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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 January 2025 (16.01.2025)

WIPO | PCT

(10) International Publication Number
WO 2025/013003 A1

(51) International Patent Classification:
H04L 41/0631 (2022.01) *H04L 41/069* (2022.01)
H04L 41/0677 (2022.01)

(21) International Application Number:
PCT/IN2024/051033

(22) International Filing Date:
03 July 2024 (03.07.2024)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
202321046098 09 July 2023 (09.07.2023) IN

(71) Applicant: **JIO PLATFORMS LIMITED** [IN/IN]; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN).

(72) Inventors: **BHATNAGAR, Aayush**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **BISHT, Sandeep**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **MISHRA, Rahul**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **NARESH, Jhoshi**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **SHARMA, Anshika**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **KASHYAP, Namrata Rammurat**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN).

(74) Agent: **JAPHET, Chinthan**; K Law (Krishnamurthy and Co.), 4th Floor, Prestige Takt, No 23, Kasturba Road Cross, Bangalore, Bangalore 560 001 (IN).

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,

(54) Title: SYSTEM AND METHOD FOR ENRICHMENT OF NETWORK ALARMS

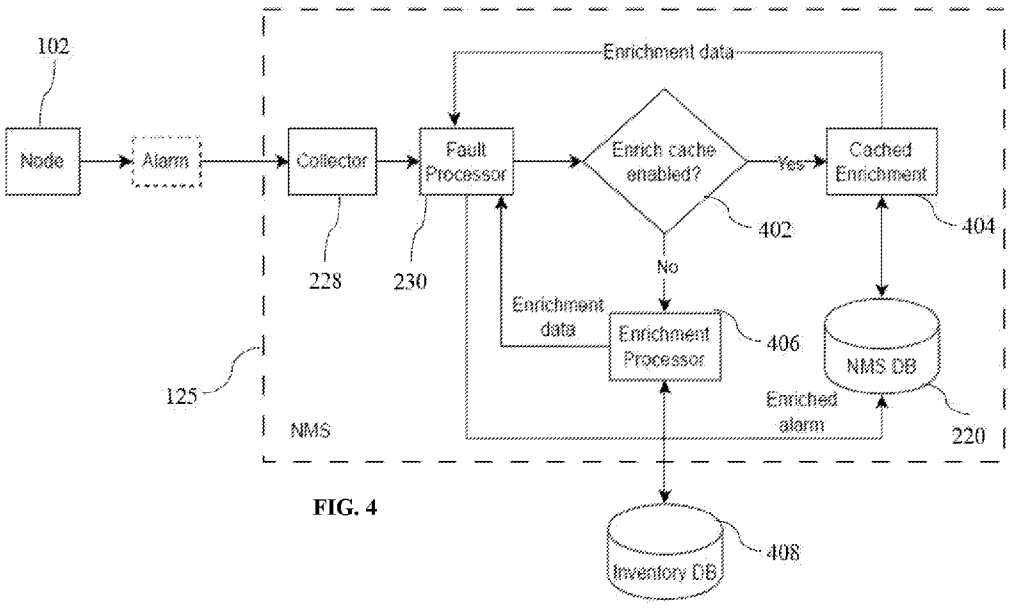

FIG. 4

(57) Abstract: A system (125) and a method of enrichment of network alarms is described A collector component (228) receives an alarm raised by a node (102) for an event. The alarm comprises one or more attributes indicating a hardware, software, or network issue associated with the node (102). A fault processor (230) identifies eligibility of the alarm for at least one of physical enrichment and logical enrichment. The eligibility is determined based on physical placement related attributes included in the alarm. Further, the fault processor (230) performs, based on the eligibility, at least one of the physical enrichment and the logical enrichment of the alarm.

WO 2025/013003 A1

[Continued on next page]

MA, MD, MG, MK, MN, MU, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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:

— *of inventorship (Rule 4.17(iv))*

Published:

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

SYSTEM AND METHOD FOR ENRICHMENT OF NETWORK ALARMS

FIELD OF THE INVENTION

[0001] The present invention generally relates to the field of network management and, more specifically, to a system and method for alarm enrichment, in a communication network.

BACKGROUND OF THE INVENTION

[0002] In network management systems, alarms are generated by network nodes to signal various events or conditions that require attention from network administrators or operators. These alarms typically contain valuable information presented in the form of attributes, providing critical details about the events and the nodes involved.

[0003] One of the challenges faced by existing network management systems is the transmission and handling of alarm data, particularly the burden associated with the vast amount of attribute information being carried by every alarm. In conventional systems, each alarm generated by a node carries all the attributes, including those related to the physical placement of the nodes within the network infrastructure.

[0004] This approach of including all attributes in each alarm results in a substantial data load being transmitted from every node to the network management system (NMS). The sheer volume of data being sent can pose a significant strain on network resources, leading to increased bandwidth consumption, latency, and potential performance degradation of the NMS.

[0005] Thus, there is a need for a solution which addresses the above mentioned shortcomings.

SUMMARY OF THE INVENTION

[0006] One or more embodiments of the present disclosure provide a system and method for performing enrichment of network alarms.

In one aspect of the present invention, a system for performing enrichment of network alarms is disclosed. The system includes a collector component configured to receive an alarm raised by a node for an event. The alarm comprises one or more attributes indicating a hardware, software, or network issue associated with the node. The system includes a fault processor configured to identify eligibility of the alarm for at least one of physical enrichment and logical enrichment. The eligibility is determined based on physical placement related attributes included in the alarm. The fault processor is also configured to perform, based on the eligibility, at least one of the physical enrichment and the logical enrichment of the alarm. The physical enrichment attributes comprise device location, device type, interface details, serial numbers, rack or cabinet number, power supply status, temperature and environmental conditions, device health and status, software and firmware versions, and connectivity information. The logical enrichment attributes comprise Internet Protocol (IP) address, routing protocols, virtual local area network (VLAN) configurations, network topology, virtual network configurations, network service mappings, logical relationships between network elements, network policies, and access control lists (ACLs).

[0007] In one aspect, the physical enrichment involves including static data of the node within the alarm, and the logical enrichment includes involves including contextual information related to network protocols, routing, virtual configurations, and logical relationships between network elements into the alarm. The fault processor performs the physical enrichment and the logical enrichment by collecting attributes by traversing across levels of an inventory provisioned for the node in an inventory database, and appending the attributes into the alarm. A Network Management System (NMS) database stores enrichment data collected during one or more of the physical enrichment and the logical enrichment. The fault processor

checks availability of the enrichment data in the NMS database prior to performing at least one of the physical enrichment and the logical enrichment of the alarm. The fault processor fetches the enrichment data for performing at least one of the physical enrichment and the logical enrichment of the alarm. A predefined time period is associated with the enrichment data, and after expiration of the predefined time period, the enrichment data becomes unusable.

[0008] In another aspect of the present invention, a method of performing enrichment of network alarms is disclosed. The method includes the step of receiving an alarm raised by a node for an event. The alarm comprising one or more attributes indicating a hardware, software, or network issue associated with the node. The method further includes the step of identifying eligibility of the alarm for at least one of physical enrichment and logical enrichment. The eligibility is determined based on physical placement related attributes included in the alarm. The method further includes the step of performing at least one of the physical enrichment and the logical enrichment of the alarm, based on the eligibility. The physical enrichment attributes comprise device location, device type, interface details, serial numbers, rack or cabinet number, power supply status, temperature and environmental conditions, device health and status, software and firmware versions, and connectivity information. The logical enrichment attributes comprise Internet Protocol (IP) address, routing protocols, virtual local area network (VLAN) configurations, network topology, virtual network configurations, network service mappings, logical relationships between network elements, network policies, and access control lists (ACLs).

[0009] In one aspect, the physical enrichment involves including static data of the node within the alarm, and the logical enrichment includes involves including contextual information related to network protocols, routing, virtual configurations, and logical relationships between network elements into the alarm. The fault processor performs the physical enrichment and the logical enrichment by collecting attributes by traversing across levels of an inventory provisioned for the node in an

inventory database, and appending the attributes into the alarm. A Network Management System (NMS) database stores enrichment data collected during one or more of the physical enrichment and the logical enrichment. The fault processor checks availability of the enrichment data in the NMS database prior to performing at least one of the physical enrichment and the logical enrichment of the alarm. The fault processor fetches the enrichment data for performing at least one of the physical enrichment and the logical enrichment of the alarm. A predefined time period is associated with the enrichment data, and after expiration of the predefined time period, the enrichment data becomes unusable.

