 may comprise a polling device in zone engine 211, a beacon programming engine 212, a causing beacon broadcasting engine 213, and personalized rendering engine 214. In some examples, computing device 210 may include additional or alternative engines. The term "engine", as used herein, may refer to a combination of hardware and programming that performs a designated function. For example as illustrated in FIG. 1, the hardware of each engine, for example, may include one or both of a processor and a machine-readable storage medium, while the programming is instructions or code stored on the machine-readable storage medium and executable by the processor to perform the designated function. In addition or as an alternative, each engine may include a set of hardware devices including electronic circuitry for implementing the functionality described below.

[0029] Polling computing devices engine 211 may poll a device 225 in zone 220. For instance, polling computing devices engine 211 may send a status request to the devices 225 in zone 220 and await a response. Alternatively, engine 211 may be subscribed to status alerts from the device 225. Zone 220 may cover an established geographic area, and may be, for example, a datacenter or a particular area within a datacenter.

[0030] Beacon programming engine 212 may configure beacon 230 to generate a zone report packet. Beacon programming engine 212 may do so in response to the computing device 210 detecting an anomaly of a device 225 in the zone 220. Beacon programming engine 212 may configure a beacon by communicating configuration instructions to the beacon 230, which may be any device or component that may broadcast data packets. Beacon is shown as a separate component from the computing device 210, but in some examples, beacon may be a built-in component of the computing device 210.

[0031] Beacon 230 may generate a zone report packet, which may include data to be communicated through a network. A zone report packet may include, among other information, a location of the device in the zone, an anomaly identifier determined by analyzing a detected symptom associated with the anomaly, and an instruction for a particular user type.

[0032] The anomaly identifier may be determined by analyzing a detected symptom associated with the anomaly. For example, computing device 210 may receive anomaly information from polling the devices 225, and send the information to cloud service 260. Cloud service 260 may perform the functionality for determining the anomaly identifier. After analyzing the symptoms, an identity of the anomaly may be determined and programmed to the zone report packet.

[0033] The instructions for a particular user type may be a set of instructions that may determine the information that is presented to a user of the particular user type. For example, different user types may be interested in different information about a particular anomaly. The instructions for a particular user type may facilitate the communication of pertinent information to particular users.

[0034] Causing beacon broadcasting engine 213 may cause beacon 230 to broadcast the zone report packet generated by beacon programming engine 212 to be received by a user device 240 associated with a user of a particular user type. For example, the zone report packet may be broadcast within a particular range of the beacon 230. When user device 240 enters the range of the beacon 230, the zone report packet may be picked up by the user device 240, which may communicate the zone report packet to the user.

[0035] In response to user device 240 receiving the zone report packet, personalized rendering engine 214 may cause to deliver, to the user device 240, a personalized rendering of the zone report packet based on the instructions for the particular user type. The personalized rendering may inform the user of user device 240 of a particular action to address the anomaly. Specifically, the personalized rendering may include information pertinent to the particular user type, and may include a particular visualization and other information.

[0036] In some examples, the personalized rendering of the zone report may be delivered from cloud services 260 via network 250. For example, when user device 240 receives the zone report packet, user device 240 may send a zone report packet delivery confirmation packet to cloud services 260 via network 250. Knowing that the zone report packet has been delivered to a user device 240 of a particular user type, cloud services 260 delivers the personalized rendering of the zone report to the user device 240. In some instances, the instructions to instruct user device 240 to send the zone report packet delivery confirmation packet may itself be programmed in the zone report packet that was caused by engine 213 to be delivered to user device 240.

[0037] FIG. 3 shows an example device anomaly detecting system 300 for detecting anomalies of devices. System 300 may include polling engine 311, beacon programming engine 312, cloud services engine 313, and beacon 320. Beacon 320 may itself include a packet receiving engine 321 and broadcasting engine 322. FIG. 3 performs similar functionality with the examples shown and described with relation to FIG. 1 and FIG. 2, and will be described with reference to FIG. 5 to illustrate the operation of system 300.

[0038] System 300 may represent a system 510E in the environment shown in FIG. 5. For example, FIG. 5 may illustrate a datacenter, where the datacenter is partitioned to various zones 515A, 515B, 515C, 515D, and 515E. Systems 510A-510E may detect anomalies of the devices of the respective zones 515. For example, system 300, which is illustrated as system 510E, may have polling engine 311 poll a plurality of devices 520E of zone 515E.

