(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 889 971 A1

(12) EUROPEAN PATENT APPLICATION
published in accordance with Art. 153(4) EPC

(43) Date of publication:
06.10.2021 Bulletin 2021/40

(21) Application number: **20741895.5**

(22) Date of filing: **06.01.2020**

(51) Int Cl.:
G16H 80/00 *(2018.01)*

(86) International application number:
PCT/CN2020/070486

(87) International publication number:
WO 2020/147605 (23.07.2020 Gazette 2020/30)

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
KH MA MD TN

(30) Priority: **15.01.2019 CN 201910036464**

(71) Applicant: **AUTEL INTELLIGENT TECHNOLOGY CORP., LTD.**
Shenzhen, Guangdong 518055 (CN)

(72) Inventor: **PANG, Shengsheng**
Shenzhen, Guangdong 518055 (CN)

(74) Representative: **Gulde & Partner**
Patent- und Rechtsanwaltskanzlei mbB
Wallstraße 58/59
10179 Berlin (DE)

(54) ONLINE DIAGNOSIS PLATFORM, PERMISSION MANAGEMENT METHOD AND PERMISSION MANAGEMENT SYSTEM FOR ONLINE DIAGNOSIS PLATFORM

(57) The present invention relates to an online diagnostic platform, and a permission management method and a permission management system thereof. The permission management method includes: when user information of a registered user is received, assigning a role in a role set to the registered user; determining a permission corresponding to the role; and generating a menu corresponding to the registered user, where the menu includes one or more function portals, the function portal being used for requesting execution of a diagnostic service function. The method uses security control policies such as the registered user, the role and the permission, and is flexible in management and relationship configuration. In addition, the permission management system is separated from a service system, has good expansibility, and can ensure stable running and data security of the system.

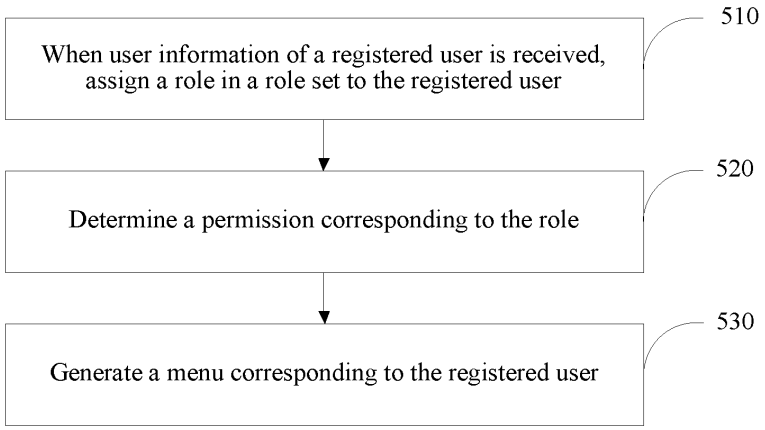

FIG. 5

EP 3 889 971 A1

Description

BACKGROUND

[0001] This application claims priority to Chinese Patent Application No. 201910036464.0, entitled "ONLINE DIAGNOSTIC PLATFORM, AND PERMISSION MANAGEMENT METHOD AND PERMISSION MANAGEMENT SYSTEM THEREOF" filed with the China National Intellectual Property Administration on January 15, 2019, which is incorporated by reference in its entirety.

Technical Field

[0002] This application relates to the field of cloud network technologies, and in particular, to an online diagnostic platform, and a permission management method and a permission management system thereof.

Related Art

[0003] With the continuous development of the Internet and the continuous progress of wireless communications technologies, cloud technologies begin to be widely applied to many different industries. An automobile diagnosis industry gradually moves from offline diagnosis to online diagnosis.

[0004] Such an online diagnostic platform or online diagnostic platform has good flexibility and it is convenient to implement centralized management and statistics of data. Each user may also conveniently execute, through the online diagnostic platform, service functions required by the user.

[0005] The online diagnostic platform or system constructed by using Internet technologies brings convenience, but also leads to data security and privacy problems. Therefore, to ensure the security of the entire online diagnostic platform, a perfect permission management system is necessary.

[0006] However, with the continuous expansion of a quantity of users and the continuous iterative update of the system, a security control policy of the existing permission management system has problems that permission management is not flexible enough, the management is complex, the subsequent function expansion of the system is not facilitated and the like. Consequently, it is easy to generate potential safety hazards such as attacks from uniform resource locator (URL) intrusion, structured query language (SQL) injection and the like.

SUMMARY

[0007] Embodiments of the present invention aim to provide an online diagnostic platform, and a permission management method and a permission management system thereof that can resolve the problems of complex permission management and poor flexibility.

[0008] To resolve the foregoing technical problems, the embodiments of the present invention further provide the following technical solution:

a permission management method. The permission management method includes: when user information of a registered user is received, assigning a role in a role set to the registered user; determining a permission corresponding to the role; and generating a menu corresponding to the registered user, where the menu includes one or more function portals, the function portal being used for requesting execution of a diagnostic service function.

[0009] In some embodiments, the step of generating a menu corresponding to the registered user includes:

determining a user attribute of the registered user, where the user attribute includes a front-end user and a back-end user;

generating a corresponding first menu when the user attribute is the front-end user; and generating a corresponding second menu when the user attribute is the back-end user.

[0010] In some embodiments, the first menu is a fixed menu and the second menu is a dynamic menu that changes with the permission of the registered user.

[0011] In some embodiments, the step of generating a corresponding second menu when the user attribute is the back-end user specifically includes:

obtaining the permission of the registered user; determining a function portal corresponding to each permission; and integrating all function portals corresponding to the permission of the registered user to form the second menu.

[0012] In some embodiments, the back-end user includes a system administrator and an operator.

[0013] The step of assigning one or more roles in the role set to the registered user to enable the registered user to have the corresponding permission specifically includes:

assigning a role to the registered user when the user attribute of the registered user is the front-end user or the system administrator; and

assigning one or more roles to the registered user when the user attribute of the registered user is the operator.

[0014] In some embodiments, the permission is a set including one or more interfaces, so that a function of an online diagnostic platform corresponding to the interface is allowed to be used.

[0015] In some embodiments, the method further includes:

determining, through the menu, a function requested to be executed by the registered user; and

verifying whether the registered user has a permission corresponding to the function requested to be executed;

allowing to execute the function if yes; and

refusing to execute the function if no.

[0016] To resolve the foregoing technical problems, the embodiments of the present invention further provide the following technical solution a permission management system.

[0017] The permission management system includes: a user management module, configured to, when user information of a registered user is received, assign a role in a role set to the registered user; a permission management module, configured to determine a permission corresponding to the role; and a menu module, configured to generate a menu corresponding to the registered user, where the menu includes one or more function portals, the function portal being used for requesting execution of a diagnostic service function.

[0018] In some embodiments, the menu module specifically includes: an attribute determination unit, a first menu generation unit and a second menu generation unit, where

the attribute determination unit is configured to determine a user attribute of the registered user, and the user attribute includes a front-end user and a back-end user;

the first menu generation unit is configured to generate a corresponding first menu when the user attribute is the front-end user; and

the second menu generation unit is configured to generate a corresponding second menu when the user attribute is the back-end user.

[0019] In some embodiments, the first menu is a fixed menu and the second menu is a dynamic menu that changes with the permission of the registered user.

[0020] In some embodiments, the second menu generation unit is specifically configured to: obtain the permission of the registered user; determine a function portal corresponding to each permission; and integrate all function portals corresponding to the permission of the registered user to form the second menu.

[0021] In some embodiments, the back-end user includes a system administrator and an operator. The user management module is specifically configured to: assign a role to the registered user when the user attribute of the registered user is the front-end user or the system administrator; and assign one or more roles to the registered user when the user attribute of the registered user is the operator.

