



(51) International Patent Classification:

H04L 12/00 (2006.01)

(21) International Application Number:

PCT/US2022/020397

(22) International Filing Date:

15 March 2022 (15.03.2022)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

17/202,921

16 March 2021 (16.03.2021)

US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:

US

17/202,921 (CON)

Filed on

16 March 2021 (16.03.2021)

(71) Applicant: JPMORGAN CHASE BANK, N.A. [US/US];

383 Madison Avenue, New York, New York 10179 (US).

(72) Inventors: ADAMO, Cristian; c/o JPMorgan Chase Bank,

N.A., 383 Madison Avenue, New York, New York 10179

(US). CASAS HERNANDEZ, Victor D.; c/o JPMorgan

Chase Bank, N.A., 383 Madison Avenue, New York, New

York 10179 (US).

(74) Agent: MUELLER, Robert W. et al.; GREENBLUM &

BERNSTEIN, P.L.C., 1950 Roland Clarke Place, Reston,

Virginia 20191 (US).

(81) Designated States (unless otherwise indicated, for every

kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ,

CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,

DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,

HR, HU, ID, IL, IN, IR, IS, IT, JM, JO, JP, KE, KG, KH,

KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA,

MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,

NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU,

RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM,

TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM,

ZW.

(84) Designated States (unless otherwise indicated, for every

kind of regional protection available): ARIPO (BW, GH,

GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ,

UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,

TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,

EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,

MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,

KM, ML, MR, NE, SN, TD, TG).

(54) Title: METHODS AND SYSTEMS FOR ANOMALY DETECTION

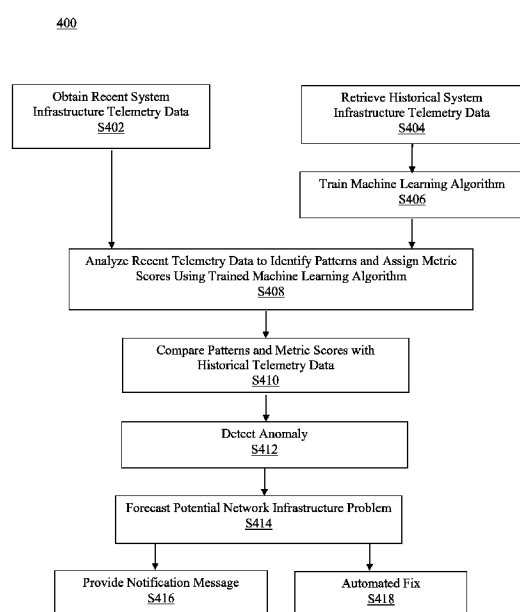


FIG. 4

(57) Abstract: A method and a system for detecting anomalies that indicate potential system infrastructure problems is provided. The method includes: obtaining a first set of telemetry data that relates to a system infrastructure events, logs, and metrics that occur during a predetermined time interval; retrieving, from a memory, historical data that relates to system infrastructure telemetry; comparing the obtained first set of telemetry data with the retrieved historical data; detecting an anomaly based on a result of the comparing; and determining a potential system infrastructure problem based on the detected anomaly. The method may include using a machine learning algorithm to analyze the obtained first set of telemetry data; identify a pattern in the data; assign scores to the events included in the data; and use the pattern and/or the scores to detect the anomaly using an artificial intelligence (AI) model that is trained using the retrieved historical data.

Declarations under Rule 4.17:

- *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))*

METHODS AND SYSTEMS FOR ANOMALY DETECTION

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This International Application claims the benefit of US Non-Provisional Application No. 17/202,921 filed March 16, 2021, the disclosure of which is expressly incorporated by reference herein in its entirety.

BACKGROUND

1. Field of the Disclosure

[0002] This technology generally relates to methods and systems for detecting anomalies, and more particularly, to methods and systems for using machine learning techniques to detect anomalies that act as indicators of future system infrastructure malfunctions.

2. Background Information

[0003] Many organizations rely on computer systems and networks to perform routine tasks. For large organizations that have thousands of users, such systems and networks may be interconnected in a large infrastructure that hosts large numbers of hardware components and many software modules that facilitate communications and interactions among the users.

[0004] When a problem occurs within the system infrastructure, the problem may be relatively small and easy to remedy, or the problem may cause delays and/or outages that are disruptive, time-consuming, and/or expensive. As a result, organizations typically use various approaches to addressing such problems when they occur and to attempting to avoid and/or prevent such problems before they occur.

[0005] Avoiding and/or preventing system infrastructure problems before they occur may be difficult, because the fact that the problem has not yet occurred means that the potential existence of the problem is not readily apparent. Accordingly, there

is a need for a method for detecting anomalies that indicate a potentiality of such a problem.

SUMMARY

[0006] The present disclosure, through one or more of its various aspects, embodiments, and/or specific features or sub-components, provides, inter alia, various systems, servers, devices, methods, media, programs, and platforms for using machine learning techniques to detect anomalies that act as indicators of future system infrastructure malfunctions.

[0007] According to an aspect of the present disclosure, a method for detecting an anomaly that acts as an indicator of a potential system infrastructure malfunction is provided. The method is implemented by at least one processor. The method includes: obtaining, by the at least one processor, a first set of telemetry data that relates to a plurality of system infrastructure telemetry that occur during a predetermined time interval; retrieving, by the at least one processor from a memory, historical data that relates to system infrastructure telemetry; comparing, by the at least one processor, the obtained first set of telemetry data with the retrieved historical data; detecting, by the at least one processor, at least one anomaly based on a result of the comparing; and determining, by the at least one processor, at least one potential system infrastructure problem based on the detected at least one anomaly. The telemetry includes at least one from among at least one event, at least one log, and at least one metric.

[0008] The method may further include applying at least one machine learning algorithm to the obtained first set of telemetry data.

[0009] The method may further include using the at least one machine learning algorithm to: analyze the obtained first set of telemetry data; identify at least one pattern based on a result of the analyzing; and compare the identified at least one pattern with the retrieved historical data to detect the at least one anomaly by using an artificial intelligence (AI) model that is trained using the retrieved historical data.

[0010] The method may further include: obtaining a catalog that includes a plurality of infrastructure fixes; selecting at least one infrastructure fix from among the plurality of infrastructure fixes based on the determined at least one potential system infrastructure problem; and applying the selected at least one infrastructure fix.

[0011] The method may further include using the at least one machine learning algorithm to assign a respective score to each of the obtained first set of telemetry data, and using each assigned respective score to detect the at least one anomaly.

[0012] The method may further include displaying, by the at least one processor on a user interface, a message that relates to the determined at least one potential system infrastructure problem.

[0013] The message may include first information that describes the determined at least one potential system infrastructure problem, second information that describes an expected result from a failure to avoid the potential system infrastructure problem, and third information that describes a time at which the potential system infrastructure problem is expected to occur.

[0014] The method may further include transmitting, by the at least one processor to a predetermined destination, an email message that relates to the determined at least one potential system infrastructure problem.

[0015] The message may include first information that describes the determined at least one potential system infrastructure problem, second information that describes an expected result from a failure to avoid the potential system infrastructure problem, and third information that describes a time at which the potential system infrastructure problem is expected to occur.

[0016] The predetermined time interval may be equal to four hours.

[0017] The predetermined time interval may be equal to twenty-four hours.

