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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
09 January 2025 (09.01.2025)

WIPO | PCT

(10) International Publication Number
WO 2025/008879 A1

(51) International Patent Classification:
H04W 4/70 (2018.01) *H04L 67/12* (2022.01)
H04W 4/50 (2018.01) *H04W 24/02* (2009.01)

(21) International Application Number:
PCT/IN2024/050749

(22) International Filing Date:
11 June 2024 (11.06.2024)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
202321044883 04 July 2023 (04.07.2023) IN

(71) Applicant: **JIO PLATFORMS LIMITED** [IN/IN]; Office - 101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Ahmedabad - 380006, Gujarat (IN).

(72) Inventors: **BHATNAGAR, Aayush**; Office - 101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Ahmedabad - 380006, Gujarat (IN). **SINGH, Kumar Gaurav**; Office - 101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Ahmedabad - 380006, Gujarat (IN). **SINGH, Amit Kumar**; Office - 101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Ahmedabad - 380006, Gujarat (IN).

(74) Agent: **SAHNEY, Garima**; SAIKRISHNA & ASSOCIATES ADVOCATES, B-140, Sector 51, Noida-201301, Uttar Pradesh (IN).

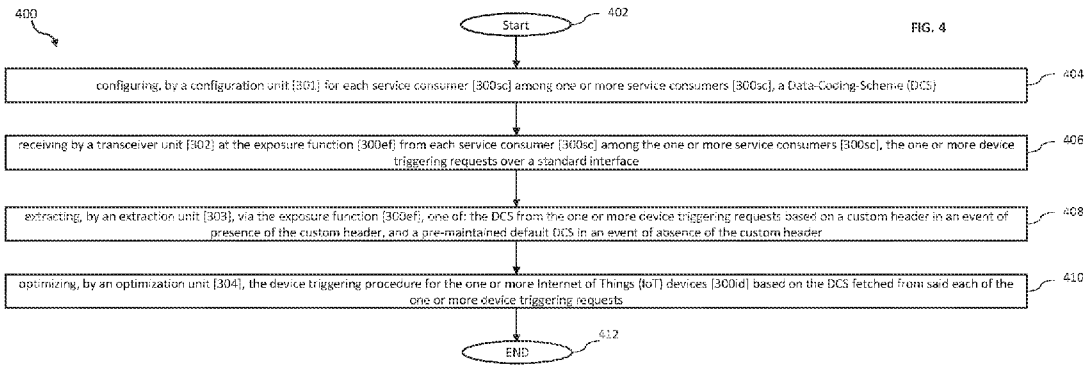
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, 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:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
— *of inventorship (Rule 4.17(iv))*

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

(54) Title: METHOD AND SYSTEM FOR OPTIMIZATION OF DEVICE TRIGGERING PROCEDURE FOR IOT DEVICES



(57) Abstract: The present disclosure relates to a method and a system for optimization of device triggering procedure for Internet of Things (IoT) device(s) [300id] in exposure function [300ef] The disclosure encompasses configuring a Data-Coding-Scheme (DCS); receiving device triggering requests over a standard interface; extracting one of: the DCS from the device triggering requests based on a custom header, and a pre- maintained default DCS; and optimizing the device triggering procedure for the IoT devices [300id] based on the DCS fetched from the device triggering requests.

WO 2025/008879 A1

METHOD AND SYSTEM FOR OPTIMIZATION OF DEVICE TRIGGERING PROCEDURE FOR IoT DEVICES

FIELD OF INVENTION

[0001] Embodiments of the present disclosure generally relate to network performance management systems. More particularly, embodiments of the present disclosure relate to a method and a system for optimization of device triggering procedure for the Internet of Things (IoT) device(s) in exposure function.

BACKGROUND

[0002] The following description of the related art is intended to provide background information pertaining to the field of the disclosure. This section may include certain aspects of the art that may be related to various features of the present disclosure. However, it should be appreciated that this section is used only to enhance the understanding of the reader with respect to the present disclosure, and not as admissions of the prior art.

[0003] Wireless communication technology has rapidly evolved over the past few decades, with each generation bringing significant improvements and advancements. The first generation of wireless communication technology was based on analogue technology and offered only voice services. However, with the advent of the second-generation (2G) technology, digital communication and data services became possible, and text messaging was introduced. The third-generation (3G) technology marked the introduction of high-speed internet access, mobile video calling, and location-based services. The fourth-generation (4G) technology revolutionized wireless communication with faster data speeds, better network coverage, and improved security. Currently, the fifth-generation (5G) technology is being deployed, promising even faster data speeds, low latency, and the ability to connect multiple devices simultaneously. With each generation, wireless communication technology has become more advanced, sophisticated, and capable of delivering more services to its users.

[0004] IoT (Internet of Things) devices are physical objects embedded with sensors, software, and connectivity features that enable them to collect, exchange, and act upon data with minimal human intervention. The IoT devices are interconnected through the internet or other communication networks to enable remote monitoring, control, and automation of various tasks.

Further, the Internet of Things (IoT) devices such as wearable technologies, smart locks, smoke detectors, home automation devices, motion Detectors etc., are connected to Communication servers in order to send alerts, notifications, and/or information about various events such as trespass, accidental falls, burglary etc. In a communication network (preferably a 5G communication network), all the IoT devices perform various task such but not limited to handling loads, introduction of new 5G use cases, etc. In a 5G communication network, the IoT devices communicate with each other via Network Exposure Functions (NEF) through a process facilitated by the NEF's capabilities to expose network resources and services. The Network exposure (sometimes exposure function), or service exposure refers to the functionality of the communication network that helps in making network capabilities, such as data and network services, easily available for communication service providers and third parties. The exposure function is responsible for securely exposing the network capabilities to application function. The NEF acts as an intermediary that enables IoT devices to access and utilize network functions, data, and resources provided by the underlying network infrastructure. This is done with the help of standardized Application Programming Interfaces (APIs) exposed by the NEF. The IoT devices can interact with each other, exchange data, and collaborate on various applications and services with the help of exposure function. For e.g., a communication done between Application Programming Interfaces (APIs) by sharing data via a Service Capability Exposure Function (SCEF)/ NEF from the Capability Server (CS)/ Application Server (AS)/ Application Function (AF). The APIs provided by the Exposure Functions may include but not limited to Subscriber Data API, QoS (Quality of Service) Management API, Session Management API etc. These APIs are generally configured on predefined rules and conditions such as standardized protocols and are exposed by the Exposure Function to authorized third-party applications through secure authentication and authorization mechanisms. The SCEF is responsible for exposing network capabilities and services to authorize third-party applications. The SCEF provides standardized APIs for accessing network functions, data, and resources, enabling developers to create innovative services and applications. While the NEF serves as an interface between the network infrastructure and external applications in the 5G environment. It exposes network resources and services through standardized APIs, allowing authorized third-party applications to access and utilize network functions, data, and resources for various use cases, such as IoT deployments, edge computing, and service innovation.

[0005] A device triggering request refers to a signal/ prompt sent from one device (preferably an IoT device) to another IoT device to perform a specific task or action. The device triggering request is governed as per a predefined protocol that is required in implementation of the receipt

of the device triggering request thus ensuring seamless interaction and optimal performance of the communication network. The data shared by the APIs via the SCEF/NEF is to be encoded with Data-Coding-Scheme (DCS) for device trigger payload. The DCS here refers to a parameter that specifies the encoding and formatting scheme used for representing data. The DCS defines how the data is structured, encoded, and interpreted by the network elements. It may include information such as data format, compression method, character set, and error detection/correction mechanisms, allowing efficient and reliable transmission of trigger-related information between the IoT devices and network components. Further, the device trigger payload refers to the data/ information included in a message sent from a service consumer such as but not limited to Services Capability Server/ Application Server and an Application Function. The device trigger payload helps in initiating a specific action or event in one or more Internet of Things (IoT) devices. The device trigger payload typically contains instructions, parameters, or identifiers necessary in the predefined protocols of the device triggering request, for the targeted IoT devices to perform the desired action. The payload may include various types of data, such as configuration settings, commands, or status updates, depending on the specific requirements of the triggering operation. However, for device triggers sent from SCEF/NEF, the 3rd Generation Partnership Project (3GPP) standard has no clarity on the DCS to be configured for the device trigger payload. Therefore, the SCEF/NEF does not get the information from the SCS/AS/AF to allow the data to be conveyed via SCEF/ NEF about the intended DCS for the data to be shared using the APIs. With the existing solutions, the SCEF/NEF are configured to share data of a pre-defined DCS format only because of limitation of the existing 3GPP standard specification. Any data shared which is not of the pre-defined DCS format does not reach the intended target which, in turn, leads to failure of data transmittal.

[0006] Further, a device trigger procedure for the IoT device in the 5G communication network refers to the sequence of actions and signalling processes involved in initiating a specific action or event. The device trigger procedure typically includes the transmission of trigger commands or messages from a service consumer to the targeted IoT devices, thereby triggering the execution of predefined tasks or operations, such as data collection, device activation, or event reporting.