[0022] In some embodiments, a server further includes a permission module. The permission module is configured to add, delete or edit any permission, and each permission includes a set of one or more interfaces, so that a function of an online diagnostic platform corresponding to the interface is allowed to be used.

[0023] In some embodiments, the server further includes an execution control module. The execution control module is configured to: determine, through the menu, a function requested to be executed by the registered user; and determine, according to the permission of the registered user, whether to execute the function requested to be executed.

[0024] To resolve the foregoing technical problems, the embodiments of the present invention further provide the following technical solution: an online diagnostic platform.

[0025] The online diagnostic platform includes: a client, configured to receive user information of a registered user and send the user information to a permission management system, where the client is further configured to display a menu generated by the permission management system according to the user information; the permission management system, configured to execute the permission management method described above to manage one or more registered users; and a service system, configured to execute a diagnostic service function according to a request of the client.

[0026] Compared with the prior art, the permission management method provided in the embodiments of the present invention uses security control policies such as the registered user, the role and the permission, and is flexible in management and relationship configuration. In addition, the permission management system is separated from a service system, has good expansibility, and can ensure stable running and data security of the system.

BRIEF DESCRIPTION OF THE DRAWINGS

[0027] One or more embodiments are described by way of example with reference to the corresponding figures in the accompanying drawings, and the descriptions are not to be construed as limiting the embodiments. Elements in the accompanying drawings that have same reference numerals are represented as similar elements, and unless otherwise particularly stated, the figures in the accompanying drawings are not drawn to scale.

FIG. 1 is a schematic diagram of an application scenario of an online diagnostic platform according to an embodiment of the present invention;

FIG. 2 is a schematic diagram of a permission management system according to an embodiment of the present invention;

FIG. 3 is a schematic diagram of a permission management system according to another embodiment

of the present invention;

FIG. 4 is a schematic diagram of a hierarchical relationship among a registered user, a role and a permission according to an embodiment of the present invention;

FIG. 5 is a method flowchart of a permission management method according to an embodiment of the present invention;

FIG. 6 is a method flowchart of a permission management method according to another embodiment of the present invention;

FIG. 7 is a schematic diagram of a use example of a front-end user shown in FIG. 1;

FIG. 8 is a schematic diagram of a use example of a back-end user shown in FIG. 1; and

FIG. 9 is a schematic structural diagram of an online diagnostic platform according to an embodiment of the present invention.

DETAILED DESCRIPTION

[0028] For ease of understanding the present invention, the present invention is described below in more detail with reference to the accompanying drawings and specific embodiments. It should be noted that when an element is referred to as being "fixed to" another element, it may be directly on the another element or there may be one or more middle elements between the elements. When an element is referred to as being "connected to" another element, it may be directly connected to the another element or there may be one or more middle elements between the elements. A direction or location relationship indicated by a term "on", "under", "inner", "outer", "bottom" or the like used in this specification is a direction or location relationship shown based on the accompanying drawings, and is intended to only conveniently describe the present invention and simplify the description, but is not intended to indicate or imply that a mentioned apparatus or element needs to have a particular direction and is constructed and operated in the particular direction. Therefore, the direction or location relationship cannot be understood as a limitation on the present invention. In addition, terms such as "first", "second" and "third" are only used for description and cannot be understood as indicating or implying relative importance.

[0029] Unless otherwise defined, meanings of all technical and scientific terms used in this specification are the same as those usually understood by a person skilled in the technical field to which the present invention belongs. In this specification, terms used in the specification of the present invention are merely intended to describe the specific embodiments, but are not intended to limit the present invention. A term "and/or" used in this specification includes any combination or all combinations of one or more related listed items.

[0030] In addition, technical features involved in different embodiments of the present invention described below may be combined with each other provided that there is no conflict with each other.

[0031] An online diagnostic platform is an electronic platform that is established in a cloud by using Internet technologies and provides corresponding information service functions for various automobile maintenance sites or automobile diagnosis maintenance operators. Based on the online diagnostic platform, the online diagnostic platform may serve as an information interaction medium in the cloud, and is connected to many nodes that are geographically located at different positions, to establish a complete maintenance diagnosis network. FIG. 1 is an example of an application scenario of a maintenance diagnosis network according to an embodiment of the present invention.

[0032] As shown in FIG. 1, the entire application scenario includes: a front-end service site 10, a back-end operation site 20, an online diagnostic platform 30, and a communication network 40.

[0033] The front-end service site 10 refers to a node that is located at the forefront of equipment maintenance and that provides a real maintenance, diagnosis and repair service, for example, a maintenance shop or a maintenance technician in a maintenance shop. The front-end service site, as a final executor and implementer of the entire maintenance diagnosis network, may be disposed at any geographic position or may be in any form or size.

[0034] The back-end operation site 20 is a node that is used for coordinating a plurality of front-end service sites 10, and implementing management of these front-end service sites 10, for example, a personnel department responsible for personnel management of a maintenance technician or a warehousing department responsible for deploying inventory accessories of a maintenance shop. Relative to the front-end service site, the back-end operation site is in back-end operation and management control, and is another type of node in the entire maintenance diagnosis network.

[0035] The online diagnostic platform 30 is an electronic computing platform constructed on the basis of a server and a database, can execute corresponding functions such as searching maintenance cases, counting maintenance accidents or annual performance or the like in response to requests sent by various nodes, and is a function and control core of the entire maintenance diagnosis network.

[0036] The communication network 40 may be any type of wireless, wired, or combined data transmission network such as a cellular communication network, a Wi-Fi network, or a private local area network. The communication network 40 is used for establishing a communication link between each node (that is, the front-end serv-

ice site 10 or the back-end operation site 20) and the online diagnostic platform 30 to implement data interaction such as instruction upload and data delivery between the node and the online diagnostic platform.

[0037] In the actual use process, the online diagnostic platform 30 usually uses a security control policy for user identity authentication to ensure stable running of the entire maintenance diagnosis network. That is, each of different nodes in the maintenance diagnosis network uses a unique registered user as label or identity information of the node. The node is permitted to use a corresponding function only after steps of identity and permission authentication.

[0038] To implement creation and login of the registered user, as shown in FIG. 1, the online diagnostic platform 30 may be provided with a user management system 31 and a login authentication system 32. The user management system 31 creates a new registered user based on a registration behavior of the user. The login authentication system 32 completes the login of the registered user in any type of authentication manner such as an account password or fingerprint recognition.

[0039] For example, a maintenance shop may register on the online diagnostic platform and obtain an account number of a registered user and a password through the user management system 31. Then, the account number and the password are used to log in to the online diagnostic platform to request the use of one or more functions of the online diagnostic platform. Finally, the online diagnostic platform determines, according to the permission of the registered user, whether to respond to the request of the registered user and execute the corresponding function.

[0040] Considering that the online diagnostic platform 30 generally requires a plurality of times of iterative version update during use, the functions that the online diagnostic platform 3 0 can perform are actually in a dynamically changing process. To maintain the expandability of the online diagnostic platform 30 and facilitate completion of functions of the functions, as shown in FIG. 9, main components of the online diagnostic platform 30 may include a service system 33, a permission management system 34 and a client 35.

[0041] The service system 33 represents a set of all functions and services that the online diagnostic platform can perform. That is, all service functions and services of the online diagnostic platform are integrated on the service system.

[0042] The permission management system 34 is used for managing and verifying the permission of the registered user to determine whether authority is obtained. The service system 33 responds to the request to perform the corresponding service function only after obtaining the authority of the permission management system 34.

[0043] The client 35 is a part that interacts with the user. The client may be executed on any type of terminal device, and is configured to receive user information of the registered user and send the user information to the permission management system. In addition, the client displays a menu generated by the permission management system according to the user information.