[0010] Other features and aspects of this invention will be apparent from the following description and the accompanying drawings. The features and advantages described in this summary and in the following detailed description are not all-inclusive, and particularly, many additional features and advantages will be apparent to one of ordinary skill in the relevant art, in view of the drawings, specification, and claims hereof. Moreover, it should be noted that the language used in the specification has been principally selected for readability and instructional purposes and may not have been selected to delineate or circumscribe the inventive subject matter, resort to the claims being necessary to determine such inventive subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] The accompanying drawings, which are incorporated herein, and constitute a part of this disclosure, illustrate exemplary embodiments of the disclosed methods and systems in which like reference numerals refer to the same parts throughout the different drawings. Components in the drawings are not necessarily to scale, emphasis instead being placed upon clearly illustrating the principles of the present disclosure. Some drawings may indicate the components using block diagrams and may not represent the internal circuitry of each component. It will be appreciated by those skilled in the art that disclosure of such drawings includes disclosure of

electrical components, electronic components or circuitry commonly used to implement such components.

[0012] **FIG. 1** illustrates a network architecture of a system for enrichment of network alarms, according to one or more embodiments of the present disclosure;

[0013] **FIG. 2** illustrates a block diagram of the system for enrichment of network alarms, according to various embodiments of the present system;

[0014] **FIG. 3** illustrates a block diagram of the system and a node communicating with each other for enrichment of alarms, according to various embodiments of the present system;

[0015] **FIG. 4** illustrates a system operation architecture for enrichment of alarms, according to one or more embodiments of the present disclosure;

[0016] **FIG. 5** illustrates a flow chart of a method of performing enrichment of alarms, according to one or more embodiments of the present disclosure.

[0017] The foregoing shall be more apparent from the following detailed description of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0018] Some embodiments of the present disclosure, illustrating all its features, will now be discussed in detail. It must also be noted that as used herein and in the appended claims, the singular forms "a", "an" and "the" include plural references unless the context clearly dictates otherwise.

[0019] Various modifications to the embodiment will be readily apparent to those skilled in the art and the generic principles herein may be applied to other embodiments. However, one of ordinary skill in the art will readily recognize that the present disclosure including the definitions listed here below are not intended to be limited to the embodiments illustrated but is to be accorded the widest scope consistent with the principles and features described herein.

[0020] A person of ordinary skill in the art will readily ascertain that the illustrated steps detailed in the figures and here below are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments.

[0021] The proposed invention introduces a novel approach of enriching alarms received at a fault processor with both dynamic and static data. The static data refers to information related to the physical attributes of the network infrastructure, while the dynamic data represents the real-time aspects of the alarm event. Present invention exhibits technical advancement of implementing a profile-based inventory level traversal. This method involves traversing the network inventory based on predefined profiles to collect the static data for physical enrichment. The static data includes details such as physical placement, location, interfaces, and other relevant attributes of the network nodes.

[0022] Once the profile-based inventory level traversal is completed, the static data obtained from the traversal is inserted into the raw alarm received at the fault processor. This enriched alarm now contains both dynamic and static data, providing a more comprehensive view of the alarm event and its physical context within the network infrastructure.

[0023] Furthermore, the invention introduces a profile-based eligibility evaluation process for logical enrichment. Based on the physical enrichment data obtained, the

alarm's eligibility for logical enrichment is determined. Logical enrichment involves incorporating contextual information related to network protocols, routing, virtual configurations, and logical relationships between network elements. If the alarm is found eligible for logical enrichment, similar profile-based traversal techniques are applied to collect the necessary data. This logical enrichment data is then combined with the previously enriched alarm, further enhancing the understanding of the alarm event and its impact on the logical aspects of the network.

[0024] By enriching the alarms with both physical and logical data, the proposed invention enables more effective fault analysis, troubleshooting, and network management within the NMS. The comprehensive information provided by the enrichment processes allows network administrators to quickly identify the root causes of alarms, accurately assess their impact, and take appropriate actions for resolution.

[0025] The invention can be implemented in a server-based network management system, where various modules collaborate for enrichment of the alarms. The inventive step lies in cache based enrichment of alarms. The physical and logical enrichment for an alarm is performed based on cached data corresponding to the alarm which is stored in a database (DB) of the NMS.

[0026] **FIG. 1** illustrates a network architecture of a system for enrichment of network alarms. The network architecture comprises a plurality of network nodes **102-1, 102-2,……,102-n**. At least one of the network nodes **102-1** through **102-n** may be configured to connect to a server **105**. For ease of disclosure, a network node whose network alarm is enriched is referred as node **102**.

[0027] The node **102** may comprise a memory such as a volatile memory (e.g., RAM), a non-volatile memory (e.g., disk memory, FLASH memory, EPROMs, etc.), an unalterable memory, and/or other types of memory. In one implementation, the memory might be configured or designed to store data. The node **102** may connect with the server **105** for sending alarms. The node **102** may be configured to connect

with the server **105** through a communication network **110**. The communication network **110** may use one or more communication interfaces/protocols such as, for example, VoIP, 802.11 (Wi-Fi), 802.15 (including Bluetooth™), 802.16 (Wi-Max), 802.22, Cellular standards such as CDMA, CDMA2000, WCDMA, Radio Frequency (e.g., RFID), Infrared, laser, Near Field Magnetics, etc.

[0028] The server **105** may include by way of example but not limitation, one or more of a standalone server, a server blade, a server rack, a bank of servers, a business telephony application server (BTAS), a server farm, hardware supporting a part of a cloud service or system, a home server, hardware running a virtualized server, one or more processors executing code to function as a server, one or more machines performing server-side functionality as described herein, at least a portion of any of the above, some combination thereof. In an embodiment, the entity may include, but is not limited to, a vendor, a network operator, a company, an organization, a university, a lab facility, a business enterprise, a defence facility, or any other facility that provides content.

[0029] Further, the server **105** may be communicably connected to a system **125**, via the communication network **110**. The system **125** may be configured to access services subscribed by enterprises, and additional services as mentioned above.

[0030] A person skilled in the art will appreciate that the plurality of nodes **102** may include end devices and intermediary devices. The end devices serve as originator of data or information flowing through the communication network **110**. For example, the end devices may include workstations, laptops, desktop computers, printers, scanners, servers (file servers, web Servers), mobile phones, tablets, and smart phones. The intermediary devices are configured to forward data from one point to another in a communication network **110**. For example, the intermediary devices may include hubs, modems, switches, routers, bridges, repeaters, security firewalls, and wireless access points.

[0031] The communication network **110** includes, by way of example but not limitation, one or more of a wireless network, a wired network, an internet, an intranet, a public network, a private network, a packet-switched network, a circuit-switched network, an ad hoc network, an infrastructure network, a Public-Switched Telephone Network (PSTN), a cable network, a cellular network, a satellite network, a fiber optic network, or some combination thereof. The communication network **110** may include, but is not limited to, a Third Generation (3G), a Fourth Generation (4G), a Fifth Generation (5G), a Sixth Generation (6G), a New Radio (NR), a Narrow Band Internet of Things (NB-IoT), an Open Radio Access Network (O-RAN), and the like.

[0032] The communication network **110** may also include, by way of example but not limitation, at least a portion of one or more networks having one or more nodes that transmit, receive, forward, generate, buffer, store, route, switch, process, or a combination thereof, etc. one or more messages, packets, signals, waves, voltage or current levels, some combination thereof, or so forth. The network may also include, by way of example but not limitation, one or more of a wireless network, a wired network, an internet, an intranet, a public network, a private network, a packet-switched network, a circuit-switched network, an ad hoc network, an infrastructure network, a Public-Switched Telephone Network (PSTN), a cable network, a cellular network, a satellite network, a fiber optic network, a VOIP or some combination thereof.

[0033] The system **125** (alternatively referred as a Network Management system (NMS) **125**) is communicably coupled to the server **105** and each of the first node **102-1**, the second node **102-2**, and the third node **102-n** via the communication network **110**. The system **125** is configured to handle repetitive alarms and auditing. The system **125** is adapted to be embedded within the server **105** or is embedded as an individual entity. However, for the purpose of description, the system **125** is described as an integral part of the server **105**, without deviating from the scope of the present disclosure.

[0034] In various embodiments, the system **125** may be generic in nature and may be integrated with any application including a System Management Facility (SMF), an Access and Mobility Management Function (AMF), a Business Telephony Application Server (BTAS), a Converged Telephony Application Server (CTAS), any SIP (Session Initiation Protocol) Application Server which interacts with core Internet Protocol Multimedia Subsystem (IMS) on Industrial Control System (ISC) interface as defined by Third Generation Partnership Project (3GPP) to host a wide array of cloud telephony enterprise services, a System Information Blocks (SIB)/ and a Mobility Management Entity (MME).

[0035] System Management Facility (SMF) is an IBM z/OS component that collects, formats, and records system and job-related information for monitoring, auditing, and performance analysis purposes. It serves as a central repository for various types of operational data generated by the z/OS operating system and related subsystems.