[0007] Furthermore, over the period of time, various solutions have been developed to improve the performance of communication devices for enhancement in device triggering procedure for IoT device(s) to specify/configure intended Data-Coding-Scheme (DCS) for each Services Capability Server (SCS)/ Application Server (AS)/ Application Function (AF) to allow

the data to be conveyed via Service Capability Exposure Function (SCEF) or Network Exposure Function (NEF) to one or more intended IoT Devices. However, there are certain challenges with existing solutions. The existing solutions, as well as the 3GPP standard, do not provide clarity on how to trigger an IoT device to share data with an intended DCS.

[0008] Thus, in order to improve the 3GPP communication standard, there exists an imperative need in the art for enhancement in device triggering procedure for an IoT device to specify/configure intended DCS for each Services Capability Server (SCS)/ Application Server (AS)/ Application Function (AF) to allow the data to be conveyed via Service Capability Exposure Function (SCEF) or Network Exposure Function (NEF) to one or more intended IoT Devices. The present disclosure aims to address this problem.

SUMMARY OF THE DISCLOSURE

[0009] This section is provided to introduce certain aspects of the present disclosure in a simplified form that are further described below in the detailed description. This summary is not intended to identify the key features or the scope of the claimed subject matter.

[00010] An aspect of the present disclosure may relate to a method for optimization of a device triggering procedure for one or more Internet of Things (IoT) devices in an exposure function. The method comprises configuring, by a configuration unit for each service consumer among one or more service consumers, a Data-Coding-Scheme (DCS). It is to be noted that each DCS is associated with a one or more device triggering requests for the one or more Internet of Things (IoT) devices. The method further comprises receiving by a transceiver unit at the exposure function from each service consumer among the one or more service consumers, the one or more device triggering requests over a standard interface. The method further comprises extracting, by an extraction unit, via the exposure function, one of: the DCS from the one or more device triggering requests based on a custom header of said each of the one or more device triggering requests in an event of presence of the custom header in the one or more device triggering requests, and a pre-maintained default DCS in an event of absence of the custom header in the one or more device triggering requests. And the method further comprises optimizing, by an optimization unit the device triggering procedure for the one or more Internet of Things (IoT) devices based on the DCS fetched from said each of the one or more device triggering requests.

[00011] In an exemplary aspect of the present disclosure, in the disclosed method, the exposure function is one of a Service Capability Exposure Function (SCEF) and a Network Exposure Function (NEF).

[00012] In an exemplary aspect of the present disclosure, in the disclosed method, the service consumer is one of a Services Capability Server (SCS), an Application Server (AS) and an Application Function (AF).

[00013] In an exemplary aspect of the present disclosure, in the disclosed method, the standard interface is a standard T8/N33 interface.

[00014] In an exemplary aspect of the present disclosure, in the disclosed method, the custom header is a "devicePayloadFormat" custom header.

[00015] In an exemplary aspect of the present disclosure, the method further comprises configuring by the optimization unit, for the exposure function, the at least one DCS fetched from said each of the one or more device triggering requests.

[00016] In an exemplary aspect of the present disclosure, in the disclosed method, the pre-maintained default DCS is maintained by the exposure function for each of the one or more device triggering requests of each service consumer, at a time of onboarding each of the service consumer.

[00017] In an exemplary aspect of the present disclosure, the method further comprises enabling by a balancing unit, one or more load balancers (LBs) to load balance the one or more device triggering requests.

[00018] Another aspect of the present disclosure may relate to a system [300] for optimization of a device triggering procedure for one or more Internet of Things (IoT) devices in an exposure function. The system comprises a configuration unit to configure, for each service consumer among one or more service consumers, a Data-Coding-Scheme (DCS) from one or more DCSs. It is to be noted that each DCS is associated with a one or more device triggering requests for the one or more IoT devices. The system further comprises a transceiver unit connected to at least the configuration unit. The transceiver unit is configured to receive, at the exposure function, from each service consumer among the one or more service consumers, the one or more device triggering requests over a standard interface. The system further comprises an extraction unit

connected to at least the transceiver unit. The extraction unit is configured to extract, via the exposure function, one of: the DCS from the one or more device triggering requests based on a custom header of said each of the one or more device triggering requests in an event of presence of the custom header in the one or more device triggering requests, and a pre-maintained default DCS in an event of absence of the custom header in the one or more device triggering requests. And the system further comprises an optimization unit connected to at least the extraction unit. The optimization unit is configured to optimize, the device triggering procedure for the one or more Internet of Things (IoT) devices based on the DCS extracted from said each of the one or more device triggering requests.

[00019] Yet another aspect of the present disclosure may relate to a non-transitory computer readable storage medium storing instruction for optimization of a device triggering procedure for one or more Internet of Things (IoT) devices in an exposure function. The instructions include executable code which, when executed by one or more units of a system, causes: a configuration unit to configure, for each service consumer among one or more service consumers, a Data-Coding-Scheme (DCS) from one or more DCSs. It is to be noted that each DCS is associated with a one or more device triggering requests for the one or more IoT devices; a transceiver unit to receive, at the exposure function, from each service consumer among the one or more service consumers, the one or more device triggering requests over a standard interface; an extraction unit to extract, via the exposure function, one of: the DCS from the one or more device triggering requests based on a custom header of said each of the one or more device triggering requests in an event of presence of the custom header in the one or more device triggering requests, and a pre-maintained default DCS in an event of absence of the custom header in the one or more device triggering requests; and an optimization unit to optimize, the device triggering procedure for the one or more Internet of Things (IoT) devices based on the DCS extracted from said each of the one or more device triggering requests.

[00020] Yet another aspect of the present disclosure may relate to a User Equipment (UE) device receiving a device triggering request. The UE device comprises a transceiver unit configured to receive, a device triggering, from a system, via a Short Message Service Center (SMSC), wherein the system performs optimization of a device triggering procedure for the UE device before the device triggering request is sent to the UE device. The system further comprises a configuration unit configured to configure, for each service consumer among one or more service consumers, a Data-Coding-Scheme (DCS) from one or more DCSs, wherein each DCS is associated with the one or more device triggering requests for the UE device. The system further

comprises a transceiver unit configured to receive, at an exposure function from each service consumer among the one or more service consumers, the one or more device triggering requests over a standard interface. The system further comprises an extraction unit configured to extract, via the exposure function, one of: the DCS from the one or more device triggering requests based on a custom header of said each of the one or more device triggering requests in an event of presence of the custom header in the one or more device triggering requests, and a pre-maintained default DCS in an event of absence of the custom header in the one or more device triggering requests. And the system further comprises an optimization unit configured to optimize, the device triggering procedure for the UE device based on the DCS extracted from said each of the one or more device triggering requests.

OBJECTS OF THE INVENTION

[00021] Some of the objects of the present disclosure, which at least one embodiment disclosed herein satisfies are listed herein below.

[00022] It is an object of the present disclosure to provide a system and a method for enhancement in device triggering procedure for Internet of Things (IoT).

[00023] It is another object of the present disclosure to specify/configure intended Data-Coding-Scheme (DCS) for each of the Services Capability Server (SCS)/ Application Server (AS)/ Application Function (AF).

[00024] It is an object of the present disclosure to allow the data to be conveyed via Service Capability Exposure Function (SCEF) or Network Exposure Function (NEF) to one or more intended IoT Devices.

[00025] It is another object of the present disclosure to specify the payload with each initiated device trigger request over standard T8/N33 interface.

[00026] It is another object of the present disclosure to maintain DCS for each SCS/AS during the onboarding of the SCEF in instances where the AS/AF cannot convey DCS through custom header solution.

[00027] It is another object of the present disclosure to provide a solution that provides solutions for existing infrastructures.

DESCRIPTION OF THE DRAWINGS

[00028] 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. Also, the embodiments shown in the figures are not to be construed as limiting the disclosure, but the possible variants of the method and system according to the disclosure are illustrated herein to highlight the advantages of the disclosure. It will be appreciated by those skilled in the art that disclosure of such drawings includes disclosure of electrical components or circuitry commonly used to implement such components.

[00029] FIG. 1 illustrates an exemplary block diagram representation of 5th generation core (5GC) network architecture.

[00030] FIG. 2 illustrates an exemplary block diagram of a computing device upon which the features of the present disclosure may be implemented in accordance with exemplary implementation of the present disclosure.

[00031] FIG. 3 illustrates an exemplary block diagram of a system [300] for optimization of a device triggering procedure for one or more Internet of Things (IoT) devices in an exposure function, in accordance with exemplary implementations of the present disclosure.

[00032] FIG. 4 illustrates a method [400] flow diagram for optimizing a device triggering procedure for one or more Internet of Things (IoT) devices in an exposure function, in accordance with exemplary implementations of the present disclosure.

