A dual-role hierarchical RBAC extended security model based on department attributes and its application

Xianghui Zhang[1,*], *Zuoping* Zhu[1], *Jianxin* Sui[2], *Yao* Huang[1], and *Chaojun* Zuo[2]

[1]State Grid, Xiangtan Power Supply Company, 411007 Xiangtan, China
[2]State Grid, Hunan Information and Communication Co., Ltd., 410004 Changsha, China

Abstract. In order to overcome the problems of the classic RBAC model, such as user identity cannot be verified, role assignment conflicts, permission leakage, complicated roles and permissions configuration, etc., this paper proposes a dual-role hierarchical RBAC extended security model based on department attributes. Firstly, based on the identity authentication mechanism, the legality of the user identity used by the system and its department attributes are authenticated, and the legal identity users are associated with their departments. Then, the roles were divided into responsibility roles and system roles in the classic RBAC model, which are defined by the system administrator is responsible for configuring system roles according to the permission control requirements of resources and operations in the system. The person in charge of the department to which the user belongs configures the role for the user according to the actual work responsibilities of each user, and the person in charge of the department is responsible for the relationship between the role and the system. Finally, this dual-role hierarchical RBAC extended security model based on department attributes is applied to the authority management scheme of a power grid business system. The security analysis and practical results show that this dual-role hierarchical RBAC extended security model based on department attributes is a system rights management solution with strong security and practicability.

1 Introduction

With the continuous and rapid development of software system development and integration, big data and cloud computing, mobile Internet communication and other technologies, as well as the high degree of cross-integration between application fields of various industries, the scale of various business management systems within the enterprise continues to expand and integrate. The degree of access is also getting higher and higher, which makes the authority control of the internal business management system of the enterprise more and more complicated, which greatly increases the labor cost of enterprise system use management and reduces the work efficiency of system use. Role-based access control (RBAC) has excellent characteristics such as flexible authorization, easy

* Corresponding author: 55462305@qq.com

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).

management and policy neutrality, and plays an important role in the realization of authorization management and access control of various application systems. It is precisely because of this that the research on the rights management and access control of RBAC in various information management systems has become a hot topic in recent years, and has attracted extensive attention from scholars at home and abroad. However, in the early classic RBAC model, due to the following problems, (1) the user identity cannot be authenticated, and staff in different departments within the enterprise use identities to apply for access authorization. (2) Users at the same level in different departments may be granted the same role will cause conflict in role assignment. (3) There may be permission leakage after role inheritance. (4) Improper configuration of roles and permissions may cause human data leakage, loss, tampering, and even system downtime. It greatly hinders the application and promotion of RBAC in information system authorization management and access control. Therefore, it is necessary to further expand and improve the security performance of the classic RBAC reference model and its practical application research.

2 Related work

Since the 1970s, various information systems have been widely used in industries. As one of the core technologies for managing information system security, access control technology has become a research focus of scholars at home and abroad. The traditional access control models mainly include discretionary access control (DAC) and mandatory access control (MAC) [1], which are mainly used to solve the management problem of shared data access authorization in computer systems. However, when the number of users or rights is huge, the management of user rights is very complicated, and its use efficiency and security will be greatly affected, and it cannot meet the increasingly extensive information system rights management needs. With the continuous improvement of the level of information and the complexity of system business management, role-based access control (RBAC) has emerged as the times require. RBAC is a role access control analysis model, which is mainly divided into the basic model RBAC0 [2], Role Hierarchy Model RBAC1 [3], Role Restriction Model RBAC2 [4] and Role Hierarchy Restriction Unified Model RBAC3 [5]. The RBAC0 model was first proposed by Ferraiolo et al. in 1992. The RBAC0 model defines the minimum set of four elements that constitute the RBAC control system, namely, user, role, session, and authority. In 1995, based on the RBAC0 model, the RBAC1 model is extended by the concept of role inheritance introduced by Sandhu et al. The RBAC2 model was extended by NIST on the basis of the RBAC0 model in 2001. It introduced the concept of constraints on the basis of RBAC0, and added the Static Separation of Duty (SSD) and the Dynamic Separation of Duty (DSD), in which SSD is used to implement mutual exclusion, cardinality constraints, and prerequisite constraints of roles in the assignment stage of users and roles. While DSD is the constraint between sessions and roles to achieve dynamic constraints on what users have When a user has two or more roles, only one role is activated at the same time. The RBAC3 model was integrated on the basis of the RBAC1 and RBAC2 models by NIST in 2004. It is a collection of the RBAC1 and RBAC2 models. Compared with the RBAC0 model, it increases both role hierarchy and constraints. However, the four classical RBAC models proposed in the early stage focus on how to control system permissions to realize users and roles, assignment of roles and permissions, and access permission constraints, while ignoring that there may be user identities that cannot be authenticated during the assignment process, Security issues such as role assignment conflicts and permission leaks, as well as complex and difficult to implement roles and permissions configuration in practical applications, have greatly hindered its popularization and application. Because of this, many researchers at home and abroad continue to work on the security extension and

