(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 2025/008876 A1

(51) International Patent Classification:
H04W 76/20 (2018.01) *H04W 12/069* (2021.01)
H04W 48/08 (2009.01) *H04W 24/04* (2009.01)

(21) International Application Number:
PCT/IN2024/050746

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

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
202321044638 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, India., Ahmedabad 380006 (IN).

(72) Inventors: **SINGH, Mukesh**; Office - 101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Ahmedabad - 380006, Gujarat, India., Ahmedabad 380006 (IN). **BHATNAGAR, Aayush**; Office - 101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Ahmedabad - 380006, Gujarat, India., Ahmedabad 380006 (IN). **SHEKHAR, Shashi**; Office - 101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Ahmedabad - 380006, Gujarat, India., Ahmedabad 380006 (IN). **SINGH, Bhupinder**; Office - 101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Ahmedabad - 380006, Gujarat, India., Ahmedabad 380006 (IN). **NADIMINTI, Manohar**; Office - 101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Ahmedabad - 380006, Gujarat, India., Ahmedabad 380006 (IN). **BISHT, Birendra Singh**; Office - 101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Ahmedabad - 380006, Gujarat, India., Ahmedabad 380006 (IN). **SINGH, Harbinder Pal**; Office - 101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Ahmedabad - 380006, Gujarat, India., Ahmedabad 380006 (IN). **AGGARWAL, Pravesh**; Office - 101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Ahmedabad - 380006, Gujarat, India., Ahmedabad 380006 (IN). **SINGH, Priyanka**; Office - 101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Ahmedabad - 380006, Gujarat, India., Ahmedabad

(54) **Title:** METHOD AND SYSTEM FOR WHITELISTING VOWIFI COMPATIBLE DEVICES

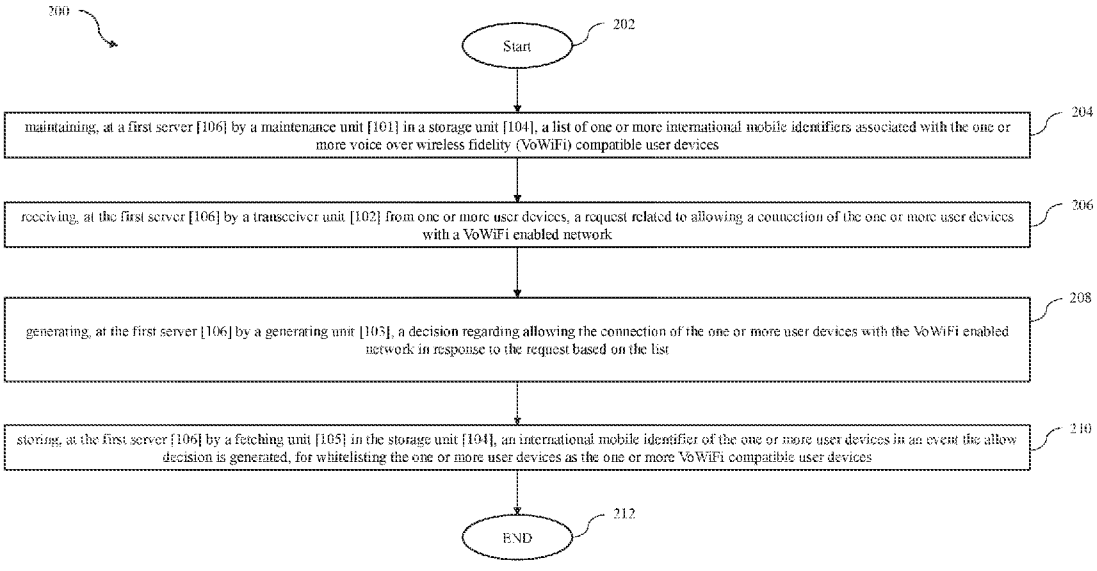

FIG. 2

(57) **Abstract:** The present disclosure relates to a method and a system for whitelisting VoWiFi compatible devices The disclosure encompasses maintaining a list of international mobile identifiers associated with one or more VoWiFi compatible user devices; receiving a request related to allowing a connection of one or more user devices with VoWiFi enabled network; generating a decision regarding allowing the connection of the one or more user devices with the VoWiFi enabled network based on the international mobile identifier of the one or more user devices and the list; and storing the international mobile identifier of the one or more user devices in an event of the allowed decision, in order to whitelist the one or more user devices as the one or more VoWiFi compatible user devices.

[Continued on next page]

WO 2025/008876 A1

380006 (IN). **SOREN, Rohit**; Office - 101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Ahmedabad - 380006, Gujarat, India., Ahmedabad 380006 (IN). **SAHU, Bidhu**; Office - 101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Ahmedabad - 380006, Gujarat, India., Ahmedabad 380006 (IN).

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

METHOD AND SYSTEM FOR WHITELISTING VoWiFi COMPATIBLE DEVICES

FIELD OF THE DISCLOSURE

[001] The present disclosure relates generally to the field of wireless communication systems. More particularly, the present disclosure relates to methods and systems for whitelisting only voice over wireless fidelity (VoWiFi) compatible devices.

BACKGROUND

[002] The following description of 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 be used only to enhance the understanding of the reader with respect to the present disclosure, and not as admissions of prior art.

[003] 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 analog 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. 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.

[004] However, there are several limitations of the existing technologies. For instance,, devices incompatible (or rogue devices) with voice over wireless fidelity (VoWiFi) keep sending connection request to a network node, and thereby keep attempting to switch from cellular to VoWiFi network. Conventionally, network nodes accept such requests and allows VoWiFi incompatible devices to switch from cellular to VoWiFi network. This results in poor user experience primarily because an incompatible VoWiFi device is connecting to the VoWiFi

network. If Connection request of VoWiFi incompatible devices is not rejected by a network node implemented on a server, network resources will be unnecessary occupied.

[005] Thus, there exists an imperative need in the art to list devices for whitelisting VoWiFi compatible devices, which the present disclosure aims to address.

OBJECTS OF THE DISCLOSURE

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

[007] It is an object of the present disclosure to provide a system and a method for whitelisting voice over wireless fidelity (VoWiFi) compatible devices.

[008] It is another object of the present disclosure to provide a solution that whitelists devices as VoWiFi compatible devices.

[009] It is another object of the present disclosure to reject rogue devices that do not support VoWiFi by checking an international mobile identifier such as an international mobile equipment identity (IMEI) of devices.

[010] It is another object of the present disclosure to save unnecessary signalling attempts and network resources by rejecting registration of rogue devices on a VoWiFi network.

SUMMARY

[011] 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.

[012] One aspect of the present disclosure relates to a method for whitelisting one or more voice over wireless fidelity (VoWiFi) compatible user devices. The method comprises maintaining a list of one or more international mobile identifiers associated with the one or more VoWiFi incompatible user devices at a first server by a maintenance unit in a storage unit. The method further comprises receiving a request related to allowing a connection of one or more user devices with a VoWiFi enabled network at the first server by a transceiver unit from the one or more user

devices. The method further comprises generating a decision regarding allowing the connection of the one or more user devices with the VoWiFi enabled network at the first server by a generating unit in response to the request based on the list. And, the method further comprises storing the international mobile identifier of the one or more user devices at the first server by a fetching unit in the storage unit in an event an allow decision is generated for whitelisting the one or more user devices as the one or more VoWiFi compatible user devices.

[013] In an exemplary aspect of the present disclosure, the first server is a session management function (SMF) server.