[00033] FIG. 5 illustrates an exemplary block diagram of a system [500] for enhancement in device triggering procedure for Internet of Things (IoT) to allow the data to be conveyed from the SCS/AS/AF via Service Capability Exposure Function (SCEF) or Network Exposure Function

(NEF) to one or more intended IoT Devices, in accordance with exemplary embodiments of the present disclosure.

[00034] FIG. 6 illustrates an exemplary method [600] flow diagram indicating the process for enhancement in device triggering procedure for Internet of Things (IoT) to allow the data to be conveyed from the SCS/AS/AF via Service Capability Exposure Function (SCEF) or Network Exposure Function (NEF) to one or more intended IoT Devices, in accordance with exemplary embodiments of the present disclosure.

[00035] The foregoing shall be more apparent from the following more detailed description of the disclosure.

DETAILED DESCRIPTION

[00036] In the following description, for the purposes of explanation, various specific details are set forth in order to provide a thorough understanding of embodiments of the present disclosure. It will be apparent, however, that embodiments of the present disclosure may be practiced without these specific details. Several features described hereafter may each be used independently of one another or with any combination of other features. An individual feature may not address any of the problems discussed above or might address only some of the problems discussed above.

[00037] The ensuing description provides exemplary embodiments only, and is not intended to limit the scope, applicability, or configuration of the disclosure. Rather, the ensuing description of the exemplary embodiments will provide those skilled in the art with an enabling description for implementing an exemplary embodiment. It should be understood that various changes may be made in the function and arrangement of elements without departing from the spirit and scope of the disclosure as set forth.

[00038] Specific details are given in the following description to provide a thorough understanding of the embodiments. However, it will be understood by one of ordinary skill in the art that the embodiments may be practiced without these specific details. For example, circuits, systems, processes, and other components may be shown as components in block diagram form in order not to obscure the embodiments in unnecessary detail.

[00039] Also, it is noted that individual embodiments may be described as a process which is depicted as a flowchart, a flow diagram, a data flow diagram, a structure diagram, or a block diagram. Although a flowchart may describe the operations as a sequential process, many of the operations may be performed in parallel or concurrently. In addition, the order of the operations may be re-arranged. A process is terminated when its operations are completed but could have additional steps not included in a figure.

[00040] The word "exemplary" and/or "demonstrative" is used herein to mean serving as an example, instance, or illustration. For the avoidance of doubt, the subject matter disclosed herein is not limited by such examples. In addition, any aspect or design described herein as "exemplary" and/or "demonstrative" is not necessarily to be construed as preferred or advantageous over other aspects or designs, nor is it meant to preclude equivalent exemplary structures and techniques known to those of ordinary skill in the art. Furthermore, to the extent that the terms "includes," "has," "contains," and other similar words are used in either the detailed description or the claims, such terms are intended to be inclusive—in a manner similar to the term "comprising" as an open transition word—without precluding any additional or other elements.

[00041] As used herein, a "processing unit" or "processor" or "operating processor" includes one or more processors, wherein processor refers to any logic circuitry for processing instructions. A processor may be a general-purpose processor, a special purpose processor, a conventional processor, a digital signal processor, a plurality of microprocessors, one or more microprocessors in association with a (Digital Signal Processing) DSP core, a controller, a microcontroller, Application Specific Integrated Circuits, Field Programmable Gate Array circuits, any other type of integrated circuits, etc. The processor may perform signal coding data processing, input/output processing, and/or any other functionality that enables the working of the system according to the present disclosure. More specifically, the processor or processing unit is a hardware processor.

[00042] As used herein, "a user equipment", "a user device", "a smart-user-device", "a smart-device", "an electronic device", "a mobile device", "a handheld device", "a wireless communication device", "a mobile communication device", "a communication device" may be any electrical, electronic and/or computing device or equipment, capable of implementing the features of the present disclosure. The user equipment/device may include, but is not limited to, a mobile phone, smart phone, laptop, a general-purpose computer, desktop, personal digital assistant, tablet computer, wearable device or any other computing device which is capable of

implementing the features of the present disclosure. Also, the user device may contain at least one input means configured to receive an input from at least one of a transceiver unit, a processing unit, a storage unit, a detection unit and any other such unit(s) which are required to implement the features of the present disclosure.

[00043] As used herein, "storage unit" or "memory unit" refers to a machine or computer-readable medium including any mechanism for storing information in a form readable by a computer or similar machine. For example, a computer-readable medium includes read-only memory ("ROM"), random access memory ("RAM"), magnetic disk storage media, optical storage media, flash memory devices or other types of machine-accessible storage media. The storage unit stores at least the data that may be required by one or more units of the system to perform their respective functions.

[00044] As used herein "interface" or "user interface refers to a shared boundary across which two or more separate components of a system exchange information or data. The interface may also be referred to a set of rules or protocols that define communication or interaction of one or more modules or one or more units with each other, which also includes the methods, functions, or procedures that may be called.

[00045] All modules, units, components used herein, unless explicitly excluded herein, may be software modules or hardware processors, the processors being a general-purpose processor, a special purpose processor, a conventional processor, a digital signal processor (DSP), a plurality of microprocessors, one or more microprocessors in association with a DSP core, a controller, a microcontroller, Application Specific Integrated Circuits (ASIC), Field Programmable Gate Array circuits (FPGA), any other type of integrated circuits, etc.

[00046] As used herein the transceiver unit include at least one receiver and at least one transmitter configured respectively for receiving and transmitting data, signals, information or a combination thereof between units/components within the system and/or connected with the system.

[00047] As discussed in the background section, the current known solutions have several shortcomings. The present disclosure aims to overcome the above-mentioned and other existing problems in this field of technology by providing method and system of optimization of a device triggering procedure for one or more Internet of Things (IoT) devices in an exposure function.

[00048] **FIG. 1** illustrates an exemplary block diagram representation of 5th generation core (5GC) network architecture, in accordance with exemplary implementation of the present disclosure. As shown in FIG. 1, the 5GC network architecture [100] includes a user equipment (UE) [102], a radio access network (RAN) [104], an access and mobility management function (AMF) [106], a Session Management Function (SMF) [108], a Service Communication Proxy (SCP) [110], an Authentication Server Function (AUSF) [112], a Network Slice Specific Authentication and Authorization Function (NSSAAF) [114], a Network Slice Selection Function (NSSF) [116], a Network Exposure Function (NEF) [118], a Network Repository Function (NRF) [120], a Policy Control Function (PCF) [122], a Unified Data Management (UDM) [124], an application function (AF) [126], a User Plane Function (UPF) [128], a data network (DN) [130], wherein all the components are assumed to be connected to each other in a manner as obvious to the person skilled in the art for implementing features of the present disclosure.

[00049] Radio Access Network (RAN) [104] is the part of a mobile telecommunications system that connects user equipment (UE) [102] to the core network (CN) and provides access to different types of networks (e.g., 5G network). It consists of radio base stations and the radio access technologies that enable wireless communication.

[00050] Access and Mobility Management Function (AMF) [106] is a 5G core network function responsible for managing access and mobility aspects, such as UE registration, connection, and reachability. It also handles mobility management procedures like handovers and paging.

[00051] Session Management Function (SMF) [108] is a 5G core network function responsible for managing session-related aspects, such as establishing, modifying, and releasing sessions. It coordinates with the User Plane Function (UPF) for data forwarding and handles IP address allocation and QoS enforcement.

[00052] Service Communication Proxy (SCP) [110] is a network function in the 5G core network that facilitates communication between other network functions by providing a secure and efficient messaging service. It acts as a mediator for service-based interfaces.

[00053] Authentication Server Function (AUSF) [112] is a network function in the 5G core responsible for authenticating UEs during registration and providing security services. It generates and verifies authentication vectors and tokens.

[00054] Network Slice Specific Authentication and Authorization Function (NSSAAF) [114] is a network function that provides authentication and authorization services specific to network slices. It ensures that UEs can access only the slices for which they are authorized.

[00055] Network Slice Selection Function (NSSF) [116] is a network function responsible for selecting the appropriate network slice for a UE based on factors such as subscription, requested services, and network policies.

[00056] Network Exposure Function (NEF) [118] is a network function that exposes capabilities and services of the 5G network to external applications, enabling integration with third-party services and applications.

[00057] Network Repository Function (NRF) [120] is a network function that acts as a central repository for information about available network functions and services. It facilitates the discovery and dynamic registration of network functions.

[00058] Policy Control Function (PCF) [122] is a network function responsible for policy control decisions, such as QoS, charging, and access control, based on subscriber information and network policies.

[00059] Unified Data Management (UDM) [124] is a network function that centralizes the management of subscriber data, including authentication, authorization, and subscription information.

[00060] Application Function (AF) [126] is a network function that represents external applications interfacing with the 5G core network to access network capabilities and services.

[00061] User Plane Function (UPF) [128] is a network function responsible for handling user data traffic, including packet routing, forwarding, and QoS enforcement.

[00062] Data Network (DN) [130] refers to a network that provides data services to user equipment (UE) in a telecommunications system. The data services may include but are not limited to Internet services, private data network related services.