practical application of the RBAC model. In terms of security extension research, Ninghui [6] et al., gave a precise definition of a series of security analysis problems in the RBAC model, using delegation to achieve RBAC management rights and using security analysis techniques to maintain ideal security properties. Ferrara [7] et al., proposed a new analysis method to prove the security of RBAC models, which uses abstract interpretation techniques to analyze programs and uses programs to verify the security of RBAC models. Ren Zhiyu [8] et al., proposed and defined the user-role delegation model (ABURA), and designed the reachability analysis algorithm and verification examples. Aftab [9] et al., proposed a permission-based hybrid access control model, which adds dynamic attributes to the RBAC model, reduces the burden of administrator rights management, and enhances the flexibility, dynamism and safety of the model. Aiming at the traditional role-based access control scheme is generally centralized, the assignment of user roles lacks fine-grainedness, and the assignment of roles and permissions is static, which is inconsistent with today's distributed and dynamic network architecture. DF-RBAC is a dynamic and fine-grained role-based access control model, which can realize the flexible assignment of roles by resource owners and the security verification of assigned roles. In terms of practical application research, Zhang [11] et al., based on the RBAC model, realized the two-level access control of information and resources in the production management system through the resource coding mechanism. Lu [12] et al. designed a secure transmission and authorization management system based on public key infrastructure and Rose-based access control principle, added the principle of grouping authority to the RBAC model, and adopted a combination of centralized authority and distributed authority management, it makes the model more flexible. Yuan [13] et al., analyzed the limitations of the existing RBAC0 model, established an extended RBAC model that crossed the role and directly faced users, and designed the document Relevant functional modules required for permission access control in the management system. Wang Jianxiang [14] et al., comprehensively used the ASP.NET MVC architecture pattern and EF technology to design and implement an authority management system. Based on Docker technology, You [15] et al., designed a role permission control model based on cloud computing and Docker technology by combining the functions of task controller, project controller and user controller. Peng Sixi [16] et al., designed an RBAC-based permission control security mechanism. According to user types and roles, authorized access to business data and functional modules is achieved through role permission control and module allocation control.

The above-mentioned relevant research results show that in terms of RBAC security extension research, the research contents that scholars focus on mainly include the security analysis and definition of the RBAC model, the computational complexity and determinability of the implementation of security analysis, and how to implement the security analysis in the existing On the basis of the model, security constraints and restrictions are added to ensure the security of RBAC when implementing rights management and access control, while ignoring how to solve the security problems such as user authentication, role assignment conflicts, and rights leakage that may exist in the model. In terms of practical application research of RBAC, scholars pay more attention to the design and implementation of rights management and access control functions based on the classic RBAC model. Few of them consider how to design and develop rights management systems, overcome the above-mentioned security flaws in the RBAC model itself, and how to configure roles and permissions. Therefore, on the basis of the above research results, this paper focuses on how to conduct extended research on the problem of insufficient security performance of the classic RBAC reference model, and applies the extended RBAC security reference model to the authority of a power grid business management information system in the management case.

3 Classic RBAC reference model

The early research on role-based access control model is mainly based on the RBAC3 reference model, and its structure is shown in Fig.1, which mainly includes User Set (U), Role Set (R), and Permission Set (P), Session Set (S), User Role Assignment (UA), Role Hierarchy inheritance (RH) , Role Permission assignment (PA) these three mapping relationships, User Session (US) and Role Session (RS), and Static Separation of Duty (SSD) and Dynamic Separation of Duty (DSD).

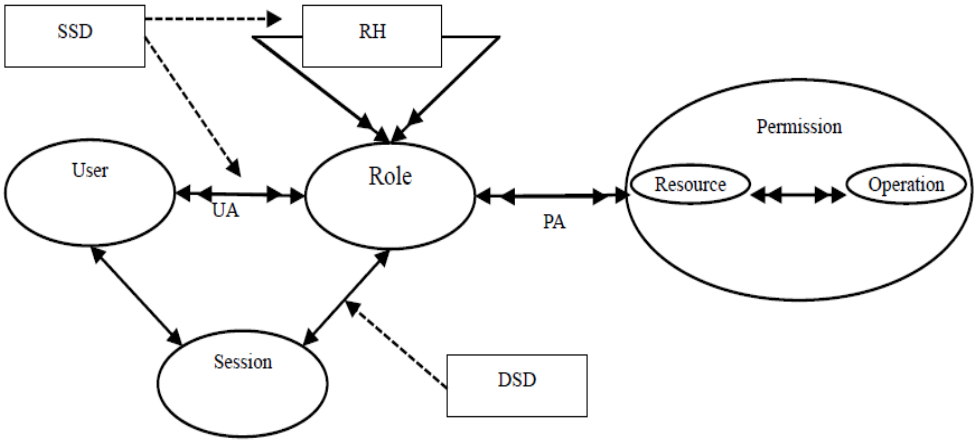

Fig.1. RBAC3 reference model.

