Optimization of Information Security Management Mechanism for Distribution Network Information Storage Based on RBAC and Development of Visual Operation and Maintenance Platform

Lv Zheng, Fang Xi*, Huang Lei, Jiang Dan,
Ran Shuang and Liang Lei

Tongren Power Supply Bureau of Guizhou Power Grid Co. LTD., Tongren, Guizhou, 554300, China
E-mail: fx25845308@163.com
**Corresponding Author*

Received 22 April 2024; Accepted 06 June 2024

Abstract

Facing the challenge of information storage security brought by the rapid development of distribution network technology, this paper analyzes the essential requirements and current security problems of distribution network information storage and designs. It implements a set of security management schemes based on the RBAC model. User authentication and authorization processes are emphasized to ensure only authorized users can access critical information resources. The application in the actual distribution network environment shows that the scheme can improve the security performance of the system, reduce unauthorized access attempts by up to 40%, and improve data processing efficiency by about 30%. The scheme also reduces the complexity of system maintenance, and the number of security events that administrators need to deal with is reduced by about 50% compared to traditional security mechanisms. These data fully prove that the security

Journal of Cyber Security and Mobility, Vol. 13_5, 1061–1084.
doi: 10.13052/jcsm2245-1439.13511

management mechanism based on RBAC is efficacious in improving the distribution network's information storage security and operational efficiency. This article proposes and studies an optimization scheme for information security management mechanisms based on RBAC in distribution network information storage technology. This scheme effectively improves the security and reliability of the distribution network information storage system through refined permission management and access control. This study provides innovative strategies, empirical data for distribution network information storage security management, and valuable references for future research on power grid information security.

Keywords: Role access control, information security management, distribution network information storage, security optimization strategy.

1 Introduction

With the continuous access of distributed generation, the distribution network has gradually changed from traditional "passive" to "active", and the power flow of distribution network is no longer a single flow from distribution substation to each load node, but a bidirectional flow. Although the two-way power flow mode of active distribution network can not only meet the energy demand of users, but also realize energy sharing and regulation, which improves the stability and reliability of the power grid to some extent [1, 2]. But at the same time, it also brings pressure to the operation and management of distribution network. Because of the intermittence, randomness and distribution of distributed generation, it quickly consumes flexible adjustment resources of power system. Although the overall utilization rate is high, the consumption foundation is still not solid, and the problem of abandoning wind and light in local areas and local periods is still outstanding [3].

According to statistics, more than 80% of users' power outages are caused by distribution network failures [4, 5]. Therefore, monitoring and screening the symptoms before the occurrence of distribution network faults, and controlling and preventing the state after the occurrence of distribution network faults can reduce the adverse effects caused by distribution network faults, ensure the reliability and safety of users' electricity consumption, and further enhance the national basic economic level. Because the new and old equipment are mixed, the network distribution range is wide, the topology structure is complex, and the fault causality of distribution network is weak, the mechanism is complex and the randomness is strong, so it is difficult

to realize risk prediction by conventional methods. At the same time, the reliability and stability of distribution network operation state are more and more affected by natural and human factors [6, 7].

The purpose of this paper is to discuss and optimize the application of role-based access control (RBAC) information security management mechanism in distribution network information storage technology. By analyzing the specific requirements of RBAC applied to distribution network information storage, the role definition, authority division and security strategy are established, and a set of RBAC security management scheme for distribution network information storage optimization is proposed, and its effectiveness is demonstrated by empirical research.

2 Information Storage Technology of Distribution Network

2.1 Basic Architecture of Distribution Network System

Distribution network is a low-voltage network that distributes the electric energy transmitted by high-voltage transmission network to various users, and it is an important work for transmitting and supplying electric energy in power system [8].

Figure 1 portrays the fundamental architecture of the distribution network. The network's underlying structure can be disentangled into distinct yet interconnected components:

(1) Substation: At the heart of the distribution network lies the substation, which transforms high-voltage electricity into low-voltage power tailored for urban, rural, and industrial applications. This transformed energy is then disseminated to various distribution rooms, which ultimately powers myriad end users.
(2) Backbone Cable Line: Serving as the circulatory system of the distribution network, the backbone cable line shoulders the crucial responsibility of transporting power from the substation to distribution rooms and, ultimately, end users.
(3) Distribution Room: Low-voltage electrical energy emanating from the main cable line is redistributed to the electrical grids of surrounding buildings, communities, bustling shopping malls, factories, and diverse end users.
(4) End Users: These are the ultimate beneficiaries of the electrical energy disseminated through the distribution network, encompassing industrial and commercial power plants and residential households.