[0018] According to another exemplary embodiment, a computing apparatus for detecting an anomaly that indicates a potential system infrastructure problem is provided. The computing apparatus includes a processor; a memory; and a communication interface coupled to each of the processor and the memory. The processor is configured to: obtain a first set of telemetry data that relates to a plurality of system infrastructure telemetry that occur during a predetermined time interval; retrieve, from the memory, historical data that relates to system infrastructure telemetry; compare the obtained first set of telemetry data with the retrieved historical data; detect at least one anomaly based on a result of the comparing; and determine at least one

potential system infrastructure problem based on the detected at least one anomaly. The telemetry includes at least one from among at least one event, at least one log, and at least one metric.

[0019] The processor may be further configured to apply at least one machine learning algorithm to the obtained first set of telemetry data.

[0020] The processor may be further configured to use the at least one machine learning algorithm to: analyze the obtained first set of telemetry data; identify at least one pattern based on a result of the analyzing; and compare the identified at least one pattern with the retrieved historical data to detect the at least one anomaly by using an artificial intelligence (AI) model that is trained using the retrieved historical data.

[0021] The computing apparatus of claim 13, wherein the processor is further configured to: obtain a catalog that includes a plurality of infrastructure fixes; select at least one infrastructure fix from among the plurality of infrastructure fixes based on the determined at least one potential system infrastructure problem; and apply the selected at least one infrastructure fix.

[0022] The processor may be further configured to use the at least one machine learning algorithm to assign a respective score to each of the obtained first set of telemetry data, and to use each assigned respective score to detect the at least one anomaly.

[0023] The computing apparatus may further include a display. The processor may be further configured to cause the display to display a user interface that includes a message that relates to the determined at least one potential system infrastructure problem.

[0024] The message may include first information that describes the determined at least one potential system infrastructure problem, second information that describes an expected result from a failure to avoid the potential system infrastructure problem, and third information that describes a time at which the potential system infrastructure problem is expected to occur.

[0025] The processor may be further configured to transmit, via the communication interface to a predetermined destination, an email message that relates to the determined at least one potential system infrastructure problem.

[0026] The message may include first information that describes the determined at least one potential system infrastructure problem, second information that describes an expected result from a failure to avoid the potential system infrastructure problem, and third information that describes a time at which the potential system infrastructure problem is expected to occur.

[0027] The predetermined time interval may be equal to four hours.

[0028] The predetermined time interval may be equal to twenty-four hours.

BRIEF DESCRIPTION OF THE DRAWINGS

[0029] The present disclosure is further described in the detailed description which follows, in reference to the noted plurality of drawings, by way of non-limiting examples of preferred embodiments of the present disclosure, in which like characters represent like elements throughout the several views of the drawings.

[0030] FIG. 1 illustrates an exemplary computer system.

[0031] FIG. 2 illustrates an exemplary diagram of a network environment.

[0032] FIG. 3 shows an exemplary system for implementing a method for using machine learning techniques to detect anomalies that act as indicators of future system infrastructure malfunctions.

[0033] FIG. 4 is a flowchart of an exemplary process for implementing a method for using machine learning techniques to detect anomalies that act as indicators of future system infrastructure malfunctions.

DETAILED DESCRIPTION

[0034] Through one or more of its various aspects, embodiments and/or specific features or sub-components of the present disclosure, are intended to bring out one or more of the advantages as specifically described above and noted below.

[0035] The examples may also be embodied as one or more non-transitory computer readable media having instructions stored thereon for one or more aspects of the present technology as described and illustrated by way of the examples herein. The instructions in some examples include executable code that, when executed by one or more processors, cause the processors to carry out steps necessary to implement the methods of the examples of this technology that are described and illustrated herein.

[0036] FIG. 1 is an exemplary system for use in accordance with the embodiments described herein. The system 100 is generally shown and may include a computer system 102, which is generally indicated.

[0037] The computer system 102 may include a set of instructions that can be executed to cause the computer system 102 to perform any one or more of the methods or computer-based functions disclosed herein, either alone or in combination with the other described devices. The computer system 102 may operate as a standalone device or may be connected to other systems or peripheral devices. For example, the computer system 102 may include, or be included within, any one or more computers, servers, systems, communication networks or cloud environment. Even further, the instructions may be operative in such cloud-based computing environment.

[0038] In a networked deployment, the computer system 102 may operate in the capacity of a server or as a client user computer in a server-client user network environment, a client user computer in a cloud computing environment, or as a peer computer system in a peer-to-peer (or distributed) network environment. The computer system 102, or portions thereof, may be implemented as, or incorporated into, various devices, such as a personal computer, a tablet computer, a set-top box, a personal digital assistant, a mobile device, a palmtop computer, a laptop computer, a desktop computer, a communications device, a wireless smart phone, a personal trusted device, a wearable device, a global positioning satellite (GPS) device, a web appliance, or any other machine capable of executing a set of instructions (sequential or otherwise) that specify

actions to be taken by that machine. Further, while a single computer system 102 is illustrated, additional embodiments may include any collection of systems or sub-systems that individually or jointly execute instructions or perform functions. The term “system” shall be taken throughout the present disclosure to include any collection of systems or sub-systems that individually or jointly execute a set, or multiple sets, of instructions to perform one or more computer functions.

[0039] As illustrated in FIG. 1, the computer system 102 may include at least one processor 104. The processor 104 is tangible and non-transitory. As used herein, the term “non-transitory” is to be interpreted not as an eternal characteristic of a state, but as a characteristic of a state that will last for a period of time. The term “non-transitory” specifically disavows fleeting characteristics such as characteristics of a particular carrier wave or signal or other forms that exist only transitorily in any place at any time. The processor 104 is an article of manufacture and/or a machine component. The processor 104 is configured to execute software instructions in order to perform functions as described in the various embodiments herein. The processor 104 may be a general-purpose processor or may be part of an application specific integrated circuit (ASIC). The processor 104 may also be a microprocessor, a microcomputer, a processor chip, a controller, a microcontroller, a digital signal processor (DSP), a state machine, or a programmable logic device. The processor 104 may also be a logical circuit, including a programmable gate array (PGA) such as a field programmable gate array (FPGA), or another type of circuit that includes discrete gate and/or transistor logic. The processor 104 may be a central processing unit (CPU), a graphics processing unit (GPU), or both. Additionally, any processor described herein may include multiple processors, parallel processors, or both. Multiple processors may be included in, or coupled to, a single device or multiple devices.

[0040] The computer system 102 may also include a computer memory 106. The computer memory 106 may include a static memory, a dynamic memory, or both in communication. Memories described herein are tangible storage mediums that can store data and executable instructions and are non-transitory during the time instructions are stored therein. Again, as used herein, the term “non-transitory” is to be interpreted not as an eternal characteristic of a state, but as a characteristic of a state that will last for a period of time. The term “non-transitory” specifically disavows

fleeting characteristics such as characteristics of a particular carrier wave or signal or other forms that exist only transitorily in any place at any time. The memories are an article of manufacture and/or machine component. Memories described herein are computer-readable mediums from which data and executable instructions can be read by a computer. Memories as described herein may be random access memory (RAM), read only memory (ROM), flash memory, electrically programmable read only memory (EPROM), electrically erasable programmable read-only memory (EEPROM), registers, a hard disk, a cache, a removable disk, tape, compact disk read only memory (CD-ROM), digital versatile disk (DVD), floppy disk, Blu-ray disk, or any other form of storage medium known in the art. Memories may be volatile or non-volatile, secure and/or encrypted, unsecure and/or unencrypted. Of course, the computer memory 106 may comprise any combination of memories or a single storage.