where, the user set U refers to an active entity that accesses system resources and operations, and may be a set composed of people, robots, or computers. Role set R is a function set composed of a certain number of access rights defined on system resources and a set of operation controls defined on system objects. It is the carrier of system rights management and access control, and is the core of the RBAC3 reference model. It represents the access control and operation of a class of users in the system. The permission set P refers to the permissions that allow the role to access data resources and operations in the system. The session set S refers to the set of mappings established between users and roles when roles are assigned to users. The static duty separation SSD is used to implement mutual exclusion, cardinality constraints, and prerequisite constraints of roles in the assignment stage of users and roles, mainly referring to the set of constraints established when assigning roles to users. The Dynamic Duty Separation DSD is used to establish a set of constraints when activating a role for a user in the session phase, so that a user can only activate one role at the same runtime. The Role Hierarchy RH is used to establish a permission inheritance relationship set between subordinate and same-level roles when configuring permissions for system roles, so as to reduce repeated permission configuration and reduce the complexity of permission management. The RBAC3 reference model associates users with roles, roles and access rights, and encapsulates the access rights of resources and operations in roles. By assigning appropriate roles to users, users can indirectly obtain access rights to the system, with logical separation of users and rights. , Simple and flexible authorization, low complexity and low management cost. However, at the same time, the RBAC3 reference model still has problems such as unverifiable user identity, possible conflicting role assignments, permission leakage, and difficult configuration of roles and permissions. Therefore, this paper focuses on the extended security model based on the RBAC3 reference model and its application practice research.

4 A dual-role hierarchical RBAC extended security model based on department attributes DRH-RBACDA

4.1 The model structure and its main idea

Aiming at the shortcomings of the classic RBAC3 reference model, this paper proposes a dual-role hierarchical RBAC extended security model based on department attributes, namely DRH-RBACDA, the structure of which is shown in Fig.2.

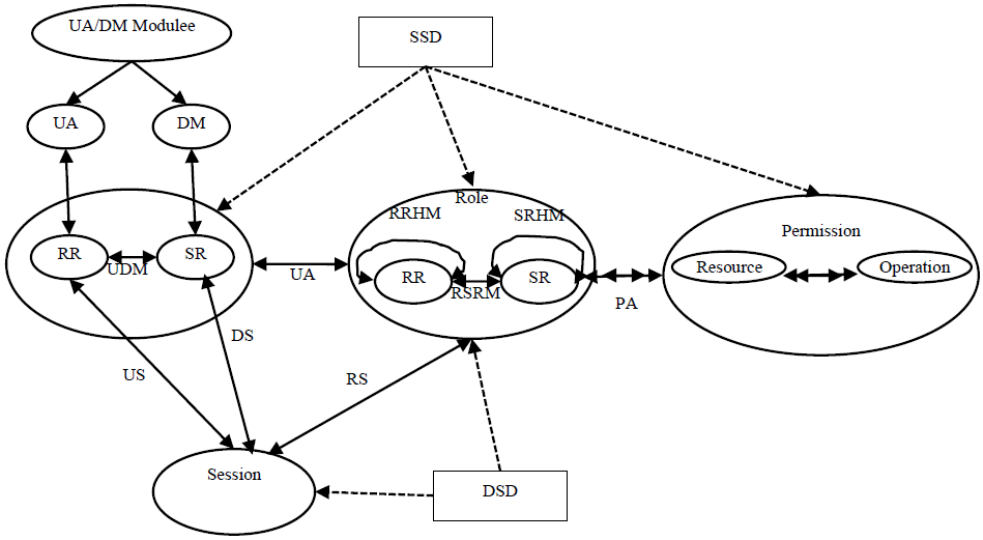

Fig. 2. DRH-RBACDA reference model.

Compared with the classic RBAC3 reference model, the core idea of the DRH-RBACDA model is to make the following extensions.

(1) In the classic RBAC3 reference model, the user identity cannot be authenticated, and the staff of different departments within the enterprise use identities to apply for access authorization. On the basis of the RBAC3 model, a user identity authentication module [17] is added to verify The legitimacy of the user's identity and the department it belongs to, that is, the person in charge of the user's department is responsible for reviewing the identity information and responsibilities and roles provided by the user during registration, such as the user's name, department, job responsibilities, and basic information such as required permissions, and configure the responsibility role for the audited legal users.

(2) In the classic RBAC3 reference model, users at the same level in different departments may be granted the same access authorization, which may lead to conflicting role assignments. Drawing on the ideas in the D-RBAC model [18], the user's department attributes is introduced on the basis of RBAC3, so as to define the user's responsibility role, that is, the scope of the role is limited by department, and the responsibility role is regarded as a role defined under the department scope, so that the conflict domain of each role is limited within a department, eliminating the need for other roles. The conflict of the same role under different departments reduces the scope of the conflict domain.