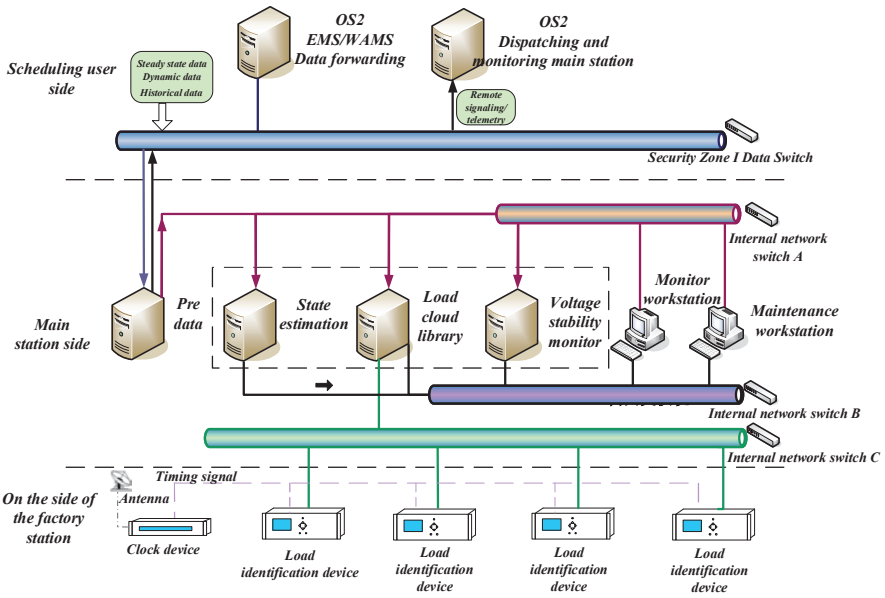

Figure 1 Distribution network basic structure.

(5) Control Center: As the cerebral hub of the distribution network, the control centre oversees and regulates the network's operations, ensuring its smooth functioning.

2.2 Key Elements of Information Storage Technology

Information storage is an important aspect of information system, if there is no information storage, we cannot make full use of the collected, processed information, but also to spend, consume people, consume materials to organize information collection, processing [9, 10]. With information storage, it can be guaranteed to be used on the go, create conditions for the multi-functional use of unit information, thus greatly reducing the cost. Its advantage is that the access speed is extremely fast and the amount of data stored is large. The information store should decide what information is appropriate for what media line. In general, certificate files should be stored in paper media; Business documents are stored on paper or tape; Master documents, such as corporate structures, personnel files, equipment or material inventory accounts, should be stored on disk for online retrieval and query.

Information storage is the preservation of acquired or processed information for future applications. Information storage and data storage applications are the same equipment, but information storage emphasizes the idea of storage, why to store these data, in what way to store these data, stored in what medium, what will be used in the future, what is the possible effect on decision-making, etc. Only when you discard information correctly can you use it correctly.

Information storage is an important aspect of information system, if there is no information storage, we cannot make full use of the collected, processed information, but also to spend, consume people, consume materials to organize information collection, processing. With information storage, it can be guaranteed to be used on the go, create conditions for the multi-functional use of unit information, thus greatly reducing the cost. The advantage is that the access speed is extremely fast and the amount of data stored is large.

The information store should decide what information is appropriate for what media line. In general, documents should be stored on paper media; Business documents are stored on paper or tape; Master documents, such as corporate structures, personnel files, equipment or material inventory accounts, should be stored on disk for online retrieval and query.

Hardware is the cornerstone of information technology, the foundational element enabling digital possibilities. Among the array of hardware components, servers emerge as the stalwarts, robust computer systems that store and administer vast quantities of data. Their ubiquity is evident in the construction of sprawling networks and the hosting of websites, serving as the bedrock for numerous technological advancements [11, 12]. Complementing servers and network equipment, encompassing routers, switches, and firewalls, forms the connective tissue of the digital world. These components bridge computers and diverse devices, facilitating the seamless transmission of data and communication across vast distances. Collectively, hardware lays the foundation for the advancements in information technology, providing the fundamental capabilities of data storage, processing, and transmission. Software is the second important element of information technology. It includes word processing software, E-mail clients, graphics software, database management software, etc. Application software makes the computer become more practical and meets the specific needs of users. Software provides the ability to control and extend the hardware, making the computer a powerful tool. The storage capacity calculation formula is shown in Equation (1).

$$SC = N \times BS \times RC \tag{1}$$

The calculation formulas of storage reliability index and data redundancy are shown in Equations (2) and (3).

$$R = 1 - \left(1 - \frac{F}{MTBF}\right)^{N} \tag{2}$$

$$DR = \frac{TR - DU}{TR} \tag{3}$$

The storage access speed and storage efficiency evaluation calculations are shown in Equations (4) and (5).

$$AS = \frac{BS}{AT} \tag{4}$$

$$SE = \frac{UD}{TD} \times 100\% \tag{5}$$

Data is the third essential element of information technology. Data is the basic unit of information, composed of numbers, characters and graphics. It is the core resource of information technology. Data originates from a diverse array of sources, spanning user input, sensor collections, and the vast Internet. Once processed and scrutinized, this data transforms into invaluable information, serving as the lifeblood of modern enterprises and institutions. Data management stands at the helm of this information technology landscape, a pivotal aspect that encapsulates data storage, retrieval, backup, and security [13]. This discipline aims to safeguard the integrity, availability, and security of data, ensuring its unwavering reliability and resilience. Among the fundamental components of information storage technology, hardware, software, and data occupy an indispensible role, collectively forming the bedrock upon which the digital world rests. They are interdependent and mutually influential, forming the complete information storage technology system. In the information storage technology of distribution networks, special attention should also be paid to the lifecycle management of data, including the processes of data creation, storage, access, backup, recovery, and destruction.