[0041] The computer system 102 may further include a display 108, such as a liquid crystal display (LCD), an organic light emitting diode (OLED), a flat panel display, a solid state display, a cathode ray tube (CRT), a plasma display, or any other type of display, examples of which are well known to skilled persons.

[0042] The computer system 102 may also include at least one input device 110, such as a keyboard, a touch-sensitive input screen or pad, a speech input, a mouse, a remote control device having a wireless keypad, a microphone coupled to a speech recognition engine, a camera such as a video camera or still camera, a cursor control device, a global positioning system (GPS) device, an altimeter, a gyroscope, an accelerometer, a proximity sensor, or any combination thereof. Those skilled in the art appreciate that various embodiments of the computer system 102 may include multiple input devices 110. Moreover, those skilled in the art further appreciate that the above-listed, exemplary input devices 110 are not meant to be exhaustive and that the computer system 102 may include any additional, or alternative, input devices 110.

[0043] The computer system 102 may also include a medium reader 112 which is configured to read any one or more sets of instructions, e.g. software, from any of the memories described herein. The instructions, when executed by a processor, can be used to perform one or more of the methods and processes as described herein. In a particular embodiment, the instructions may reside completely, or at least partially,

within the memory 106, the medium reader 112, and/or the processor 110 during execution by the computer system 102.

[0044] Furthermore, the computer system 102 may include any additional devices, components, parts, peripherals, hardware, software or any combination thereof which are commonly known and understood as being included with or within a computer system, such as, but not limited to, a network interface 114 and an output device 116. The output device 116 may be, but is not limited to, a speaker, an audio out, a video out, a remote-control output, a printer, or any combination thereof.

[0045] Each of the components of the computer system 102 may be interconnected and communicate via a bus 118 or other communication link. As shown in FIG. 1, the components may each be interconnected and communicate via an internal bus. However, those skilled in the art appreciate that any of the components may also be connected via an expansion bus. Moreover, the bus 118 may enable communication via any standard or other specification commonly known and understood such as, but not limited to, peripheral component interconnect, peripheral component interconnect express, parallel advanced technology attachment, serial advanced technology attachment, etc.

[0046] The computer system 102 may be in communication with one or more additional computer devices 120 via a network 122. The network 122 may be, but is not limited to, a local area network, a wide area network, the Internet, a telephony network, a short-range network, or any other network commonly known and understood in the art. The short-range network may include, for example, Bluetooth, Zigbee, infrared, near field communication, ultraband, or any combination thereof. Those skilled in the art appreciate that additional networks 122 which are known and understood may additionally or alternatively be used and that the exemplary networks 122 are not limiting or exhaustive. Also, while the network 122 is shown in FIG. 1 as a wireless network, those skilled in the art appreciate that the network 122 may also be a wired network.

[0047] The additional computer device 120 is shown in FIG. 1 as a personal computer. However, those skilled in the art appreciate that, in alternative embodiments of the present application, the computer device 120 may be a laptop computer, a tablet

PC, a personal digital assistant, a mobile device, a palmtop computer, a desktop computer, a communications device, a wireless telephone, a personal trusted device, a web appliance, a server, or any other device that is capable of executing a set of instructions, sequential or otherwise, that specify actions to be taken by that device. Of course, those skilled in the art appreciate that the above-listed devices are merely exemplary devices and that the device 120 may be any additional device or apparatus commonly known and understood in the art without departing from the scope of the present application. For example, the computer device 120 may be the same or similar to the computer system 102. Furthermore, those skilled in the art similarly understand that the device may be any combination of devices and apparatuses.

[0048] Of course, those skilled in the art appreciate that the above-listed components of the computer system 102 are merely meant to be exemplary and are not intended to be exhaustive and/or inclusive. Furthermore, the examples of the components listed above are also meant to be exemplary and similarly are not meant to be exhaustive and/or inclusive.

[0049] In accordance with various embodiments of the present disclosure, the methods described herein may be implemented using a hardware computer system that executes software programs. Further, in an exemplary, non-limited embodiment, implementations can include distributed processing, component/object distributed processing, and parallel processing. Virtual computer system processing can be constructed to implement one or more of the methods or functionalities as described herein, and a processor described herein may be used to support a virtual processing environment.

[0050] As described herein, various embodiments provide optimized methods and systems for using machine learning techniques to detect anomalies that act as indicators of future system infrastructure malfunctions.

[0051] Referring to FIG. 2, a schematic of an exemplary network environment 200 for implementing a method for using machine learning techniques to detect anomalies that act as indicators of future system infrastructure malfunctions is illustrated. In an exemplary embodiment, the method is executable on any networked computer platform, such as, for example, a personal computer (PC).

[0052] The method for using machine learning techniques to detect anomalies that act as indicators of future system infrastructure malfunctions in a manner that is implementable in various computing platform environments may be implemented by a System Infrastructure Anomaly Detection (SIAD) device 202. The SIAD device 202 may be the same or similar to the computer system 102 as described with respect to FIG. 1. The SIAD device 202 may store one or more applications that can include executable instructions that, when executed by the SIAD device 202, cause the SIAD device 202 to perform actions, such as to transmit, receive, or otherwise process network messages, for example, and to perform other actions described and illustrated below with reference to the figures. The application(s) may be implemented as modules or components of other applications. Further, the application(s) can be implemented as operating system extensions, modules, plugins, or the like.

[0053] Even further, the application(s) may be operative in a cloud-based computing environment. The application(s) may be executed within or as virtual machine(s) or virtual server(s) that may be managed in a cloud-based computing environment. Also, the application(s), and even the SIAD device 202 itself, may be located in virtual server(s) running in a cloud-based computing environment rather than being tied to one or more specific physical network computing devices. Also, the application(s) may be running in one or more virtual machines (VMs) executing on the SIAD device 202. Additionally, in one or more embodiments of this technology, virtual machine(s) running on the SIAD device 202 may be managed or supervised by a hypervisor.

[0054] In the network environment 200 of FIG. 2, the SIAD device 202 is coupled to a plurality of server devices 204(1)-204(n) that hosts a plurality of databases 206(1)-206(n), and also to a plurality of client devices 208(1)-208(n) via communication network(s) 210. A communication interface of the SIAD device 202, such as the network interface 114 of the computer system 102 of FIG. 1, operatively couples and communicates between the SIAD device 202, the server devices 204(1)-204(n), and/or the client devices 208(1)-208(n), which are all coupled together by the communication network(s) 210, although other types and/or numbers of communication networks or systems with other types and/or numbers of connections and/or configurations to other devices and/or elements may also be used.

[0055] The communication network(s) 210 may be the same or similar to the network 122 as described with respect to FIG. 1, although the SIAD device 202, the server devices 204(1)-204(n), and/or the client devices 208(1)-208(n) may be coupled together via other topologies. Additionally, the network environment 200 may include other network devices such as one or more routers and/or switches, for example, which are well known in the art and thus will not be described herein. This technology provides a number of advantages including methods, non-transitory computer readable media, and NIAD devices that efficiently implement a method for using machine learning techniques to detect anomalies that act as indicators of future system infrastructure malfunctions.

[0056] By way of example only, the communication network(s) 210 may include local area network(s) (LAN(s)) or wide area network(s) (WAN(s)), and can use TCP/IP over Ethernet and industry-standard protocols, although other types and/or numbers of protocols and/or communication networks may be used. The communication network(s) 210 in this example may employ any suitable interface mechanisms and network communication technologies including, for example, teletraffic in any suitable form (e.g., voice, modem, and the like), Public Switched Telephone Network (PSTNs), Ethernet-based Packet Data Networks (PDNs), combinations thereof, and the like.