[0044] The online diagnostic platform 30 may further include a database 36 for storing data or instruction information.

[0045] The database 36 may be any type of data storage device that can store a program instruction and the data and support searching for the stored data in any storage policy. In some embodiments, the database 36 may be further a distributed storage system.

[0046] In this embodiment, the service system 33 and the permission management system 34 may be implemented by using a same hardware device or different hardware devices, or may be implemented by using two mutually independent function modules formed by dividing a same hardware device. The client 35 may be a mobile application or a web page node (that is, log in by inputting a website through a web engine) running on any system (for example, Windows, Android or iOS system).

[0047] The online diagnostic platform shown in FIG. 1 and FIG. 9 decouples the service system from the permission management system, so that the service system and the permission management system are independent of each other and do not affect each other. The permission management system 34 prevents "an illegal user" from accessing the system, and restricts the user to access of only an authorized function, thereby ensuring that the online diagnostic platform runs stably and safely without affecting the expansion or update of service functions on the service system 33.

[0048] As the quantity and complexity of the functions of the online diagnostic platform 30 increase, the permission management system 34 of the online diagnostic platform can implement better and more flexible permission management by using the permission management system provided in this embodiment of the present invention, to obtain convenience in use. FIG. 2 is a functional block diagram of a permission management system according to an embodiment of the present invention.

[0049] As shown in FIG. 2, the permission management system includes: a user management module 210, a permission management module 220 and a menu module 230.

[0050] There may be a pre-created role set in the permission management system. Based on a role in the role set, the permission management module 220 is configured to assign one or more permissions to the role.

[0051] The "role" is a logical concept used for marking a permission set including one or more permissions. The role is constructed as one of levels in the permission management to simplify the operation of permission assignment. For example, the "role" may be a technician or a maintenance shop. The permissions of the technician include access to cases, questioning cases, and sharing (making) cases, and the permissions of the maintenance shop include managing a technician and managing

equipment information.

[0052] All created roles as elements in the set form the role set. Certainly, the role set may be edited or modified. According to requirements of an actual condition, in some embodiments, editing operations such as deleting and merging may be further performed on existing roles in the role set.

[0053] The user management module 210 is configured to assign one or more roles in the role set to the registered user. After a role is assigned to the registered user, the registered user has the permission of the role.

[0054] The "registered user" refers to unique identity information that the online diagnostic platform uses to identify or distinguish different nodes. The registered user may be specifically in any appropriate form. For example, the registered user may include an account name and a password, a biometric feature (for example, a fingerprint) or a fixed identification code (for example, a network IP address), or the like provided that a node can be uniquely defined.

[0055] The permission refers to authority that may perform some functions. The permission as a safety judgment standard or rule distinguishes actual conditions of different registered users, and prohibits harmful operations to ensure the safe running of the online diagnostic platform.

[0056] Preferably, each permission is a set including one or more interfaces through which a function or a service corresponding to the service system is allowed to be invoked. In this way, a mode of refining permission control to an interface hierarchy can basically meet various permission requirements of different users in the actual use process.

[0057] The menu module 230 is configured to generate a menu corresponding to the registered user. The "menu" is a combination of one or more function portals. The menu may be displayed on a display screen of a terminal device in any type of form (for example, a list bar), for a user to request the online diagnostic platform to perform the corresponding function.

[0058] That is, each function portal corresponds to a function. When the user selects or taps a function portal, the online diagnostic platform receives a request of performing the function.

[0059] Based on the permission definition mode refined to the interface hierarchy, as shown in FIG 3, compared with the permission management system shown in FIG. 2, the permission management system may further include a permission editing module 240.

[0060] The permission editing module 240 is configured to provide editing functions for an interface set, for example, adding, deleting, or editing any permission, for example, adjusting an interface of a permission.

[0061] In the permission management system provided in this embodiment, the permission management of the registered user is implemented by assigning the role to the existing registered user and assigning the permission of the role, and a two-level mapping relationship of the registered user-role-permission shown in FIG. 4 may be formed.

[0062] The two-level mapping relationship may help simplify the workload of the permission management and improve flexibility of management. For example, when a function is newly added to the online diagnostic platform, a permission of the new function can be simply given to a role through the permission management module 220, so that permission editing of the newly added function can be completed without traversing all registered users.

[0063] Still referring to FIG. 1, in an application scenario, each node may be any type of terminal device. The terminal device such as a personal computer, a smartphone, an automobile diagnostic device or a tablet computer includes at least a communication module and an input/output device through which a user joins the communication network 40 and is configured to implement interaction with the user. However, the online diagnostic platform 20 needs to present a corresponding interactive interface to the user on the terminal devices, so that the user can send a request instruction and specify a permission of the user.

[0064] Different nodes may belong to different categories. To implement personalized and refined interaction, in some embodiments, as shown in FIG. 3, the menu module 230 specifically includes: an attribute determination unit 231, a first menu generation unit 232 and a second menu generation unit 233.

[0065] The attribute determination unit 231 is configured to determine a user attribute of the registered user. The user attribute refers to a type of a node corresponding to the registered user, and may be determined by relevant information submitted during registration and the like.

[0066] According to the application scenario shown in FIG. 1, the user attribute may include both a front-end user and a back-end user. The front-end user indicates that the registered user belongs to the front-end service site 10. The back-end user indicates that the registered user belongs to the back-end operation site 20.

[0067] Based on a classification result of the attribute determination unit 231, different menus are generated for registered users of different user attributes by using the first menu generation unit 232 and the second menu generation unit 233 separately.

[0068] The first menu generation unit 232 is configured to generate a corresponding first menu when the user attribute is the front-end user. The second menu generation unit 233 is configured to generate a corresponding second menu when the user attribute is the back-end user.

[0069] Specifically, the first menu may be a fixed menu. The fixed menu means that the function portal constituting the menu is basically unchanged, and is determined by the function or the service that the service system can provide. In this way, all function portals may be seen on the terminal device. If the registered user taps the function portal without the corresponding permission, the reg-

istered user is prompted that the permission has not been obtained.

[0070] The second menu is a dynamic menu that changes with the permission of the registered user. The dynamic menu means that the menu changes with different registered users and only some function portals are displayed on the terminal device.

[0071] To generate the dynamic menu, the second menu generation unit needs to obtain the permission of the registered user, then determine a function portal corresponding to each permission and integrate all function portals corresponding to the permission of the registered user to form a dynamic menu adaptive to the permission of the registered user.

[0072] In some other embodiments, the back-end user may be further subdivided into a system administrator and an operator.

[0073] The system administrator is a registered user who maintains the entire online diagnostic platform and operates the permission management system, and has the highest permission relative to other registered users. The operator refers to an operating manager who has a local permission and is located at the backend relative to the front-end user.

[0074] It can be understood that permissions of the front-end user and the system administrator have been determined when the entire online diagnostic platform is launched. A permission of the operator is constantly changing during use and running.

[0075] Therefore, for different registered users, the user management module 210 may be specifically configured to assign a role to the registered user when the user attribute of the registered user is the front-end user or the system administrator; and, assign one or more roles to the registered user according to the change of an actual condition when the user attribute of the registered user is the operator.

[0076] In this way, an association relationship shown in FIG. 4 may be formed: there is a one-to-one correspondence between the front-end user or the system administrator and the role. The operator may have corresponding permissions by assigning a plurality of different roles to the operator.

[0077] Still referring to FIG. 3, to prevent illegal access and restrict the registered user to access of only the authorized function, the permission management system may further include at least an execution control module 250.

[0078] The execution control module 250 is a verification module, and is configured to determine, through the menu, a function requested to be executed by the registered user; and then determine, according to the permission of the registered user, whether to execute the function requested to be executed.