[00063] **FIG. 2** illustrates an exemplary block diagram of a computing device [1000] upon which the features of the present disclosure may be implemented in accordance with exemplary implementation of the present disclosure. In an implementation, the computing device [1000] may also implement a method for optimization of a device triggering procedure for one or more Internet of Things (IoT) devices in an exposure function, utilising the system. In another implementation, the computing device [1000] itself implements the method for optimization of a device triggering procedure for one or more Internet of Things (IoT) devices in an exposure function, using one or more units configured within the computing device [1000], wherein said one or more units are capable of implementing the features as disclosed in the present disclosure.

[00064] The computing device [1000] may include a bus [1002] or other communication mechanism for communicating information, and a hardware processor [1004] coupled with bus [1002] for processing information. The hardware processor [1004] may be, for example, a general-purpose microprocessor. The computing device [1000] may also include a main memory [1006], such as a random-access memory (RAM), or other dynamic storage device, coupled to the bus [1002] for storing information and instructions to be executed by the processor [1004]. The main memory [1006] also may be used for storing temporary variables or other intermediate information during execution of the instructions to be executed by the processor [1004]. Such instructions, when stored in non-transitory storage media accessible to the processor [1004], render the computing device [1000] into a special-purpose machine that is customized to perform the operations specified in the instructions. The computing device [1000] further includes a read only memory (ROM) [1008] or other static storage device coupled to the bus [1002] for storing static information and instructions for the processor [1004].

[00065] A storage device [1010], such as a magnetic disk, optical disk, or solid-state drive is provided and coupled to the bus [1002] for storing information and instructions. The computing device [1000] may be coupled via the bus [1002] to a display [1012], such as a cathode ray tube (CRT), Liquid crystal Display (LCD), Light Emitting Diode (LED) display, Organic LED (OLED) display, etc. for displaying information to a computer user. An input device [1014], including alphanumeric and other keys, touch screen input means, etc. may be coupled to the bus [1002] for communicating information and command selections to the processor [1004]. Another type of user

input device may be a cursor control [1016], such as a mouse, a trackball, or cursor direction keys, for communicating direction information and command selections to the processor [1004], and for controlling cursor movement on the display [1012]. This input device typically has two degrees of freedom in two axes, a first axis (e.g., x) and a second axis (e.g., y), that allow the device to specify positions in a plane.

[00066] The computing device [1000] may implement the techniques described herein using customized hard-wired logic, one or more ASICs or FPGAs, firmware and/or program logic which in combination with the computing device [1000] causes or programs the computing device [1000] to be a special-purpose machine. According to one implementation, the techniques herein are performed by the computing device [1000] in response to the processor [1004] executing one or more sequences of one or more instructions contained in the main memory [1006]. Such instructions may be read into the main memory [1006] from another storage medium, such as the storage device [1010]. Execution of the sequences of instructions contained in the main memory [1006] causes the processor [1004] to perform the process steps described herein. In alternative implementations of the present disclosure, hard-wired circuitry may be used in place of or in combination with software instructions.

[00067] The computing device [1000] also may include a communication interface [1018] coupled to the bus [1002]. The communication interface [1018] provides a two-way data communication coupling to a network link [1020] that is connected to a local network [1022]. For example, the communication interface [1018] may be an integrated services digital network (ISDN) card, cable modem, satellite modem, or a modem to provide a data communication connection to a corresponding type of telephone line. As another example, the communication interface [1018] may be a local area network (LAN) card to provide a data communication connection to a compatible LAN. Wireless links may also be implemented. In any such implementation, the communication interface [1018] sends and receives electrical, electromagnetic or optical signals that carry digital data streams representing various types of information.

[00068] The computing device [1000] can send messages and receive data, including program code, through the network(s), the network link [1020] and the communication interface [1018]. In the Internet example, a server [1030] might transmit a requested code for an application program through the Internet [1028], the ISP [1026], the local network [1022] and the communication interface [1018]. The received code may be executed by the processor [1004] as

it is received, and/or stored in the storage device [1010], or other non-volatile storage for later execution.

[00069] Referring to **FIG. 3**, an exemplary block diagram of a system [300] for optimization of a device triggering procedure for one or more Internet of Things (IoT) devices [300id] in an exposure function [300ef], is shown, in accordance with the exemplary implementations of the present disclosure. It is to be noted that the exposure function [300ef] may include but not limited to one of a Service Capability Exposure Function (SCEF) and a Network Exposure Function (NEF). The system [300] comprises at least one configuration unit [301], at least one transceiver unit [302], at least one extraction unit [303], at least one optimization unit [304] and at least one balancing unit [305]. Also, all of the components/ units of the system [300] are assumed to be connected to each other unless otherwise indicated below. As shown in the system [300], all units within the system [300] should also be assumed to be connected to each other. Also, in Fig. 3 only a few units are shown, however, the system [300] may comprise multiple such units or the system [300] may comprise any such numbers of said units, as required to implement the features of the present disclosure. Further, in an implementation, the system [300] may be a part of the user device / or may be independent of but in communication with the user device (may also referred herein as a UE). In another implementation, the system [300] may reside in a server or a network entity. In yet another implementation, the system [300] may reside partly in the server/ network entity and partly in the user device.

[00070] The system [300] is configured for optimization of the device triggering procedure for one or more Internet of Things (IoT) devices [300id] in an exposure function [300ef], with the help of the interconnection between the components/units of the system [300].

[00071] The configuration unit [301] configures, for each service consumer [300sc] among one or more service consumers [300sc], a Data-Coding-Scheme (DCS) from one or more DCSs. It is to be noted that each DCS is associated with one or more device triggering requests for the one or more IoT devices [300id]. It is further noted that the service consumer [300sc] is one of a Services Capability Server (SCS), an Application Server (AS) and an Application Function (AF). Here, the one or more device triggering requests refers to a signal/ prompt sent from one IoT device [300id] to another IoT device [300id2] to perform a specific task or action. The one or more device triggering request may be governed as per a predefined protocol that are required in implementation of the receipt of the device triggering request for information exchange, thus ensuring seamless interaction and optimal performance of the communication network.

[00072] The transceiver unit [302] is configured to receive, at the exposure function [300ef], from each service consumer [300sc] among the one or more service consumers [300sc], the one or more device triggering requests over a standard interface. It is to be noted that the standard interface is a standard T8/N33 interface.

[00073] The extraction unit [303] is configured to extract, via the exposure function [300ef], one of: the DCS from the one or more device triggering requests based on a custom header of said each of the one or more device triggering requests in an event of presence of the custom header in the one or more device triggering requests, and a pre-maintained default DCS in an event of absence of the custom header in the one or more device triggering requests. It is to be noted that the custom header is a "devicePayloadFormat" custom header. It is further noted that the pre-maintained default DCS is maintained by the exposure function [300ef] for each of the one or more device triggering requests of each service consumer [300sc], at a time of onboarding of each service consumer [300sc].

[00074] The optimization unit [304] is configured to optimize, the device triggering procedure for the one or more Internet of Things (IoT) devices [300id] based on the DCS extracted from said each of the one or more device triggering requests. It is important to note that to optimize the device triggering procedure for the one or more IoT devices [300id], the optimization unit [304] is further configured to configure, for the exposure function [300ef], the DCS fetched from said each of the device triggering requests.

[00075] The balancing unit [305] is configured to enable one or more load balancers (LBs) to load balance the one or more device triggering requests. The one or more load balancers (LBs) may include but are not limited to edge load balancers.

[00076] Referring to FIG. 4, an exemplary method flow diagram [400] for optimization of a device triggering procedure for one or more Internet of Things (IoT) devices [300id] in an exposure function [300ef], in accordance with exemplary implementations of the present disclosure is shown. In an implementation the method [400] is performed by the system [300]. Further, in an implementation, the system [300] may be present in a server device to implement the features of the present disclosure. Also, as shown in Fig. 4, the method [400] starts at step [402]. In an exemplary aspect of the present disclosure, with reference to the disclosed method

[400], the exposure function [300ef] is one of a Service Capability Exposure Function (SCEF) and a Network Exposure Function (NEF).

[00077] At step [404], the method [400] comprises configuring, by a configuration unit [301] for each service consumer [300sc] among one or more service consumers [300sc], a Data-Coding-Scheme (DCS). It is to be noted that each DCS is associated with a one or more device triggering requests for the one or more Internet of Things (IoT) devices [300id]. Here, the one or more device triggering requests refers to a signal/ prompt sent from one IoT device [300id] to another IoT device [300id2] to perform a specific task or action. The one or more device triggering request may be governed as per a predefined protocol that are required in implementation of the receipt of the device triggering request for information exchange, thus ensuring seamless interaction and optimal performance of the communication network.

[00078] In an exemplary aspect of the present disclosure, with reference to the disclosed method [400], the service consumer [300sc] is one of a Services Capability Server (SCS), an Application Server (AS) and an Application Function (AF).