[0057] The SIAD device 202 may be a standalone device or integrated with one or more other devices or apparatuses, such as one or more of the server devices 204(1)-204(n), for example. In one particular example, the SIAD device 202 may include or be hosted by one of the server devices 204(1)-204(n), and other arrangements are also possible. Moreover, one or more of the devices of the SIAD device 202 may be in a same or a different communication network including one or more public, private, or cloud networks, for example.

[0058] The plurality of server devices 204(1)-204(n) may be the same or similar to the computer system 102 or the computer device 120 as described with respect to FIG. 1, including any features or combination of features described with respect thereto. For example, any of the server devices 204(1)-204(n) may include, among other features, one or more processors, a memory, and a communication interface, which are

coupled together by a bus or other communication link, although other numbers and/or types of network devices may be used. The server devices 204(1)-204(n) in this example may process requests received from the SIAD device 202 via the communication network(s) 210 according to the HTTP-based and/or JavaScript Object Notation (JSON) protocol, for example, although other protocols may also be used.

[0059] The server devices 204(1)-204(n) may be hardware or software or may represent a system with multiple servers in a pool, which may include internal or external networks. The server devices 204(1)-204(n) hosts the databases 206(1)-206(n) that are configured to store historical system telemetry data and machine learning algorithm application-specific data that is usable for detecting anomalies that act as indicators of future system infrastructure malfunctions.

[0060] Although the server devices 204(1)-204(n) are illustrated as single devices, one or more actions of each of the server devices 204(1)-204(n) may be distributed across one or more distinct network computing devices that together comprise one or more of the server devices 204(1)-204(n). Moreover, the server devices 204(1)-204(n) are not limited to a particular configuration. Thus, the server devices 204(1)-204(n) may contain a plurality of network computing devices that operate using a master/slave approach, whereby one of the network computing devices of the server devices 204(1)-204(n) operates to manage and/or otherwise coordinate operations of the other network computing devices.

[0061] The server devices 204(1)-204(n) may operate as a plurality of network computing devices within a cluster architecture, a peer-to peer architecture, virtual machines, or within a cloud architecture, for example. Thus, the technology disclosed herein is not to be construed as being limited to a single environment and other configurations and architectures are also envisaged.

[0062] The plurality of client devices 208(1)-208(n) may also be the same or similar to the computer system 102 or the computer device 120 as described with respect to FIG. 1, including any features or combination of features described with respect thereto. For example, the client devices 208(1)-208(n) in this example may include any type of computing device that can interact with the SIAD device 202 via communication network(s) 210. Accordingly, the client devices 208(1)-208(n) may be

mobile computing devices, desktop computing devices, laptop computing devices, tablet computing devices, virtual machines (including cloud-based computers), or the like, that host chat, e-mail, or voice-to-text applications, for example. In an exemplary embodiment, at least one client device 208 is a wireless mobile communication device, i.e., a smart phone.

[0063] The client devices 208(1)-208(n) may run interface applications, such as standard web browsers or standalone client applications, which may provide an interface to communicate with the SIAD device 202 via the communication network(s) 210 in order to communicate user requests and information. The client devices 208(1)-208(n) may further include, among other features, a display device, such as a display screen or touchscreen, and/or an input device, such as a keyboard, for example.

[0064] Although the exemplary network environment 200 with the SIAD device 202, the server devices 204(1)-204(n), the client devices 208(1)-208(n), and the communication network(s) 210 are described and illustrated herein, other types and/or numbers of systems, devices, components, and/or elements in other topologies may be used. It is to be understood that the systems of the examples described herein are for exemplary purposes, as many variations of the specific hardware and software used to implement the examples are possible, as will be appreciated by those skilled in the relevant art(s).

[0065] One or more of the devices depicted in the network environment 200, such as the SIAD device 202, the server devices 204(1)-204(n), or the client devices 208(1)-208(n), for example, may be configured to operate as virtual instances on the same physical machine. In other words, one or more of the SIAD device 202, the server devices 204(1)-204(n), or the client devices 208(1)-208(n) may operate on the same physical device rather than as separate devices communicating through communication network(s) 210. Additionally, there may be more or fewer SIAD devices 202, server devices 204(1)-204(n), or client devices 208(1)-208(n) than illustrated in FIG. 2.

[0066] In addition, two or more computing systems or devices may be substituted for any one of the systems or devices in any example. Accordingly, principles and advantages of distributed processing, such as redundancy and replication also may be implemented, as desired, to increase the robustness and performance of the

devices and systems of the examples. The examples may also be implemented on computer system(s) that extend across any suitable network using any suitable interface mechanisms and traffic technologies, including by way of example only teletraffic in any suitable form (e.g., voice and modem), wireless traffic networks, cellular traffic networks, Packet Data Networks (PDNs), the Internet, intranets, and combinations thereof.

[0067] The SIAD device 202 is described and shown in FIG. 3 as including a system infrastructure anomaly detection module 302, although it may include other rules, policies, modules, databases, or applications, for example. As will be described below, the system infrastructure anomaly detection module 302 is configured to implement a method for using machine learning techniques to detect anomalies that act as indicators of future system infrastructure malfunctions in an automated, efficient, scalable, and reliable manner.

[0068] An exemplary process 300 for implementing a method for using machine learning techniques to detect anomalies that act as indicators of future system infrastructure malfunctions by utilizing the network environment of FIG. 2 is shown as being executed in FIG. 3. Specifically, a first client device 208(1) and a second client device 208(2) are illustrated as being in communication with SIAD device 202. In this regard, the first client device 208(1) and the second client device 208(2) may be “clients” of the SIAD device 202 and are described herein as such. Nevertheless, it is to be known and understood that the first client device 208(1) and/or the second client device 208(2) need not necessarily be “clients” of the SIAD device 202, or any entity described in association therewith herein. Any additional or alternative relationship may exist between either or both of the first client device 208(1) and the second client device 208(2) and the SIAD device 202, or no relationship may exist.

[0069] Further, SIAD device 202 is illustrated as being able to access a historical system telemetry and anomalies data repository 206(1) and a machine learning algorithm applications database 206(2). The system infrastructure anomaly detection module 302 may be configured to access these databases for implementing a method for using machine learning techniques to detect anomalies that act as indicators of future system infrastructure malfunctions.

[0070] The first client device 208(1) may be, for example, a smart phone. Of course, the first client device 208(1) may be any additional device described herein. The second client device 208(2) may be, for example, a personal computer (PC). Of course, the second client device 208(2) may also be any additional device described herein.

[0071] The process may be executed via the communication network(s) 210, which may comprise plural networks as described above. For example, in an exemplary embodiment, either or both of the first client device 208(1) and the second client device 208(2) may communicate with the SIAD device 202 via broadband or cellular communication. Of course, these embodiments are merely exemplary and are not limiting or exhaustive.

[0072] Upon being started, the system infrastructure anomaly detection module 302 executes a process for using machine learning techniques to detect anomalies that act as indicators of future system infrastructure malfunctions. An exemplary process for detecting anomalies that act as indicators of future system infrastructure malfunctions is generally indicated at flowchart 400 in FIG. 4.