(3) In view of the problem of permission leakage after role inheritance in the classic RBAC3 reference model, the idea of SDTR-OBAC model [19, 20] is used. First, the roles are divided into responsibility roles and system roles, and then the mapping relationship between the responsibility roles and system roles is established, and the role definition in the classic RBAC3 reference model is extended to a role tuples composed of (responsibility

roles, system roles), to achieve the separation of the logical structure of responsibility roles and system roles. Responsibility roles and system roles define different inheritance relationships within their scopes, which overcomes the problem of permission leakage in the classic RBAC3 reference model due to single role inheritance, and it also solves the problem of excessive roles, permissions, or redundancy in distributed environments with a large number of similar organizations.

(4) In the classic RBAC3 reference model, because the system administrators are not familiar with the job responsibilities of the personnel in each department, there may be security problems such as artificial data leakage, loss, tampering, and even system downtime caused by improper configuration of roles and permissions. Assign the user's responsibility role to the person in charge of the user's department for management, and the department leader dynamically assigns the responsibility role to the employee according to the job responsibilities of the employee, and is responsible for the mapping management between the responsibility role and the system role. Assign the system role to the system Managers are responsible for management, and system managers configure system roles according to the authority control requirements of resources and operations in the system, reducing the risk of inappropriate configuration caused by the unified responsibility of system management for both role and authority configuration management.

As shown in the structure in Figure 2, the DRH-RBACDA security model mainly includes User set (U), Department set (D), Responsibility Role set (RR), System Role set (SR), Permission set (P) and Session set (S). User and Department Map (UDM), User Department and Responsibility Role Map (UDRRM), Responsibility and System Role Map (RSRM), Role and Permission Map (RPM), Responsibility Role Hierarchical Map (RRHM), System Role Hierarchical Map (SRHM). User Session (US), Department Session (DS), Role Session (RS). Static Responsibilities Separation of two constraints (SSD) and Dynamic Separation of Duties (DSD). User Authentication and Department Management Module (UA/DM).

4.2 Model collection

The main sets included in the DRH-RBACDA model are defined as follows.

(1) User set $U=\{u_1,u_2,\ldots,u_n\}$, a set composed of several system users.

(2) Department set $D=\{d_1,d_2,\ldots,d_n\}$, which is a set composed of several different departments with internal responsibilities and division of labor within the enterprise.

(3) Responsibility role set $RR=\{rr_1,rr_2,\ldots,rr_n\}$, which is a set of different roles with different job responsibilities within several enterprise departments.

(4) The system role set $SR=\{sr_1,sr_2,\ldots,sr_n\}$, which consists of several groups including different system resource access and functional operation permissions.

(5) Permission set $P=\{p_1,p_2,\ldots,p_n\}$, which consists of a set of two-tuples consisting of all data of the system or other resources and operations that can be represented by data, that is, p=(res, opt), where, $res \in Res$, $opt \in Opt$.

(6) Session set $S=\{s_1,s_2,\ldots,s_n\}$, a set composed of several system access communication processes.

4.3 Mapping relationship

The main mapping relationships included in the DRH-RBACDA security model are defined as follows.

(1) The mapping relationship between users and their departments (UDM), $U \to 2^D$. It indicates the department $d \in D$ to which the user $u \in U$ belongs, multiple users can

belong to the same department, and a user can also belong to multiple different departments. There is an n-to-n mapping relationship with the department.

(2) The function mapping relationship between "user + department" and responsibility roles (UDRRM), $(U, D) \to 2^{RR}$. It means assigning responsibility roles $rr \in RR$ to users $u \in U$ in the department $d \in D$. Multiple "user + departments" can be assigned the same responsibility role, one "User + Department" can also be assigned to several different responsibility roles. There is an n-to-n mapping relationship between "User + Department" and responsibility roles.

(3) The mapping relationship between responsibility roles and system roles (RSRM), $RR \to 2^{SR}$. It indicates that the corresponding system roles are assigned to the responsibility roles $rr \in RR$. Multiple responsibility roles can be mapped to a system role, and a responsibility role can also be assigned to a set of system roles, and there is an n-to-n relationship between responsibility roles and system roles.

(4) Responsibility Role Hierarchical Map (RRHM) $U \times D \times RR \to 2^{RR}$. It indicates that between superior and subordinate users in the same department, superior users can acquire the subordinate users' responsibility roles through inheritance, which is indirectly realized through the inheritance relationship of responsibility roles. Inheritance of system access authorization between subordinate and subordinate users in the department reduces the repeated system authorization between subordinate and subordinate users in the department. On the contrary, if the user is not in the same department, the upper and lower levels cannot obtain access authorization to the system through the inheritance of responsibilities and roles, preventing permission leakage between different departments due to the inheritance of roles.

(5) System Role Hierarchical Map (SRHM), $SR \to 2^{SR}$. It indicates that there is an inheritance relationship between the access authorizations of system roles, and high-level system roles can inherit the access authorization tasks of low-level system roles, thereby reducing duplicates. Role authorization reduces the workload of rights management and access control.