[0036] Access and Mobility Management Function (AMF) is a key component in 5G mobile networks, responsible for managing access to the network and handling mobility-related functions for user equipment (UE), such as smartphones, tablets, and IoT devices. AMF works closely with other network functions to facilitate seamless connectivity, mobility, and quality of service for mobile users.

[0037] Business Telephony Application Server (BTAS) is a server-based system that provides telephony services and applications for businesses. It serves as a central platform for managing and delivering various voice communication services, such as voice calls, voicemail, conferencing, and interactive voice response (IVR) systems.

[0038] Converged Telephony Application Server (CTAS) is a server-based system that integrates various telephony and communication services into a single platform, enabling businesses to streamline their communication infrastructure and offer a wide range of communication features. CTAS combines traditional telephony services with advanced IP-based communication capabilities to provide a unified and cohesive communication experience.

[0039] SIP (Session Initiation Protocol) application server is a server-based system that facilitates the establishment, management, and termination of communication sessions using the SIP protocol. SIP application servers play a central role in IP-based telecommunications networks, enabling a wide range of real-time communication services, including voice calls, video calls, instant messaging, presence, and multimedia conferencing.

[0040] Internet Protocol Multimedia Subsystem (IMS) is a standardized architecture that enables the delivery of multimedia communication services over IP networks, including voice, video, messaging, and presence services. IMS is designed to provide a framework for delivering real-time communication services in a flexible, scalable, and interoperable manner.

[0041] Cloud telephony enterprise services refer to communication solutions delivered over the cloud that cater specifically to the needs of businesses and organizations. These services leverage cloud technology to provide scalable, flexible, and cost-effective communication solutions, including voice calls, messaging, collaboration tools, and contact center capabilities.

[0042] System Information Blocks (SIBs) are messages broadcast by a base station (eNodeB in LTE, NodeB in UMTS, or eNB in 5G) to provide essential information to mobile devices (UEs) in a cellular network. SIBs contain network-related information necessary for UEs to access and operate within the network efficiently. These blocks are periodically transmitted over broadcast channels, allowing UEs to receive and decode them even when they are not actively engaged in communication.

[0043] In the context of mobile networks, specifically in the LTE (Long-Term Evolution) and 5G architectures, the Mobility Management Entity (MME) is a key network element responsible for managing mobility-related functions for user equipment (UE) or mobile devices. The MME is part of the Evolved Packet Core (EPC) network in LTE and the 5G Core (5GC) network in 5G, serving as a control plane entity that handles signaling and control procedures for mobility management.

[0044] Operational and construction features of the system **125** will be explained in detail successively with respect to different figures. **FIG. 2** illustrates a block diagram of the system **125** for enrichment of network alarms, according to one or more embodiments of the present disclosure.

[0045] As per the illustrated embodiment, the system **125** includes one or more processors **205**, a memory **210**, and an input/output interface unit **215**. The one or more processors **205**, hereinafter referred to as the processor **205**, may be implemented as one or more microprocessors, microcomputers, microcontrollers, digital signal processors, central processing units, state machines, logic circuitries, single board computers, and/or any devices that manipulate signals based on operational instructions. As per the illustrated embodiment, the system **125** includes the processor **205**. However, it is to be noted that the system **125** may include multiple processors as per the requirement and without deviating from the scope of the present disclosure. Among other capabilities, the processor **205** is configured to fetch and execute computer-readable instructions stored in the memory **210**. The memory **210** may be configured to store one or more computer-readable instructions or routines in a non-transitory computer-readable storage medium, which may be fetched and executed to create or share data packets over a network service. The memory **210** may include any non-transitory storage device including, for example, volatile memory such as RAM, or non-volatile memory such as EPROM, flash memory, and the like.

[0046] In an embodiment, the input/output (I/O) interface unit **215** includes a variety of interfaces, for example, interfaces for data input and output devices, referred to as Input/Output (I/O) devices, storage devices, and the like. The I/O interface unit **215** facilitates communication of the system **125**. In one embodiment, the I/O interface unit **215** provides a communication pathway for one or more components of the system **125**. Examples of such components include, but are not limited to, the nodes **102**, an NMS database **220**, and a distributed cache **225**.

[0047] The NMS database **220** is one of, but is not limited to, a centralized database, a cloud-based database, a commercial database, an open-source database, a distributed database, an end-user database, a graphical database, a No-Structured Query Language (NoSQL) database, an object-oriented database, a personal database, an in-memory database, a document-based database, a time series database, a wide column database, a key value database, a search database, a cache database, and so forth. The foregoing examples of the NMS database **220** types are non-limiting and may not be mutually exclusive e.g., a database can be both commercial and cloud-based, or both relational and open-source, etc.

[0048] The distributed cache **225** is a pool of Random-Access Memory (RAM) of multiple networked computers into a single in-memory data store for use as a data cache to provide fast access to data. The distributed cache **225** is essential for applications that need to scale across multiple servers or are distributed geographically. The distributed cache **225** ensures that data is available close to where it's needed, even if the original data source is remote or under heavy load.

[0049] Further, the processor **205**, in an embodiment, may be implemented as a combination of hardware and programming (for example, programmable instructions) to implement one or more functionalities of the processor **205**. In the examples described herein, such combinations of hardware and programming may be implemented in several different ways. For example, the programming for the processor **205** may be processor-executable instructions stored on a non-transitory machine-readable storage medium and the hardware for the processor **205** may comprise a processing resource (for example, one or more processors), to execute such instructions. In the present examples, the memory **210** may store instructions that, when executed by the processing resource, implement the processor **205**. In such examples, the system **125** may comprise the memory **210** storing the instructions and the processing resource to execute the instructions, or the memory **210** may be separate but accessible to the system **125** and the processing resource. In other examples, the processor **205** may be implemented by electronic circuitry.

[0050] For the system **125** to perform enrichment of network alarms, the processor **205** includes a collector component **228** and a fault processor **230** communicably coupled to each other.

[0051] The collector component **228** of the processor **205** is communicably connected to each of the first node **102-1**, the second node **102-2**, and the third node **102-n** via the communication network **110**. Accordingly, the collector component **228** is configured to receive an alarm raised by the node **102** for an event. The alarm comprises one or more attributes indicating a hardware, software, or network issue associated with the node **102**. The fault processor **230** identifies eligibility of the alarm for at least one of physical enrichment and logical enrichment. The eligibility is determined based on physical placement related attributes included in the alarm. Further, the fault processor **230** performs at least one of the physical enrichment and the logical enrichment of the alarm, based on the eligibility of the alarm. The physical enrichment involves including static data of the node within the alarm. The logical enrichment includes involves including contextual information related to network protocols, routing, virtual configurations, and logical relationships between network elements into the alarm. The physical enrichment and the logical enrichment is performed by collecting attributes by traversing across levels of an inventory provisioned for the node in an inventory database **408**, and appending the attributes into the alarm.

[0052] The NMS database **220** of the system **125** serves as a non-structured (NoSQL) database that stores the enrichment data collected during one or more of the physical enrichment and the logical enrichment. The database **220** plays a crucial role in persistently storing and managing the enrichment data, ensuring its availability for enrichment of the alarms.

[0053] Referring to **FIG. 3** illustrating a block diagram of the system **125** and the first node **102-1** communicating with each other for enrichment of alarms, a preferred embodiment of the system **125** is described. It is to be noted that the embodiment with respect to **FIG. 3** will be explained with respect to the first node

102-1 for the purpose of description and illustration and should nowhere be construed as limited to the scope of the present disclosure.

[0054] The first node **102-1** includes one or more primary processors **305** communicably coupled to the processor **205** of the system **125**. The one or more primary processors **305** are coupled with a memory unit **310** storing instructions which are executed by the one or more primary processors **305**. Execution of the stored instructions by the one or more primary processors **305** enables the first node **102-1** to provide an alarm corresponding to an event. The first node **102-1** further includes a kernel **315** which is a core component serving as the primary interface between hardware components of the first network device **110a** and the plurality of services at the NMS database **220**. The kernel **315** is configured to provide the plurality of services on the first node **102-1** to resources available in the communication network **110**. The resources include one of a Central Processing Unit (CPU), memory components such as Random Access Memory (RAM) and Read Only Memory (ROM).