[0039] Upon receiving an anomaly from a device, such as device 525, beacon programming engine 312 may configure beacon 320 to generate a zone report packet. As illustrated in FIG. 3, beacon 320 may be a built-in communications engine of the system

300. The zone report packet may include, among other information, a location of the device in the zone, an anomaly identifier determined by analyzing a detected symptom associated with the anomaly, and an instruction for a particular user type. To determine the anomaly identifier, cloud services engine 313 may deliver the anomaly along with anomaly symptoms to a cloud service, which may determine the anomaly identifier by running functionality to analyze the symptoms associated with the anomaly.

[0040] Upon receiving the instructions to generate a zone report packet by packet receiving engine 321, beacon 320 may broadcast the zone report packet by broadcast engine 322. As an illustration, a zone report packet may be communicated via wireless communication 531 from system 510E. A user device 540 of a particular user type 545 may receive the zone report packet by wireless communication 532 when the user device 540 is in range.

[0041] Upon user device 540 receiving the zone report packet, user device 540 may send a zone report packet delivery confirmation packet to the cloud services. In response to acknowledging that the zone report packet has been delivered to a user device 540 of the particular user type 545, the cloud services may generate a personalized rendering of the zone report and deliver that personalized rendering to the user device 540 to be accessed by the particular user type 545.

[0042] FIG. 4 is a flow diagram depicting an example method 400 for detecting computing device anomalies. The various processing blocks and/or data flows depicted in FIG. 4 are described in greater detail herein. The described operations may be accomplished using some or all of the system components described in detail above and, in some implementations, various operations may be performed in different sequences and various operations may be omitted. Additional operations may be performed along with some or all of the operations shown in the depicted flow diagrams. Some operations may be performed simultaneously. Accordingly, method 400 as illustrated (and described in greater detail below) is meant be an example and, as such, should not be viewed as limiting. Method 400 may be implemented in the form of executable instructions stored on a machine-readable storage medium, such as by computing device 210, and/or in the form of electronic circuitry.

[0043] In an operation 410, method 400 may include polling a device in a device zone. For instance, the zone may cover an established geographic area, and may be, for example, a datacenter or a particular area within a datacenter. Referring to FIG. 2, polling device in zone engine 211 may be responsible for implementing operation 410.

[0044] In an operation 420, method 400 may include communicating with a cloud service to deliver an anomaly to cloud service. The cloud service may analyze symptoms of the anomaly to determine an anomaly identifier for the anomaly. In an operation 430, method 400 may include receiving the anomaly identifier determined by the cloud service. Referring to FIG. 2, cloud services 260 may determine the anomaly identifier which is then received by beacon programming engine 212 of computing device 210.

[0045] In an operation 440, method 400 may include generating a zone report. For example, a zone report may include a location of the device in the zone, an anomaly identifier determined by analyzing a detected symptom associated with the anomaly, and an instruction for a particular user type. Referring to FIG. 2, beacon programming engine 212 may cause beacon 230 to generate the zone report for zone 220. Alternatively, computing device 210 may generate the zone report, which then sent to the beacon 230.

[0046] In an operation 450, method 400 may include delivering a beacon programming packet to a beacon. Referring to FIG. 2, beacon programming engine 212 may deliver the beacon programming packet to beacon 230 to generate the zone report for zone 220

[0047] In an operation 460, method 400 may include causing beacon to broadcast a zone report packet to be received by a user device associated with a user of a particular user type. Referring to FIG. 2, for example, the zone report packet may be broadcast within a particular range of beacon 230. When user device 240 enters the range of the beacon 230, the zone report packet may be picked up by the user device 240.

[0048] In an operation 470, method 400 may include receiving a packet delivery confirmation packet by a cloud service. Referring to FIG. 2, upon receiving the zone report packet, user device 240 may confirm delivery of the zone report packet to cloud services 260. Doing so may allow the cloud services 260 to determine a personalized rendering of the zone report for a user of the particular user type. In an operation 480, method 400 may include delivering the personalized rendering of the zone report to the user device of the

user. The user of the particular user type may view the personalized rendering to understand the detected anomaly and actions for responding to the anomaly.

[0049] FIG. 5 is an example environment having devices being monitored by example systems for detecting anomalies of devices. FIG. 5 was described herein in relation to FIG. 3.