(6) User Session Mapping Relationship (US), $S \to U$. It represents the mapping from session to user. During the process of session communication, the associated user participating in the session is found through this mapping relationship.

(7) Department Session Mapping Relationship (DS), $(S,U) \to D$. It represents the mapping from session to user in the department. In the process of session communication, the department where the user $u \in U$ participates in the session $s \in S$ is found through this mapping relationship.

(8) Role Session Mapping Relationship (RS), $(S,U,D) \to R$. It represents the mapping from session to user role. In the process of session communication, the role $r \in R$ of the user $u \in U$ participating in the session $s \in S$ in the department $d \in D$ is found through the mapping relationship.

(9) The mapping relationship between the role tuples and the system permissions (RPA), $(D,U,S,R) \to 2^{P}$. It indicates that in the process of the user $u \in U$ in the department $d \in D$ participating in the session $s \in S$, a set of access authorizations to the system are obtained through the role $r \in R$. Multiple roles can grant the same permission, and a role can grant multiple different permissions. There is an n-to-n mapping relationship between roles and permissions.

According to the description of the main mapping relationship definitions in the above DRH-RBACDA security model, the relationship between users, departments, responsibility roles, system roles, and permissions is shown in Fig.3. The structure in Figure 3 shows that the relationship from the user to the system authority is not a simple one-to-one or one-to-

many transfer relationship, but a complex many-to-many transfer relationship. Therefore, in order to ensure the security of the model, it is necessary to implement appropriate constraints on the transitive relationship. The constraints in the DRH-RBACDA security model are further described below.

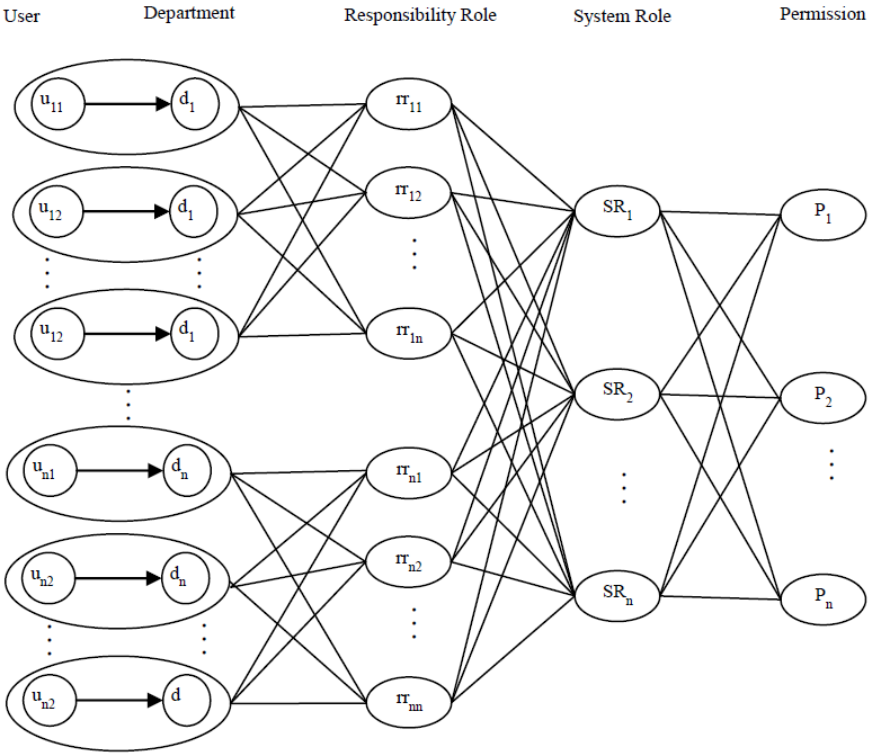

Fig.3. The mapping relationship among "user + department", responsibility role, system role, and system authority.

4.4 Constraint

Constraints refer to restrictions on the execution of mapping relationships such as UDM, UDRRM, and RSRM in the DRH-RBACDA model, and are the premise to ensure the security of the model. Since the DRH-RBACDA model designs its responsibilities and system roles according to the responsibilities of users in administrative positions, it is necessary to ensure the security of the configuration of permissions for users with different administrative responsibilities, and to prevent potential security risks caused by role conflicts and permission leakage. Therefore, this paper mainly discusses the constraints of separation of duties, including the constraints of static separation of duties and constraints of dynamic separation of duties. Among them, the static duty separation constraint is used to realize the mutual exclusion of the user's affiliation department, the mutual exclusion of assigning responsibility roles, the cardinality constraint on the number of user assignment responsibility roles, the cardinality constraint on the number of roles in the responsibility role mapping system, the responsibility role inheritance and the system role inheritance. Prerequisite constraints, etc., are similar to the SSD static duty separation constraints in the classic RBAC reference model, and will not be elaborated here. Next, we focus on the dynamic separation of duties constraints.Dynamic Responsibility Separation DSD is used to specify the department to which the user belongs (UDM), the “user + department”

configuration responsibility role (UDRRM), and the set of constraints established when the responsibility role is associated with the system role (RSRM) in the session phase, so as to achieve the same session During the communication process, a user can only belong to one department, a "user + department" can only activate one responsibility role, and a responsibility role can only be associated with several specified system roles. Therefore, dynamic duty separation constraints can be defined for UDM, UDRRM and RSRM respectively. Due to the limited length of the article, this paper only gives the formal definition of UDRRM dynamic duty separation constraints, and the formal definitions of other dynamic duty separation constraints are similar.