[0073] In the process 400 of FIG. 4, at step S402, the system infrastructure anomaly detection module 302 obtains recent system infrastructure telemetry data that has occurred during a predefined time interval. The telemetry data includes data that relates to events, logs, and/or metrics. In an exemplary embodiment, the recent telemetry data may be obtained over a four-hour interval, a 24-hour interval, or any other suitable interval. Further, the recent telemetry data may be updated periodically, such as, for example, every 30 minutes, every hour, or every two hours, so that the obtaining of recent system infrastructure data is performed on a “rolling” basis.

[0074] At step S404, the system infrastructure anomaly detection module 302 retrieves historical system infrastructure telemetry data from a memory, such as, for example, historical system telemetry and anomalies data repository 206(1). Then, at step S406, the system infrastructure anomaly detection module 302 uses the retrieved historical telemetry data to train a machine learning algorithm, such as, for example, an algorithm that is stored in machine learning algorithm applications database 206(2).

[0075] At step S408, the system infrastructure anomaly detection module 302 analyzes the obtained recent telemetry data in order to identify patterns in the data. In an exemplary embodiment, the machine learning algorithm may be used to assign one or more scores to the obtained recent telemetry data. For example, the machine learning algorithm may include metrics that are defined within the algorithm, and the algorithm may then compute numerical values that act as scores for each such metric with respect to the obtained recent telemetry data.

[0076] At step S410, the system infrastructure anomaly detection module 302 compares the results of the analysis performed in step S408 with the retrieved historical data. Then, at step S412, the system infrastructure anomaly detection module 302 detects an anomaly in the recent telemetry data. In an exemplary embodiment, the machine learning algorithm may be used to compare the identified patterns and/or computed metric scores of the recent telemetry data with similar patterns and metric scores from the retrieved historical telemetry data, and when those patterns and/or metric scores in the historical data are correlated with subsequent system infrastructure problems, an anomaly may be detected.

[0077] At step S414, the system infrastructure anomaly detection module 302 forecasts a potential system infrastructure problem based on the detected anomaly. In an exemplary embodiment, when the machine learning algorithm determines that the detected anomaly is associated with a particular type of system infrastructure problem, the particular problem may be diagnosed as a likely occurrence unless the anomaly is addressed.

[0078] At step S416, the system infrastructure anomaly detection module 302 provides a notification message that relates to the potential system infrastructure problem. In an exemplary embodiment, the notification message includes a description of the problem, an expected result of the problem if not addressed or avoided before the problem occurs, and/or a time frame at which the problem is expected to occur. The notification message may be displayed on a user interface of a user, such as, for example, a network administrator or other person that monitors the network and addresses problems and/or potential problems. Alternatively, the notification message may be provided in an email message that is transmitted to users that may be affected

by the potential network infrastructure problem. Other alternatives for the notification message include incident systems, application programming interfaces (APIs), and streaming systems.

[0079] At step S418, the system infrastructure anomaly detection module 302 may implement an automated fix of the forecasted problem. In an exemplary embodiment, depending on the type of problem that has been diagnosed, the problem may be remedied and/or prevented by automatic application of a means for solving the problem.

[0080] Accordingly, with this technology, an optimized process using machine learning techniques to detect anomalies that act as indicators of future system infrastructure malfunctions is provided.

[0081] A method and a system for detecting, forecasting and fixing potential anomaly infrastructure problems using AI/ML methodologies is provided. The method includes: obtaining a first set of telemetry data that relates to a system infrastructure events, logs, and metrics that occur during a predetermined time interval; retrieving, from a memory, historical data that relates to system infrastructure telemetry to train an AI model; use the train AI model in conjunction with the obtained first set of telemetry data to produce an anomaly score; detecting an anomaly based on the result of the score; and determining a potential system infrastructure problem based on the detected anomaly.

[0082] An additional method includes obtaining a first set of telemetry data that relates to a system infrastructure events, logs, and metrics that occur during a predetermined time interval; retrieving, from a memory, historical data that relates to system infrastructure telemetry to train an AI model; using the trained AI model in conjunction with the obtained first set of telemetry data to produce forecasted pattern for potential anomalous events in the future; detecting a future anomaly based on the result of the forecast; and determining a future potential system infrastructure problem based on the forecasted pattern.

[0083] A third method that retrieves the output of the detect or forecast method; obtains a first set of infrastructure fixes catalog; and applies a recommended fix given

the potential anomalous behavior detected to correct any potential future negative behavior from happening in the system infrastructure is also provided.

[0084] The method may include using a machine learning algorithm to analyze the obtained first set of telemetry data; identify a pattern in the data; assign scores to the events included in the data; and use the pattern and/or the scores to detect the anomaly using an artificial intelligence (AI) model that is trained using the retrieved historical data.

[0085] Although the invention has been described with reference to several exemplary embodiments, it is understood that the words that have been used are words of description and illustration, rather than words of limitation. Changes may be made within the purview of the appended claims, as presently stated and as amended, without departing from the scope and spirit of the present disclosure in its aspects. Although the invention has been described with reference to particular means, materials and embodiments, the invention is not intended to be limited to the particulars disclosed; rather the invention extends to all functionally equivalent structures, methods, and uses such as are within the scope of the appended claims.

[0086] For example, while the computer-readable medium may be described as a single medium, the term “computer-readable medium” includes a single medium or multiple media, such as a centralized or distributed database, and/or associated caches and servers that store one or more sets of instructions. The term “computer-readable medium” shall also include any medium that is capable of storing, encoding or carrying a set of instructions for execution by a processor or that cause a computer system to perform any one or more of the embodiments disclosed herein.

[0087] The computer-readable medium may comprise a non-transitory computer-readable medium or media and/or comprise a transitory computer-readable medium or media. In a particular non-limiting, exemplary embodiment, the computer-readable medium can include a solid-state memory such as a memory card or other package that houses one or more non-volatile read-only memories. Further, the computer-readable medium can be a random access memory or other volatile re-writable memory. Additionally, the computer-readable medium can include a magneto-optical or optical medium, such as a disk or tapes or other storage device to capture

carrier wave signals such as a signal communicated over a transmission medium. Accordingly, the disclosure is considered to include any computer-readable medium or other equivalents and successor media, in which data or instructions may be stored.

[0088] Although the present application describes specific embodiments which may be implemented as computer programs or code segments in computer-readable media, it is to be understood that dedicated hardware implementations, such as application specific integrated circuits, programmable logic arrays and other hardware devices, can be constructed to implement one or more of the embodiments described herein. Applications that may include the various embodiments set forth herein may broadly include a variety of electronic and computer systems. Accordingly, the present application may encompass software, firmware, and hardware implementations, or combinations thereof. Nothing in the present application should be interpreted as being implemented or implementable solely with software and not hardware.

[0089] Although the present specification describes components and functions that may be implemented in particular embodiments with reference to particular standards and protocols, the disclosure is not limited to such standards and protocols. Such standards are periodically superseded by faster or more efficient equivalents having essentially the same functions. Accordingly, replacement standards and protocols having the same or similar functions are considered equivalents thereof.

[0090] The illustrations of the embodiments described herein are intended to provide a general understanding of the various embodiments. The illustrations are not intended to serve as a complete description of all of the elements and features of apparatus and systems that utilize the structures or methods described herein. Many other embodiments may be apparent to those of skill in the art upon reviewing the disclosure. Other embodiments may be utilized and derived from the disclosure, such that structural and logical substitutions and changes may be made without departing from the scope of the disclosure. Additionally, the illustrations are merely representational and may not be drawn to scale. Certain proportions within the illustrations may be exaggerated, while other proportions may be minimized. Accordingly, the disclosure and the figures are to be regarded as illustrative rather than restrictive.