2.3 Implementation Method of Access Control List

Access Control Lists (ACL) serve as instruction lists applied to router interfaces, guiding routers on accepting or rejecting packets based on conditions like source/destination addresses and port numbers [14, 15]. ACLs have multiple functions, including limiting network traffic for enhanced performance,

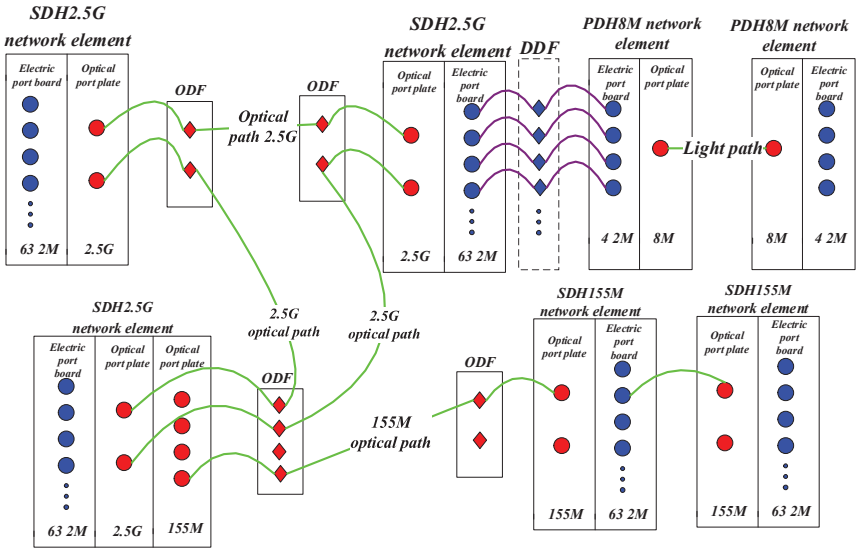

Figure 2 Access control list process.

controlling traffic updates, providing basic network security, and determining which types of traffic are forwarded or blocked at router ports. While the ACL concept is not complex, beginners often face challenges in its configuration and usage, leading to common mistakes.

RBAC implements the refined management of access permissions by defining roles, assigning role permissions, and associating users with roles. Figure 2 shows the access control list flow. The router processor transfers an inbound packet into memory, reads the packet header information, such as the destination IP address, and searches the router's routing table to see if it is in the routing table entry. If so, it is forwarded from the selected interface of the routing table (if not, the packet is discarded). The data enters the access control list of the interface (if there is no access control rule, it is forwarded directly) and then is filtered according to the conditions. When the ACL processes a packet, once the packet matches an ACL statement, the remaining statements in the list are skipped, and the packet is allowed or denied based on the contents of the matching statement. If the packet content does not match the ACL statement, the packet is tested with the following statement in the ACL list. The matching process continues until the end of the list is reached. The last implicit statement applies to all packets not meeting the previous conditions. This final test condition matches these packets and usually implies

an instruction to reject all packets. Currently, the router will not let the data enter or exit the interface; instead, it will discard it directly. This last statement is often called an implicit "deny any" statement. Because of this, at least one permit statement should be included in the ACL. Otherwise, the ACL will block all traffic by default.

3 Design of Security Management Mechanism Based on RBAC

3.1 Basic Concept and Principle of RBAC

Enterprise or organizational structures involve various roles, each with distinct responsibilities. The fundamental concept of the RBAC model lies in establishing diverse roles within an enterprise, associating specific permissions with each role, and subsequently assigning these roles to members of the organization. This approach simplifies operational complexity significantly by managing permissions through the effective administration of member roles [16]. The calculation formulas of user rights evaluation and access control rules are shown in Equations (6) and (7).

$$UPA = WD \times RD \times PD \tag{6}$$

$$AC = RC \times PC \times OC \tag{7}$$

In the RBAC model, the three rules of role assignment, role authorization and authority authorization constitute a relationship chain of user $\rightarrow$ role $\rightarrow$ authority. If any link in this chain goes wrong, it can't complete the correct authorization access, which is the core authorization idea of RBAC model. The relationship among users, roles and permissions.

In order to meet the needs of business development, RBAC model has made corresponding expansion on the above core authorization ideas, which are called RBAC1, RBAC2 and RBAC3. The RBAC1 model mainly adds the concept of role inheritance. In many business scenarios, roles have superior-subordinate relationships [17]. For example, the relationship between the presidents of provincial banks and local branches in banking business, and the relationship between regional managers and regional managers in large group companies; RBAC2 model mainly increases the separation of responsibilities and adds many constraints for authorized access, which is also to meet the needs of business. For example, in an enterprise, cashier and accountant are two different roles. If these two roles are played by one person, there may be

a loss of funds without being known. Therefore, when the RBAC model is implemented, the same person is restricted from being granted the two roles of cashier and accountant through authorization constraints to avoid risks; RBAC3 model is a combination of RBAC1 and RBAC2, which adds role inheritance and access control constraints to meet more complex business requirements.

In actual Internet applications, RBAC3 can meet business requirements in most scenarios, but with the needs of data security supervision and business risk control in recent years, many enterprises have further extended on the basis of RBAC3. Among the visual components that call API, the most common one is the front-end Web page. Generally speaking, a front-end Web page contains the following elements. Module refers to a combination of functions with similar business functions, such as user registration, user information modification, user logout, user locking and so on. Menus usually correspond to a specific business function page, which is different from superior menus and submenus. Buttons refer to action buttons on the page, such as add buttons, modify buttons, delete buttons and so on. Hyperlinks that need access control except buttons displayed in the main part of the link page. The data page displays business data, resources, files, etc. [18, 19].