[0079] That is, when the registered user has the permission, the execution control module determines to respond to the request and executes the corresponding function. When the registered user does not have the permission, the execution control module refuses to respond. Certainly, after refusing to respond, the execution control module may further display prompt information to inform the registered user that the registered user does not have the permission or inform the registered user of a possible manner of obtaining the permission.

[0080] Data, such as the role set, the permission of each role, and the storage device of the role assigned to the registered user, generated in the operation process of the foregoing function modules (such as the user management module 210, the permission management module 220 and the menu module 230) may all be stored in the database 260. Specifically, any type of database having a data retrieval function may be used.

[0081] A person skilled in the art may be further aware that, the function modules (such as the user management module 210, the permission management module 220 and the menu module 230) described in this embodiment of the present invention may be implemented by electronic hardware, computer software, or a combination thereof. To clearly describe the interchangeability between the hardware and the software, steps executed by the exemplary function modules have generally been described based on functions in the above description. Whether the functions are executed in a mode of hardware or software depends on particular applications and design constraint conditions of the technical solutions.

[0082] The described functions for each particular application may be implemented by using different methods, but it should not be considered that such implementation goes beyond the scope of the present invention. The computer software may be stored in a computer readable storage medium. When being executed, the program may include the processes of the embodiments of the foregoing methods. The storage medium may be a magnetic disk, an optical disc, a read-only memory, a random access memory, or the like.

[0083] Based on the permission management system disclosed in the foregoing embodiments, an embodiment of the present invention further provides a permission management method. The permission management method can be applied to any type of online platform or system, thereby providing the convenience and flexibility in permission management. FIG. 5 is a method flowchart of a permission management method according to an embodiment of the present invention. As shown in FIG. 5, the permission management method includes the following steps.

[0084] 510. When user information of a registered user is received, assign a role in a role set to the registered user.

[0085] The step of assigning the role may be performed when the registered user is newly created, or may be performed in the use process of the registered user. The "assign" may include: giving the role to the registered user and reducing the role owned by the registered user.

[0086] 520. Determine a permission corresponding to the role.

[0087] The permission of the role may be configured by the system administrator through the online diagnostic platform according to an actual condition. The role set is a set of roles as elements. In some embodiments, in addition to creating a new role, editing operations such as deleting may be further performed on existing roles in the role set.

[0088] Specifically, to adequately meet various permission requirements of the online diagnostic platform, the permission may be a set including one or more interfaces to refine the permission to an interface hierarchy. These interfaces are functional interfaces of the service system, and may be allowed to be used by using the corresponding functions.

[0089] 530. Generate a menu corresponding to the registered user. The menu includes one or more function portals.

[0090] The function portal is used for requesting execution of a diagnostic service function.

[0091] The menu refers to a set of the one or more function portals and is displayed on the terminal device through any type of interactive interface. The user may request to execute corresponding functions of the online diagnostic platform through the function portals. Generating different menus for different registered users helps meet personalized needs of different registered users.

[0092] The permission management method provides a two-layer association mode of "registered user-role-permission" to complete permission assignment and control of the online diagnostic platform, and can provide good flexibility and facilitate adaptation to function update of a service system.

[0093] In the process of permission management, how to present the permission of the user to the user in a targeted manner is also a problem worth thinking about. FIG. 6 is a method flowchart of a permission management method according to another embodiment of the present invention. As shown in FIG. 6, the method includes the following steps.

[0094] 610. When user information of a registered user is received, assign a role in a role set to the registered user.

[0095] 620. Determine a permission corresponding to the role.

[0096] 630. Generate a menu corresponding to the registered user.

[0097] Specifically, according to identities of users and use requirements, these users may be roughly classified into several different types such as a front-end user and a back-end user. Based on two different user attributes of the front-end user and the back-end user, step 630 may specifically include:

first, determining a user attribute of the registered user; and then, according to different user attributes, generating a corresponding first menu when the user attribute is the front-end user and generating a corresponding second menu when the user attribute is the back-end user.

[0098] The first menu may be a fixed menu whose function portal is unchanged. The second menu is a dynamic menu that changes with the permission of the registered user, and changes correspondingly according to different registered users.

[0099] In some embodiments, the step of generating the second menu may include the following steps: first, obtaining the permission of the registered user; then, determining a function portal corresponding to each permission; and finally, integrating all function portals corresponding to the permission of the registered user to form the second menu.

[0100] Further, the back-end user may be further subdivided into two roles of an operator and a system administrator. Based on the feature of the classification, an association relationship between the registered user and the role may be different.

[0101] A role is assigned to the registered user when the user attribute of the registered user is the front-end user or the system administrator. One or more roles are assigned to the registered user when the user attribute of the registered user is the operator.

[0102] In some other embodiments, the permission management method may further include a permission verification process for the registered user to ensure that illegal access or operations are not performed and restrict the registered user to execution of the operations only within a permission range. Still referring to FIG. 6, the verification process may include the following steps.

[0103] 640. Determine, through the menu, a function requested to be executed by the registered user.

[0104] As described above, a plurality of different function portals are integrated on the menu. Therefore, the online diagnostic platform may determine, according to the function portal tapped or selected by the user, the function requested to be executed.

[0105] 650. Verify whether the registered user has a permission corresponding to the function requested to be executed. If yes, perform step 660; and if no, perform step 670.

[0106] The verification may be specifically completed in any manner. For example, whether the registered user has such a permission is determined in a matching or searching manner.

[0107] 660. Allow to execute the function.

[0108] When the registered user has the permission, the online diagnostic platform may provide a manner such as authority authentication or the interface, so that the online diagnostic platform may perform the function, for example, accessing a piece of data.

[0109] 670. Refuse to execute the function.

[0110] When the registered user does not have the permission, the system refuses to execute the function, so as to ensure the safety of the running of the system. Certainly, the system may further publish appropriate prompt information to help the user after refusing to execute the function.

[0111] The permission management method provided in this embodiment of the present invention can prevent

the illegal access or an illegal request, perform permission management on registration, restrict the registered user to access of the function only within the permission range and ensure stable running and safety of the system. In addition, the method may dynamically adjust the association relationship between different levels and has a feature of flexible configuration. The permission control is also refined to the interface hierarchy of the service system, to meet various permission requirements of users to a great extent.

[0112] FIG. 7 and FIG. 8 are specific examples of the operation processes of the front-end user and the back-end user respectively on the online diagnostic platform shown in FIG. 1.

[0113] As shown in FIG. 7, the front-end user may create a registered user through a user management system (S71). After the registered user is successfully created, the permission management system configures a corresponding permission for the registered user by assigning a role (S72).

[0114] After the front-end user passes a login authentication system of the online diagnostic platform (S73) and is successfully verified by an account password, the permission management system executes a corresponding initialization process and loads a permission of a currently logged-in registered user (S74) to complete a login operation of the registered user (S75).

[0115] A function execution request initiated by the front-end user is determined through a function portal integrated on a fixed menu (S76). The permission management system intercepts the request and verifies whether there is a permission (S77). If there is the permission, the request is provided to a service system (S78) and an execution result of the request is returned (S79).

[0116] As shown in FIG. 8, the back-end user includes two types: a system administrator and an operator. The system administrator may create a new registered user for the operator in the user management system (S81), and operate the permission management system to configure a permission for the registered user (S82).

[0117] Then, the operator can request login of the registered user through the login authentication system (S83). After an account password is successfully verified, the permission management system executes a corresponding initialization process and loads a permission of a currently logged-in registered user (S84) to complete the login of the registered user (S85).