[0091] One or more embodiments of the disclosure may be referred to herein, individually and/or collectively, by the term “invention” merely for convenience and without intending to voluntarily limit the scope of this application to any particular invention or inventive concept. Moreover, although specific embodiments have been illustrated and described herein, it should be appreciated that any subsequent arrangement designed to achieve the same or similar purpose may be substituted for the specific embodiments shown. This disclosure is intended to cover any and all subsequent adaptations or variations of various embodiments. Combinations of the above embodiments, and other embodiments not specifically described herein, will be apparent to those of skill in the art upon reviewing the description.

[0092] The Abstract of the Disclosure is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, various features may be grouped together or described in a single embodiment for the purpose of streamlining the disclosure. This disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter may be directed to less than all of the features of any of the disclosed embodiments. Thus, the following claims are incorporated into the Detailed Description, with each claim standing on its own as defining separately claimed subject matter.

[0093] The above disclosed subject matter is to be considered illustrative, and not restrictive, and the appended claims are intended to cover all such modifications, enhancements, and other embodiments which fall within the true spirit and scope of the present disclosure. Thus, to the maximum extent allowed by law, the scope of the present disclosure is to be determined by the broadest permissible interpretation of the following claims and their equivalents, and shall not be restricted or limited by the foregoing detailed description.

What is claimed is:

1. A method for detecting an anomaly that indicates a potential system infrastructure problem, the method being implemented by at least one processor, the method comprising:

obtaining, by the at least one processor, a first set of telemetry data that relates to a plurality of system infrastructure telemetry that occur during a predetermined time interval;

retrieving, by the at least one processor from a memory, historical data that relates to system infrastructure telemetry;

comparing, by the at least one processor, the obtained first set of telemetry data with the retrieved historical data;

detecting, by the at least one processor, at least one anomaly based on a result of the comparing; and

determining, by the at least one processor, at least one potential system infrastructure problem based on the detected at least one anomaly,

wherein the telemetry includes at least one from among at least one event, at least one log, and at least one metric.

2. The method of claim 1, further comprising applying at least one machine learning algorithm to the obtained first set of telemetry data.

3. The method of claim 2, further comprising using the at least one machine learning algorithm to:

analyze the obtained first set of telemetry data;

identify at least one pattern based on a result of the analyzing; and

compare the identified at least one pattern with the retrieved historical data to detect the at least one anomaly by using an artificial intelligence (AI) model that is trained using the retrieved historical data.

4. The method of claim 3, further comprising:

obtaining a catalog that includes a plurality of infrastructure fixes;

selecting at least one infrastructure fix from among the plurality of infrastructure fixes based on the determined at least one potential system infrastructure problem; and
applying the selected at least one infrastructure fix.

5. The method of claim 2, further comprising using the at least one machine learning algorithm to assign a respective score to each of the obtained first set of telemetry data, and using each assigned respective score to detect the at least one anomaly.

6. The method of claim 1, further comprising displaying, by the at least one processor on a user interface, a message that relates to the determined at least one potential system infrastructure problem.

7. The method of claim 6, wherein the message includes first information that describes the determined at least one potential system infrastructure problem, second information that describes an expected result from a failure to avoid the potential system infrastructure problem, and third information that describes a time at which the potential system infrastructure problem is expected to occur.

8. The method of claim 1, further comprising transmitting, by the at least one processor to a predetermined destination, an email message that relates to the determined at least one potential system infrastructure problem.

9. The method of claim 8, wherein the message includes first information that describes the determined at least one potential system infrastructure problem, second information that describes an expected result from a failure to avoid the potential system infrastructure problem, and third information that describes a time at which the potential system infrastructure problem is expected to occur.

10. The method of claim 1, wherein the predetermined time interval is equal to four hours.

11. A computing apparatus for detecting an anomaly that indicates a potential system infrastructure problem, the computing apparatus comprising:

- a processor;
- a memory; and
- a communication interface coupled to each of the processor and the memory, wherein the processor is configured to:
 - obtain a first set of telemetry data that relates to a plurality of network infrastructure telemetry that occur during a predetermined time interval;
 - retrieve, from the memory, historical data that relates to system infrastructure telemetry;
 - compare the obtained first set of telemetry data with the retrieved historical data;
 - detect at least one anomaly based on a result of the comparing; and
 - determine at least one potential system infrastructure problem based on the detected at least one anomaly,

wherein the telemetry includes at least one from among at least one event, at least one log, and at least one metric.

12. The computing apparatus of claim 11, wherein the processor is further configured to apply at least one machine learning algorithm to the obtained first set of telemetry data.

13. The computing apparatus of claim 12, wherein the processor is further configured to use the at least one machine learning algorithm to:

- analyze the obtained first set of telemetry data;
- identify at least one pattern based on a result of the analyzing; and
- compare the identified at least one pattern with the retrieved historical data to detect the at least one anomaly by using an artificial intelligence (AI) model that is trained using the retrieved historical data.

14. The computing apparatus of claim 13, wherein the processor is further configured to:

- obtain a catalog that includes a plurality of infrastructure fixes;
- select at least one infrastructure fix from among the plurality of infrastructure fixes based on the determined at least one potential system infrastructure problem;
- and
- apply the selected at least one infrastructure fix.

15. The computing apparatus of claim 12, wherein the processor is further configured to use the at least one machine learning algorithm to assign a respective score to each of the obtained first set of telemetry data, and to use each assigned respective score to detect the at least one anomaly.

16. The computing apparatus of claim 11, further comprising a display, and wherein the processor is further configured to cause the display to display a user interface that includes a message that relates to the determined at least one potential system infrastructure problem.