[0055] In the preferred embodiment, the collector component **228** of the processor **205** is communicably connected to the kernel **315** of the first node **102-1**. The collector component **228** is configured to collect the alarms corresponding to network events. The alarms comprise alarm comprise one or more attributes indicating a hardware, software, or network issue associated with the node first node **102-1**. The processor **205** further include the fault processor **230** communicably connected to the collector component **228** to identify eligibility of the alarm for at least one of physical enrichment and logical enrichment. The eligibility is determined based on physical placement related attributes included in the alarm. Successively, based on the eligibility, the fault processor **230** performs at least one of the physical enrichment and the logical enrichment of the alarm. the physical enrichment and the logical enrichment is performed by collecting attributes by traversing across levels of an inventory provisioned for the node in an inventory database **408**, and appending the attributes into the alarm.

[0056] The physical enrichment involves including static data of the node within the alarm, and the logical enrichment includes involves including contextual information related to network protocols, routing, virtual configurations, and logical relationships between network elements into the alarm. The physical enrichment attributes comprise a device location, device type, interface details, serial numbers, rack or cabinet number, power supply status, temperature and environmental conditions, device health and status, software and firmware versions, and connectivity information. The logical enrichment attributes comprise Internet Protocol (IP) address, routing protocols, virtual local area network (VLAN) configurations, network topology, virtual network configurations, network service mappings, logical relationships between network elements, network policies, and access control lists (ACLs).

[0057] An IP address, or Internet Protocol address, is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves two main purposes: identifying the host or network interface and providing the location of the device in the network. There are two primary versions of IP addresses currently in use: IPv4, which consists of four sets of numbers separated by periods (e.g., 192.0.2.1), and IPv6, which uses a longer hexadecimal format (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). IP addresses are essential for devices to communicate with each other over the internet.

[0058] Routing protocols are a set of rules or algorithms that determine the best path for data packets to travel from one network to another in a computer network. These protocols are essential for routers to exchange information and make decisions about how to forward data across interconnected networks. A few common routing protocols include Distance Vector Routing Protocol, Link-State Routing Protocol, Hybrid Routing Protocol, and Border Gateway Protocol.

[0059] VLAN (Virtual Local Area Network) configurations involve setting up and managing virtual LANs within a network infrastructure. VLANs allow you to

segment your network logically, even if devices physically connect to the same switch or router.

[0060] Network topology refers to the physical or logical layout of a computer network. It defines how devices such as computers, servers, switches, routers, and other peripherals are interconnected and how data flows between them. A few common network topologies include star topology, bus topology, ring topology, mesh topology, and tree topology.

[0061] Virtual network configurations involve setting up and managing virtual networks within a physical network infrastructure. These virtual networks operate independently of the physical hardware, allowing for greater flexibility, scalability, and resource optimization.

[0062] Network service mapping is the process of identifying and documenting the relationships and dependencies between network services and the underlying IT infrastructure components that support them. This mapping provides a visual representation of how various services are interconnected and how they rely on specific hardware, software, and configurations within the network.

[0063] Logical relationships between network elements refer to the connections and dependencies that exist between various components in a network at a conceptual or logical level. These relationships define how data flows, how devices communicate, and how services are delivered within the network.

[0064] Network policies are sets of rules, guidelines, and procedures that govern how a network is managed, configured, secured, and used. These policies define the acceptable use of network resources, establish security measures, and outline procedures for network administration. A few common types of network policies include Acceptable user policy, security policy, access control policy, data retention policy, and network configuration policy.

[0065] The NMS database **220** of the system **125** stores the enrichment data collected during one or more of the physical enrichment and the logical enrichment.

Thereafter, when another alarm is received, the fault processor **230** checks availability of the enrichment data in the NMS database **220** prior to performing at least one of the physical enrichment and the logical enrichment of the alarm. In case the enrichment data is identified to be present, the fault processor **230** fetches the enrichment data for performing at least one of the physical enrichment and the logical enrichment of the alarm. The enrichment data can also be associated with an expiry time i.e. predefined time period so that the enrichment data cannot be used post expiration of the predefined time period.

[0066] **FIG. 4** illustrates a system operation architecture for enrichment of alarms, according to one or more embodiments of the present disclosure. The collector component (labelled as collector) **228** receives alarms corresponding to network events from a node **102**. The collector component **228** passes the alarm to the fault processor **230** in a data stream. Upon receiving the alarm, the fault processor **230** determines if enrich cache for the node **102** is enabled or not, at block **402**. If identified to be enabled, the fault processor **230** performs cached enrichment, at block **404**. To perform cached enrichment, the fault processor **230** fetches enrichment data corresponding to the node **102** from the NMS database (NMS D/B) **220**. The enrichment data includes physical enrichment attributes and logical enrichment attributes. Alternatively, at block **402**, if cached enrichment is identified to be not enabled, an enrichment processor **406** performs physical enrichment using a node profile or a global profile (when node profile is not available) stored in an inventory to obtain physical enrichment parameters. Subsequently, if the alarm is identified to be eligible for logical enrichment, logical enrichment is also performed using the inventory and one or more physical enrichment attributes to obtain the logical enrichment attributes.

[0067] Subsequently, the physical enrichment attributes and the logical enrichment attributes are provided as enrichment data to the fault processor **230**. The fault processor **230** uses the enrichment data to obtain an enriched alarm. The fault processor **230** also stores the enriched alarm in the NMS database **220**. The enriched

alarm or the enrichment data may be stored along with a timer (predefined time period) for future cached enrichment processing.

[0068] **FIG. 5** illustrates a flow chart of a method **500** of performing enrichment of alarms, according to one or more embodiments of the present disclosure. For the purpose of description, the method **500** is described with the embodiments as illustrated in **FIGS. 1** and **4** and should nowhere be construed as limiting the scope of the present disclosure.

[0069] At step **505,** the method **500** includes the step of receiving an alarm corresponding to a network event, by a processor. The alarm may include dynamic data and alarm data. The alarm data refers to information generated by network devices or systems to indicate abnormal or noteworthy events, conditions, or failures within the network infrastructure. Such alarms are generated in response to predefined conditions or thresholds being met, signaling potential issues that require attention from network administrators or automated systems. In one implementation, a collector of a network management system may receive the alarm from a node and may pass the alarm in a data stream to a fault processor.

[0070] At step **510,** the method **500** includes the step of determining whether cached enrichment is enabled or not. The fault processor checks availability of enrichment data corresponding to the node and a related timer. The enrichment data may include physical enrichment attributes and logical enrichment attributes associated with a node, stored in an NMS database. To determine the duration for which the enrichment data corresponding to a specific node has been stored in the NMS database, a configurable predefined timer is used. For example, where the corresponding enrichment data is available in the NMS DB and where the timer is less than 24 hours, the method may proceed to step **515**.

[0071] At step **515,** the method **500** includes the step of performing physical enrichment and logical enrichment of the alarm based on cached enrichment data

corresponding to the alarm stored in the NMS database. For performing the physical enrichment and the logical enrichment of the alarm, enrichment data including physical enrichment attributes and logical enrichment attributes corresponding to the node are fetched from a cached storage of the NMS database. Successively, the alarm is enriched using the enrichment data. In a scenario, when the enrichment data is not available in the NMS database or the enrichment data is available in the NMS database but the timer is above 24 hours, the method may proceed to step **520**.

[0072] At step **520,** the method **500** includes the step of performing physical enrichment of the alarm using an inventory based on a set of predefined parameters to obtain physical enrichment attributes. For example, the physical enrichment attributes may include device location, device type, interface details, serial numbers, rack or cabinet number, power supply status, temperature and environmental conditions, device health and status, software and firmware versions, and connectivity information. The inventory may include a plurality of node profiles associated with a plurality of nodes that are registered with the NMS. In an embodiment, the node profiles may be configurable. For instance, every node profile can be configured with separate order of level traversals with AND or OR logic between the levels. For e.g.: order="level-1| level-2| level-3, level-4| level-5, level-6| level-7, level-8".

[0073] Furthermore, the profile configurations can be changed in runtime and are readily applicable. This means that the profiles, which define the specific criteria and rules for inventory level traversal, can be modified dynamically during system operation. The ability to change profiles in runtime allows for immediate adjustments to the alarm processing flow based on evolving network conditions or management requirements. The changes made to the profiles take effect immediately, ensuring that the system adapts swiftly to varying scenarios.

[0074] Furthermore, index and record type particulars for each level traversal in the inventory database (DB) are also maintained. As the system traverses each

inventory level during the alarm processing flow, it maintains the necessary information about the index and record types associated with that particular level. This information is crucial for efficient retrieval and processing of the relevant data during traversal.

[0075] Yet further, the value of a known attribute that needs to be searched is configurable against the attribute of the index of the current level traversal. This flexibility allows the system to adapt to different inventory structures and search requirements. Administrators can configure which attribute of the inventory index corresponds to the known attribute they are searching for. By defining this mapping between attributes, the system can effectively retrieve the desired data during traversal, enabling efficient data processing and analysis.