[0118] Similar to the process shown in FIG. 8, the operator initiates a function execution request through the function portal integrated on the dynamic menu (S86). The permission management system intercepts the request and verifies whether there is a permission (S87). If there is the permission, the request is provided to a service system (S88) and an execution result of the request is returned (S89).

[0119] Finally, it should be noted that the foregoing embodiments are merely intended for describing the technical solutions of the present invention, but not for limiting the present invention. Under the idea of the present invention, the foregoing embodiments or technical features in different embodiments may also be combined, the steps may be implemented in any order, and there are many other variations of different aspects of the present invention as described above, which are not provided in detail for brevity. Although the present invention is described in detail with reference to the foregoing embodiments, persons of ordinary skill in the art should understand that they may still make modifications to the technical solutions described in the foregoing embodiments or make equivalent replacements to some technical features thereof, without departing from the scope of the technical solutions of the embodiments of the present invention.

Claims

1. A permission management method, comprising:

   when user information of a registered user is received, assigning a role in a role set to the registered user;
   determining a permission corresponding to the role; and
   generating a menu corresponding to the registered user, wherein the menu comprises one or more function portals, the function portal being used for requesting execution of a diagnostic service function.

2. The permission management method according to claim 1, wherein the step of generating a menu corresponding to the registered user comprises:

   determining a user attribute of the registered user, wherein the user attribute comprises a front-end user and a back-end user;
   generating a corresponding first menu when the user attribute is the front-end user; and
   generating a corresponding second menu when the user attribute is the back-end user.

3. The permission management method according to claim 2, wherein the first menu is a fixed menu and the second menu is a dynamic menu that changes with the permission of the registered user.

4. The permission management method according to claim 2 or 3, wherein the step of generating a corresponding second menu when the user attribute is the back-end user specifically comprises:

   obtaining the permission of the registered user;
   determining a function portal corresponding to each permission; and
   integrating all function portals corresponding to

the permission of the registered user to form the second menu.

5. The permission management method according to any of claims 2 to 4, wherein the backend user comprises a system administrator and an operator, and the step of assigning one or more roles in the role set to the registered user to enable the registered user to have the corresponding permission specifically comprises:

assigning a role to the registered user when the user attribute of the registered user is the front-end user or the system administrator; and
assigning one or more roles to the registered user when the user attribute of the registered user is the operator.

6. The permission management method according to any of claims 1 to 5, wherein the permission is a set comprising one or more interfaces, so that a function of an online diagnostic platform corresponding to the interface is allowed to be used.

7. The permission management method according to any of claims 2 to 5, further comprising:

determining, through the menu, a function requested to be executed by the registered user; and
verifying whether the registered user has a permission corresponding to the function requested to be executed;
allowing to execute the function if yes; and
refusing to execute the function if no.

8. A permission management system, comprising:

a user management module, configured to, when user information of a registered user is received, assign a role in a role set to the registered user;
a permission management module, configured to determine a permission corresponding to the role; and
a menu module, configured to generate a menu corresponding to the registered user, wherein the menu comprises one or more function portals, the function portal being used for requesting execution of a diagnostic service function.

9. The permission management system according to claim 8, wherein the menu module specifically comprises: an attribute determination unit, a first menu generation unit and a second menu generation unit, wherein

the attribute determination unit is configured to determine a user attribute of the registered user, and the user attribute comprises a front-end user and a back-end user;
the first menu generation unit is configured to generate a corresponding first menu when the user attribute is the front-end user; and
the second menu generation unit is configured to generate a corresponding second menu when the user attribute is the back-end user.

10. The permission management system according to claim 9, wherein the first menu is a fixed menu and the second menu is a dynamic menu that changes with the permission of the registered user.

11. The permission management system according to claim 9, wherein the second menu generation unit is specifically configured to: obtain the permission of the registered user; determine a function portal corresponding to each permission; and integrate all function portals corresponding to the permission of the registered user to form the second menu.

12. The permission management system according to claim 9, wherein the back-end user comprises a system administrator and an operator, and
the user management module is specifically configured to: assign a role to the registered user when the user attribute of the registered user is the front-end user or the system administrator; and assign one or more roles to the registered user when the user attribute of the registered user is the operator.

13. The permission management system according to any of claims 8 to 12, further comprising a permission editing module, wherein
the permission editing module is configured to add, delete or edit any permission, and each permission comprises a set of one or more interfaces, so that a function of an online diagnostic platform corresponding to the interface is allowed to be used.

14. The permission management system according to any of claims 8 to 12, further comprising an execution control module, wherein
the execution control module is configured to: determine, through the menu, a function requested to be executed by the registered user; and determine, according to the permission of the registered user, whether to execute the function requested to be executed.

15. An online diagnostic platform, comprising:

a client, configured to receive user information of a registered user and send the user information to a permission management system, wherein the client is further configured to display

a menu generated by the permission management system according to the user information;
the permission management system, configured to execute the permission management method according to any of claims 1 to 7 to manage one or more registered users; and
a service system, configured to execute a diagnostic service function according to a request of the client.

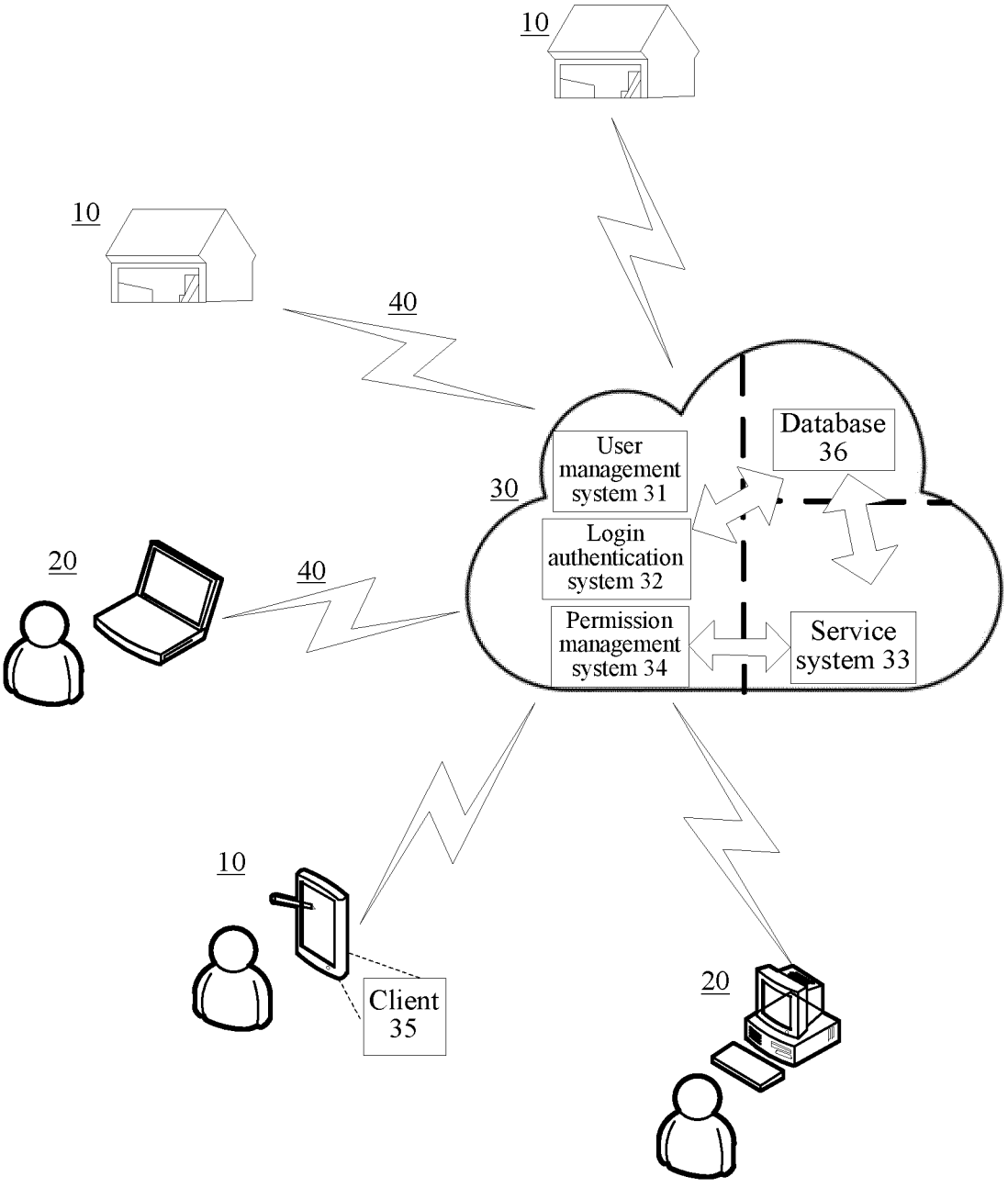
10
10
40
30
User management system 31
Database 36
Login authentication system 32
Permission management system 34
Service system 33
20
40
10
Client 35
20