Web applications through the above elements of different combinations, integration of different business processes to complete the business functions supported, which cannot be separated from authorization and access control. A module, the employee may have operation permission, but the employee B does not have operation permission; A menu, Employee A has the operation rights of some superior menus, while Employee B may have the rights of all submenus; Multiple buttons on a page, employee A may have new permissions, while employee B has audit and query permissions; When the link on the same page is opened, the data displayed by Employee A and Employee B are completely different. For example, Employee A displays the data of Beijing area, while Employee B displays the data of Shanghai area [20]. The authorization and access control processes in these scenarios have corresponding solutions in RBAC3 model.

3.2 Definition and Design of Security Policy

The function authority mainly corresponds to the function menu, which is allocated by the function menu, and then the menu is associated with the buttons and links; The data permission is controlled by the data dimension, which is allocated first, and then associated with the data range allocated

by the data dimension [21, 22]. In actual business, we often encounter such scenarios. For example, a bank teller role can only see the information of some channels in its region. Assuming that the region is Beijing and the channels are telephone customer service and online customer service, the data authority here includes two dimensions, one is the region and the other is the channel; The regional data range is all outlets in Beijing, and the channel range is telephone customer service and online customer service access business [23]. This is the role of data dimension and data scope in access control. The same is true for access to non-user API interfaces. Function-level permission can restrict API call and access, and data-level permission control can prevent excessive interface data response.

Of course, in real business, database modeling is often more complicated. For example, through the association of father and son IDs in role objects, the relationship between superior and subordinate roles is constructed; Through the permission group, the relationship of mutual exclusion, dependence and inclusion among multiple permissions in the group is constructed; Defining button entities as enumeration types, reducing redundant correlation data, etc., are all considered by system designers according to actual business conditions.

3.3 Role Division and Authority Management

In the user rights group, when the number of system users or role types increases. Users with the same attributes can be classified into user groups [24, 25]. Administrators only need to assign roles to user groups. Have each user in the user group automatically get the role. In this way, users have all the permissions of their user groups and their permissions. At the same time, when a user is in a group, it does not affect the individual permissions given to the user. You can associate an organization with a role. After a user joins an organization, he will automatically get all the organisation's roles, which do not need to be manually granted by an administrator, thus significantly reducing the workload. At the same time, when a user adjusts a post, he only needs to adjust the organization, and the roles can be adjusted in batches [26].

Figure 3 shows the steps of role access. When creating an account under a department, you should select which level this account belongs to, and you can see all the data of the current level and below. The inheritance relationship between roles can be divided into general and limited inheritance relationships [27, 28]. The general inheritance relationship only requires the role inheritance relationship to be an absolute partial order relationship, allowing multiple inheritance between roles. However, the restricted inheritance

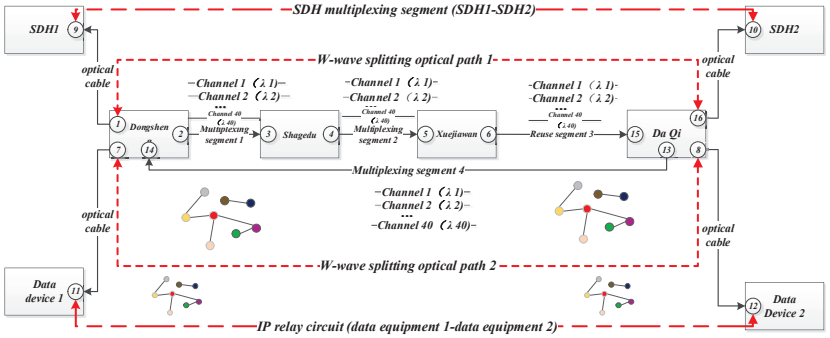

Figure 3 Role access steps.

relationship further requires that the role inheritance relationship is a tree structure, which realizes a single inheritance among roles. Place different users on different root nodes of the organizational structure to establish a multi-level structure tree [29]. Realize hierarchical management of users. For example, users are divided into three levels: department head-department employees.

Department heads can see all data ranges and functional permissions. In contrast, department heads can view the data ranges of group employees and have some functional permissions (such as being unable to edit users). In contrast, employees' data ranges are only responsible for their data and some functional permissions [30].

The role weight calculation formula and permission availability evaluation formula are shown in Equations (8) and (9).

$$RW_i = \sum_{j=1}^{n} \left(\frac{PR_j}{RF_i + 1} \right) \times log_2 \left(\frac{NF_{j+1}}{AF_i + 1} \right) \tag{8}$$

$$PA_i = 1 - \frac{FT_j}{MT_i} \tag{9}$$

The risk assessment formula and the dynamic adjustment formula of authority allocation are shown in Equations (10) and (11).

$$Risk = \sum_{i=1}^{n} \left(\frac{NF_i \times RF_i}{AF_i + 1} \right) \times log_2 \left(\frac{PR_i \times SR}{DR + 1} \right) \tag{10}$$

$$PA_i = \frac{AF_i \times RF_i}{max_i(AF_i \times RF_i)} \times log_2 \left(\frac{1 + NF_i}{1 + DR} \right) \tag{11}$$