[014] In an exemplary aspect of the present disclosure, the generation of the decision is based on a comparison of the international mobile identifier of the one or more user devices from which the request is received with the list of the one or more international mobile identifiers associated with the one or more VoWiFi compatible devices. The decision is one of an allow decision and a forbid decision. The allow decision is generated in an event the generating unit at the first server allows connection of the one or more user devices with the VoWiFi enabled network, and the forbid decision is generated in an event the generating unit at the first server forbids connection of the one or more user devices with the VoWiFi enabled network.

[015] In an exemplary aspect of the present disclosure, for the generation of the decision regarding allowing the connection of the one or more user devices with the VoWiFi enabled network, the method comprises: searching, by the generating unit at the first server, the international mobile identifier of the one or more user devices from which the request is received in the list of the one or more international mobile identifiers associated with the one or more VoWiFi incompatible devices; and generating, by the generating unit at the first server, one of the allow decision and the forbid decision. The allow decision is generated in an event the international mobile identifier of the one or more user devices from which the request is received is found in the list of the one or more international mobile identifiers associated with the one or more VoWiFi compatible devices, and the forbid decision is generated in an event the international mobile identifier of the one or more user devices from which the request is received is not found in the list of the one or more international mobile identifiers associated with the one or more VoWiFi compatible devices.

[016] Another aspect of the present disclosure also relates to a system for whitelisting one or more voice over wireless fidelity (VoWiFi) compatible user devices. The system comprises a

maintenance unit configured to maintain a list of one or more international mobile identifiers associated with the one or more VoWiFi compatible user devices at the first server in a storage unit. The system further comprises a transceiver unit which is configured to receive a request at the first server from one or more user devices. It is important to note that the request relates to allowing a connection of the one or more user devices with a VoWiFi enabled network. The system further comprises a generating unit which is further configured to generate a decision at the first server. It is important to note that the decision is regarded to allowing the connection of the one or more user devices with the VoWiFi enabled network in response to the request based on the list. The system further comprises a fetching unit which is configured to store the international mobile identifier of the one or more user devices at the first server in the storage unit in an event an allow decision is generated for whitelisting the one or more user devices as the one or more VoWiFi compatible user device.

[017] Yet another aspect of the present disclosure also relates to a non-transitory computer readable storage medium storing instructions for whitelisting one or more voice over wireless fidelity (VoWiFi) compatible user devices. The instructions when executed by one or more units of a system configured for whitelisting the one or more voice over wireless fidelity (VoWiFi) compatible user devices, cause a maintenance unit of said system to maintain a list of one or more international mobile identifiers associated with the one or more VoWiFi compatible user devices at the first server in a storage unit. The instructions upon execution further cause a transceiver unit of said system to receive a request at the first server from one or more user devices. It is important to note that the request relates to allowing a connection of the one or more user devices with a VoWiFi enabled network. The instructions upon execution further cause a generating unit of said system to generate a decision at the first server. It is important to note that the decision is regarded to allowing the connection of the one or more user devices with the VoWiFi enabled network in response to the request based on the list. Also, the instructions upon execution further cause a fetching unit of said system to store the international mobile identifier of the one or more user devices at the first server in the storage unit in an event an allow decision is generated for whitelisting the one or more user devices as the one or more VoWiFi compatible user device.

[018] Another aspect of the present disclosure also relates to a user equipment for whitelisting one or more voice over wireless fidelity (VoWiFi) compatible user devices, the user equipment comprises: a memory; a processor coupled to the memory, the processor is configured to: transmit, to a system, a request related to allowing a connection of the one or more user devices with a VoWiFi enabled network, and receive from the system, a response associated with the request, wherein the response associated with the request is received based on: maintaining, by the system,

a list of one or more international mobile identifiers associated with the one or more voice over wireless fidelity (VoWiFi) compatible user devices, generating, by the system, a decision regarding allowing the connection of the one or more user devices with the VoWiFi enabled network in response to the request based on the list, and storing, by the system, an international mobile identifier of the one or more user devices in an event an allow decision is generated, for whitelisting the one or more user devices as the one or more VoWiFi compatible user devices.

BRIEF DESCRIPTION OF DRAWINGS

[019] 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.

[020] FIG. 1A illustrates an exemplary block diagram representation of 5th generation core (5GC) network architecture [100A], in accordance with exemplary embodiment of the present disclosure.

[021] FIG.1B illustrates an exemplary block diagram of a system [100] for whitelisting VoWiFi compatible devices, in accordance with exemplary embodiments of the present disclosure.

[022] FIG.2 illustrates an exemplary method flow diagram indicating process [200] for whitelisting VoWiFi compatible user devices, in accordance with exemplary embodiments of the present disclosure.

[023] FIG.3 illustrates an exemplary flow chart of a process [300] for whitelisting VoWiFi compatible devices, in accordance with exemplary embodiments of the present disclosure.

[024] FIG. 4 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.

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

DESCRIPTION

[026] 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 can 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. Some of the problems discussed above might not be fully addressed by any of the features described herein. Example embodiments of the present disclosure are described below, as illustrated in various drawings in which like reference numerals refer to the same parts throughout the different drawings.

[027] 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.

[028] It should be noted that the terms "mobile device", "user equipment", "user device", “communication device”, “device” and similar terms are used interchangeably for the purpose of describing the disclosure. These terms are not intended to limit the scope of the disclosure or imply any specific functionality or limitations on the described embodiments. The use of these terms is solely for convenience and clarity of description. The disclosure is not limited to any particular type of device or equipment, and it should be understood that other equivalent terms or variations thereof may be used interchangeably without departing from the scope of the disclosure as defined herein.

[029] 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,

networks, processes, and other components may be shown as components in block diagram form in order not to obscure the embodiments in unnecessary detail. In other instances, well-known circuits, processes, algorithms, structures, and techniques may be shown without unnecessary detail in order to avoid obscuring the embodiments.

[030] 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 can 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.

[031] 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.

[032] As used herein, an "electronic device", or "portable electronic device", or "user device" or "communication device" or "user equipment" or "device" refers to any electrical, electronic, electromechanical and computing device. The user device is capable of receiving and/or transmitting one or parameters, performing function/s, communicating with other user devices and transmitting data to the other user devices. The user equipment may have a processor, a display, a memory, a battery and an input-means such as a hard keypad and/or a soft keypad. The user equipment may be capable of operating on any radio access technology including but not limited to IP-enabled communication, Zig Bee, Bluetooth, Bluetooth Low Energy, Near Field Communication, Z-Wave, Wi-Fi, Wi-Fi direct, VoWiFi etc. For instance, the user equipment may include, but not limited to, a mobile phone, smartphone, virtual reality (VR) devices, augmented reality (AR) devices, laptop, a general-purpose computer, desktop, personal digital assistant, tablet computer, mainframe computer, or any other device as may be obvious to a person skilled in the art for implementation of the features of the present disclosure.

[033] Further, the user device and/or a system as described herein to implement technical features as disclosed in the present disclosure may also comprise a "processor" or "processing unit", wherein processor refers to any logic circuitry for processing instructions. The 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 Processor (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 is a hardware processor.

[034] As portable electronic devices and wireless technologies continue to improve and grow in popularity, the advancing wireless technologies for data transfer are also expected to evolve and replace the older generations of technologies. In the field of wireless data communications, the dynamic advancement of various generations of cellular technology are also seen. The development, in this respect, has been incremental in the order of second generation (2G), third generation (3G), fourth generation (4G), and now fifth generation (5G), and more such generations are expected to continue in the forthcoming time.