UDRRM Dynamic Separation of Duties Constraints UDRRM-SoD: $UDRRM-SoD \subseteq (2^{RRD^+} \times N)$. Where, $RRD^+ \subseteq (RR \times D^+)$, $D^+ = D \cup \{?,*\}$. N represents a set of natural numbers satisfying the relation $\forall (rrd, n) \in UDRRM-SoD$, $|rrd| \geq n \geq 2$, $n \in N$. The dynamic duty separation constraint $(rrd, n) \in UDRRM-SoD$ indicates that n mutually exclusive "department + duty role" pairs rrd cannot be assigned to user u during the session. The wildcard "?" indicates the same department $d_i \in D$ in the department set D . The wildcard "*" indicates the department set D in any of the different departments $\forall d_i \neq d_j \in D$.

4.5 Authentication

In the actual application process, the confidential information about the identity of the employees in the same department is easily known to each other directly or indirectly, such as the user's job responsibility number, name, date of birth, and even ID number or login password, etc., which involve user's confidential identity information. The traditional classic RBAC reference model does not provide a corresponding user identity authentication mechanism. Therefore, users in the enterprise LAN may apply for access authorization from the system administrator by disguising their identities, resulting in permission leakage. To this end, this paper draws on the core idea of the HTTPS security protocol to realize user identity authentication, and at the same time, assigns the person in charge of the department to assume the responsibility of user identity authentication management within the department. In the DRH-RBACDA security model, a user authentication module is added between users and department sessions. The HTTPS security protocol is enabled in the user authentication module, and the authentication management of the legality of the user's identity and the department to which it belongs is completed by means of ciphertext communication, thereby preventing the risk of system authority leakage caused by the fraudulent use of the user's identity information. Considering that HTTPS is already a widely used and very mature secure communication protocol, due to space limitations, this article will not repeat the entire process of HTTPS to achieve user identity authentication [17].

4.6 Model Analysis

Compared with the traditional classic RBAC reference model, the DRH-RBACDA security model proposed in this paper has the following characteristics.

(1) Increased security. The DRH-RBACDA security model introduces an identity authentication mechanism to verify the legitimacy of the user's identity and the department to which it belongs, effectively reducing the risk of illegal users using their identities to apply for authorization, and increasing the security of the model application.

(2) The role conflict domain is reduced, and the risk of permission leakage caused by role inheritance is lower. In the DRH-RBACDA security model, the department is the active domain for role assignment and authorization, which avoids the conflict of role assignment of the same type of users between different departments, limits the scope of role inheritance, and reduces the risk of permission leakage caused by role inheritance.

(3) Role management is convenient and flexible. The DRH-RBACDA security model divides the single role in the classic RBAC model into responsibility roles and system roles. The responsibility roles are assigned to the department heads for management, and the system roles are managed by the system administrators. Using role management is more convenient and flexible.

(4) The assignment of authority is flexible and the risk of leakage is reduced. In the DRH-RBACDA security model, the user's authority is assigned by the person in charge of the department. The system administrator only needs to classify and assign system access and operation authority according to the system role, and does not need to pay attention to how the system business and management consider the allocation of user authority. This makes permission assignment more flexible, and at the same time reduces the risk of permission leakage due to improper role configuration and other factors.

(5) It is more practical. The DRH-RBACDA security model considers that the system administrator is not familiar with the division of business, and there may be the risk of permission leakage caused by improper role and permission configuration. The user roles and permission configuration in the classic RBAC model are unified and centralized for management by the system administrator. The model is expanded to be managed collaboratively by department administrators and system management, which is more suitable for actual work needs and enhances the practicability of the model.

5 The application of DRH-RBACDA security model in a power grid business authority management system

With the continuous improvement of power grid business technology and information construction level, it is an inevitable trend to build a unified and interconnected power grid business management information system based on computer network communication, so as to improve work efficiency and management level. However, due to the complexity of the power grid company's business, the large number of company departments and users, and the different business rights requirements of users in different levels of subsidiary departments, the security management of user access rights in the power grid business management information system has become the key to the efficiency of such systems. Therefore, based on the DRH-RBACDA security model, this article uses the .Net Framework 4.5, C# programming language, Visual Studio 2019+SQL Server 2019+IIS3.0 integrated development environment under the Windows 10 system platform, and the MVC software development method and the B/S mode were used to design and implement a business information permission management system of a power grid company.