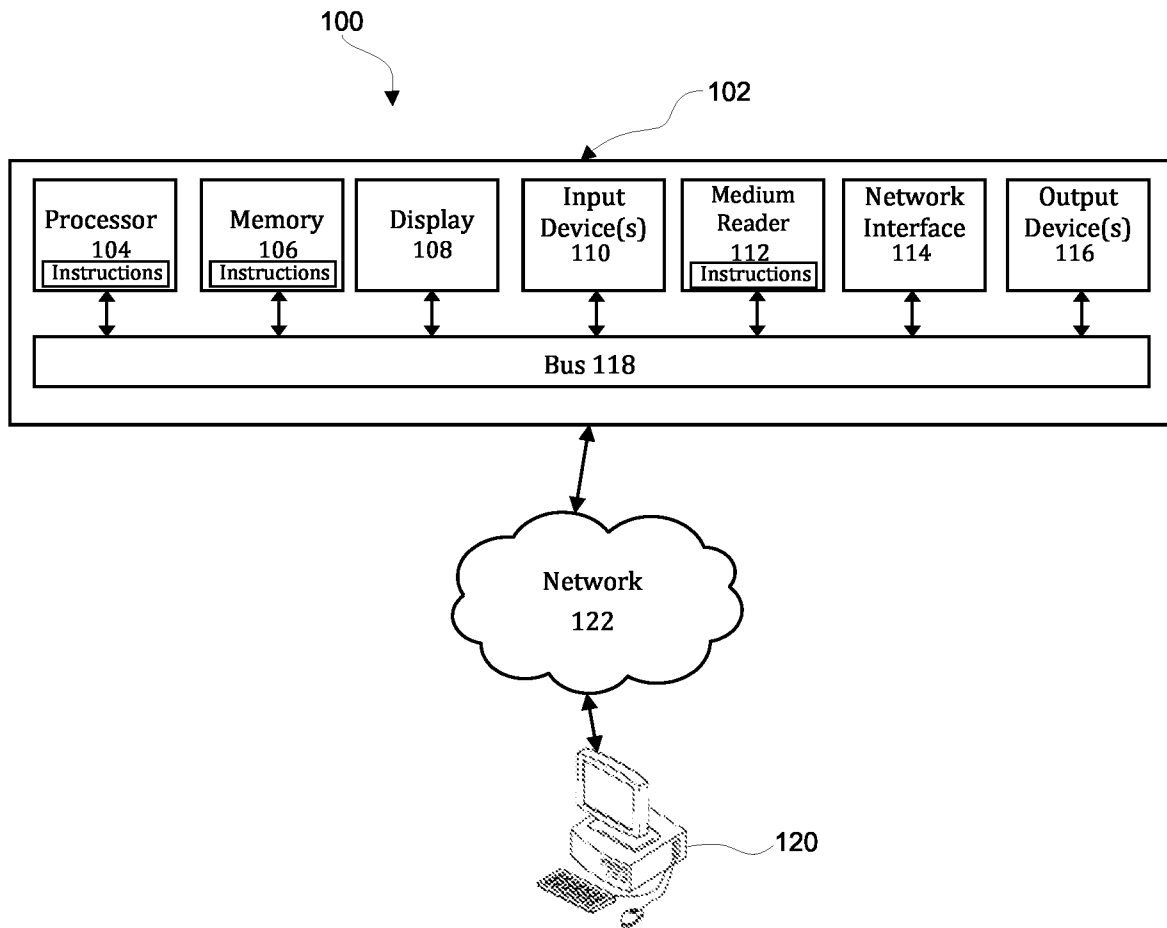
17. The computing apparatus of claim 16, wherein the message includes first information that describes the determined at least one potential system infrastructure problem, second information that describes an expected result from a failure to avoid the potential system infrastructure problem, and third information that describes a time at which the potential system infrastructure problem is expected to occur.

18. The computing apparatus of claim 11, wherein the processor is further configured to transmit, via the communication interface to a predetermined destination, an email message that relates to the determined at least one potential system infrastructure problem.

19. The computing apparatus of claim 18, wherein the message includes first information that describes the determined at least one potential system infrastructure problem, second information that describes an expected result from a failure to avoid

the potential system infrastructure problem, and third information that describes a time at which the potential system infrastructure problem is expected to occur.