[035] Radio Access Technology (RAT) refers to the technology used by mobile devices/ user equipment (UE) to connect to a cellular network. It refers to the specific protocol and standards that govern the way devices communicate with base stations, which are responsible for providing the wireless connection. Further, each RAT has its own set of protocols and standards for communication, which define the frequency bands, modulation techniques, and other parameters used for transmitting and receiving data. Examples of RATs include GSM (Global System for Mobile Communications), CDMA (Code Division Multiple Access), UMTS (Universal Mobile Telecommunications System), LTE (Long-Term Evolution), and 5G. The choice of RAT depends on a variety of factors, including the network infrastructure, the available spectrum, and the mobile device's/device's capabilities. Mobile devices often support multiple RATs, allowing them to connect to different types of networks and provide optimal performance based on the available network resources.

[036] As discussed in the background section, devices incompatible with VoWiFi keeps sending connection request to a network node, and thereby keeps attempting to switch from a cellular

network to a VoWiFi network. This increases load on the VoWiFi network as well as results in poor user experience.

[037] The present disclosure aims to overcome the above-mentioned and other existing problems in the field of wireless communication technology by providing a method and a system for whitelisting VoWiFi compatible devices.

[038] Hereinafter, exemplary embodiments of the present disclosure will be described with reference to the accompanying drawings.

[039] FIG. 1A illustrates an exemplary block diagram representation of 5th generation core (5GC) network architecture, in accordance with exemplary embodiment of the present disclosure. As shown in FIG. 1A, the 5GC network architecture [100A] includes a user equipment (UE) [102a], a radio access network (RAN) [104a], an access and mobility management function (AMF) [106a], a Session Management Function (SMF) [108a], a Service Communication Proxy (SCP) [110a], an Authentication Server Function (AUSF) [112a], a Network Slice Specific Authentication and Authorization Function (NSSAAF) [114a], a Network Slice Selection Function (NSSF) [116a], a Network Exposure Function (NEF) [118a], a Network Repository Function (NRF) [120a], a Policy Control Function (PCF) [122a], a Unified Data Management (UDM) [124a], an application function (AF) [126a], a User Plane Function (UPF) [128a], a data network (DN) [130a], 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.

[040] The User Equipment (UE) [102a] interfaces with the network via the Radio Access Network (RAN) [104a]; the Access and Mobility Management Function (AMF) [106a] manages connectivity and mobility, while the Session Management Function (SMF) [108a] administers session control; the service communication proxy (SCP) [110a] routes and manages communication between network services, enhancing efficiency and security, and the Authentication Server Function (AUSF) [112a] handles user authentication; the Network Slice Specific Authentication and Authorization Function (NSSAAF) [114a] for integrating the 5G core network with existing 4G LTE networks i.e., to enable Non-Standalone (NSA) 5G deployments, the Network Slice Selection Function (NSSF) [116a], Network Exposure Function (NEF) [118a], and Network Repository Function (NRF) [120a] enable network customization, secure interfacing with external applications, and maintain network function registries respectively; the Policy Control Function (PCF) [122a] develops operational policies, and the Unified Data Management

(UDM) [124a] manages subscriber data; the Application Function (AF) [126a] enables application interaction, the User Plane Function (UPF) [128a] processes and forwards user data, and the Data Network (DN) [130a] connects to external internet resources; collectively, these components are designed to enhance mobile broadband, ensure low-latency communication, and support massive machine-type communication, solidifying the 5GC as the infrastructure for next-generation mobile networks.

[041] **Radio Access Network (RAN) [104a]** is the part of a mobile telecommunications system that connects user equipment (UE) [102a] 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.

[042] **Access and Mobility Management Function (AMF) [106a]** 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.

[043] **Session Management Function (SMF) [108a]** 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.

[044] **Service Communication Proxy (SCP) [110a]** 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.

[045] **Authentication Server Function (AUSF) [112a]** 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.

[046] **Network Slice Specific Authentication and Authorization Function (NSSAAF) [114a]** 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.

[047] **Network Slice Selection Function (NSSF) [116a]** 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.

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

[049] **Network Repository Function (NRF) [120a]** 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.

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

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

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

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

[054] **Data Network (DN) [130a]** 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.

[055] Referring to FIG.1B, an exemplary block diagram of a system [100] for whitelisting one or more voice over wireless fidelity (VoWiFi) compatible user devices is shown, in accordance with the exemplary embodiments of the present disclosure.

[056] Further, in accordance with the present disclosure, it is to be acknowledged that the functionality described for the various the 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.

[057] As used herein, the one or more VoWiFi compatible devices are electronic devices that offers their user(s) a flexibility to make voice calls in areas with poor cellular coverage (and to reduce cellular voice call charges in some cases) by utilizing Wi-Fi networks for voice communication. The VoWiFi compatible devices support making voice calls over Wi-Fi networks instead of relying solely on traditional cellular networks. The VoWiFi compatible devices may include but not limited to smartphones, tablets, and other mobile devices equipped with the necessary hardware and software to enable VoWiFi functionality.

[058] The system [100] comprises at least one first server [106] having at least one maintenance unit [101], at least one transceiver unit [102], at least one generating unit [103], at least one storage unit [104] and at least one fetching unit [105]. In an implementation, the system [100] is implemented in a session management function/facility (SMF) residing at a server in a 5G communication network. It is important to note that the first server [106] is a SMF server (sometimes also referred as SMF).

[059] As used herein, the first server [106] may include a hardware unit that is capable of serving requests and performing various tasks in a networked environment (preferable a 5G communication network). The first server [106] is a server that may encompass different types of hardware configurations and architectures that may be obvious to a person skilled in the art to perform technical functionalities as disclosed in the present disclosure. The first server [106] may also refer to any computing device or system capable of providing services or resources to other devices or users via such devices in the communication network. The first server [106] may perform various tasks such as signal coding, data processing, input/output processing, and any other functionality required to facilitate tasks such as handling requests from client devices, managing network connections, executing applications, managing data storage, and coordinating resource allocation with respect to its designated roles and responsibilities in the communication

network that enables the working of the system [100] according to the present disclosure. Since the first server [106] being the SMF server, it is important to note that SMF server plays a crucial role in managing an establishment, modification, and termination of user sessions. It acts as a control point for the user plane, facilitating the routing of user data packets between User Equipment (UE) (such as a communication device including but not limited to a mobile cell phone) and external data networks. The SMF is responsible for assigning IP addresses to UEs by establishing Quality of Service (QoS) parameters for user sessions and ensuring seamless handovers between different network nodes. Additionally, the SMF enables the implementation of network policies and enforcement of security mechanisms to safeguard user data and network resources. Thus, the SMF plays a central role in optimizing the performance and efficiency of user sessions in the 5G communication network.

[060] As used herein, the storage unit [104] (also referred to as "memory unit" and/or "memory") 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. Also, the storage unit is configured to store a data that is required by one or more units of the system [100] to perform their respective operations.

[061] Additionally, the maintenance unit [101], the generating unit [103], and the fetching unit [105] are processors. The 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 DSP core, a controller, a microcontroller, Application Specific Integrated Circuits, Field Programmable Gate Array circuits, any other type of integrated circuits, etc. Also, the transceiver unit [102] includes a transmitter unit having capabilities to transmit data/signals and a receiver unit having capabilities to receive data/signals.