[0050] The foregoing disclosure describes examples for generating recommended inputs for changing an outcome of a predictive model. The disclosed examples may include systems, devices, computer-readable storage media, and methods for generating recommended inputs. For purposes of explanation, certain examples are described with reference to the components illustrated in FIGS. 1-5. The functionality of the illustrated components may overlap, however, and may be present in a fewer or greater number of elements and components. All or part of the functionality of illustrated elements may co-exist or be distributed among several geographically dispersed locations. Moreover, the disclosed examples may be implemented in various environments and are not limited to the illustrated implementations.

[0051] Further, the sequence of operations described in connection with FIGS. 1-5 are examples and are not intended to be limiting. Additional or fewer operations or combinations of operations may be used or may vary without departing from the scope of the disclosed examples. Furthermore, implementations consistent with the disclosed examples need not perform the sequence of operations in any particular order. Thus, the present disclosure merely sets forth possible examples of implementations, and many variations and modifications may be made to the described examples. All such modifications and variations are intended to be included within the scope of this disclosure and protected by the following claims.

[0052] The terminology used herein is for the purpose of describing particular examples only and is not intended to be limiting. As used herein, the singular forms "a," "an," and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. The term "plurality," as used herein, is defined as two or more than two. The term "another," as used herein, is defined as at least a second or more. The term "coupled," as used herein, is defined as connected, whether directly without any

intervening elements or indirectly with at least one intervening elements, unless otherwise indicated. Two elements can be coupled mechanically, electrically, or communicatively linked through a communication channel, pathway, network, or system. The term “and/or” as used herein refers to and encompasses any and all possible combinations of a set of the associated listed items. It will also be understood that, although the terms first, second, third, etc. may be used herein to describe various elements, these elements should not be limited by these terms, as these terms are only used to distinguish one element from another unless stated otherwise or the context indicates otherwise. As used herein, the term "includes" means includes but not limited to, the term "including" means including but not limited to. The term "based on" means based at least in part on.

I/We Claim:

1. A computing device, comprising a processor and a non-transitory machine-readable storage medium encoded with instructions executable by the processor, the non-transitory storage medium comprising instructions to:

poll a device in a zone covered by the computing device;

in response to detecting an anomaly of the device in the zone, configure a beacon to generate a zone report packet, wherein the zone report packet comprises a location of the device in the zone, an anomaly identifier determined by analyzing a detected symptom associated with the anomaly, and an instruction for a particular user type; and

cause the beacon to broadcast the zone report packet to be received by a user device associated with a user of the particular user type.

2. The computing device of claim 1, wherein the zone covers a plurality of devices in an established geographic area.

3. The computing device of claim 1, wherein the beacon is a separate device wirelessly connected to the computing device.

4. The computing device of claim 1, wherein the beacon is a built-in connectivity engine of the computing device.

5. The computing device of claim 1, comprising instructions to cause to deliver, to the user device, a personalized rendering of the zone report packet based on the instruction for the particular user type, wherein the personalized rendering informs the user of a particular action to address the anomaly.

6. The computing device of claim 5, wherein the personalized rendering delivered to the user is delivered from a cloud service.

7. The computing device of claim 6, wherein the anomaly identifier is determined by the cloud service, wherein the cloud service analyzes the detected symptom associated with the anomaly.

8. A device anomaly detecting system, comprising:

a computing device, the computing device comprising:

a polling engine to poll a device in a zone covered by the computing device, wherein the zone covers a plurality of devices in an established geographic area; and

a beacon programming engine to deliver, in response to detecting an anomaly of the device in the zone, a beacon programming packet, wherein the beacon programming packet comprises a zone report, wherein the zone report comprises a location of the device in the zone, an anomaly identifier determined by analyzing a detected symptom associated with the anomaly, and an instruction for a particular user type; and

a beacon, the beacon comprising:

a packet receiving engine to receive the beacon programming packet; and

a broadcast engine to broadcast a zone report packet to be received by a user device associated with a user of the particular user type, wherein the zone report packet comprises the zone report.

9. The device anomaly detecting system of claim 8, wherein the beacon is a built-in connectivity engine of the computing device.

10. The device anomaly detecting system of claim 8, the computing device comprising a cloud services engine to communicate with a cloud service, wherein the cloud service engine is to deliver the anomaly to the cloud service, and the cloud service is to determine the anomaly identifier by analyzing the detected symptom associated with the anomaly.

11. The device anomaly detecting system of claim 10, wherein the cloud service is to:

receive a zone report packet delivery confirmation from the user device; and

in response to receiving the delivery confirmation packet, deliver, to the user device, a personalized rendering of the zone report packet based on the instruction for the particular user type, wherein the personalized rendering informs the user of a particular action to address the anomaly.