FIG. 1

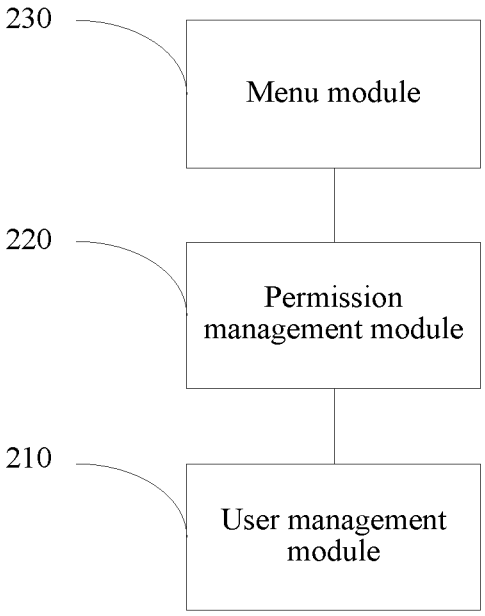
230
Menu module
220
Permission management module
210
User management module

FIG. 2

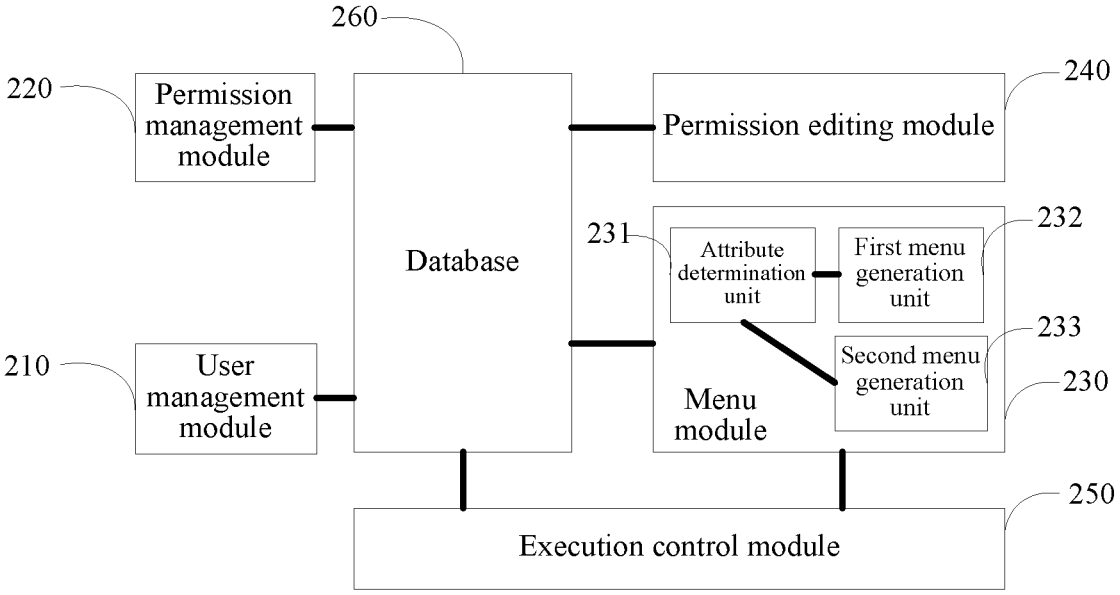
260
220
Permission management module
Database
Permission editing module
240
231
Attribute determination unit
First menu generation unit
232
233
Second menu generation unit
230
Menu module
210
User management module
250
Execution control module

FIG. 3

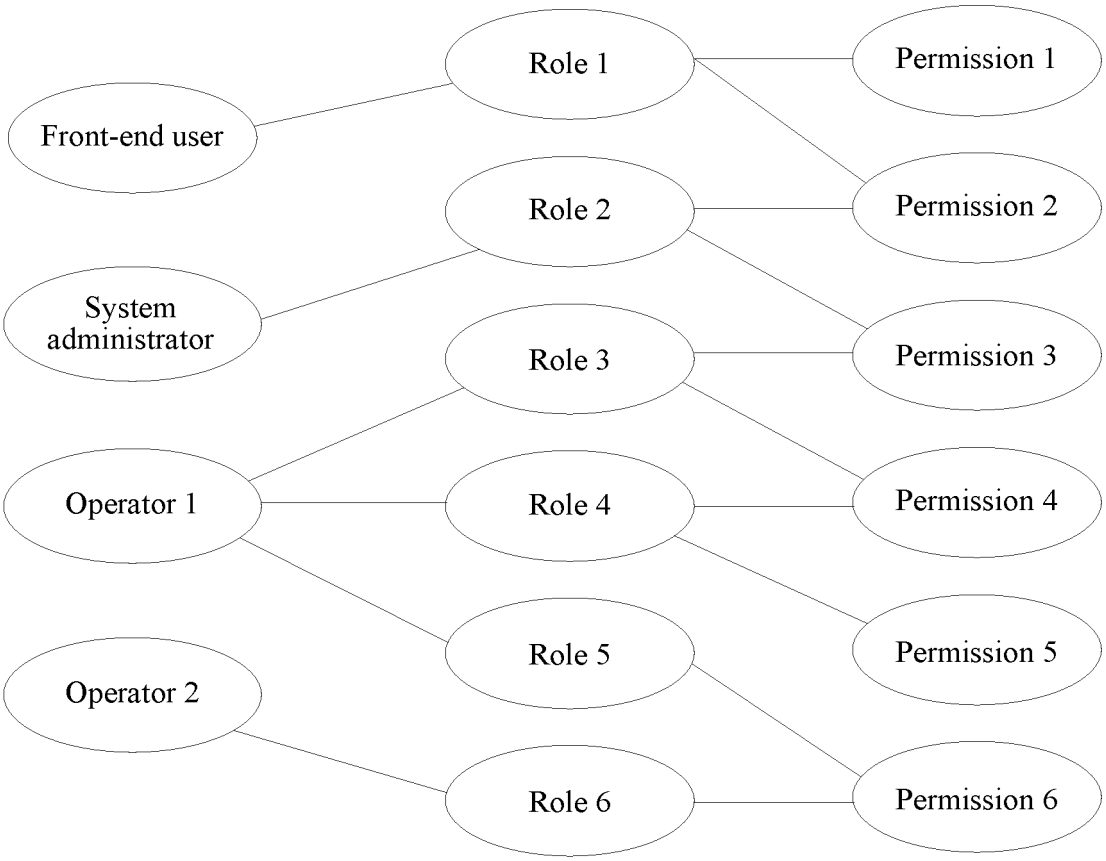
Front-end user
System administrator
Operator 1
Operator 2
Role 1
Role 2
Role 3
Role 4
Role 5
Role 6
Permission 1
Permission 2
Permission 3
Permission 4
Permission 5
Permission 6