[062] Also, all of the components/ units of the system [100] are assumed to be connected to each other unless otherwise indicated below. Also, in Fig. 1 only a few units are shown, however, the system [100] may comprise multiple such units or the system [100] may comprise any such numbers of said units, as required to implement the features of the present disclosure. Further, in an implementation, the system [100] may reside in a server or a network entity. In yet another implementation, the system [100] may reside partly in the server/ network entity and partly in the user device.

[063] The system [100] is configured for whitelisting one or more VoWiFi compatible user devices, with the help of the interconnection between the components/units of the system [100].

[064] In order to whitelist the one or more VoWiFi compatible devices, the maintenance unit [101] of the system [100] is configured to maintain a list of one or more international mobile identifiers associated with the one or more VoWiFi compatible user devices at the first server [106] in the storage unit [104].

[065] In an implementation of the disclosure, the one or more international mobile identifiers may be derived from one or more international mobile equipment identity type allocation codes (IMEI TACs).

[066] The maintenance unit [101] is connected to the transceiver unit [102], wherein the transceiver unit [102] is configured to receive at the first server [106] from the one or more user devices, a request related to allowing a connection of one or more user devices with a VoWiFi enabled network. Since the Type Allocation Code (TAC) indicates a manufacturer and model of a particular device, based on a TAC of the one or more user devices, the system [100] at the first server [106] (e.g., the SMF server) decides which user device(s) should be allowed to connect to the VoWiFi enabled network. Based on the decision of the first server [106] say the SMF, one or more VoWiFi compatible device identified from the one or more user devices connects to the VoWiFi enabled network. Particularly, the generating unit [103] is configured to generate a decision regarding allowing the connection of the one or more user devices with the VoWiFi enabled network at the first server [106] in response to the request, based on the list. The fetching unit [105] is then configured to store the international mobile identifier of the one or more user devices at the first server [106] in the storage unit [104] in an event an allow decision is generated for whitelisting the one or more user devices as the one or more VoWiFi compatible user devices.

[067] In an implementation of the disclosure, the generation of the decision is based on a comparison of the international mobile identifier of the one or more user devices from which the request is received with the list of the one or more international mobile identifier associated with the one or more VoWiFi compatible devices.

[068] In an implementation of the disclosure, the decision is one of an allow decision and a forbid decision. It is emphasized that the allow decision is generated in an event the generating unit [103]

at the first server [106] allows connection of the one or more user devices with the VoWiFi enabled network while the forbid decision is generated in an event the generating unit [103] at the first server [106] forbids connection of the one or more user devices with the VoWiFi enabled network.

[069] In an implementation of the disclosure, the generating unit [103] for generating the decision regarding allowing the connection of the one or more user devices with the VoWiFi enabled network (i.e., one of the allow decision and the forbid decision), is also configured to search the international mobile identifier of the one or more user devices from which the request is received in the list of the one or more international mobile identifiers associated with the one or more VoWiFi incompatible devices. It is also to be noted that the allow decision is generated in an event the international mobile identifier of the one or more user devices from which the request is received is found in the list of the one or more international mobile identifiers associated with the one or more VoWiFi compatible devices, and the forbid decision is generated in an event the international mobile identifier of the one or more user devices from which the request is received is not found in the list of the one or more international mobile identifiers associated with the one or more VoWiFi compatible devices.

[070] In an implementation, the fetching unit [105] is configured to store the international mobile identifiers of the one or more user devices at the first server [106] in the storage unit [104] in an event when the allow decision is generated, for whitelisting the one or more user devices as the one or more VoWiFi compatible user devices. In another implementation, the fetching unit [105] is configured to store international mobile identifiers of all VoWiFi incompatible devices therefore acting as a temporary memory. In said implementation, an international mobile identifier of one or more user devices requesting connection to a VoWiFi enabled network is matched with the stored international mobile identifiers of the all VoWiFi incompatible devices. If a match is found, the one or more user devices requesting connection to the VoWiFi enabled network is not allowed to connect and the request sent by said one or more user devices is denied by the system [100].

[071] In yet another implementation, a non-transitory computer readable storage medium storing instructions for whitelisting one or more voice over wireless fidelity (VoWiFi) compatible user devices is disclosed. The instructions when executed by one or more units of a system [100] configured for whitelisting the one or more voice over wireless fidelity (VoWiFi) compatible user devices, cause a maintenance unit [101] of said system [100] to maintain a list of one or more international mobile identifiers associated with the one or more VoWiFi compatible user devices at the first server [106] in a storage unit [104]. The instructions upon execution further cause a

transceiver unit [102] of said system [100] to receive a request at the first server [106] from one or more user devices. It is important to note that the request relates to allowing a connection of the one or more user devices with a VoWiFi enabled network. The instructions upon execution further cause a generating unit [103] of said system [100] to generate a decision at the first server [106]. It is important to note that the decision is regarded to allowing the connection of the one or more user devices with the VoWiFi enabled network in response to the request based on the list. Also, the instructions upon execution further cause a fetching unit [105] of said system [100] to store the international mobile identifier of the one or more user devices at the first server [106] in the storage unit [104] in an event an allow decision is generated for whitelisting the one or more user devices as the one or more VoWiFi compatible user device.

[072] Referring to FIG.2 an exemplary method flow diagram [200], for whitelisting one or more VoWiFi compatible user devices, in accordance with exemplary embodiments of the present disclosure is shown. In an implementation of the disclosure, the method [200] is performed by the system [100]. As shown in FIG. 2, the method [200] starts at step [202].

[073] At step [204], the method [200] as disclosed by the present disclosure comprises maintaining a list of one or more international mobile identifiers associated with the one or more voice over wireless fidelity (VoWiFi) compatible user devices at a first server [106] by a maintenance unit [101] in a storage unit [104].

[074] In an implementation of the disclosure, the one or more international mobile identifiers may be derived from one or more international mobile equipment identity type allocation codes (IMEI TACs).

[075] In an implementation of the disclosure the first server [106] is a session management function/facility (SMF) server (sometimes also referred as SMF). Since the first server [106] being the SMF server, it is furthermore important to note that SMF server plays a crucial role in managing an establishment, modification, and termination of user sessions. It acts as a control point for the user plane, facilitating the routing of user data packets between User Equipment (UE) (such as a communication device including but not limited to a mobile cell phone) and external data networks. The SMF is responsible for assigning IP addresses to UEs by establishing Quality of Service (QoS) parameters for user sessions and ensuring seamless handovers between different network nodes. Additionally, the SMF enables the implementation of network policies and enforcement of security mechanisms to safeguard user data and network resources. Thus, the SMF

plays a central role in optimizing the performance and efficiency of user sessions in the 5G communication network.

[076] Next, at step [206], the method [200] as disclosed by the present disclosure comprises receiving from one or more user devices at the first server [106] by a transceiver unit [102], a request related to allowing a connection of the one or more user devices with a VoWiFi enabled network.

[077] Next, at step [208], the method [200] as disclosed by the present disclosure comprises generating at the first server [106] by a generating unit [103], a decision regarding allowing the connection of the one or more user devices with the VoWiFi enabled network in response to the request based on the list.

[078] In an implementation of the disclosure, in the method [200], the generation of the decision is based on a comparison of an international mobile identifier of the one or more user devices from which the request is received with the list of the one or more international mobile identifiers associated with the one or more VoWiFi compatible devices. Further, the decision is one of an allow decision and a forbid decision. It is also important to note that the allow decision is generated in an event the generating unit [103] at the first server [106] allows connection of the one or more user devices with the VoWiFi enabled network while the forbid decision is generated in an event the generating unit [103] at the first server [106] forbids connection of the one or more user devices with the VoWiFi enabled network.