[00079] At step [406], the method [400] comprises receiving by a transceiver unit [302] at the exposure function [300ef] from each service consumer [300sc] among the one or more service consumers [300sc], the one or more device triggering requests over a standard interface.

[00080] In an exemplary aspect of the present disclosure, with reference to the disclosed method [400], the standard interface is a standard T8/N33 interface.

[00081] At step [408], the method [400] comprises extracting, by an extraction unit [303], via the exposure function [300ef], one of: the DCS from the one or more device triggering requests based on a custom header of said each of the one or more device triggering requests in an event of presence of the custom header in the one or more device triggering requests, and a pre-maintained default DCS in an event of absence of the custom header in the one or more device triggering requests.

[00082] In an exemplary aspect of the present disclosure, with reference to the disclosed method [400], the custom header is a "devicePayloadFormat" custom header.

[00083] In an exemplary aspect of the present disclosure, with reference to the disclosed method [400], the pre-maintained default DCS is maintained by the exposure function [300ef] for each of the one or more device triggering requests of each service consumer [300sc], at a time of onboarding of the each service consumer [300sc].

[00084] At step [410], the method [400] comprises optimizing, by an optimization unit [304], the device triggering procedure for the one or more Internet of Things (IoT) devices [300id] based on the DCS fetched from said each of the one or more device triggering requests.

[00085] In an exemplary aspect of the present disclosure, the method [400] further comprises configuring by the optimization unit [304] for the exposure function [300ef], the at least one DCS fetched from said each of the one or more device triggering requests.

[00086] In an exemplary aspect of the present disclosure, the method [400] further comprises enabling by a balancing unit [305], one or more load balancers (LBs) to load balance the one or more device triggering requests.

[00087] **FIG. 5** illustrates an exemplary block diagram of a system [500] for enhancement in device triggering procedure for Internet of Things (IoT) to allow the data to be conveyed from the SCS/AS/AF [506] via Service Capability Exposure Function (SCEF) or Network Exposure Function (NEF) [512] to one or more intended IoT Devices [508], in accordance with exemplary embodiments of the present disclosure. The system [500] comprises at least one processing unit [502] and at least one storage unit [504]. Also, all of the components/ units of the system [500] are assumed to be connected to each other unless otherwise indicated below. Also, in Fig. 5 only a few units are shown, however, the system [500] may comprise multiple such units or the system [500] may comprise any such numbers of said units, as required to implement the features of the present disclosure. Further, in an implementation, the system [500] may be a part of the user device / or may be independent of but in communication with the user device (may also referred herein as a UE). In another implementation, the system [500] may reside in a server or a network entity. In yet another implementation, the system [500] may reside partly in the server/ network entity and partly in the user device.

[00088] The system [500] is configured for enhancement in device triggering procedure for Internet of Things (IoT) to allow the data to be conveyed from the SCS/AS/AF [506] via Service Capability Exposure Function (SCEF) or Network Exposure Function (NEF) [512] to one or more

intended IoT Device [508], with the help of the interconnection between the components/units of the system [500].

[00089] In order to enhance device triggering procedure for Internet of Things (IoT) to allow the data to be conveyed from the SCS/AS/AF [506] via Service Capability Exposure Function (SCEF) or Network Exposure Function (NEF) [512] to one or more intended IoT Devices, the processing unit [502] of the system [500] is configured to provide SCEF [512] with DCS required to allow the communication from the first API to the second API.

[00090] In an embodiment, the processing unit [502] commands the SCEF [512] to fetch DCS associated with each device trigger request on standard T8/N33 interface. Upon this, the processing unit [502] commands SCS/AS/AF [506] to adapt this requirement and specify intended DCS while initiating device trigger request over T8/N33 interface. Thereby, the data shall transmit from the first API to the Second API using the fetched DBS.

[00091] In another embodiment, the SCEF [512] will be configured to store the DCS information in cache/Database (DB) for each SCS/AS/AF [506] based on parameters required by various services (for e.g., a device trigger, Monitoring Events (MontE) Non-IP data delivery (NIDD) Background data transfer (BDT) MSISDN-Less MO) specified at the time of its on-boarding which will later be used in each device trigger request initiated from a respective SCS/AS/AF [506]. This embodiment allows the present disclosure to be used for the existing APIs without needing to change the API.

[00092] In the system [500] a Provisioning Gateway (G/W) UI [516] is used to provide the SCS/AS/AF [506] along with all the configurations that must be required by SCEF [512] with respect to that SCS/AS/AF [506]. An Edge Load Balancer (ELB) [514] will load balance the provisioning request towards SCEF [512] instances. The SCS/AS/AF [506] will initiate device trigger create/replace request, which is to be delivered to an IoT device. The SCEF [512] will check whether device payload format is provided in the request. If not, the SCEF [512] will fetch that information from the configurations provided while provisioning an SCS/AS/AF [506]. The SCEF [512] will initiate the device trigger towards Short Message Service Centre (SMSC) [510] with device payload format along with all the other relevant information. The SMSC [510] will deliver device trigger to the IoT device [508].

[00093] The storage unit [504] is configured to store the information required to enable the system [500] as disclosed in the present disclosure.

[00094] **FIG. 6** illustrates an exemplary method [600] flow diagram indicating the process for enhancement of device triggering procedure for Internet of Things (IoT) to allow the data to be conveyed from the SCS/AS/AF via Service Capability Exposure Function (SCEF) or Network Exposure Function (NEF) to one or more intended IoT Devices, in accordance with exemplary embodiments of the present disclosure.

[00095] In an implementation the method [600] is performed by the system [500]. As shown in FIG. 6, the method [600] involves following steps:

Step [601] of receiving Device Trigger Request from SCS/AS/AF

Step [602] of checking if the Trigger Payload Format is Specified. If the answer to the previous step is positive, then the method [600] proceeds to next step [603]. If the answer to the previous step in negative, then the method [600] executes step [6021] of using the payload format configured at the time of SCS/AS/AF provisioning and then proceeds to step [6022] of fetching the payload format for specific SCS/AS/AF.

Step [603] of submitting the device trigger along with payload format to the SMSC and proceed for communication.

[00096] The present disclosure further discloses a non-transitory computer readable storage medium storing instructions for optimization of a device triggering procedure for one or more Internet of Things (IoT) devices [300id] in an exposure function [300ef], the instructions include executable code which, when executed by one or more units of a system, causes: a configuration unit [301] to configure, for each service consumer [300sc] among one or more service consumers [300sc], a Data-Coding-Scheme (DCS) from one or more DCSs. It is to be noted that each DCS is associated with a one or more device triggering requests for the one or more IoT devices [300id]; a transceiver unit [302] to receive, at the exposure function [300ef], from each service consumer [300sc] among the one or more service consumers [300sc], the one or more device triggering requests over a standard interface; an extraction unit [303] to extract, via the exposure function [300ef], one of: the DCS from the one or more device triggering requests based on a custom header of said each of the one or more device triggering requests in an event of presence of the custom header in the one or more device triggering requests, and a pre-maintained default DCS in an event of absence of the custom header in the one or more device triggering requests; and an optimization unit [304] to optimize, the device triggering procedure for the one or more Internet of Things (IoT) devices [300id] based on the DCS extracted from said each of the one or more device triggering requests.

[00097] The present disclosure further discloses a User Equipment (UE) device receiving a device trigger. The UE device comprises a transceiver unit configured to receive, a device triggering, from a system [300], via a Short Message Service Center (SMSC), wherein the system [300] performs optimization of a device triggering procedure for the UE device before the device triggering request is sent to the UE device. The system [300] further comprises a configuration unit [301] configured to configure, for each service consumer [300sc] among one or more service consumers [300sc], a Data-Coding-Scheme (DCS) from one or more DCSs, wherein each DCS is associated with the one or more device triggering requests for the UE device. The system [300] further comprises a transceiver unit [302] configured to receive, at an exposure function [300ef] from each service consumer [300sc] among the one or more service consumers [300sc], the one or more device triggering requests over a standard interface. The system [300] further comprises an extraction unit [303] configured to extract, via the exposure function [300ef], one of: the DCS from the one or more device triggering requests based on a custom header of said each of the one or more device triggering requests in an event of presence of the custom header in the one or more device triggering requests, and a pre-maintained default DCS in an event of absence of the custom header in the one or more device triggering requests. And the system [300] further comprises an optimization unit [304] configured to optimize, the device triggering procedure for the UE device based on the DCS extracted from said each of the one or more device triggering requests.

[00098] As is evident from the above, the present disclosure provides a technically advanced solution for the optimization of the device triggering procedure for one or more Internet of Things (IoT) devices [300id] in an exposure function [300ef]. The said technically advanced solution allows the data to be conveyed from the service consumer [300sc] such as but not limited to SCS/AS/AF via the exposure function [300ef] such as but not limited to SCEF/NEF to one or more intended IoT devices [300id]. Various advantages of the present disclosure are as follows:

Clarity on how to trigger the IoT device [300id] by sharing data with an intended DCS.