5.1 Requirement analysis of permission management function

According to the analysis of the business requirements of a power grid company, the functions and security requirements of its authority management system are as follows.

(1) Complete identity authentication for all users, and dynamically generate accessible system pages. Through the verification of user information such as user name, password, job code, department number, etc., determine the user's responsibilities and roles and associated system roles, and then according to User responsibility roles and associated

system roles match the user's access function menu and data operation authority, and generate accessible system pages.

(2) Provide a flexible and convenient system authority management module. For department managers, design and implement flexible and convenient user responsibility role management, role inheritance management, and system role association mapping management function modules. For system managers, design and implement flexible and convenient departments Management information management, system role authorization management, role access authority constraint management, access time constraint management and other system authority management modules.

(3) Provide a visual system management interface that is easy to operate. The visual operation interface of the system should be different according to the different roles of users, and the function menu should be different according to the different roles of users. At the same time, it also provides convenient modification operations of departments, responsibilities, system roles, and permissions. The system needs the menu operation to be simple and practical, safe and stable, etc.

5.2 Permission management database design

Based on the core idea of the DRH-RBACDA security model, and combined with the actual demand analysis of the power grid company's business information permission management system. The database table relationship of the permission management system is designed in SQL Server 2019 is shown in Fig.4, which shows the dimension table structures and their field descriptions, as well as join relationships between tables.

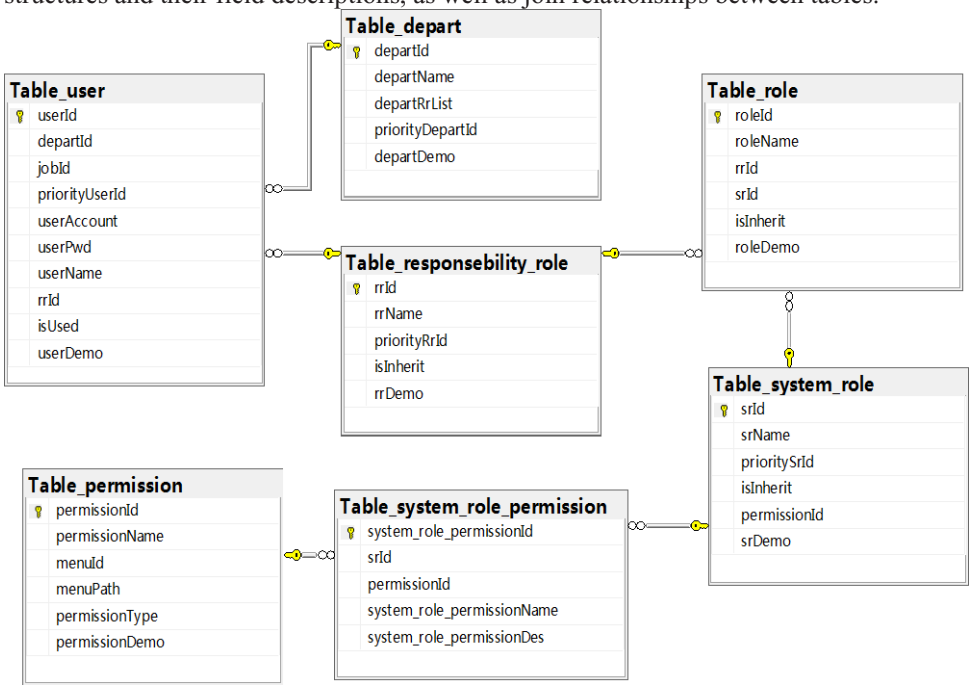

Fig.4. E-R Diagram of database table relationship for permission management based on DRH-RBACDA.

The main information fields and their meanings in the tables shown in Figure 4 are described as follows.

(1) Table_user: Save the identity and login information of system users, including user code, department code, job responsibility code, user priority code, login account, login password, user name, role code and other information fields.

(2) Table_depart: Save company department information, including information fields such as department code, department name, department role list, department priority code, and department description.

(3) Table_responsebility_role: Save the user's responsibility role information, including the responsibility role code, the responsibility role name, the responsibility role priority code, whether inheritance is allowed, the responsibility role description and other information fields.

(4) Table_system_role: Save system role information, including system role code, system role name, system role priority code, whether inheritance is allowed, permission code and other information fields.

(5) Table_role: Save user role information, including role code, role name, role code associated with responsibilities, role code associated with the system, whether inheritance is allowed, role description and other information fields.

(6) Table_permission: Save system permission information, including permission code, permission name, system function menu Id, system function menu path, permission type, permission description and other information.

5.3 System implementation

According to the above description of the relevant model, the analysis of permission management function requirements, and the structure relationship of the permission management database, taking the permission management function module of the department head as an example, its actual operation effect is shown in Fig.5.

Fig.5. Power Grid business information rights management system control panel.