12. A method for detecting anomalies of devices, comprising:

polling, by a computing device, a device in a zone covered by the computing device;

in response to detecting an anomaly of the device in the zone, generate, by the computing device, a zone report comprising a location of the device in the zone and an anomaly identifier determined by analyzing a detected symptom associated with the anomaly;

deliver, by the computing device, a beacon programming packet to a beacon, wherein the beacon programming packet comprises the zone report and an instruction for a particular user type; and

cause, by the computing device, a beacon, upon receiving the beacon programming packet, to broadcast a zone report packet to be received by a user device of the particular user type, wherein the zone report packet comprises the zone report.

13. The method of claim 12, wherein the zone covers a plurality of devices in an established geographic area.

14. The method of claim 12, comprising communicating, by the computing device, with a cloud service to deliver the anomaly to the cloud service, and to receive the anomaly identifier determined by the cloud service.

15. The method of claim 14, comprising:

receiving, by the cloud service, a zone report packet delivery confirmation

generated by the user device; and

in response to receiving the delivery confirmation packet, delivering to the user device a personalized rendering of the zone report packet based on the instruction for the particular user type, wherein the personalized rendering informs the user of a particular action to address the anomaly.

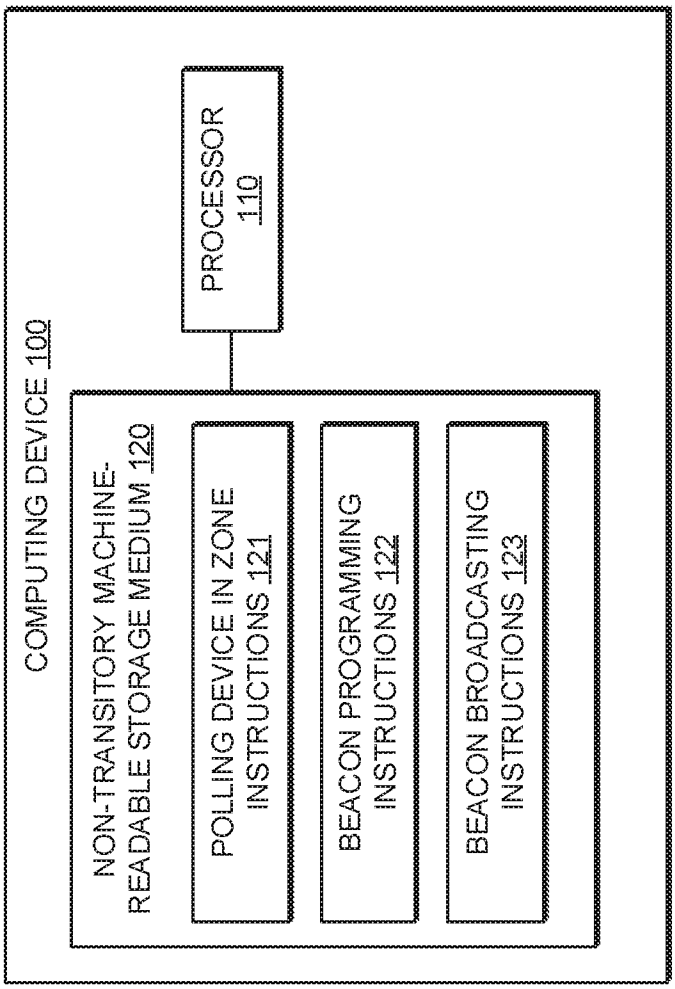
COMPUTING DEVICE 100
PROCESSOR 110
NON-TRANSITORY MACHINE-READABLE STORAGE MEDIUM 120
POLLING DEVICE IN ZONE INSTRUCTIONS 121
BEACON PROGRAMMING INSTRUCTIONS 122
BEACON BROADCASTING INSTRUCTIONS 123