FIG. 4

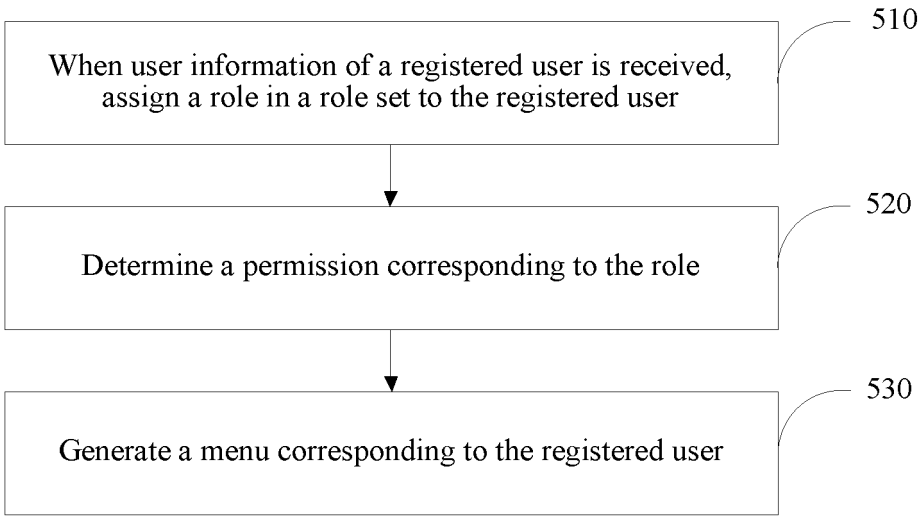
When user information of a registered user is received, assign a role in a role set to the registered user
510
Determine a permission corresponding to the role
520
Generate a menu corresponding to the registered user
530

FIG. 5

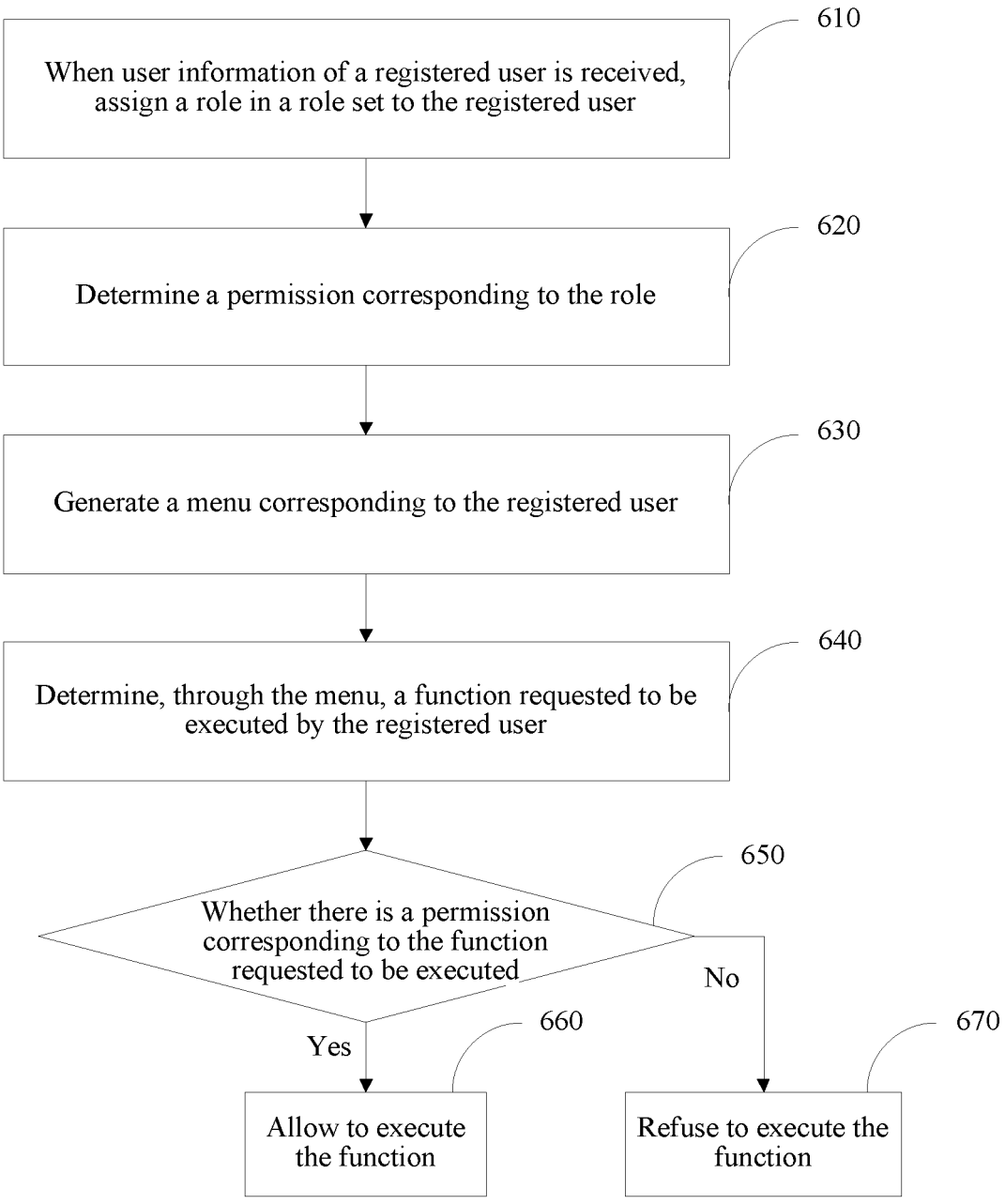
When user information of a registered user is received, assign a role in a role set to the registered user
610
Determine a permission corresponding to the role
620
Generate a menu corresponding to the registered user
630
Determine, through the menu, a function requested to be executed by the registered user
640
Whether there is a permission corresponding to the function requested to be executed
650
No
Yes
660
Allow to execute the function
670
Refuse to execute the function