[0076] Furthermore, the inventory also includes a global profile, for cases where a node cannot be recognized. Thus, in step **520**, physical enrichment of the alarm is performed based on the corresponding profile or a global profile, to obtain one or more physical enrichment attributes.

[0077] At step **525,** the method **500** includes the step of performing logical enrichment of the alarm based on the one or more physical enrichment attributes and the inventory to obtain logical enrichment attributes. The logical enrichment attributes may include IP addressing, routing protocols, VLAN configurations, network topology, virtual network configurations, network service mappings, logical relationships between network elements, network policies, and access control lists (ACLs). For performing the logical enrichment, all levels of the inventory may be traversed, and the responses obtained from each level traversal are stored in a map, with the key being the name of the corresponding level. As the system progresses through the inventory levels, responses and associated data is collected from each traversal. These responses are then organized and stored in a map structure, where the key corresponds to the name or identifier of the respective level.

[0078] At step **530,** the method **500** includes the step of appending the physical enrichment attributes and the logical enrichment attributes to the alarm for its enrichment. The enriched alarm is also sent to the NMS database for storing and a timer is associated with it.

[0079] The present invention further discloses a non-transitory computer-readable medium having stored thereon computer-readable instructions. The computer-readable instructions are executed by the processor **205**. The processor **205** is configured to receive an alarm raised by a node for an event. The alarm comprises one or more attributes indicating a hardware, software, or network issue associated with the node. The processor **205** is further configured to identify eligibility of the alarm for at least one of physical enrichment and logical enrichment. The eligibility is determined based on physical placement related attributes included in the alarm. The processor **205** is further configured to perform at least one of the physical enrichment and the logical enrichment of the alarm, based on the eligibility. The processor **205** is further configured to store enrichment data collected during one or more of the physical enrichment and the logical enrichment in an NMS database **220**.

[0080] A person of ordinary skill in the art will readily ascertain that the illustrated embodiments and steps in description and drawings (FIGS.1-5) are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments.

[0081] The above described techniques (of enriching alarms) of the present disclosure provide multiple advantages, including enhancing the alarm processing flow within the NMS by incorporating dynamic and static data enrichment, configurable attribute search, and cached storage mechanisms. It improves efficiency, scalability, and adaptability, leading to streamlined network management, efficient fault analysis, and improved operational performance within the NMS. Further, the described techniques leverage cached storage of enrichment data within the NMS database, resulting in an advantage of improved processing efficiency. By utilizing previously stored enrichment data, the system minimizes the need for redundant data retrieval during alarm processing. This reduces the overall processing time and resource utilization, enhancing the system's performance and enabling faster response to alarms. The utilization of cached enrichment data ensures that alarms are enriched with relevant information more quickly and effectively, contributing to streamlined network management and enhanced operational efficiency.

[0082] The present invention offers multiple advantages over the prior art and the above listed are a few examples to emphasize on some of the advantageous features. The listed advantages are to be read in a non-limiting manner.

[0083] Server: A server may include or comprise, by way of example but not limitation, one or more of a standalone server, a server blade, a server rack, a bank of servers, a server farm, hardware supporting a part of a cloud service or system, a home server, hardware running a virtualized server, one or more processors executing code to function as a server, one or more machines performing server-side functionality as described herein, at least a portion of any of the above, some combination thereof. In an embodiment, the entity may include, but is not limited to, a vendor, a network operator, a company, an organization, a university, a lab facility, a business enterprise, a defence facility, or any other facility that provides content.

[0084] Network: A network may include, by way of example but not limitation, at least a portion of one or more networks having one or more nodes that transmit,

receive, forward, generate, buffer, store, route, switch, process, or a combination thereof, etc. one or more messages, packets, signals, waves, voltage or current levels, some combination thereof, or so forth. The network may also include, by way of example but not limitation, one or more of a wireless network, a wired network, an internet, an intranet, a public network, a private network, a packet-switched network, a circuit-switched network, an ad hoc network, an infrastructure network, a Public-Switched Telephone Network (PSTN), a cable network, a cellular network, a satellite network, a fiber optic network, or some combination thereof.

[0085] UE/ Wireless Device: A wireless device or a user equipment (UE) may include, but are not limited to, a handheld wireless communication device (e.g., a mobile phone, a smart phone, a phablet device, and so on), a wearable computer device (e.g., a head-mounted display computer device, a head-mounted camera device, a wristwatch computer device, and so on), a Global Positioning System (GPS) device, a laptop computer, a tablet computer, or another type of portable computer, a media playing device, a portable gaming system, and/or any other type of computer device with wireless communication capabilities, and the like. In an embodiment, the UEs may communicate with the system via set of executable instructions residing on any operating system. In an embodiment, the UEs may include, but are not limited to, any electrical, electronic, electro-mechanical or an equipment or a combination of one or more of the above devices such as virtual reality (VR) devices, augmented reality (AR) devices, laptop, a general-purpose computer, desktop, personal digital assistant, tablet computer, mainframe computer, or any other computing device, wherein the computing device may include one or more in-built or externally coupled accessories including, but not limited to, a visual aid device such as camera, audio aid, a microphone, a keyboard, input devices for receiving input from a user such as touch pad, touch enabled screen, electronic pen and the like. It may be appreciated that the UEs may not be restricted to the mentioned devices and various other devices may be used.

[0086] System (for example, computing system): A system may include one or more processors coupled with a memory, wherein the memory may store instructions which when executed by the one or more processors may cause the system to perform offloading/onloading of broadcasting or multicasting content in networks. An exemplary representation of the system for such purpose, in accordance with embodiments of the present disclosure. In an embodiment, the system may include one or more processor(s). The one or more processor(s) may be implemented as one or more microprocessors, microcomputers, microcontrollers, edge or fog microcontrollers, digital signal processors, central processing units, logic circuitries, and/or any devices that process data based on operational instructions. Among other capabilities, the one or more processor(s) may be configured to fetch and execute computer-readable instructions stored in a memory of the system. The memory may be configured to store one or more computer-readable instructions or routines in a non-transitory computer readable storage medium, which may be fetched and executed to create or share data packets over a network service. The memory may comprise any non-transitory storage device including, for example, volatile memory such as Random-Access Memory (RAM), or non-volatile memory such as Electrically Erasable Programmable Read-only Memory (EPROM), flash memory, and the like. In an embodiment, the system may include an interface(s). The interface(s) may comprise a variety of interfaces, for example, interfaces for data input and output devices, referred to as input/output (I/O) devices, storage devices, and the like. The interface(s) may facilitate communication for the system. The interface(s) may also provide a communication pathway for one or more components of the system. Examples of such components include, but are not limited to, processing unit/engine(s) and a database. The processing unit/engine(s) may be implemented as a combination of hardware and programming (for example, programmable instructions) to implement one or more functionalities of the processing engine(s). In examples described herein, such combinations of hardware and programming may be implemented in several different ways. For example, the programming for the processing engine(s) may be processor executable instructions

stored on a non-transitory machine-readable storage medium and the hardware for the processing engine(s) may comprise a processing resource (for example, one or more processors), to execute such instructions. In the present examples, the machine-readable storage medium may store instructions that, when executed by the processing resource, implement the processing engine(s). In such examples, the system may include the machine-readable storage medium storing the instructions and the processing resource to execute the instructions, or the machine-readable storage medium may be separate but accessible to the system and the processing resource. In other examples, the processing engine(s) may be implemented by electronic circuitry. In an aspect, the database may comprise data that may be either stored or generated as a result of functionalities implemented by any of the components of the processor or the processing engines.

[0087] Computer System: A computer system may include an external storage device, a bus, a main memory, a read-only memory, a mass storage device, communication port(s), and a processor. A person skilled in the art will appreciate that the computer system may include more than one processor and communication ports. The communication port(s) may be any of an RS-232 port for use with a modem-based dialup connection, a 10/100 Ethernet port, a Gigabit or 10 Gigabit port using copper or fiber, a serial port, a parallel port, or other existing or future ports. The communication port(s) may be chosen depending on a network, such a Local Area Network (LAN), Wide Area Network (WAN), or any network to which the computer system connects. The main memory may be random access memory (RAM), or any other dynamic storage device commonly known in the art. The read-only memory may be any static storage device(s) including, but not limited to, a Programmable Read Only Memory (PROM) chips for storing static information e.g., start-up or basic input/output system (BIOS) instructions for the processor. The mass storage device may be any current or future mass storage solution, which may be used to store information and/or instructions. The bus communicatively couples the processor with the other memory, storage, and communication blocks. The bus can be, e.g. a Peripheral Component Interconnect (PCI) / PCI Extended (PCI-X) bus,

Small Computer System Interface (SCSI), universal serial bus (USB), or the like, for connecting expansion cards, drives, and other subsystems as well as other buses, such a front side bus (FSB), which connects the processor to the computer system. Optionally, operator and administrative interfaces, e.g. a display, keyboard, and a cursor control device, may also be coupled to the bus to support direct operator interaction with the computer system. Other operator and administrative interfaces may be provided through network connections connected through the communication port(s). In no way should the aforementioned exemplary computer system limit the scope of the present disclosure.