[079] In an implementation of the disclosure, in the method [200], for the generation of the decision regarding allowing the connection of the one or more user devices with the VoWiFi enabled network, the method [200] comprises searching by the generating unit [103] at the first server [106], the international mobile identifier of the one or more user devices from which the request is received in the list of the one or more international mobile identifiers associated with the one or more VoWiFi incompatible devices. The method [200] then comprises generating one of the allow decision and the forbid decision by the generating unit [103] at the first server [106]. It is important to note that the allow decision is generated in an event the international mobile identifier of the one or more user devices from which the request is received is found in the list of the one or more international mobile identifiers associated with the one or more VoWiFi compatible devices while the forbid decision is generated in an event the international mobile identifier of the one or more user devices from which the request is received is not found in the

list of the one or more international mobile identifiers associated with the one or more VoWiFi compatible devices.

[080] Next, at step [210], the method [200] as disclosed by the present disclosure comprises storing the international mobile identifier of the one or more user devices at the first server [106] in the storage unit [104] by a fetching unit [105], in an event the allow decision is generated, for whitelisting the one or more user devices as the one or more VoWiFi compatible user devices.

[081] Thereafter, the method terminates at step [212].

[082] Referring to FIG. 3 an exemplary flow chart of a process [300] for whitelisting one or more VoWiFi compatible devices, in accordance with exemplary embodiments of the present disclosure is shown. As depicted in FIG.3, at [step 1], an evolved Packet Data Gateway (ePDG) [302] queries a SMF server [304] by sending a create session request (CSR).

[083] As used herein, the ePDG [302] here refers to a network element for facilitating secure data transmission for one or more user devices in a communication network. The functions of ePDG [302] may include enabling secure and efficient connectivity, QoS policy enforcement for managing traffic, bandwidth and network resources allocation etc. of the one or more user devices in the communication network.

[084] Also, in an implementation, the CSR may involve generation of an encrypted request by the ePDG [302], to establish secure communication channels between the ePDG [302] and other network entities. It may be used by the ePDG [302] to authenticate itself to user device(s) for establishment of secure connections thereby ensuring the integrity and confidentiality of data transmitted over the communication network.

[085] Also, in an implementation of the disclosure, the SMF server [304] maintains a list of one or more international mobile identifiers associated with one or more voice over wireless fidelity (VoWiFi) compatible user devices. Further, when the one or more user devices (via ePDG [302]) sends the CSR (may also called as attach request) to the SMF server [304] for allowing a connection of the one or more user devices with a VoWiFi enabled network, the SMF server [304] generates a decision regarding allowing the connection of the one or more user devices with the VoWiFi enabled network in response to the request based on the list of one or more international mobile identifiers associated with the one or more VoWiFi compatible user devices. Particularly,

as indicates at [step 2] in FIG. 3, the SMF server [304] checks international mobile identifier of the one or more user devices in the CSR for generating the decision. After checking the list for the international mobile identifier of the one or more user devices, the SMF server [304] as indicated at [step 3] in FIG. 3 sends to the ePDG [302] a Create Session Response (Success or Reject) based on the checking. Therefore, the SMF server [304] successfully allows or rejects the one or more user devices for the VoWiFi enabled network.

[086] **FIG. 2** illustrates an exemplary block diagram of a computing device [1000] (also referred herein as computing system [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 whitelisting only voice over wireless fidelity (VoWiFi) compatible devices utilising the system. In another implementation, the computing device [1000] itself implements the method for optimising the network management process 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.

[087] The computing device [1000] may include a bus [1002] or other communication mechanism for communicating information, and a hardware processor [1004] coupled with the 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].

[088] 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 controller [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.

[089] 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.

[090] 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]. The local network [1022] is further connected to a host [1024]. 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.

[091] 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 host [1024], 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.

[092] In an embodiment of the present disclosure as disclosed herein, the present disclosure relates to a user equipment such as an administrator user equipment for whitelisting one or more voice over wireless fidelity (VoWiFi) compatible user devices. The user equipment comprises a memory and a processor coupled to the memory. The processor is configured to maintain, at a first server by a maintenance unit in a storage unit, a list of one or more international mobile identifiers associated with the one or more voice over wireless fidelity (VoWiFi) compatible user devices; receive, at the first server by a transceiver unit from one or more user devices, a request related to allowing a connection of the one or more user devices with a VoWiFi enabled network, generate, at the first server by a generating unit, a decision regarding allowing the connection of the one or more user devices with the VoWiFi enabled network in response to the request based on the list; and store, at the first server by a fetching unit in the storage unit, an international mobile identifier of the one or more user devices in an event an allow decision is generated, for whitelisting the one or more user devices as the one or more VoWiFi compatible user devices.

[093] The present disclosure also relates to a user equipment for whitelisting one or more voice over wireless fidelity (VoWiFi) compatible user devices, the user equipment comprises: a memory; a processor coupled to the memory, the processor is configured to: transmit, to a system [100], a request related to allowing a connection of the one or more user devices with a VoWiFi enabled network, and receive from the system [100], a response associated with the request, wherein the response associated with the request is received based on: maintaining, by the system [100], a list of one or more international mobile identifiers associated with the one or more voice over wireless fidelity (VoWiFi) compatible user devices, generating, by the system [100], a decision regarding allowing the connection of the one or more user devices with the VoWiFi enabled network in response to the request based on the list, and storing, by the system [100], an international mobile identifier of the one or more user devices in an event an allow decision is generated, for whitelisting the one or more user devices as the one or more VoWiFi compatible user devices.

[094] The present disclosure also relates to a non-transitory computer readable storage medium storing instructions for whitelisting one or more voice over wireless fidelity (VoWiFi) compatible user devices. The instructions when executed by one or more units of a system configured for whitelisting the one or more voice over wireless fidelity (VoWiFi) compatible user devices, cause a maintenance unit of said system to maintain a list of one or more international mobile identifiers associated with the one or more VoWiFi compatible user devices at the first server in a storage unit. The instructions upon execution further cause a transceiver unit of said system to receive a request at the first server from one or more user devices. It is important to note that the request relates to allowing a connection of the one or more user devices with a VoWiFi enabled network. The instructions upon execution further cause a generating unit of said system to generate a decision at the first server. It is important to note that the decision is regarded to allowing the connection of the one or more user devices with the VoWiFi enabled network in response to the request based on the list. Also, the instructions upon execution further cause a fetching unit of said system to store the international mobile identifier of the one or more user devices at the first server in the storage unit in an event an allow decision is generated for whitelisting the one or more user devices as the one or more VoWiFi compatible user device.

[095] As is evident from the above, the present disclosure provides a technically advanced solution for whitelisting of VoWiFi compatible devices. Further, implementing the features of the present disclosure enables one to reduce load on a VoWiFi network that is created by connection of VoWiFi incompatible devices. Furthermore, implementing the feature of the present disclosure improves user experience by whitelisting VoWiFi compatible devices. With the help of checking international mobile identifiers of user devices in SMF, an optimization is achieved to identify and bar rogue device(s) from establishing a connection with VoWiFi network thereby leading to reduction in network traffic and improved network performance.

[096] While considerable emphasis has been placed herein on the disclosed embodiments, it will be appreciated that many embodiments can be made and that many changes can be made to the embodiments without departing from the principles of the present disclosure. These and other changes in the embodiments 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.