FIG. 1

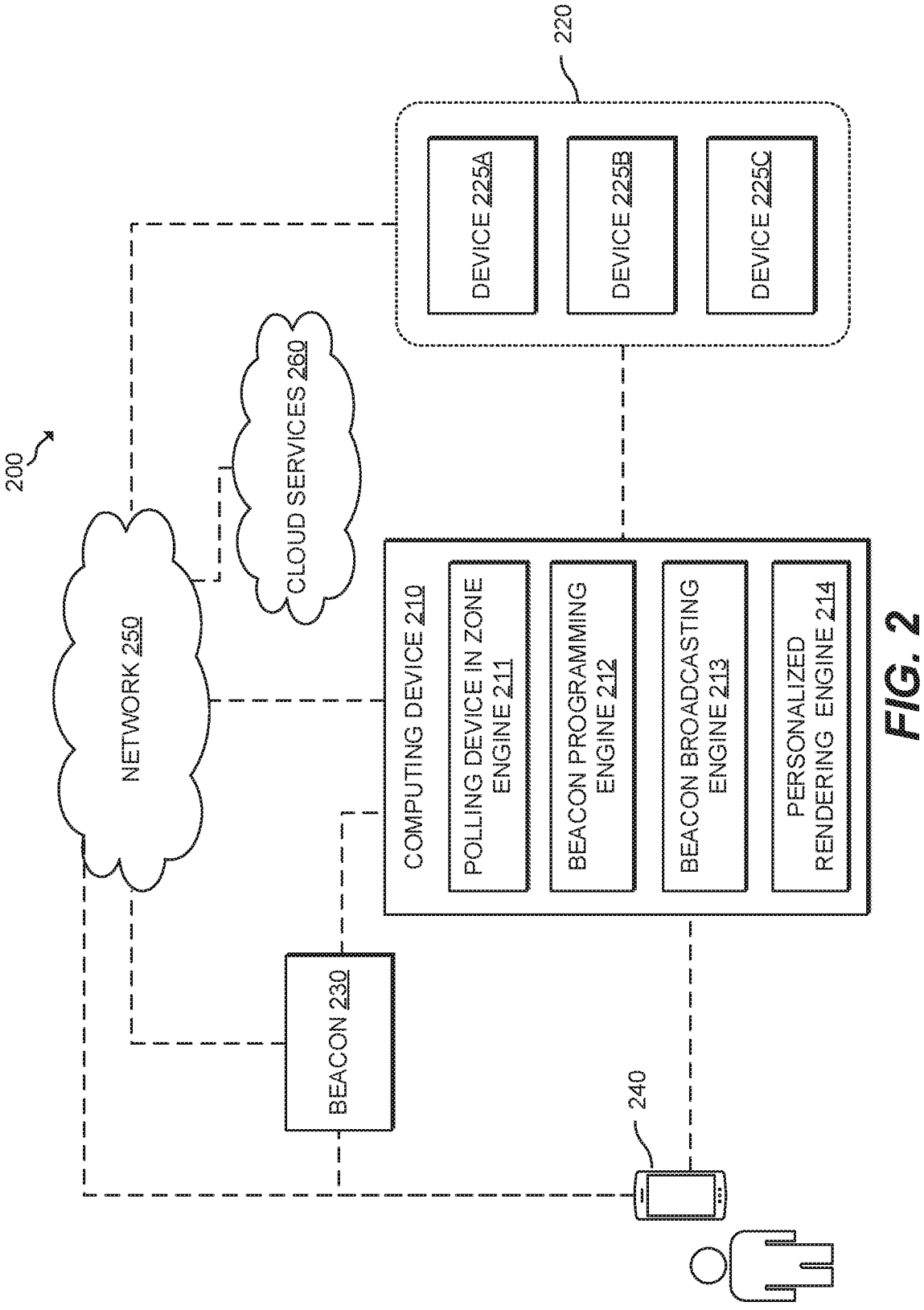
200
220
DEVICE 225A
DEVICE 225B
DEVICE 225C
CLOUD SERVICES 260
NETWORK 250
COMPUTING DEVICE 210
POLLING DEVICE IN ZONE ENGINE 211
BEACON PROGRAMMING ENGINE 212
BEACON BROADCASTING ENGINE 213
PERSONALIZED RENDERING ENGINE 214
BEACON 230
240