Reduced chances of failure of transmission of data as the exposure function [300ef] is aware of the DCS.

Ability to use the existing APIs and share data with different DCS.

Ability to share data with different DCS data types, for e.g., 7 bit, 8 bit, 16 bit and the like.

[00099] While considerable emphasis has been placed herein on the disclosed implementations, it will be appreciated that many implementations can be made and that many changes can be made to the implementations without departing from the principles of the present

disclosure. These and other changes in the implementations of the present disclosure will be apparent to those skilled in the art, whereby it is to be understood that the foregoing descriptive matter to be implemented is illustrative and non-limiting.

Further, in accordance with the present disclosure, it is to be acknowledged that the functionality described for the various components/units can be implemented interchangeably. While specific embodiments may disclose a particular functionality of these units for clarity, it is recognized that various configurations and combinations thereof are within the scope of the disclosure. The functionality of specific units as disclosed in the disclosure should not be construed as limiting the scope of the present disclosure. Consequently, alternative arrangements and substitutions of units, provided they achieve the intended functionality described herein, are considered to be encompassed within the scope of the present disclosure.

We Claim

1. A method [400] for optimization of a device triggering procedure for one or more Internet of Things (IoT) devices [300id] in an exposure function [300ef], the method [400] comprises:

configuring, by a configuration unit [301] for each service consumer [300sc] among one or more service consumers [300sc], a Data-Coding-Scheme (DCS), wherein each DCS is associated with a one or more device triggering requests for the one or more Internet of Things (IoT) devices [300id];

receiving, by a transceiver unit [302] at the exposure function [300ef] from each service consumer [300sc] among the one or more service consumers [300sc], the one or more device triggering requests over a standard interface;

extracting, by the an extraction unit [303], via the exposure function [300ef], one of: the DCS from the one or more device triggering requests based on a custom header of said each of the one or more device triggering requests in an event of presence of the custom header in the one or more device triggering requests, and a pre-maintained default DCS in an event of absence of the custom header in the one or more device triggering requests; and

optimizing, by an optimization unit [304] the device triggering procedure for the one or more Internet of Things (IoT) devices [300id] based on the DCS fetched from said each of the one or more device triggering requests.

2. The method [400] as claimed in claim 1, wherein the exposure function [300ef] is one of a Service Capability Exposure Function (SCEF) and a Network Exposure Function (NEF).

3. The method [400] as claimed in claim 1, wherein the service consumer [300sc] is one of a Services Capability Server (SCS), an Application Server (AS) and an Application Function (AF).

4. The method [400] as claimed in claim 1, wherein the standard interface is a standard T8/N33 interface.

5. The method [400] as claimed in claim 1, wherein the custom header is a "devicePayloadFormat" custom header.

6. The method [400] as claimed in claim 1, wherein to optimize the device triggering procedure for the one or more Internet of Things (IoT) devices [300id], the method [400] comprises configuring by the optimization unit [304] for the exposure function [300ef], the at least one DCS fetched from said each of the one or more device triggering requests.

7. The method [400] as claimed in claim 1, wherein the pre-maintained default DCS is maintained by the exposure function [300ef] for each of the one or more device triggering requests of each service consumer [300sc], at a time of onboarding of each service consumer [300sc].

8. The method [400] as claimed in claim 1, the method [400] comprises enabling by a balancing unit [305], one or more load balancers (LBs) to load balance the one or more device triggering requests.

9. A system [300] for optimization of a device triggering procedure for one or more Internet of Things (IoT) devices [300id] in an exposure function [300ef], the system [300] comprises:

- a configuration unit [301] to configure, for each service consumer [300sc] among one or more service consumers [300sc], a Data-Coding-Scheme (DCS) from one or more DCSs, wherein each DCS is associated with one or more device triggering requests for the one or more Internet of Things (IoT) devices [300id],
- a transceiver unit [302] connected to at least the configuration unit [301], the transceiver unit [302] configured to receive, at the exposure function [300ef] from each service consumer [300sc] among the one or more service consumers [300sc], the one or more device triggering request over a standard interface;
- an extraction unit [303] connected to at least the transceiver unit [302], the extraction unit [303] configured to extract, via the exposure function [300ef], one of: the DCS from the one or more device triggering requests based on a custom header of said each of the one or more device triggering requests in an event of presence of the custom header in the one or more device triggering requests, and a pre-maintained default DCS in an event of absence of the custom header in the one or more device triggering requests, and
- an optimization unit [304] connected to at least the extraction unit [303], the optimization unit [304] configured to optimize, the device triggering procedure for the

one or more Internet of Things (IoT) devices [300id] based on the DCS extracted from said each of the one or more device triggering requests.

10. The system [300] as claimed in claim 9, wherein the exposure function [300ef] is one of a Service Capability Exposure Function (SCEF) and a Network Exposure Function (NEF).

11. The system [300] as claimed in claim 9, wherein the service consumer [300sc]is one of a Services Capability Server (SCS), an Application Server (AS) and an Application Function (AF).

12. The system [300] as claimed in claim 9, wherein the standard interface is a standard T8/N33 interface.

13. The system [300] as claimed in claim 9, wherein the custom header is a "devicePayloadFormat" custom header.

14. The system [300] as claimed in claim 9, wherein to optimize the device triggering procedure for the one or more Internet of Things (IoT) devices [300id], the at least one optimization unit [304] is further configured to configure for the exposure function [300ef], the at least one DCS fetched from said each of the device triggering requests.

15. The system [300] as claimed in claim 9, wherein the pre-maintained default DCS is maintained by the exposure function [300ef] for each of the one or more device triggering requests of each service consumer [300sc], at a time of onboarding of each service consumer [300sc].

16. The system [300] as claimed in claim 9, wherein a balancing unit [305] is configured to enable one or more load balancers to load balance the one or more device triggering requests.

17. A User Equipment (UE) device receiving, the UE device comprising:
a transceiver unit configured to:

receive, a device triggering, from a system [300], via a Short Message Service Center (SMSC), wherein the system [300] performs optimization of a device triggering procedure for the UE device before the device triggering is sent to the UE device,

wherein the system [300] comprises:

a configuration unit [301], wherein the configuration unit [301] is configured to configure, for each service consumer [300sc] among one or more service consumers [300sc], a Data-Coding-Scheme (DCS) from one or more DCSs, wherein each DCS is associated with one or more device triggering requests for the UE device;

a transceiver unit [302] configured to receive, at an exposure function [300ef] from each service consumer [300sc] among the one or more service consumers [300sc], the one or more device triggering requests over a standard interface;

an extraction unit [303] configured to extract, via the exposure function [300ef], one of: the DCS from the one or more device triggering requests based on a custom header of said each of the one or more device triggering requests in an event of presence of the custom header in the one or more device triggering requests, and a pre-maintained default DCS in an event of absence of the custom header in the one or more device triggering requests; and

an optimization unit [304] configured to optimize, the device triggering procedure for the UE device based on the DCS extracted from said each of the one or more device triggering requests.

18. The UE device as claimed in claim 17, wherein the UE device belongs to a group consisting of one or more Internet of Things (IoT) devices.

19. A non-transitory computer-readable storage medium storing instructions for optimization of a device triggering procedure for one or more Internet of Things (IoT) devices [300id] in an exposure function [300ef], the storage medium comprising executable code which, when executed by one or more units of a system, causes:

- a configuration unit [301] to configure, for each service consumer [300sc] among one or more service consumers [300sc], a Data-Coding-Scheme (DCS) from one or more DCSs, wherein each DCS is associated with a one or more device triggering requests for the one or more IoT devices [300id];

- a transceiver unit [302] connected to at least the configuration unit [301], the transceiver unit [302] to receive, at the exposure function [300ef], from each service consumer [300sc] among the one or more service consumers [300sc], the one or more device triggering requests over a standard interface;
- an extraction unit [303] connected to at least the transceiver unit [302], the extraction unit [303] to extract, via the exposure function [300ef], one of: the DCS from the one or more device triggering requests based on a custom header of said each of the one or more device triggering requests in an event of presence of the custom header in the one or more device triggering requests, and a pre-maintained default DCS in an event of absence of the custom header in the one or more device triggering requests; and
- an optimization unit [304] connected to at least the extraction unit [303], the optimization unit [303] to optimize, the device triggering procedure for the one or more Internet of Things (IoT) devices [300id] based on the DCS extracted from said each of the one or more device triggering requests.