Fig.5 shows the effect of the authority control panel of the director of the financial department of the power grid company. The director of the financial department can conveniently manage the responsibilities, roles, operate permissions, access permissions of his subordinate employees through the authority control panel, as well as the permissions and inheritance relationship among his subordinate employees.

6 Conclusion

Access control is the core technology to ensure the security of information systems, and RBAC is one of the widely used access control technologies in recent years. This paper

firstly introduces the research progress of RBAC at home and abroad, the main structure and core principle of the classic RBAC reference analysis model. Then, the insufficiency of the classic RBAC reference analysis model in terms of security performance is analyzed in detail, and the problems existing in the classic RBAC reference analysis model in such aspects as unverifiable user identity, role assignment conflict, permission leakage, complicated role and permission configuration, etc. For its shortcomings, comprehensively introduce measures such as HTTPS user authentication, user department attributes, and dual-role stratification, and propose an extended security model DRH-RBACDA, which is a classic RBAC. Finally, in order to further strengthen and promote the application of the DRH-RBACDA extended security model in the field of information system security, a power grid business information permission management system was designed and developed by taking the permission management of a power grid company's business information system as a practical application case. The actual application effect monitoring shows that DRH-RBACDA is a safe and efficient information system rights management solution.

This work was supported by the Authorization Integration Management Automation Technology Research Project of State Grid Xiangtan Power Supply Company under Grant 5216C0220007.

References

1. Department of Defense. Trusted computer system evaluation criteria (TESEC), DOD 5200. 28-STD [S]. (1985).
2. Ferraiolo D, Kuhn D R. Role-based access control ［C］//Proc of the 15th National Computer Security Conference. Washington DC: IEEE Computer Society, 554-563, (1992).
3. Sandhu R,Coyne E,Feinstein H,et al. Role-based access control models [J]. IEEE Computer, **29**(2):38-47, (1996).
4. Ferraiolo D,Sandhu R,Gavrila S,et al. Proposed NIST standard for role-based access control [J]. ACM Trans on Information and System Security, **4**(3):224-274, (2001).
5. ANSI. American national standard for information technology: role-based access control [S]. New York:American National Standards Institute, (2004).
6. Ninghui L I , Tripunitara M V . Security analysis in role-based access control [J]. Acm Transactions on Information & System Security, **9**(4):391-420, (2006).
7. Ferrara A L,Madhusudan P,Parlato G. Security analysis of role-based access control through program verification [C] //Proc of the 25th IEEE Computer Security Foundations Symposium. Cambridge: IEEE Press, 113-125, (2012).
8. Zhiyu REN, Xingyuan CHEN. Reachability analysis for attribute based user-role assignment model [J]. Journal of Computer Applications, **34**(02):428-432, 2014.
9. Aftab M U , Qin Z , Hundera N W , et al. Permission-Based Separation of Duty in Dynamic Role-Based Access Control Model [J]. Symmetry, (5):1033-1048, (2019).
10. Liu D, Dong A, Yan B, et al. DF-RBAC: Dynamic and Fine-grained Role-Based Access Control Scheme with Smart Contract [J]. Procedia Computer Science, **187**(2):359-364, (2021).
11. Zhang S, Yan M, University X A, et al. Application and Implementation of Production Management System Based on RBAC Authorization Management [J]. Microcomputer Applications, **18**(5):892-1011, (2016).

12. Lu G, Zhao L, Yang K. The design of the secure transmission and authorization management system based on RBAC. IEEE, **9**(03):452-470, (2015).
13. Yuan D. Design and Implementation of Document Management System Based on Extended Role-Based Access Control Model [J]. Ship Electronic Engineering, **6**(02):250-255, (2017).
14. Jianxiang WANG, Hongze WANG. Design of rights management system based on MVC [J]. Electronic Components and Information Technology, **5**(12):165-172, (2021).
15. You LI, Hui SUN, Daqing GONG. Research and Design of Docker Technology Based Authority Management System [J]. Computational Intelligence and Neuroscience, 5325694-5325694, (2022).
16. Sixi PENG, Peng PENG. Security Mechanism of Student Charge System with B/S Structure Based on RBAC [J]. Journal of Shantou University (Natural Science Edition), **36**(01):12-20, (2021).
17. Jianyou ZHOU. Research and Implementation of Unified Identity Authentication System [D]. Xidian University, (2010).
18. Jun YAN, Zheng-lian SU, Hai-feng LING, et al. Department-role based finely granular access control model in management information system [J]. Journal of Computer Applications, **31**(02):523-526, 2011.
19. Hou-ren XIONG, Xing-yuan CHEN, Bin ZHANG, et al. Scalable Access Control Model Based on Double-tier Role and Organization [J]. Journal of Electronics & Information Technology, **37**(07):1612-1619, (2015).
20. Zhi-yu REN, Xing-yuan CHEN, and Di-bin SHAN. Cross-domain authorization management model based on two-tier role mapping [J]. Joumal of Computer Applications, **33**(9):2511-2515, (2013).