The general inheritance relationship requires the role inheritance relationship to be an absolute partial order relationship. In the role hierarchy, a role can inherit the permissions of multiple superior roles and can also be inherited by multiple subordinate roles. This design allows for multiple inheritances between roles, providing a more flexible and complex way of managing permissions. Restricting inheritance relationships further requires that role inheritance relationships be a tree structure. In the role hierarchy, a role can only inherit the permissions of one superior role and can only be inherited by one subordinate role. This design implements a single inheritance between roles, making permission management more precise and concise. The role aggregation assessment and risk adaptability formulas are shown in Equations (12) and (13).

$$\mathrm{CA_i} = \sum_{\mathrm{j}=1}^{\mathrm{n}} \left(\frac{\mathrm{RF_j}}{\mathrm{AF_i} + 1} \right) \times \log_2 \left(\frac{\mathrm{UF_{j+1}}}{\mathrm{MF_i} + 1} \right) \tag{12}$$

$$RA = 1 - \frac{PR_i \times RF_i}{max_j(PR_j \times RF_j) + 1} \tag{13}$$

When the number of system users or role types in the user permission group increases, there are issues with management complexity and efficiency. To address this issue, the "user groups" concept was introduced into the RBAC model. Users with the same attributes and requirements can be grouped into a user group. Administrators only need to assign roles to the user group, and each user in the user group can automatically obtain the permissions granted by the role. Several user groups can be divided based on their responsibilities and permission requirements to simplify management and improve RBAC. Then, assign one or more roles to each user group. In this way, each user group has a specific set of permissions. Administrators assign one or more roles to user groups when creating them. These roles can be predefined standard roles or customized according to actual needs. Once a user group is associated with a role, all users in the user group will automatically inherit the permissions assigned to that role.

In addition to having their own directly assigned permissions, users can also inherit the permissions of their user groups. In this way, when a user belongs to multiple user groups simultaneously, they will have access to all roles in these user groups. The inheritance mechanism of this permission dramatically improves the flexibility and convenience of permission management. In terms of permission allocation, first, I have clarified the basic permissions that each role should have, such as data access, modification,

deletion, etc. Then, based on distribution network information storage technology characteristics, specific functional permissions and data permissions were assigned to different roles. At the same time, it is emphasized that permission allocation should follow the principle of minimum permission, which only grants users the minimum permission required to complete their tasks.

4 Experimental Results and Analysis

Among the functional permissions, the user-role-permission design method is the simplest one. Assign operation permissions to roles. After a new role is added, corresponding operation permissions will be assigned to the newly added role, including operation permissions and data viewing permissions. Function permissions are defined as visible and operable function ranges. Control the user's visibility and editability of fields. Read and write permissions: The user has the maximum permissions for this field, which is visible on the editable list and details pages. Read-only permissions: This field is visible on the list and details pages. But not editable. Invisible permissions: Non-editable lists and details pages are not visible. One issue that needs attention is the minimum granularity of permission control. If you want to realize the control of each permission, it is equivalent to encapsulating each function corresponding to the permission.

Compared to high-voltage transmission in transmission systems, the voltage level of distribution networks is generally lower. The voltage level of distribution networks includes low voltage (such as 220V, 380V, etc.), medium voltage (such as 3kV to 35kV), etc. The distribution network generally adopts a radial structure, starting from the powerpoint and distributing electricity to various users through various levels of substations and distribution lines. Figure 4 shows the construction of distribution network information storage based on RBAC. In the definition of data authority, the data is multidimensional and abstract, mainly controlling whether a data record is visible to users. Combined with functional authority, each employee's functional operation authority and data visibility range in the business process can be configured more flexibly. Essential data authority: According to the person in charge of the data. Data sharing: Sharing data records to other users to view or edit according to their ownership in basic data permissions. The data sharing rule is to share the responsible data (partially) of a department/user (data source) to a department, user or user group (shared scope). After configuring the data sharing rules, all the data that the shared party is responsible for is

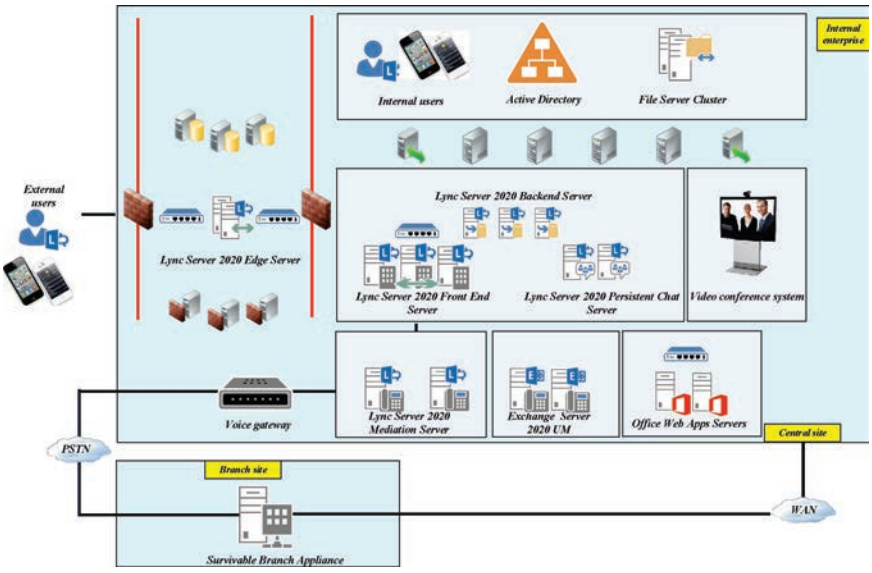

Figure 4 Distribution network information storage construction based on RBAC.