20. The computing apparatus of claim 11, wherein the predetermined time interval is equal to four hours.

**FIG. 1**

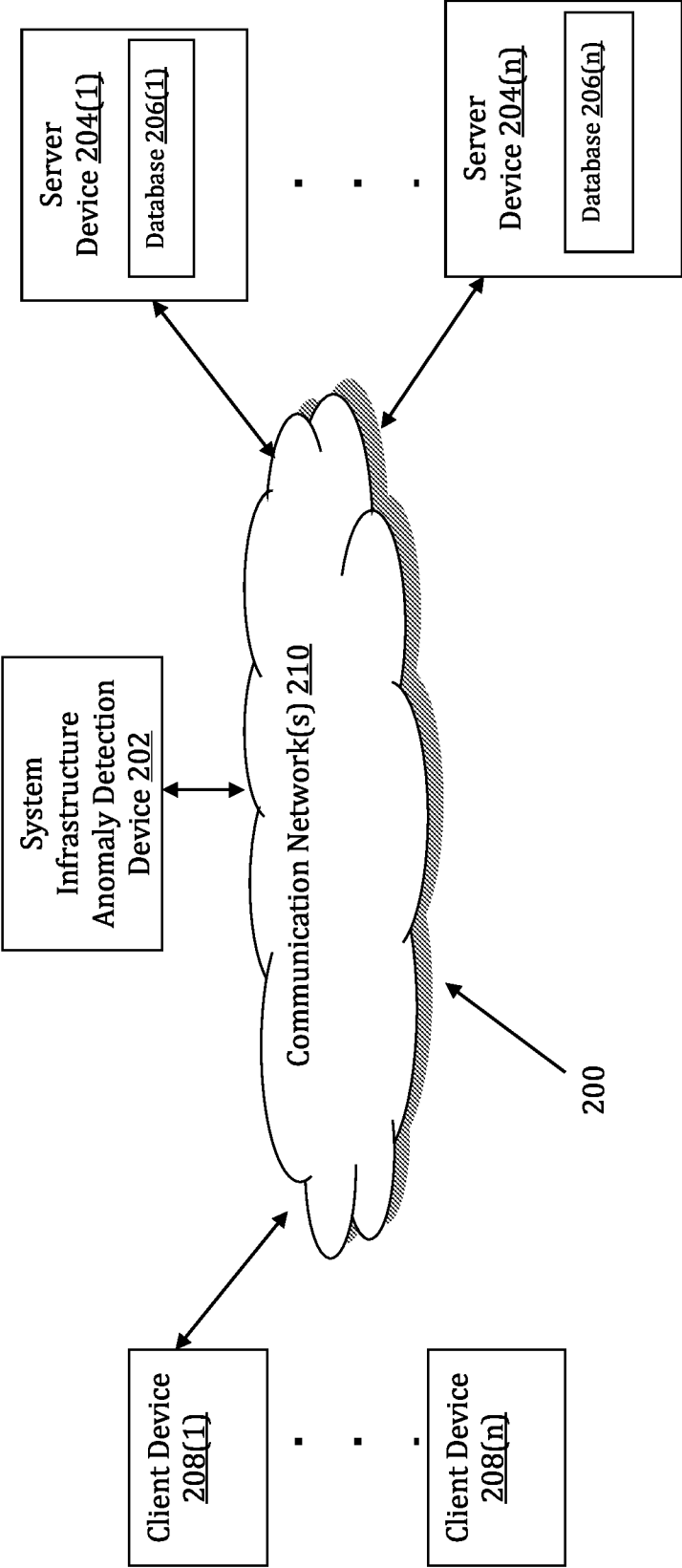
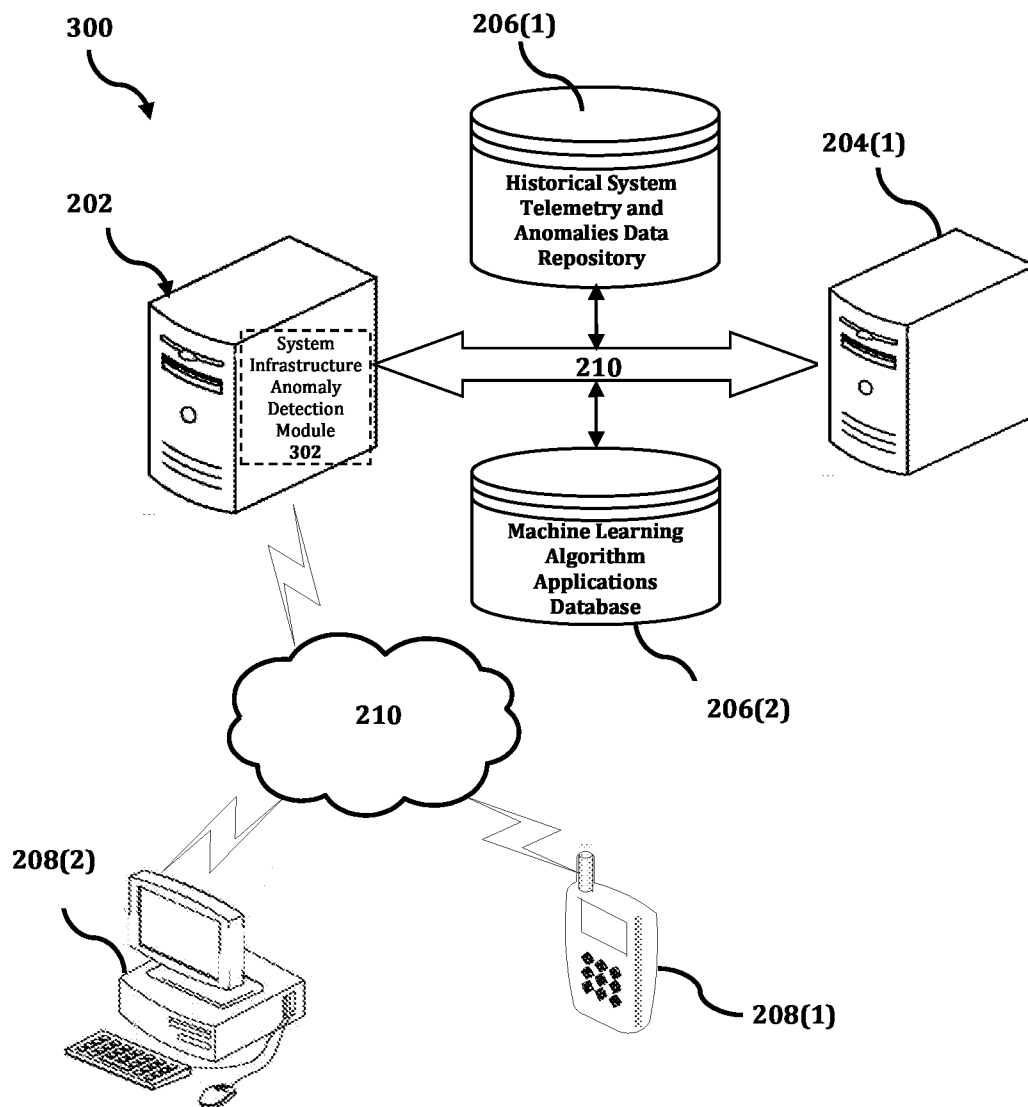
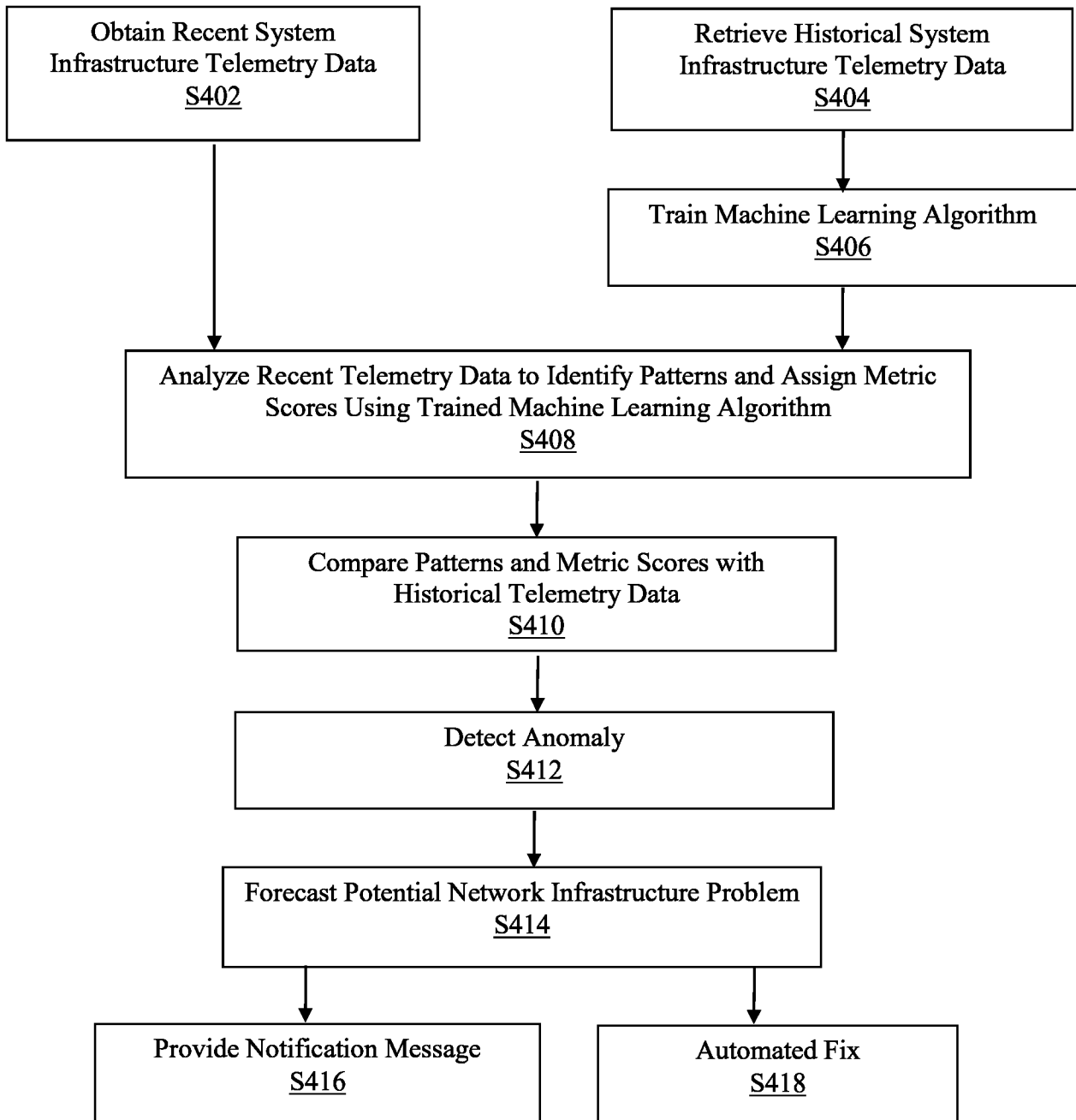


FIG. 2

**FIG. 3**

400**FIG. 4**

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2022/020397

A. CLASSIFICATION OF SUBJECT MATTER

IPC: H04L 12/00

CPC: H04L 12/00

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)

CPC: H04L 41/0654, 04, 0816, 16, 22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB ((data ir ubfir\$5) neare 5 (interval)) and ((log or table) near5 (data or info\$5)) near 5 telemetry

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2016/0234087 A1 11 August 2016 (11.08.2016) , entire document.	1-20
Y	US 2017/0235622 A1 (BOYAPALLE ET AL.) 17 August 2017 (17.08.2017) , entire document.	1-20

☐ 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

“D” document cited by the applicant in the international application

“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

31 March 2022 (31.03.2022)

Date of mailing of the international search report

04 April 2022 (04.04.2022)

Name and mailing address of the ISA/US

COMMISSIONER FOR PATENTS MAIL STOP PCT,
ATTN: ISA/US P.O. BOX 1450 ALEXANDRIA, VA
22313-1450, UNITED STATES OF AMERICA

Facsimile No. (571)273-8300

Authorized officer

HARRY KIM

Telephone No. 571-272-4300