FIG. 2

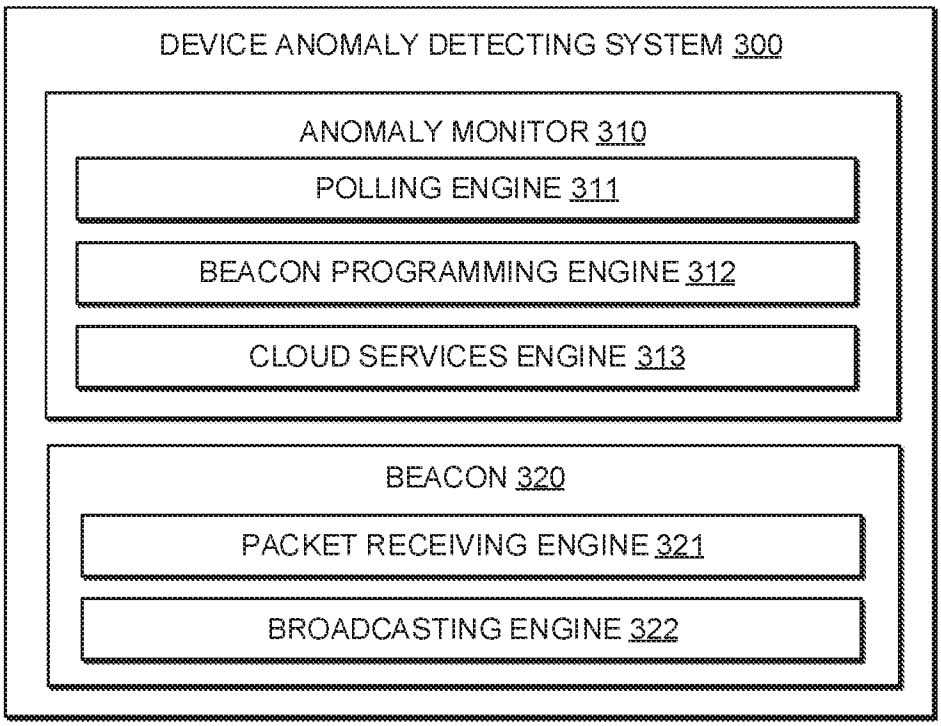
DEVICE ANOMALY DETECTING SYSTEM 300
ANOMALY MONITOR 310
POLLING ENGINE 311
BEACON PROGRAMMING ENGINE 312
CLOUD SERVICES ENGINE 313
BEACON 320
PACKET RECEIVING ENGINE 321
BROADCASTING ENGINE 322

FIG. 3

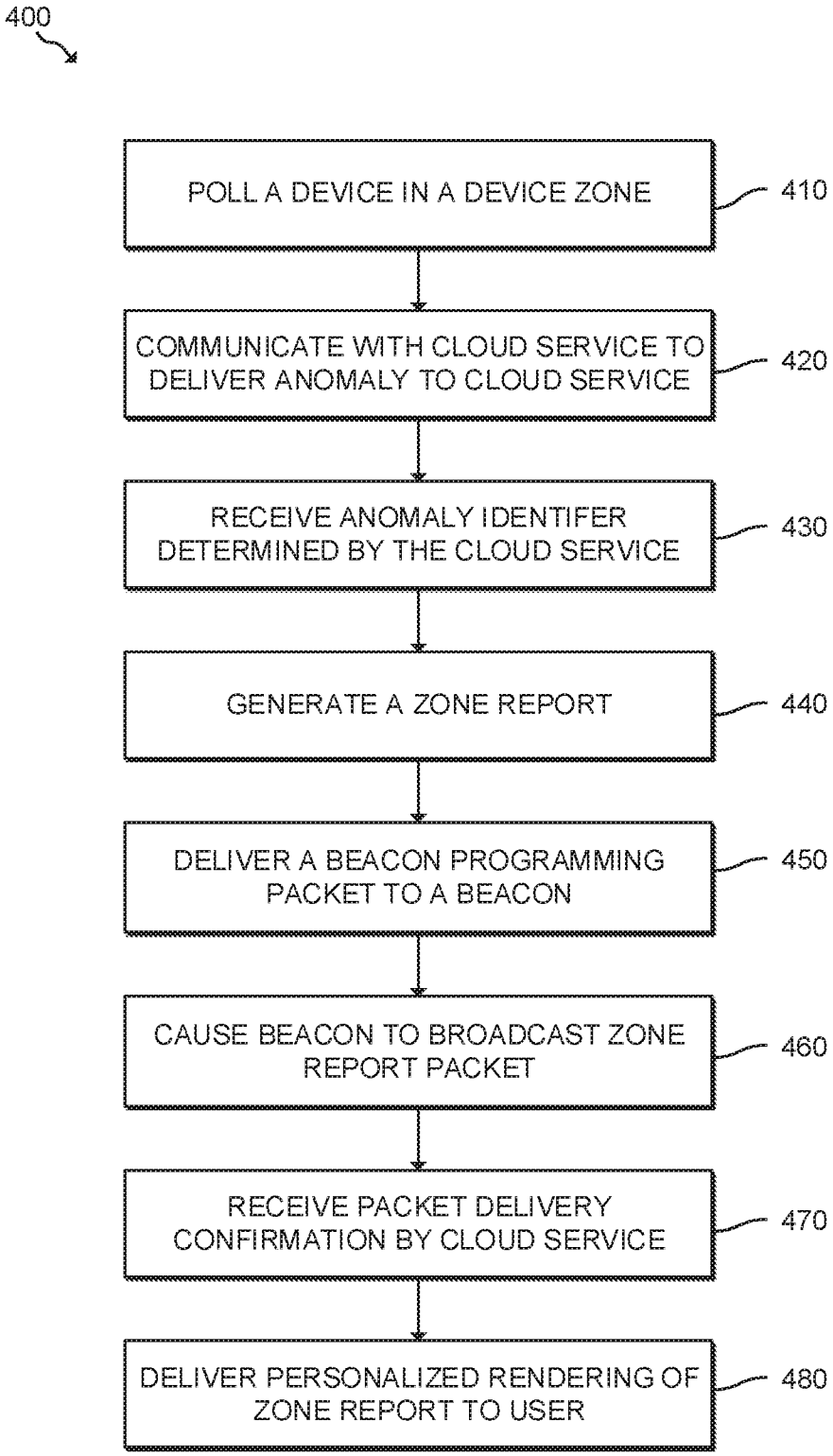
400
POLL A DEVICE IN A DEVICE ZONE
410
COMMUNICATE WITH CLOUD SERVICE TO DELIVER ANOMALY TO CLOUD SERVICE
420
RECEIVE ANOMALY IDENTIFER DETERMINED BY THE CLOUD SERVICE
430
GENERATE A ZONE REPORT
440
DELIVER A BEACON PROGRAMMING PACKET TO A BEACON
450
CAUSE BEACON TO BROADCAST ZONE REPORT PACKET
460
RECEIVE PACKET DELIVERY CONFIRMATION BY CLOUD SERVICE
470
DELIVER PERSONALIZED RENDERING OF ZONE REPORT TO USER
480