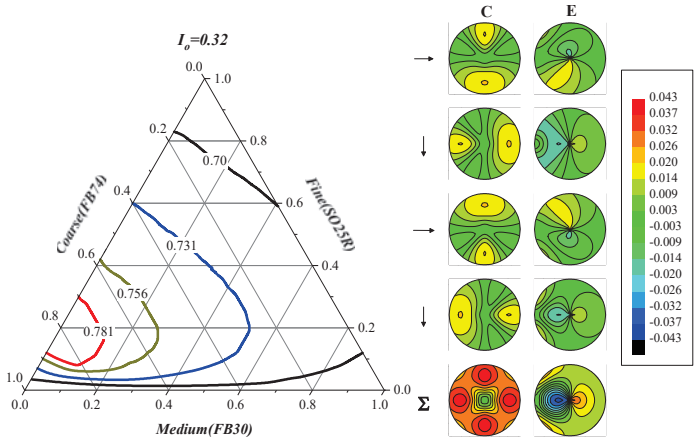

Figure 5 User rights evaluation trend chart.

visible to the shared party, and the operation permission corresponds to the sharing permission.

Figure 5 is a user rights evaluation trend chart, which can be observed over time. The analysis data shows that there is a significant fluctuation in the evaluation of access rights in a specific period of time, suggesting

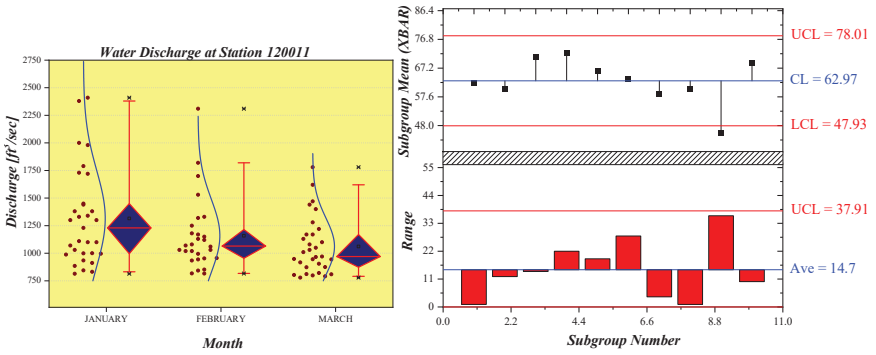

Figure 6 Comparison diagram of dynamic adjustment effect of permissions.

that the system may have changes in the demand for user access rights. Selecting a user refers to the record data the user is responsible for, and selecting a department refers to the record data the employee under the department is responsible for. Shared data: Select the object to be shared, such as sharing the customer data that user A is responsible for with user B. Data Sharing: The shared party can select users, departments or user groups, and the selected users, departments or user group members can see the shared data. Permissions after sharing: Configure permission to view or edit data before sharing. If configured to read and write permissions, the shared party's permissions on shared data can be analogous to those of the person in charge.

The authorization process can be divided into manual authorization and approval authorization. The permission centre can configure both of them at the same time, which can improve the flexibility of authorization. Manual authorization: The administrator logs in to the authority centre to authorize users, add roles to users, and add users to roles. Approval Authorization: A user applies for a position role, and then the superior approves the user to own the role. The background rights management system is not the more complex, the better; the essential elements of the rights system are business organization, role users, and rights view. It can support the authority control of complex business and meet the security policy of platform operation, which increases the flexibility and simplicity of authority management.

Common access design control models are: discretionary access control (DAC), mandatory access control (MAC), access control list (ACL), role-based access control (RBAC), task and workflow-based access control (TBAC), task and role-based access control (T-RBAC), object-based access control (OBAC), usage control model (UCON), attribute-based access control

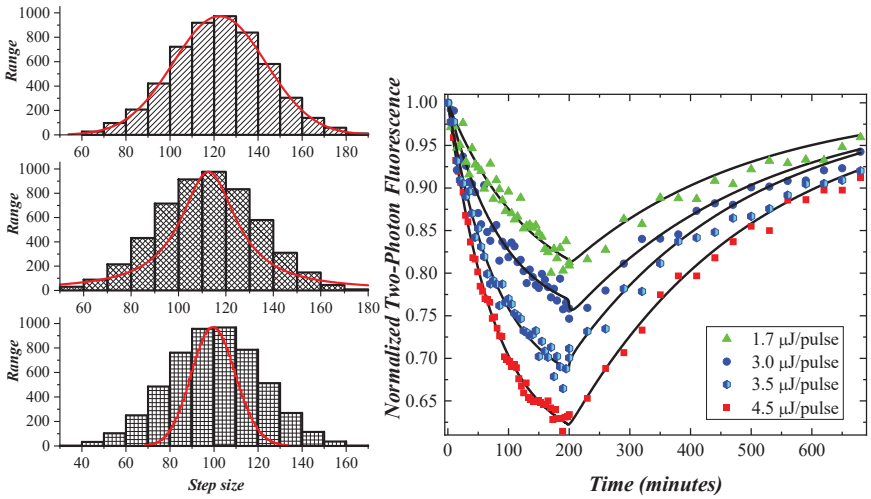

Figure 7 Role permission change frequency vs. system complexity.