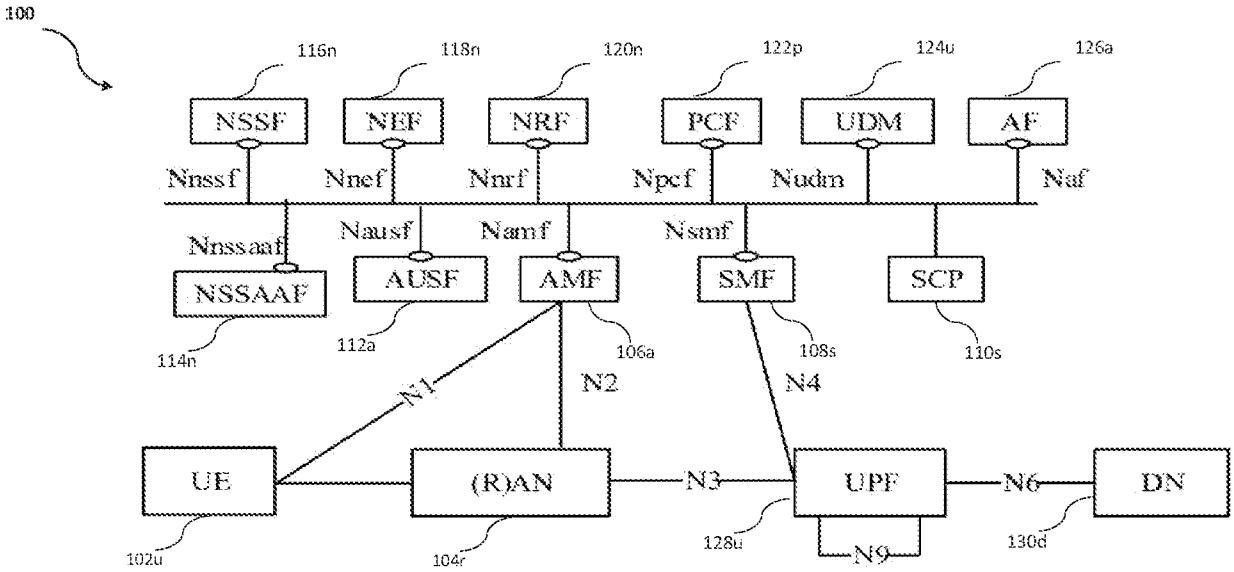

100
116n
118n
120n
122p
124u
126a
NSSF
NEF
NRF
PCF
UDM
AF
Nnssf
Nnef
Nnrf
Npcf
Nudm
Naf
Nnssaaf
Nausf
Namf
Nsmf
NSSAAF
AUSF
AMF
SMF
SCP
114n
112a
106a
108s
110s
N1
N2
N4
UE
(R)AN
N3
UPF
N6
DN
102u
104r
128u
N9
130d

FIG. 1

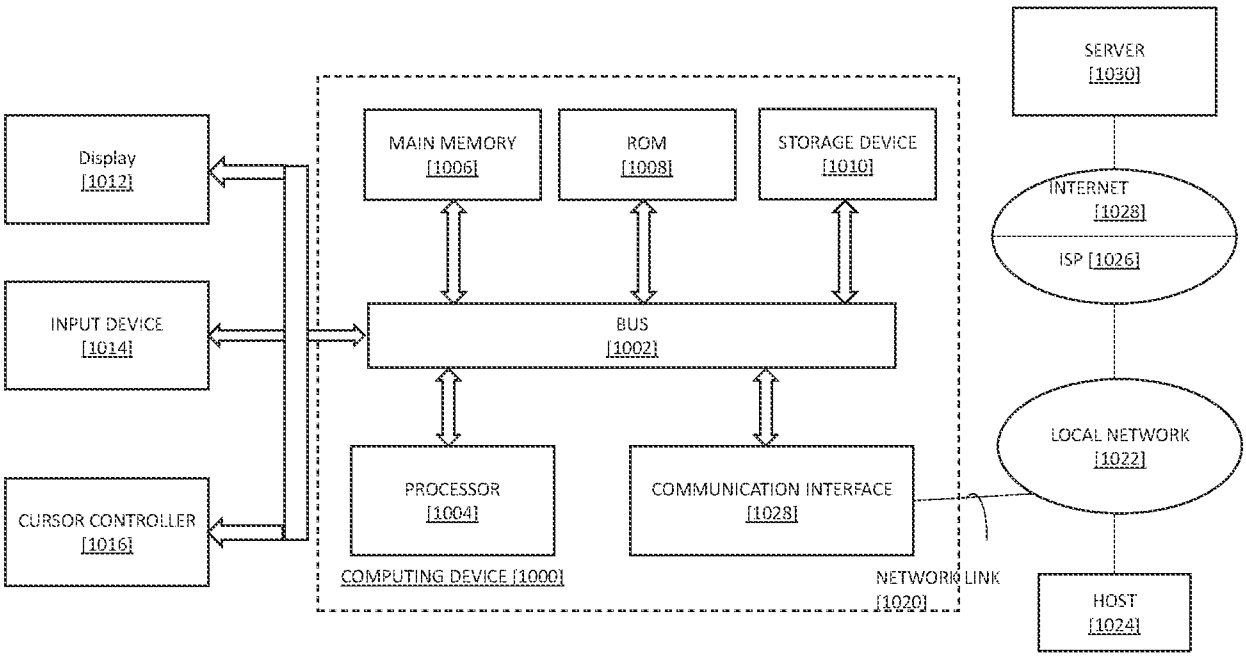

SERVER
[1030]
Display
[1012]
MAIN MEMORY
[1006]
ROM
[1008]
STORAGE DEVICE
[1010]
INTERNET
[1028]
ISP [1026]
INPUT DEVICE
[1014]
BUS
[1002]
LOCAL NETWORK
[1022]
CURSOR CONTROLLER
[1016]
PROCESSOR
[1004]
COMMUNICATION INTERFACE
[1028]
COMPUTING DEVICE [1000]
NETWORK LINK
[1020]
HOST
[1024]

FIG. 2

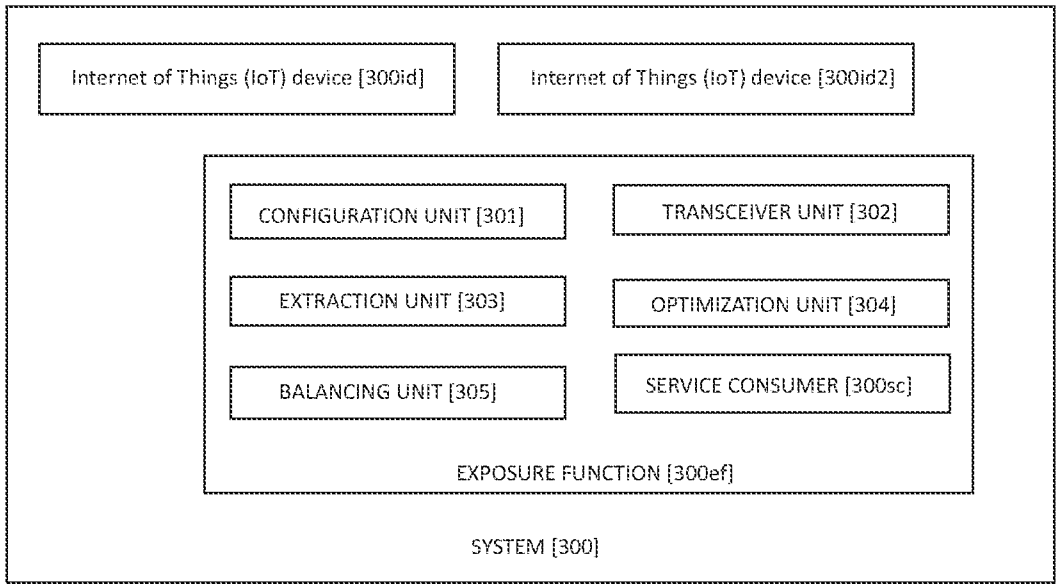

Internet of Things (IoT) device [300id]
Internet of Things (IoT) device [300id2]
CONFIGURATION UNIT [301]
TRANSCEIVER UNIT [302]
EXTRACTION UNIT [303]
OPTIMIZATION UNIT [304]
BALANCING UNIT [305]
SERVICE CONSUMER [300sc]
EXPOSURE FUNCTION [300ef]
SYSTEM [300]