REFERENCE NUMERALS

[0088] Node – 102;

[0089] Server – 105;

[0090] Communication network - 110;

[0091] System - 125;

[0092] One or more processors -205;

[0093] Memory – 210;

[0094] Input/output interface unit – 215;

[0095] NMS Database – 220;

[0096] Distributed cache – 225;

[0097] Collector component – 228;

[0098] Fault processor – 230;

[0099] First node – 102-1;

[00100] Primary processor of first node - 305;

[00101] Memory unit of first node – 310;

[00102] Kernel of the first node – 315;

[00103] Enrichment processor – 406; and

[00104] Inventory database - 408.

We Claim:

1. A method of enrichment of network alarms, the method comprising the steps of:

receiving, by a collector component (228), an alarm raised by a node (102) for an event, the alarm comprising one or more attributes indicating a hardware, software, or network issue associated with the node;

identifying, by a fault processor (230), eligibility of the alarm for at least one of physical enrichment and logical enrichment, wherein the eligibility is determined based on physical placement related attributes included in the alarm; and

performing, by the fault processor (230), based on the eligibility, at least one of the physical enrichment and the logical enrichment of the alarm.

2. The method as claimed in claim 1, wherein the physical enrichment involves including static data of the node within the alarm, and the logical enrichment includes involves including contextual information related to network protocols, routing, virtual configurations, and logical relationships between network elements into the alarm.

3. The method as claimed in claim 1, wherein the physical enrichment and the logical enrichment is performed by collecting attributes by traversing across levels of an inventory provisioned for the node in an inventory database (408), and appending the attributes into the alarm.

4. The method as claimed in claim 1, comprising storing, by the fault processor (230), enrichment data collected during one or more of the physical enrichment and the logical enrichment in a Network Management System (NMS) database (220).

5. The method as claimed in claim 4, comprising checking, by the fault processor (230), availability of the enrichment data in the NMS database (220) prior

to performing at least one of the physical enrichment and the logical enrichment of the alarm.

6. The method as claimed in claim 5, comprising fetching, by the fault processor (230), the enrichment data for performing at least one of the physical enrichment and the logical enrichment of the alarm.

7. The method as claimed in claim 6, comprising associating a predefined time period with the enrichment data, wherein after expiration of the predefined time period, the enrichment data becomes unusable.

8. The method as claimed in claim 1, the physical enrichment attributes comprising one or more of a device location, device type, interface details, serial numbers, rack or cabinet number, power supply status, temperature and environmental conditions, device health and status, software and firmware versions, and connectivity information.

9. The method as claimed in claim 1, the logical enrichment attributes comprising one or more of Internet Protocol (IP) address, routing protocols, virtual local area network (VLAN) configurations, network topology, virtual network configurations, network service mappings, logical relationships between network elements, network policies, and access control lists (ACLs).

10. A system (125) for enrichment of network alarms, the system comprising:

a collector component (228) configured to receive an alarm raised by a node (102) for an event, the alarm comprising one or more attributes indicating a hardware, software, or network issue associated with the node (102); and

a fault processor (230) configured to:

identify eligibility of the alarm for at least one of physical enrichment and logical enrichment, wherein the eligibility is determined based on physical placement related attributes included in the alarm; and

perform, based on the eligibility, at least one of the physical enrichment and the logical enrichment of the alarm.

11. The system as claimed in claim 10**,** wherein the physical enrichment involves including static data of the node within the alarm, and the logical enrichment includes involves including contextual information related to network protocols, routing, virtual configurations, and logical relationships between network elements into the alarm.

12. The system as claimed in claim 10, wherein the fault processor (230) performs the physical enrichment and the logical enrichment by collecting attributes by traversing across levels of an inventory provisioned for the node (102) in an inventory database (408), and appending the attributes into the alarm.

13. The system as claimed in claim 12, comprises a Network Management System (NMS) database (220) for storing enrichment data collected during one or more of the physical enrichment and the logical enrichment.

14. The system as claimed in claim 13, wherein the fault processor (230) checks availability of the enrichment data in the NMS database (220) prior to performing at least one of the physical enrichment and the logical enrichment of the alarm.

15. The system as claimed in claim 14, wherein the fault processor fetches the enrichment data for performing at least one of the physical enrichment and the logical enrichment of the alarm.

16. The system as claimed in claim 15, wherein a predefined time period is associated with the enrichment data, and after expiration of the predefined time period, the enrichment data becomes unusable.

17. The system as claimed in claim 10, wherein the physical enrichment attributes comprise one or more of a device location, device type, interface details, serial numbers, rack or cabinet number, power supply status, temperature and environmental conditions, device health and status, software and firmware versions, and connectivity information.

18. The system as claimed in claim 10, wherein the logical enrichment attributes comprise one or more of Internet Protocol (IP) address, routing protocols, virtual local area network (VLAN) configurations, network topology, virtual network configurations, network service mappings, logical relationships between network elements, network policies, and access control lists (ACLs).

19. A non-transitory computer-readable medium having stored thereon computer-readable instructions that, when executed by a processor, cause the processor (205) to:

receive an alarm raised by a node (102) for an event, the alarm comprising one or more attributes indicating a hardware, software, or network issue associated with the node (102);

identify eligibility of the alarm for at least one of physical enrichment and logical enrichment, wherein the eligibility is determined based on physical placement related attributes included in the alarm; and

perform, based on the eligibility, at least one of the physical enrichment and the logical enrichment of the alarm.

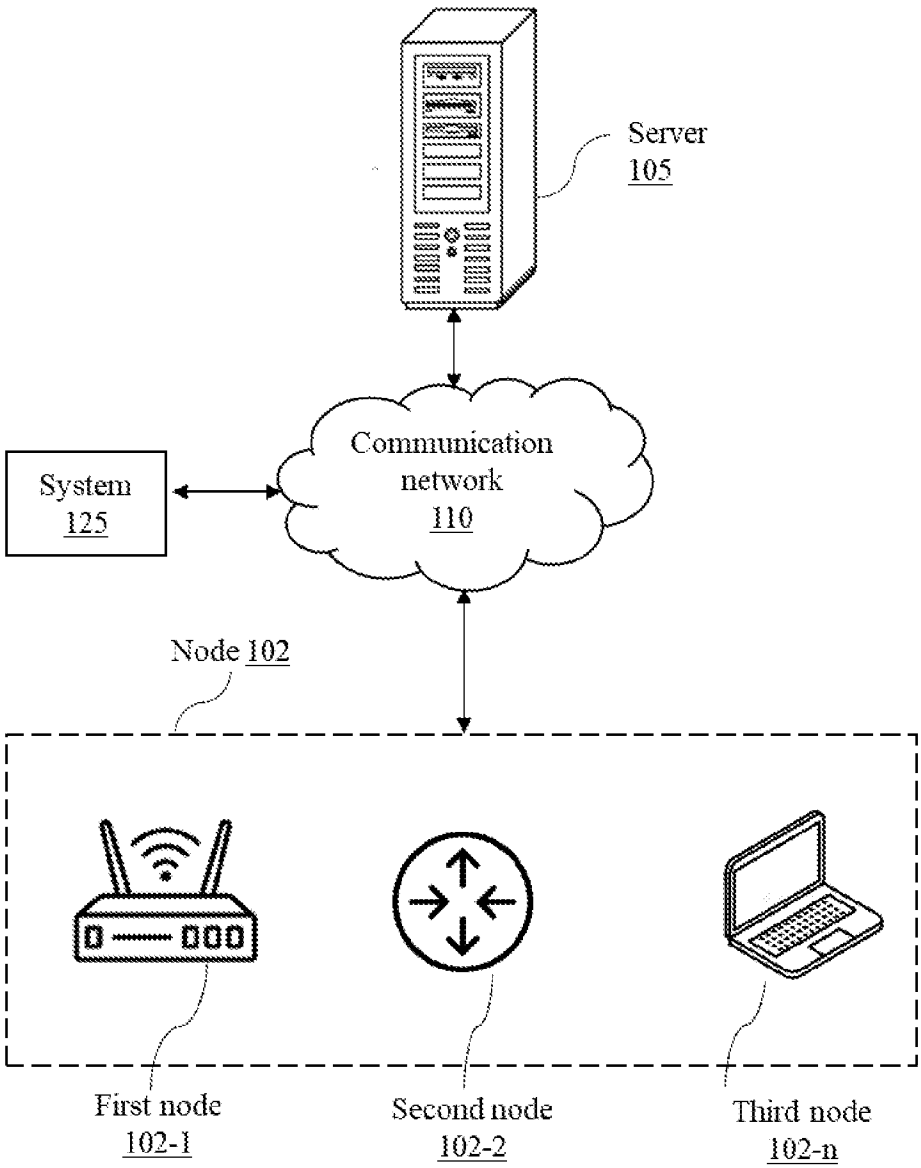
Server
105
Communication
network
110
System
125
Node 102
First node
102-1
Second node
102-2
Third node
102-n