FIG. 6

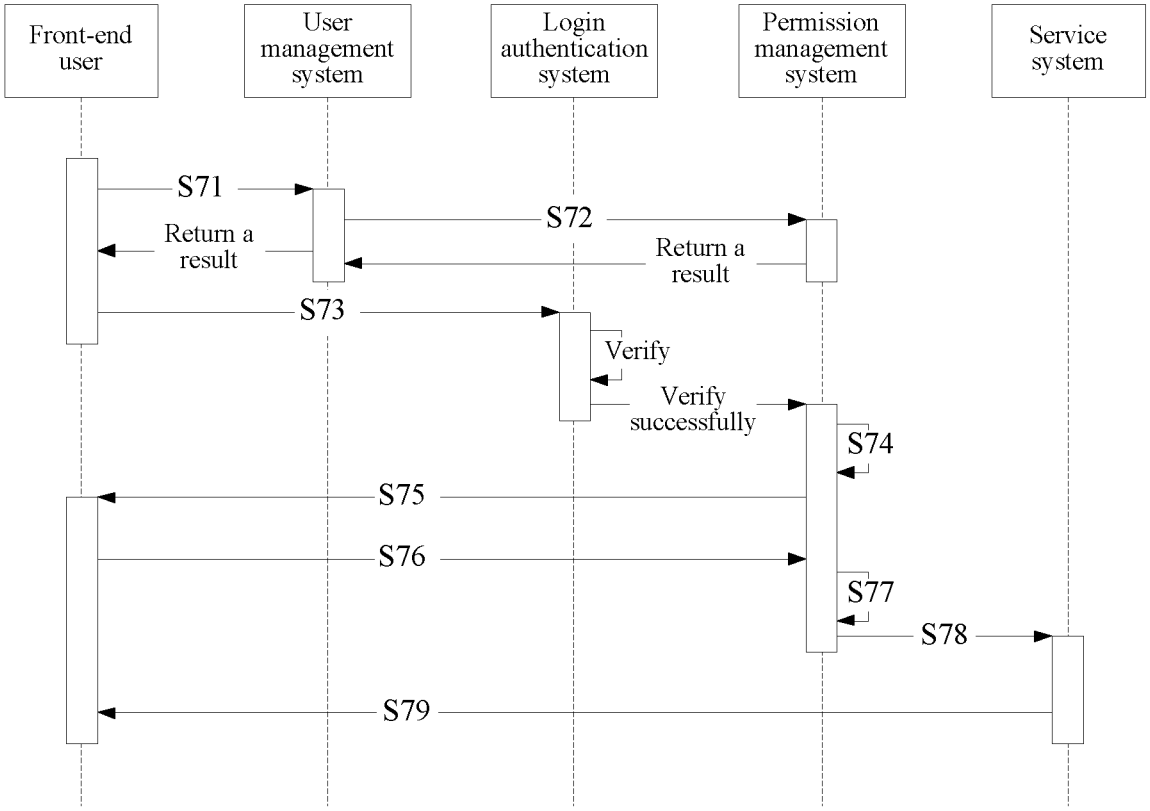
Front-end user
User management system
Login authentication system
Permission management system
Service system
S71
Return a result
S72
Return a result
S73
Verify
Verify successfully
S74
S75
S76
S77
S78
S79

FIG. 7

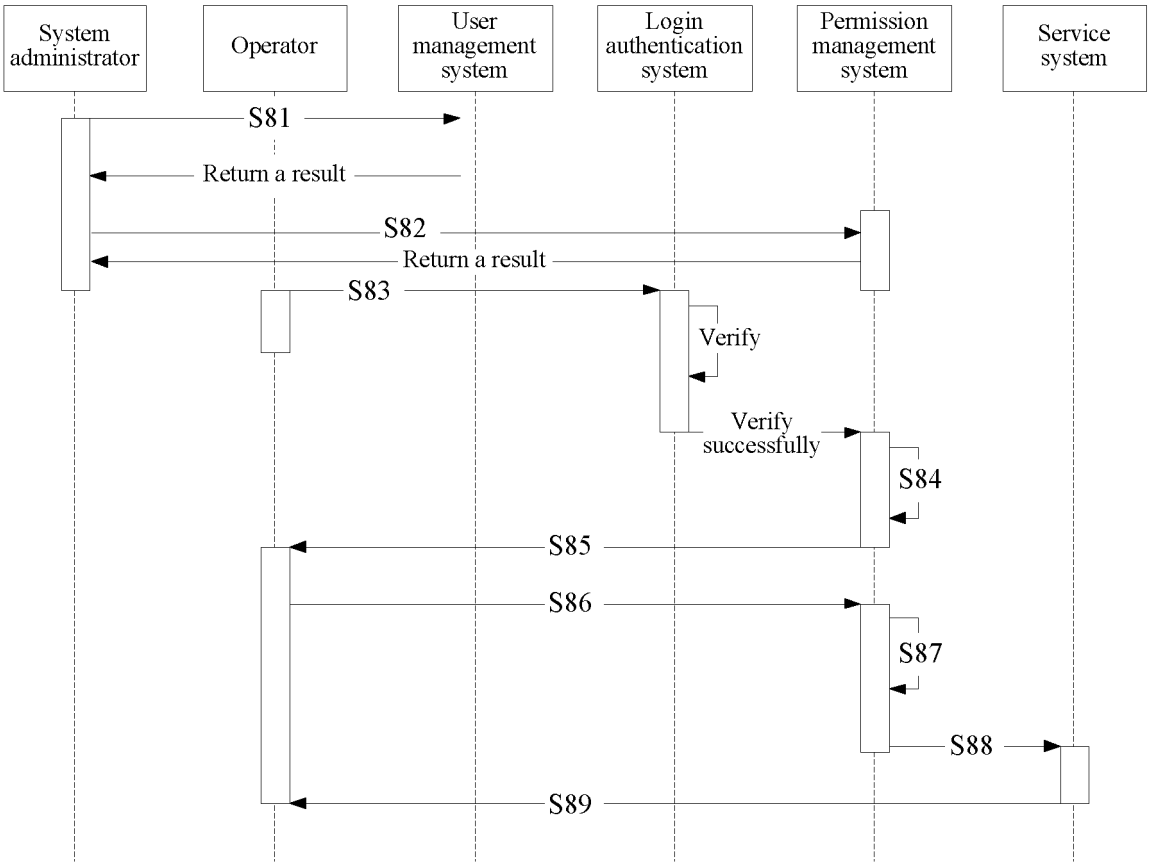
System administrator
Operator
User management system
Login authentication system
Permission management system
Service system
S81
Return a result
S82
Return a result
S83
Verify
Verify successfully
S84
S85
S86
S87
S88
S89

FIG. 8

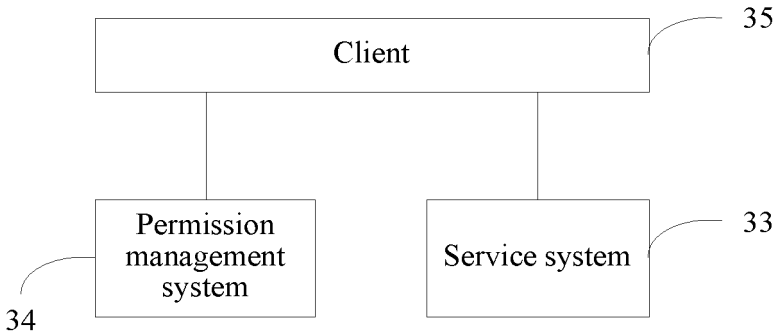
Client
35
Permission management system
34
Service system
33

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/070486

A. CLASSIFICATION OF SUBJECT MATTER

G16H 80/00(2018.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G16H

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

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

CNPAT, CNKI, WPI, EPODOC: 注册, 用户, 角色, 权限, 分配, 菜单, 动态, 映射, 多个, user, register+, distribut+, role, permission, menu, function

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109817347 A (AUTEL INTELLIGENT TECHNOLOGY CORP., LTD.) 28 May 2019 (2019-05-28) claims 1-15	1-15
Y	CN 108600177 A (BEIJING WONDERSOFT TECHNOLOGY CO., LTD.) 28 September 2018 (2018-09-28) description, paragraphs [0006]-[0026]	1-15
Y	CN 105303084 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.) 03 February 2016 (2016-02-03) description, paragraphs [0025]-[0035]	1-15
A	US 2015156251 A1 (ZTE CORP.) 04 June 2015 (2015-06-04) entire document	1-15

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

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

Date of the actual completion of the international search	Date of mailing of the international search report
19 March 2020	**03 April 2020**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/070486

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 109817347 A	28 May 2019	None	
CN 108600177 A	28 September 2018	None	
CN 105303084 A	03 February 2016	None	
US 2015156251 A1	04 June 2015	US 9467502 B2	11 October 2016
		EP 2830287 A4	05 August 2015
		CN 102868729 A	09 January 2013
		CN 102868729 B	04 May 2018
		WO 2013178110 A1	05 December 2013
		EP 2830287 A1	28 January 2015

Form PCT/ISA/210 (patent family annex) (January 2015)

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- CN 201910036464 **[0001]**