FIG. 3

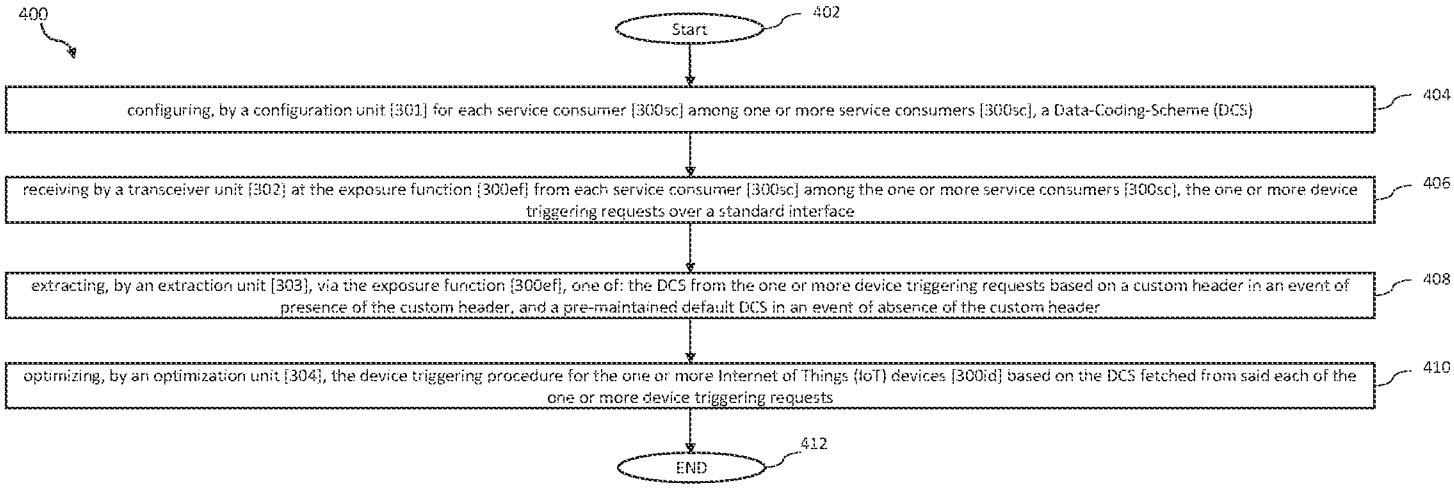

400
Start
402
configuring, by a configuration unit [301] for each service consumer [300sc] among one or more service consumers [300sc], a Data-Coding-Scheme (DCS)
404
receiving by a transceiver unit [302] at the exposure function [300ef] from each service consumer [300sc] among the one or more service consumers [300sc], the one or more device triggering requests over a standard interface
406
extracting, by an extraction unit [303], via the exposure function [300ef], one of: the DCS from the one or more device triggering requests based on a custom header in an event of presence of the custom header, and a pre-maintained default DCS in an event of absence of the custom header
408
optimizing, by an optimization unit [304], the device triggering procedure for the one or more Internet of Things (IoT) devices [300id] based on the DCS fetched from said each of the one or more device triggering requests
410
END
412

FIG. 4

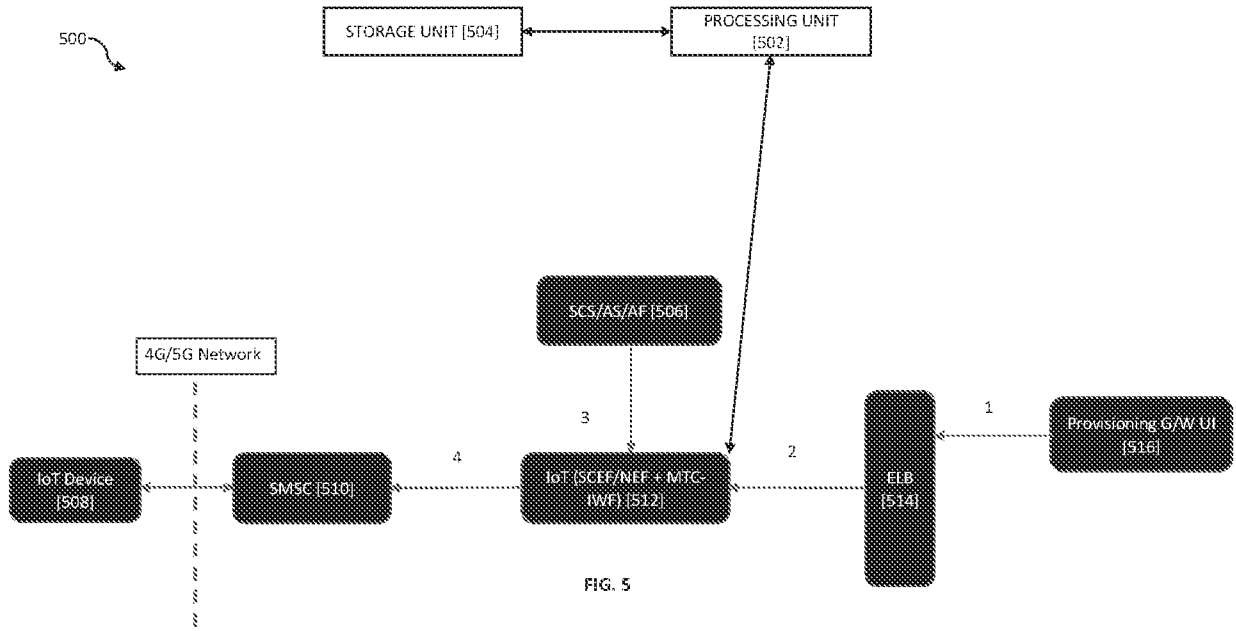

500
STORAGE UNIT [504]
PROCESSING UNIT [502]
SCS/AS/AF [506]
4G/5G Network
3
1
Provisioning G/W UI [516]
IoT Device [508]
4
SMSC [510]
IoT (SCEF/NEF + MTC-IWF) [512]
2
ELB [514]

FIG. 5

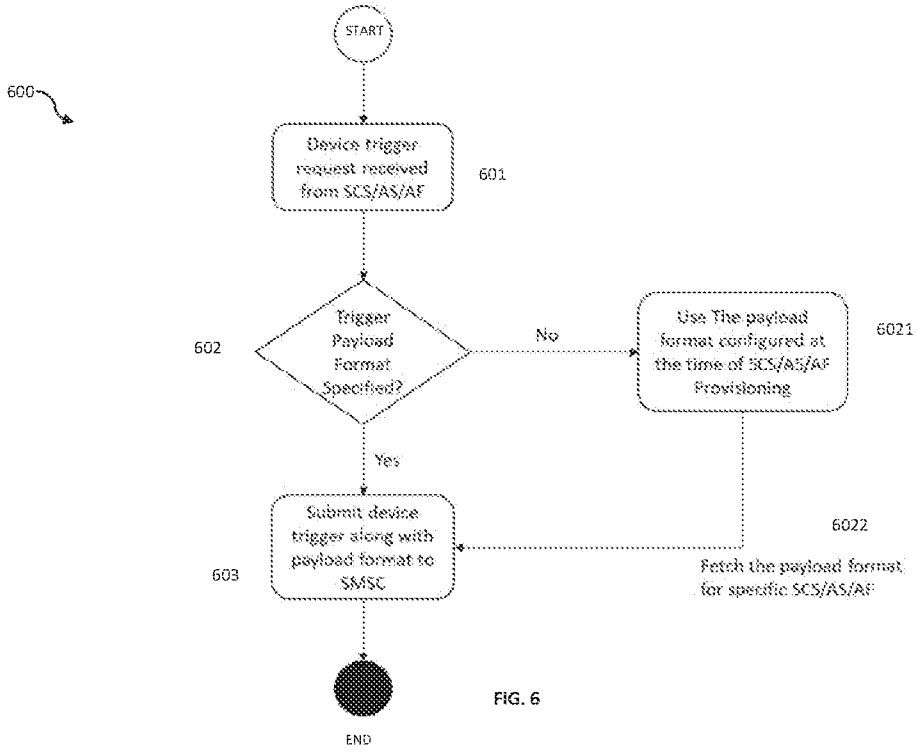

600
START
Device trigger request received from SCS/AS/AF
601
Trigger Payload Format Specified?
602
No
Use The payload format configured at the time of SCS/AS/AF Provisioning
6021
Yes
Submit device trigger along with payload format to SMSC
603
6022
Fetch the payload format for specific SCS/AS/AF
END

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IN2024/050749

A. CLASSIFICATION OF SUBJECT MATTER
H04W4/70,H04W4/50,H04L67/12,H04W24/02 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)

H04W, 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, Google Patents
Keywords - Optimization, DCS, Data-Coding-Scheme, trigger, procedure

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US20190025806A1 (STRONG FORCE IOT PORTFOLIO 2016 LLC) 24 JAN 2019 (24-01-2019) Para. [0471-0479], [0481-0486], [0514-0521]	1-19
Y	US20210219151A1 (TELEFONAKTIEBOLAGET LM ERICSSON AB) 15 JUL 2021 (15-07-2021) Para. [0155-0163]	1-19
Y	WO2013166230A2 (INTERDIGITAL PATENT HOLDINGS INC.) 07 NOV 2013 (07-11-2013) Para. [0015-0019], [0101-0109]	1-19

☐ 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
01-10-2024	01-10-2024
Name and mailing address of the ISA/ Indian Patent Office Plot No.32, Sector 14,Dwarka,New Delhi-110075 Facsimile No.	Authorized officer Saurabh Saxena Telephone No. +91-1125300200

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IN2024/050749

Citation	Pub.Date	Family	Pub.Date
US 20190025806 A1	24-01-2019	US 2019129405 A1	02-05-2019
		US 2018284737 A1	04-10-2018
		US 2019137988 A1	09-05-2019
		US 2020096990 A1	26-03-2020
US 20210219151 A1	15-07-2021	US 2021219151 A1	15-07-2021
		EP 3811651 A1	28-04-2021
		WO 2019243874 A1	26-12-2019