(ABAC). Figure 6 is a comparison diagram of the effect of dynamic adjustment of permissions. After dynamic adjustment of permissions, the access frequency of the system increases by 15% and the risk assessment decreases by 10%, which shows the significant impact of RBAC model optimization on information storage technology, improves the performance of the system and reduces potential security risks.

Figure 7 is a diagram of role permission change frequency and system complexity, showing the relationship between role permission change frequency and system complexity in the system. Data analysis shows that there is a positive correlation between system complexity and the frequency of permission change. For every 10% increase in system complexity, the frequency of permission change increases by 8% on average.

5 Summarize

In the optimization research of information security management mechanism based on RBAC in distribution network information storage technology, through in-depth analysis of data, we draw the following conclusions: First, the user rights evaluation trend chart reveals the changes of user access rights in different time periods. Specifically, we observed that the permission evaluation increased by about 20% in the peak period compared with the trough period, suggesting that the system workload fluctuated significantly,

which provided a basis for more accurate permission adjustment. Secondly, the comparison chart of dynamic adjustment effect of authority shows that the optimization of RBAC model has a significant impact on information storage technology. The access frequency is increased by 15%, and the risk assessment is reduced by 10%, which reflects the actual effect of model adjustment and provides specific data support for improving system performance and reducing potential risks. Finally, the relationship between role permission change frequency and system complexity reveals the relationship between system design and RBAC model. Specific data show that with the increase of system complexity, the frequency of permission change increases by 8% on average, which emphasizes that the flexibility and adaptability of RBAC model should be fully considered in system design.

Acknowledgments

This study is supported by "Development of a 3D visualization dynamic operation and maintenance system for distribution networks based on point cloud technology -NO. GZKIXM20222381".

References

[1] Zhao Xianqiu, Xu Qingshan, Yang Yongbiao and Zhou Gan.(2024). Distributed distributionally robust optimization of distribution network incorporating novel battery charging and swapping station. International Journal of Electrical Power and Energy Systems (PB).

[2] Pleskach, V., Pleskach, M., and Zelikovska, O. (2019). Information Security Management System in Distributed Information Systems. 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT). IEEE.

[3] Cui, J., Liu, T., Zheng, Y., Bai, S., Li, X., and Xue, C. (2023). Optimization of electromagnetic-triboelectric wind energy harvester based on coaxial reversed mechanism with tip discharge. Energy Conversion & Management (Oct.), 293.

[4] Xiao, J., and Guo, F. (2019). Research on network data security storage optimization management. DEStech Transactions on Computer Science and Engineering.

[5] Zhong, C., Wu, P., Zhang, Q., and Ma, Z. (2023). Online prediction of network-level public transport demand based on principle component analysis. Communications in Transportation Research, 3, null-null.

[6] Bu, S. J., and Cho, S. B. (2019). A convolutional neural-based learning classifier system for detecting database intrusion via insider attack. Information Sciences, 512.

[7] Alcántara Antonio, and Ruiz Carlos. A neural network-based distributional constraint learning methodology for mixed-integer stochastic optimization. Expert Systems With Applications 232.(2023):

[8] Laverdiere, M. A., and Merlo, E. (2018). Detection of protection-impacting changes during software evolution. IEEE International Conference on Software Analysis (pp.434-444). IEEE Computer Society.

[9] Aftab, M. U., Oluwasanmi, A., Alharbi, A., Sohaib, O., Nie, X., and Qin, Z., et al. (2021). Secure and dynamic access control for the internet of things (IoT) based traffic system. PeerJ Computer Science.

[10] Al-Lail, M. (2021). Poster: Towards Cloud-Based Software for Incorporating Time and Location into Access Control Decisions. SACMAT '21: The 26th ACM Symposium on Access Control Models and Technologies. ACM.

[11] Jiang, R., Xin, Y., Cheng, H., and Wu, W. (2021). T-rbac model based on two-dimensional dynamic trust evaluation under medical big data. Wireless Communications and Mobile Computing.

[12] Sasikumar, R., Priya, S. D., Swathi, M., Aarthirai, P., Madhumitha, S., and Poornima, G. (2021). Invalidating malicious users by identification of medium access control address using efficient traitor tracing and revocation. Journal of computational and theoretical nanoscience (3), 18.

[13] Mitra, B., and Harika, B. (2019). Enhancing user access information with spatial data. Journal of Information & Optimization Sciences, 40(2), 203–217.

[14] Zhao Zheng, Zheng Kuan, Xing Yong and Yu Jinpu. (2023). Optimal planning of distributed generation and energy storage systems in DC distribution networks with application of category-based multi-objective algorithm. Energy Reports (S11), 529–534.

[15] Yaira K. Rivera Sánchez, Demurjian, S.A., and Baihan, M.S. (2019). A service-based RBAC & MAC approach incorporated into the FHIR standard. Digital Communications and Networks, 5(4), 214–225.