FIG. 4

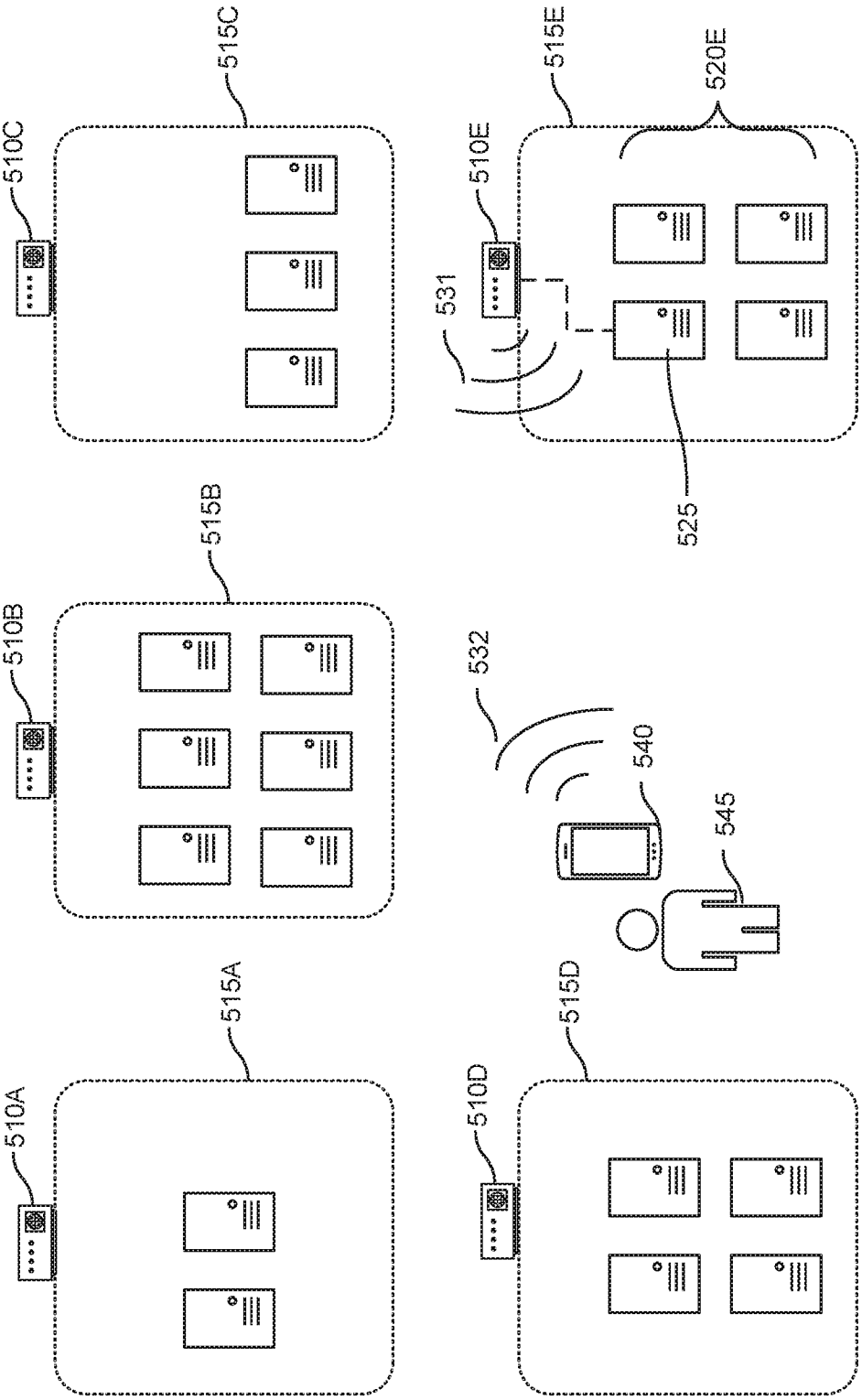
515C
510C
515B
510B
515A
510A
515E
520E
510E
531
525
532
540
545
515D
510D