We Claim:

1. A method for whitelisting one or more voice over wireless fidelity (VoWiFi) compatible user devices, the method comprising:
   - maintaining, at a first server [106] by a maintenance unit [101] in a storage unit [104], a list of one or more international mobile identifiers associated with the one or more voice over wireless fidelity (VoWiFi) compatible user devices;
   - receiving, at the first server [106] by a transceiver unit [102] from one or more user devices, a request related to allowing a connection of the one or more user devices with a VoWiFi enabled network;
   - generating, at the first server [106] by a generating unit [103], a decision regarding allowing the connection of the one or more user devices with the VoWiFi enabled network in response to the request based on the list; and
   - storing, at the first server [106] by a fetching unit [105] in the storage unit [104], an international mobile identifier of the one or more user devices in an event an allow decision is generated, for whitelisting the one or more user devices as the one or more VoWiFi compatible user devices.

2. The method as claimed in claim 1, wherein the first server [106] is a session management function (SMF) server.

3. The method as claimed in claim 1, wherein the generation of the decision is based on a comparison of the international mobile identifier of the one or more user devices from which the request is received with the list of the one or more international mobile identifiers associated with the one or more VoWiFi compatible devices,

   wherein the decision is one of an allow decision and a forbid decision, the allow decision being generated in an event the generating unit [103] at the first server [106] allows connection of the one or more user devices with the VoWiFi enabled network, and the forbid decision being generated in an event the generating unit [103] at the first server [106] forbids connection of the one or more user devices with the VoWiFi enabled network.

4. The method as claimed in claim 3, wherein for the generation of the decision regarding allowing the connection of the one or more user devices with the VoWiFi enabled network, the method comprises:

- searching, by the generating unit [103] at the first server [106], the international mobile identifier of the one or more user devices from which the request is received in the list of the one or more international mobile identifiers associated with the one or more VoWiFi incompatible devices; and
- generating, by the generating unit [103] at the first server [106], one of the allow decision and the forbid decision,

wherein the allow decision is generated in an event the international mobile identifier of the one or more user devices from which the request is received is found in the list of the one or more international mobile identifiers associated with the one or more VoWiFi compatible devices, and the forbid decision is generated in an event the international mobile identifier of the one or more user devices from which the request is received is not found in the list of the one or more international mobile identifiers associated with the one or more VoWiFi compatible devices.

5. A system [100] for whitelisting one or more voice over wireless fidelity (VoWiFi) compatible user devices, the system [100] comprising:
   - a maintenance unit [101], the maintenance unit [101] being configured to maintain, at a first server [106] in a storage unit [104], a list of one or more international mobile identifiers associated with the one or more voice over wireless fidelity (VoWiFi) compatible user devices;
   - a transceiver unit [102] connected with the maintenance unit [101], the transceiver unit [102] being configured to receive, at the first server [106] from one or more user devices, a request related to allowing a connection of the one or more user devices with a VoWiFi enabled network;
   - a generating unit [103] connected to the transceiver unit [102], the generating unit [103] being configured to generate, at the first server [106], a decision regarding allowing the connection of the one or more user devices with the VoWiFi enabled network in response to the request based on the list; and
   - a fetching unit [105] connected to the generating unit [103], the fetching unit [105] being configured to store, at the first server [106] in the storage unit [104], the international mobile identifier of the one or more user devices in an event an allow decision is generated, for whitelisting the one or more user devices as the one or more VoWiFi compatible user devices.

6. The system [100] as claimed in claim 5, wherein the first server [106] is a session management function (SMF) server.

7. The system [100] as claimed in claim 5, wherein the generation of the decision is based on a comparison of the international mobile identifier of the one or more user devices from which the request is received with the list of the one or more international mobile identifiers associated with the one or more VoWiFi compatible devices,

wherein the decision is one of an allow decision and a forbid decision, the allow decision being generated in an event the generating unit [103] at the first server [106] allows connection of the one or more user devices with the VoWiFi enabled network, and the forbid decision being generated in an event the generating unit [103] at the first server [106] forbids connection of the one or more user devices with the VoWiFi enabled network.

8. The system [100] as claimed in claim 7, wherein the generating unit [103] for generating the decision regarding allowing the connection of the one or more user devices with the VoWiFi enabled network, is configured to:

- search, at the first server [106], the international mobile identifier of the one or more user devices from which the request is received in the list of the one or more international mobile identifiers associated with the one or more VoWiFi incompatible devices, and
- generate one of the allow decision and the forbid decision,

wherein the allow decision is generated in an event the international mobile identifier of the one or more user devices from which the request is received is found in the list of the one or more international mobile identifiers associated with the one or more VoWiFi compatible devices, and the forbid decision is generated in an event the international mobile identifier of the one or more user devices from which the request is received is not found in the list of the one or more international mobile identifiers associated with the one or more VoWiFi compatible devices.

9. A user equipment for whitelisting one or more voice over wireless fidelity (VoWiFi) compatible user devices, the user equipment comprises:

a memory; and

a processor coupled to the memory, the processor is configured to:

- transmit, to a system [100], a request related to allowing a connection of the one or more user devices with a VoWiFi enabled network, and
- receive from the system [100], a response associated with the request,

wherein the response associated with the request is received based on:

maintaining, by the system [100], a list of one or more international mobile identifiers associated with the one or more voice over wireless fidelity (VoWiFi) compatible user devices,

generating, by the system [100], a decision regarding allowing the connection of the one or more user devices with the VoWiFi enabled network in response to the request based on the list, and

storing, by the system [100], an international mobile identifier of the one or more user devices in an event an allow decision is generated, for whitelisting the one or more user devices as the one or more VoWiFi compatible user devices.

10. A non-transitory computer readable storage medium storing instructions for whitelisting one or more voice over wireless fidelity (VoWiFi) compatible user devices, the instructions include executable code which, when executed by a one or more units of a system, causes:

- a maintenance unit [101] to maintain, at a first server [106] in a storage unit [104], a list of one or more international mobile identifiers associated with the one or more voice over wireless fidelity (VoWiFi) compatible user devices;
- a transceiver unit [102] to receive, at the first server [106] from one or more user devices, a request related to allowing a connection of the one or more user devices with a VoWiFi enabled network;
- a generating unit [103] to generate, at the first server [106], a decision regarding allowing the connection of the one or more user devices with the VoWiFi enabled network in response to the request based on the list; and
- a fetching unit [105] to store, at the first server [106] in the storage unit [104], the international mobile identifier of the one or more user devices in an event an allow decision is generated, for whitelisting the one or more user devices as the one or more VoWiFi compatible user devices.