FIG. 1

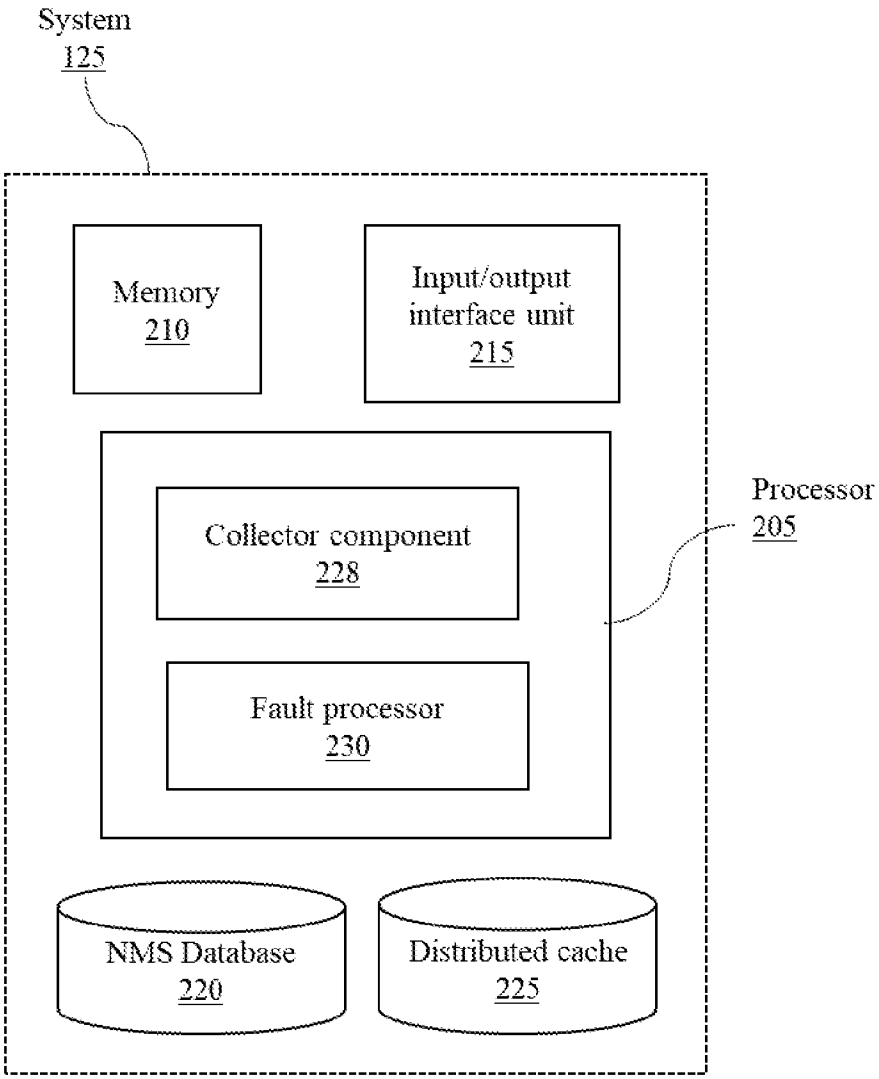
System
125
Memory
210
Input/output
interface unit
215
Processor
205
Collector component
228
Fault processor
230
NMS Database
220
Distributed cache
225

FIG. 2

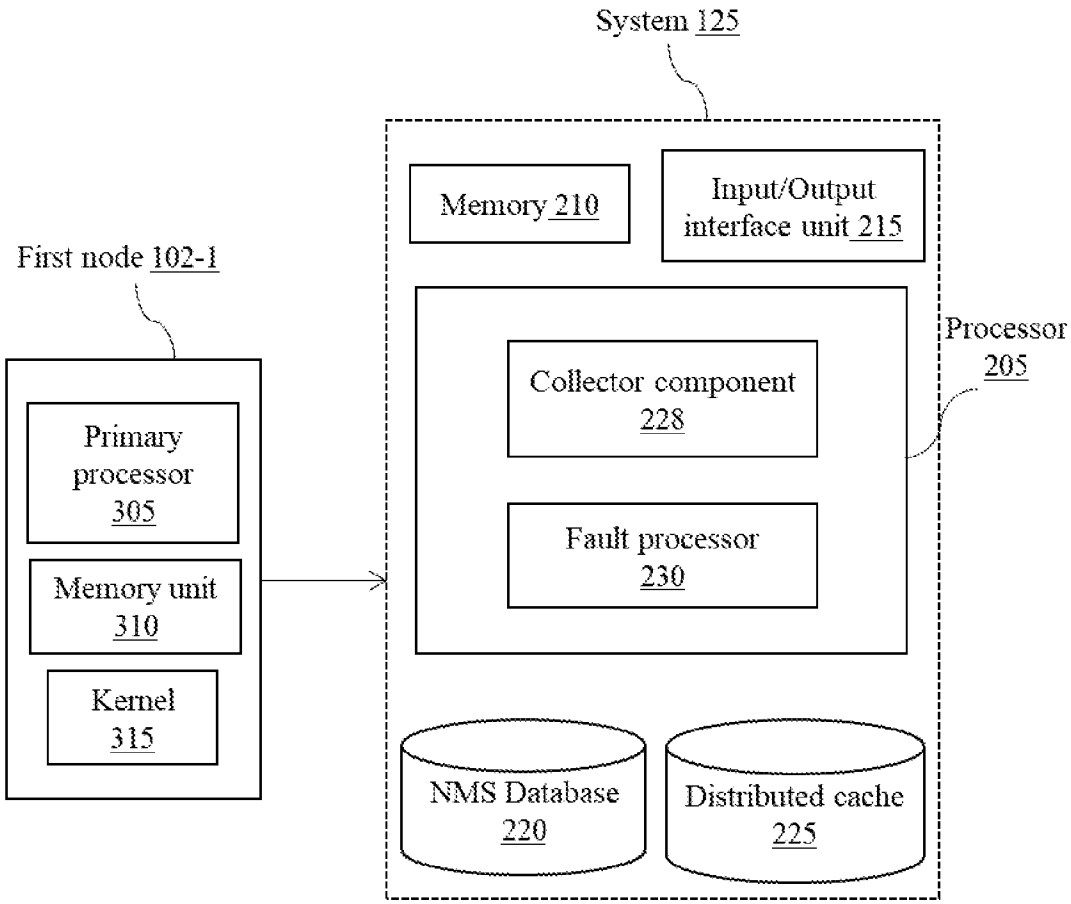
System 125
Memory 210
Input/Output interface unit 215
First node 102-1
Processor 205
Collector component 228
Primary processor 305
Fault processor 230
Memory unit 310
Kernel 315
NMS Database 220
Distributed cache 225