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2016/030200

A. CLASSIFICATION OF SUBJECT MATTER

G06F 11/30(2006.01)i, G06F 15/16(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)
G06F 11/30; G01S 5/14; G06F 15/173; H04Q 7/00; G06Q 30/00; G01S 3/02; G06F 15/16

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: monitor, anomaly, poll, zone, server, broadcast, beacon, data center, and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2014-0006597 A1 (MRITTIKA GANGULI et al.) 02 January 2014 See paragraphs [0018]-[0021], [0028], [0050], and [0062]-[0063]; and figure 1.	1-15
Y	US 2008-0167896 A1 (RAYMOND D. FAST et al.) 10 July 2008 See paragraphs [0090], [0149], [0152], [0248], [0258]-[0259], and [0288]; and figure 2.	1-15
A	US 2013-0024559 A1 (ADHIKARY SUSANTA et al.) 24 January 2013 See paragraphs [0009] and [0021]; and figure 3.	1-15
A	US 2006-0170591 A1 (CYRIL HOURI) 03 August 2006 See paragraphs [0011] and [0027]; and figure 1.	1-15
A	WO 2013-014672 A1 (LIGHT CYBER LTD.) 31 January 2013 See paragraphs [0007] and [0084]; and figure 1.	1-15

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

☒ See patent family annex.

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

Date of the actual completion of the international search	Date of mailing of the international search report
30 November 2016 (30.11.2016)	**30 November 2016 (30.11.2016)**

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

Authorized officer
NHO, Ji Myong
Telephone No. +82-42-481-8528

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2016/030200

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014-0006597 A1	02/01/2014	CN 104380277 A	25/02/2015
		DE 112013003180 T5	07/05/2015
		US 9207988 B2	08/12/2015
		WO 2014-004318 A1	03/01/2014
US 2008-0167896 A1	10/07/2008	CA 2555221 A1	25/08/2005
		CA 2555221 C	28/10/2014
		US 2006-0181411 A1	17/08/2006
		US 2010-0026495 A1	04/02/2010
		US 2012-086552 A1	12/04/2012
		US 7327258 B2	05/02/2008
		US 7528723 B2	05/05/2009
		US 7978076 B2	12/07/2011
		US 8350700 B2	08/01/2013
		WO 2005-078473 A1	25/08/2005
US 2013-0024559 A1	24/01/2013	US 8892728 B2	18/11/2014
US 2006-0170591 A1	03/08/2006	US 2007-0126635 A1	07/06/2007
		US 2008-0268870 A1	30/10/2008
		US 2008-0274752 A1	06/11/2008
		US 7397424 B2	08/07/2008
		US 7696923 B2	13/04/2010
		US 8565788 B2	22/10/2013
		US 9392406 B2	12/07/2016
WO 2013-014672 A1	31/01/2013	EP 2737404 A1	04/06/2014
		EP 2737404 A4	29/04/2015
		US 2014-0165207 A1	12/06/2014