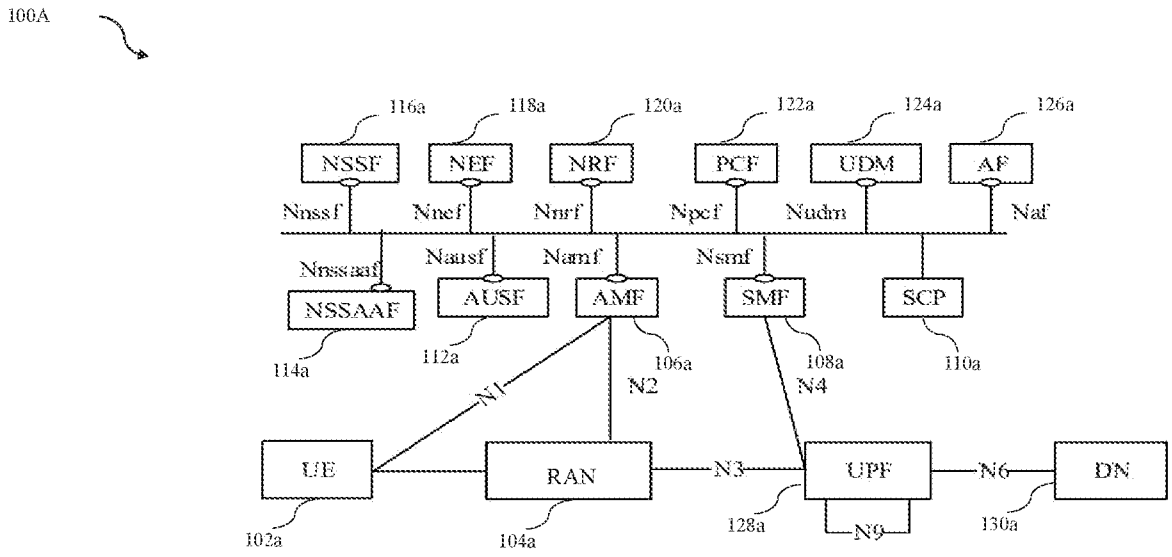
100A
116a
118a
120a
122a
124a
126a
NSSF
NEF
NRF
PCF
UDM
AF
Nnssf
Nnef
Nnrf
Npcf
Nudm
Naf
Nnssaaf
Nausf
Namf
Nsmf
NSSAAF
AUSF
AMF
SMF
SCP
114a
112a
106a
108a
110a
N1
N2
N4
UE
RAN
N3
UPF
N6
DN
102a
104a
128a
N9
130a

FIG. 1A

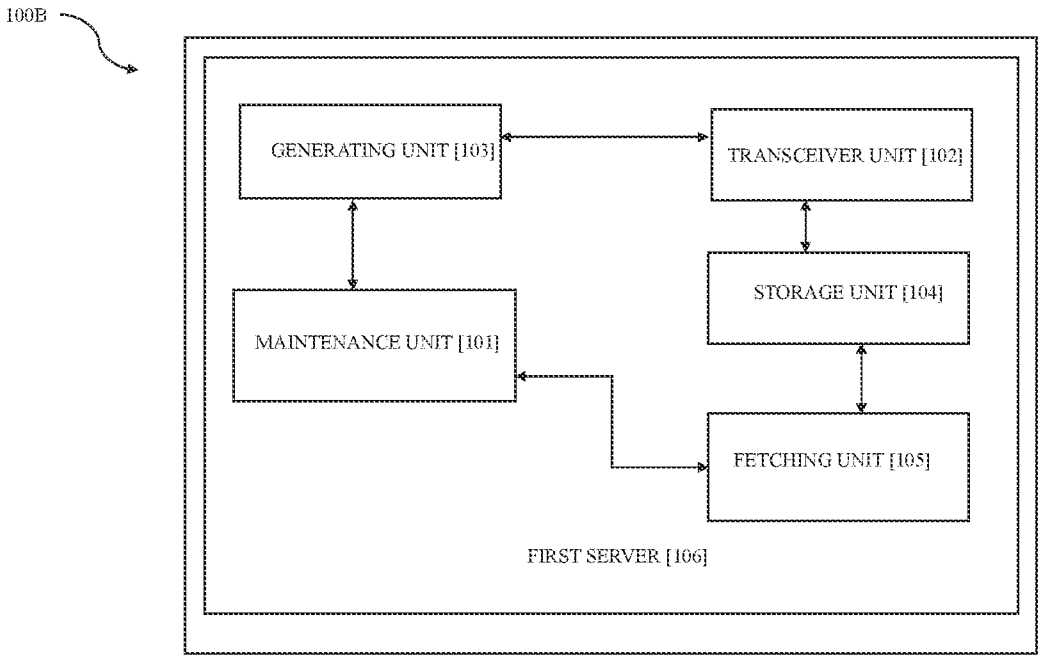
100B
GENERATING UNIT [103]
TRANSCEIVER UNIT [102]
STORAGE UNIT [104]
MAINTENANCE UNIT [101]
FETCHING UNIT [105]
FIRST SERVER [106]

FIG. 1B

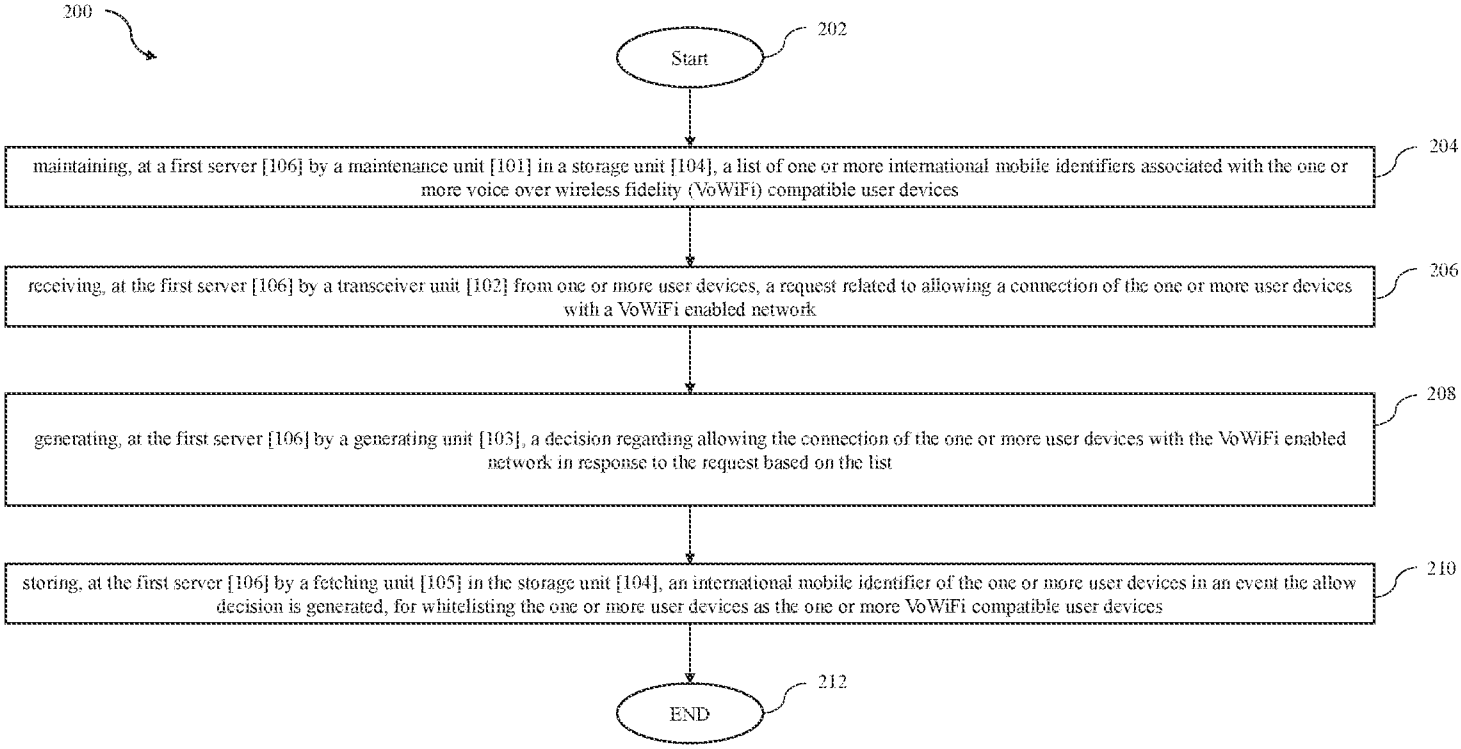
200
Start
202
maintaining, at a first server [106] by a maintenance unit [101] in a storage unit [104], a list of one or more international mobile identifiers associated with the one or more voice over wireless fidelity (VoWiFi) compatible user devices
204
receiving, at the first server [106] by a transceiver unit [102] from one or more user devices, a request related to allowing a connection of the one or more user devices with a VoWiFi enabled network
206
generating, at the first server [106] by a generating unit [103], a decision regarding allowing the connection of the one or more user devices with the VoWiFi enabled network in response to the request based on the list
208
storing, at the first server [106] by a fetching unit [105] in the storage unit [104], an international mobile identifier of the one or more user devices in an event the allow decision is generated, for whitelisting the one or more user devices as the one or more VoWiFi compatible user devices
210
END
212