FIG. 3

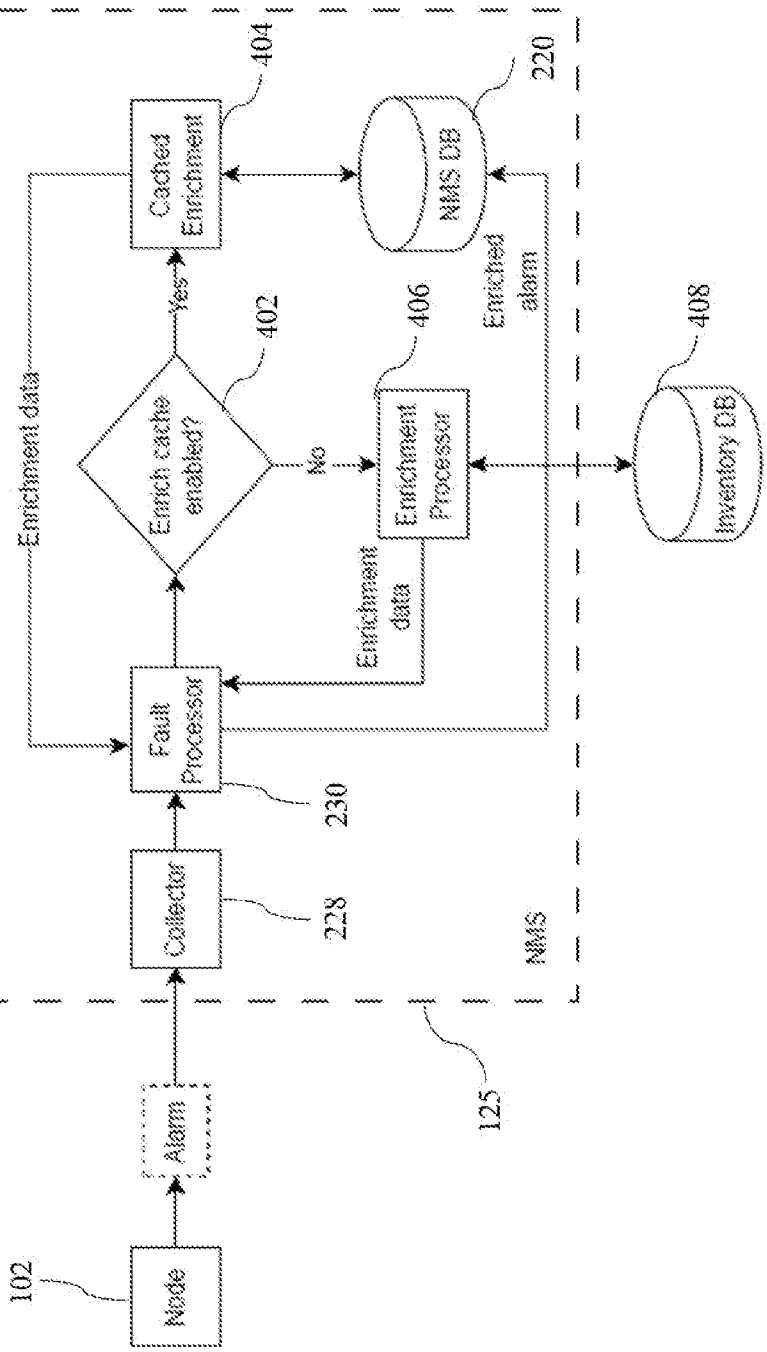
102
Node
Alarm
125
NMS
228
Collector
230
Fault Processor
Enrichment data
Enrich cache enabled?
402
Yes
No
404
Cached Enrichment
406
Enrichment Processor
Enrichment data
220
NMS DB
Enriched alarm
408
Inventory DB

FIG. 4

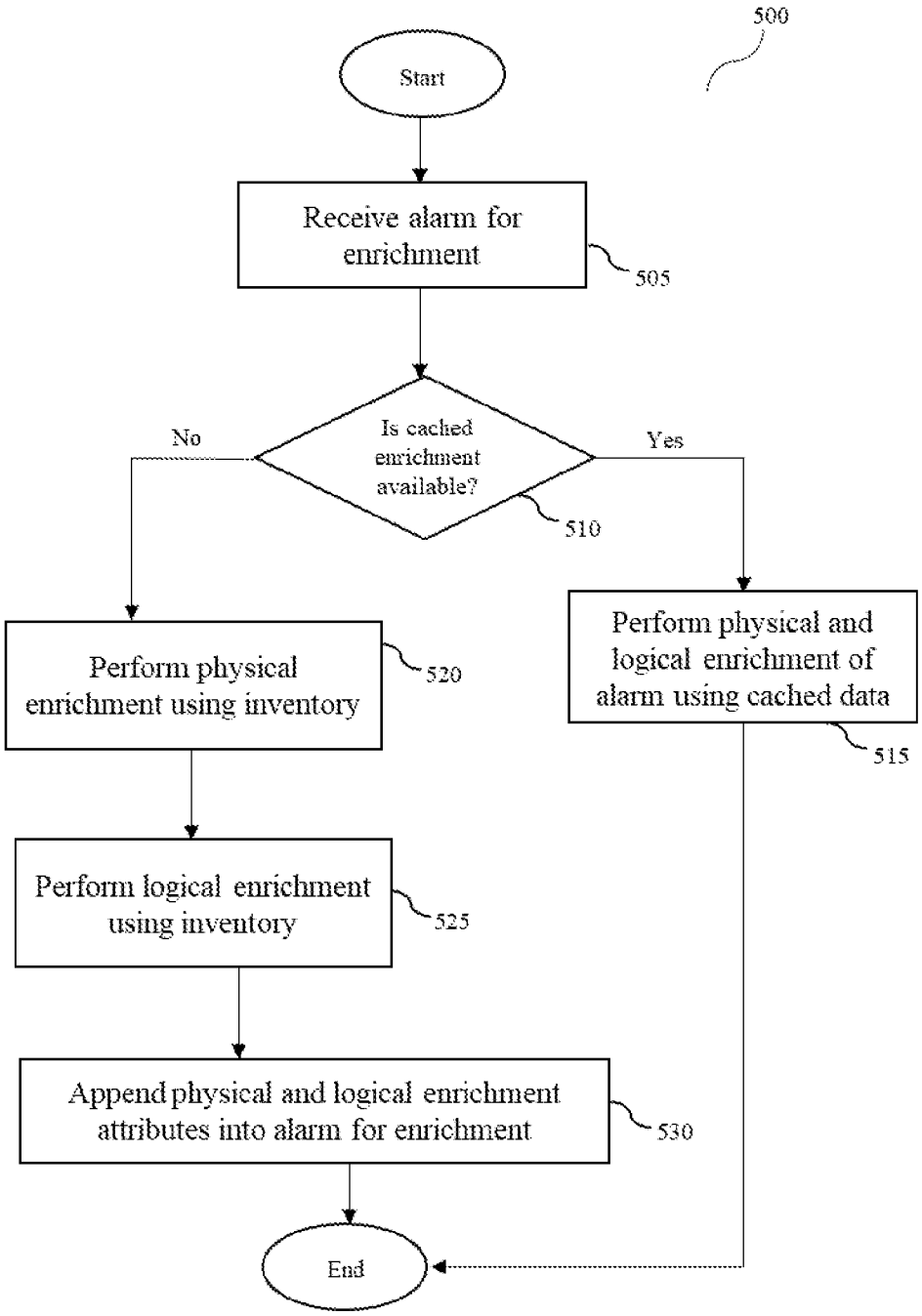
500
Start
Receive alarm for enrichment
505
Is cached enrichment available?
510
No
Yes
Perform physical enrichment using inventory
520
Perform physical and logical enrichment of alarm using cached data
515
Perform logical enrichment using inventory
525
Append physical and logical enrichment attributes into alarm for enrichment
530
End

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IN2024/051033

A. CLASSIFICATION OF SUBJECT MATTER
H04L41/0631,H04L41/0677,H04L41/069 Version=2024.01

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

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

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

PatSeer, IPO Internal Database

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN110798348 B; (HAINAN ELECTRIC POWER INDUSTRY DEVELOPMENT CO. LTD.); 16 DECEMBER 2022 (16/12/2022) (English Translation Copy from Google Patents) Page 3 lines 5-16; Page 6 lines 13-29 ; Figs. 2-3 and related text	1-19
Y	US20170155539 A1; (CENX INC CANADA [ET] [AL.]); 01 JUNE 2017 (01/06/2017) Paragraphs [0006]-[0010], [0035]-[0048] & Fig. 2	1-19
A	US20220086036 A1; (HUAWEI TECHNOLOGIES CO. LTD.); 17 MARCH 2022 (17/03/2022) Paragraphs [0008]-[0017], [0070]-[0081] & Figs. 5-6	1, 10 & 19
A	US10797938 B2; (ACCENTURE GLOBAL SOLUTIONS LTD.); 06 OCTOBER 2020 (06/10/2020) Col. 2 lines 6-23; Col.5 lines 14-22; Col. 6 lines 45-66; Figs. 4-6 and related text	1-3, 10-13 & 19

☐ 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	Date of mailing of the international search report
25-10-2024	25-10-2024
Name and mailing address of the ISA/ Indian Patent Office Plot No.32, Sector 14,Dwarka,New Delhi-110075 Facsimile No.	Authorized officer Jugal Kishor Telephone No. +91-1125300200

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IN2024/051033

Citation	Pub.Date	Family	Pub.Date
CN 110798348 B	16-12-2022	CN 110798348 A	14-02-2020
US 20170155539 A1	01-06-2017	US 9571334 B2	14-02-2017
		US 20160218911 A1	28-07-2016
US 20220086036 A1	17-03-2022	US 11996974 B2	28-05-2024
		WO 2020238810 A1	03-12-2020
		EP 3965371 A4	07-09-2022
		EP 3965371 A1	09-03-2022
		CN 112073208 B	14-01-2022
		CN 112073208 A	11-12-2020
US 10797938 B2	06-10-2020	US 20190379577 A1	12-12-2019