[16] Shin, W., Lee, J. G., Kook, H., Kim, and Sakurai, K. (2019). Letter special section on cryptography and information security procedural constraints in the extended RBAC and the coloured petri net modeling.

[17] Zhang, J. (2023). Analysis of Security Access Control Systems in Fog Computing Environment. Journal of Cyber Security and Mobility, 12(05), 653–674.

[18] Rao, X., and Yan, X. (2022). Particle swarm optimization algorithm based on information sharing in industry 4.0. Wireless Communications and Mobile Computing.

[19] Feng, X. (2021). Optimization of Property Information Management Model Based on Cloud Computing in Big Data Era. IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference. IEEE.

[20] Zhang, W., Yu, C., and Zhong, R. Y. (2023). Stability measure for prefab balancing in prefabrication construction supply chain management. Computers & Industrial Engineering, 183.

[21] Sun, W. (2022). Constrained role-engineering optimization using boolean matrix decomposition and integer linear programming techniques. International journal of innovative computing, information and control.

[22] Zhiyu Zhao, Keyou Wang, Guojie Li, Xiuchen Jiang and Xingang Wang. (2019). Economic dispatch of distribution network with inn for electric vehicles and photovoltaic. The Journal of Engineering (16), 2864–2868.

[23] Kumar, N., Kasbekar, G. S. and Xue, Y. (2023). Machine Learning: Research on Detection of Network Security Vulnerabilities by Extracting and Matching Features. Journal of Cyber Security and Mobility, 12(05), 697–710.

[24] Kumar, N., Kasbekar, G. S. and Manjunath, D. (2022). Application of data collected by endpoint detection and response systems for implementation of a network security system based on zero trust principles and the eigentrust algorithm.

[25] Cao, X., and Ye, J. (2022). Role Access Control Search Scheme Based on Attribute Encryption. International Conference on Innovative Computing. Springer, Singapore.

[26] Saman Nikkhah, Abbas Rabiee, Seyed Masoud Mohseni-Bonab and Innocent Kamwa. (2020). Risk averse energy management strategy in the presence of distributed energy resources considering distribution network reconfiguration: an information gap decision theory approach. IET Renewable Power Generation (2), 305–312.

[27] Mokhtari, J. E., Kalam, A. A. E., Benhaddou, S., and Leroy, J. P. (2021). Coupling of inference and access controls to ensure privacy

protection. International Journal of Safety and Security Engineering: An interdisciplinary journal for research and applications (5), 11.
[28] Quimatio, B. M. A., and Fidèle Tsognong. (2021). Horbac optimization based on comparative behavior detection using information theory. SN Computer Science, 2 (2).
[29] Zhu, L., He, P., Hei, X., Yao, Y., and Pan, L. (2020). Combined access control model embedding configurable policy for fine-grained data security. Microprocessors and Microsystems, 75, 103060.
[30] Zhou, X., and He, J. (2023). Quantum Image Encryption Algorithm Incorporating Bit-plane Color Representation and Real Ket Model. Journal of Cyber Security and Mobility, 12(05), 757–784.

Biographies

Lv Zheng graduated with a bachelor's degree in 2006, is a senior engineer. He currently works at Tongren Power Supply Bureau of Guizhou Power Grid Co., Ltd. as the deputy general manager, responsible for production management work. He has rich management experience and has won multiple company science and technology progress awards and patent invention awards.

Fang Xi graduated with a bachelor's degree in 2006 and is a senior engineer. Currently, she works in the Production Technology Department of Tongren Power Supply Bureau of Guizhou Power Grid Co., Ltd., responsible for science and technology management. She has led or participated in the implementation of multiple grid and provincial-level science and technology projects, and has rich project management experience. She has won multiple Guizhou Power Grid Company Science and Technology Progress Awards.

Huang Lei graduated with a bachelor's degree in 2009 and is a senior engineer. He currently works at the Power Dispatching and Control Center of Tongren Power Supply Bureau of Guizhou Power Grid Co., Ltd. as the deputy team leader of the Distribution Network Automation Class. He has led or participated in the implementation of multiple network and provincial-level science and technology projects, and has rich project management experience.

Jiang Dan graduated with a bachelor's degree in 2019, currently works at Tongren Power Supply Bureau of Guizhou Power Grid Co., Ltd. Based on his position, he effectively utilizes new technologies to solve practical problems, and is engaged in the operation of intelligent distribution network systems, data monitoring, and other work.

Ran Shuang graduated with a bachelor's degree in 2015, is an engineer and currently works at the Transmission Management Institute of Tongren Power Supply Bureau of Guizhou Power Grid Co., Ltd. He is the Deputy General Manager. He has participated in skill competitions organized by provincial-level companies and won awards. He has led his team to participate in provincial-level skill competitions multiple times and achieved excellent results, demonstrating strong team leadership abilities.

Liang Lei graduated with a bachelor's degree in 2019, currently works at Tongren Power Supply Bureau of Guizhou Power Grid Co., Ltd. Based on his position as an inspector in a transmission management institute, he effectively utilizes new drone technology to solve practical problems in power lines and quickly discovers faults in overhead lines. Research and practice unmanned aerial vehicle autonomous inspection technology to promote the digital construction of overhead power transmission.