FIG. 2

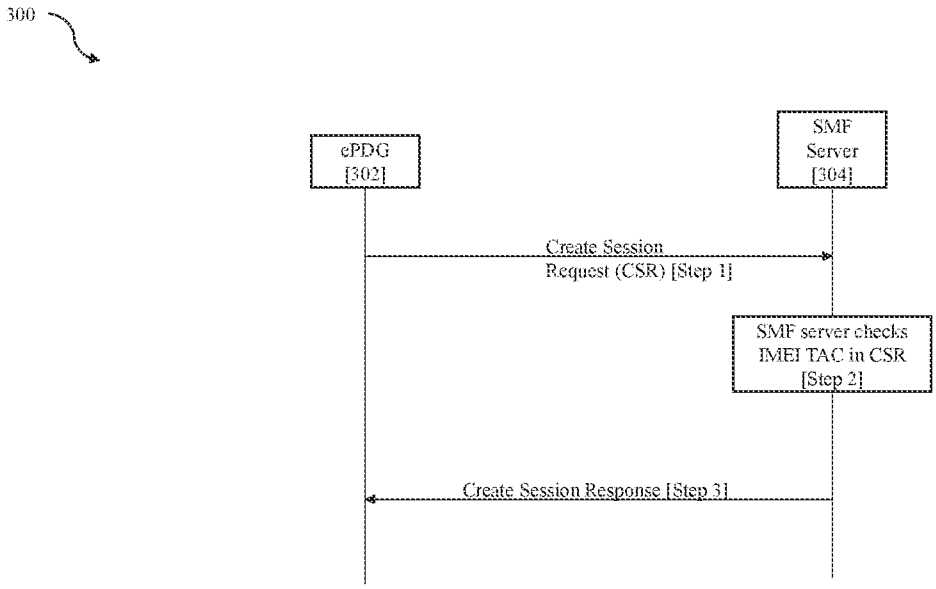
300
ePDG
[302]
SMF
Server
[304]
Create Session
Request (CSR) [Step 1]
SMF server checks
IMEI TAC in CSR
[Step 2]
Create Session Response [Step 3]

FIG. 3

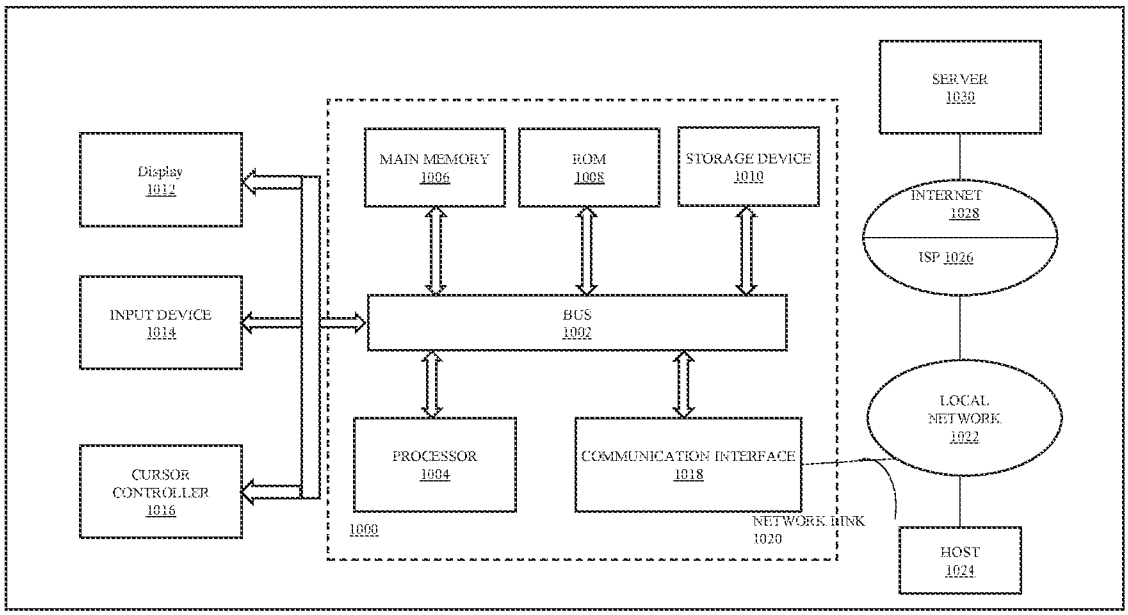
SERVER
1030
Display
1012
MAIN MEMORY
1006
ROM
1008
STORAGE DEVICE
1010
INTERNET
1028
ISP 1026
INPUT DEVICE
1014
BUS
1002
LOCAL
NETWORK
1022
CURSOR
CONTROLLER
1016
PROCESSOR
1004
COMMUNICATION INTERFACE
1018
1000
NETWORK LINK
1020
HOST
1024

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IN2024/050746

A. CLASSIFICATION OF SUBJECT MATTER
H04W76/20,H04W48/08,H04W12/069,H04W24/04 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

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, Keywords (Synonyms):VoWiFi,whitelisting,IMEI,allowing,connection,decision,SMF

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN115996368A (UNIHUB CHINA INFORMATION TECHNOLOGY CO LTD) 21 APRIL 2023 (21-04-2023) (English Translation Copy from Google Patents) Abstract, Description	1-10
Y	CN107529160A (ZTE Corp) 29 DECEMBER 2017 (29-12-2017) (English Translation Copy from Google Patents) Abstract, Description	1-10
Y	CN109862552A (XIAN HUAWEI TECHNOLOGIES CO LTD) 07 JUNE 2019 (07-06-2019) (English Translation Copy from Google Patents) Abstract, Description	1-10
Y	CN110149677A (SHENZHEN FURI ZHONGNUO ELECTRONIC TECHNOLOGY CO.,LTD.) 20 AUGUST 2019 (20-08-2019) (English Translation Copy from Google Patents) Abstract, Description	1-10

☐ 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
26-09-2024	26-09-2024

Name and mailing address of the ISA/	Authorized officer
Indian Patent Office Plot No.32, Sector 14,Dwarka,New Delhi-110075 Facsimile No.	Subhadip Das Telephone No. +91-1125300200

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IN2024/050746

Citation	Pub.Date	Family	Pub.Date
CN 107529160 A	29-12-2017	WO 2017219673 A1	28-12-2017