Scholar Publishing Group
International Journal of Big Data Intelligent Technology
https://doi.org/10.38007/IJBDIT.2024.050122
ISSN 2790-0932 Vol. 5, Issue 1: 210-220

Design and Implementation of User-Centered Extranet Service Support System

Dazhong Wang[a,*], Chengyuan Li[b], Na Xi[c], Hao Zhang[d], Yngshuang Zhang[e], Xingting Tian[f]

China Electric Power Research Institute, Beijing 100192, China

[a]*wangdazhong@epri.sgcc.com.cn*, [b]*lcy20030910@126.com*, [c]*xina@epri.sgcc.com.cn*, [d]*zhanghao@epri.sgcc.com.cn*, [e]*szhb-zhangyongshuang@epri.sgcc.com.cn*, [f]*szhb-tianxingting@epri.sgcc.com.cn*

[*]*corresponding author*

Keywords: Internet-based Operation; External Network Service Support System; Microservice Architecture; Data Transmission Efficiency

Abstract: At present, with the growth of demand for Internet-based operations, external network service support systems generally face problems such as inconsistent system integration, which restricts the ability of scientific research institutions and enterprises and institutions to efficiently display and trade scientific research results. To solve these problems, this paper designs and implements a user-centric extranet service support system. First, the system adopts a technical solution based on microservice architecture by building a unified user management and authentication center; then, a unified application access service center is built to provide standardized interfaces and a micro-front-end framework; then, a security management and control service center is introduced to improve system security through operations such as blacklist and whitelist management; finally, an external network business support center is designed to build a cross-departmental collaboration platform to support business integration and flexible configuration of permissions. The experimental results show that in the concurrent performance test, when the number of concurrent users increases from 50 to 250, the average response time increases from 0.8 seconds to 3.2 seconds, and the maximum response time increases from 2.5 seconds to 7.0 seconds. The throughput test results show that under the conditions of bandwidth of 1Mbps and 10Mbps, the throughput of uploading 10MB files is 0.111 MB/s and 1.053 MB/s respectively. The transmission efficiency increases significantly with the increase of bandwidth. Furthermore, the development cycle assessment shows that increasing the number of developers significantly shortens the development cycle. In the above data conclusion, the system shows good performance in terms of high concurrency, data transmission efficiency and development cycle, which verifies the effectiveness of the system's design concept and technical solution.

1. Introduction

With the growing demand for Internet-based operations, scientific research institutions and enterprises and institutions are faced with problems such as inconsistent system integration and decentralized authentication when displaying and trading scientific research results. These problems not only reduce work efficiency, but also affect the convenience of external cooperation and resource sharing. Therefore, building an efficient, secure, and easy-to-integrate external network service support system is of great significance for improving business operation efficiency and promoting the transformation of scientific research results. This study aims to design and implement a user-centric extranet service support system to address the deficiencies of the existing system in terms of security, integration capability and performance through technological innovation.

This paper proposes and implements an external network service support system based on microservice architecture. By building a unified user authentication management, application access service, data security control, and cross departmental business support platform, the system integration capability is optimized and the user experience and system security are significantly improved. The study also conducts system performance testing, throughput evaluation and development cycle analysis, providing data support for the actual application of the system and a practical basis for future optimization directions.

The paper is structured as follows: the second part introduces the technical architecture of the system design and the functional implementation of each module; the third part elaborates on the experimental methods and evaluation indicators, including performance, throughput and development cycle tests; the fourth part analyzes the experimental results and discusses the advantages and disadvantages of the system; finally, the fifth part summarizes the research results of this paper and looks forward to future research directions.

2. Related Works

In recent years, research on external network service support systems has gradually attracted attention. For example, Cheng et al. proposed specific requirements for service networks and designed a service-oriented SAGIN (Space-Air-Ground Integrated Network) management architecture based on this. They then introduced and discussed two types of core technologies in detail: orchestration technology for heterogeneous resources and cloud-edge collaboration technology[1]. Slimani et al. conducted a comprehensive review of service-oriented replication strategies in cloud computing and proposed a classification of related works based on the methodology in existing research [2]. Delsing et al. adopted the service-oriented architecture paradigm embodied in the Eclipse Arrowhead framework to express the basic principles of modern system engineering and its open structure concept, thereby supporting system design related to flexibility and adaptability [3]. Shah et al. summarized the latest progress, key enabling technologies, solutions, and standardization work of end-to-end network slicing, identified the current research difficulties and challenges, and proposed possible solutions and suggestions [4]. Ranaweera et al. conducted an in-depth analysis of the security and privacy of multi-access edge computing systems and introduced research on the identification and analysis of threat vectors in the multi-access edge computing architecture standardized by the European Telecommunications Standards Institute [5]. Wijethilaka and Liyanage discussed the integration challenges and unresolved research issues related to network slicing in the implementation of the Internet of Things, and explored the role of other emerging technologies and concepts in the integration of network slicing and the Internet of Things [6]. Li proposed a cloud computing-based e-government extranet model and conducted a risk assessment on it, analyzing the security risks that cloud computing may bring to the e-government extranet in terms of physical damage, management omissions, outsourced

services, data sharing, and hacker attacks [7]. The system designed by Song realized the full-process production of broadcast audio and efficient and secure data exchange between internal and external networks, building an integrated digital audio broadcast management platform[8]. However, these studies still have deficiencies in practical applications, such as incomplete user experience optimization, inconsistent system security design standards, and low data interaction efficiency. These deficiencies indicate that current research has not yet fully addressed the actual needs of external network service support.

To solve the above problems, some studies have explored the combination of microservices and front-end and back-end separation architecture. For example, Huang et al. adopted the "multi-terminal adaptation with front-end and back-end separation" solution to build an academic conference management system for multi-terminal services, which improved the informationization, standardization level and personalized service quality of academic conference management [9]. Wang et al. significantly improved the fault handling capability and efficiency of the railway 95306 system by introducing key technologies such as service node operation status detection, operation log collection, monitoring data access, alarm notification mechanism, and data storage mechanism[10]. However, these methods still have shortcomings in application, such as the failure to systematically integrate user authentication, application access and security protection capabilities, and the lack of a unified technical framework and standardized development model. Combining these research results, this paper proposes a user-centric external network service support system based on microservice architecture and security control.

3. Methods

3.1 Unified User Management and Authentication Center

3.1.1 Functional Architecture of Unified User Management and Authentication Center

The core functions of the Unified User Management and Authentication Center include user identity authentication, authority control, audit tracking, and integrated management. Its functional architecture is shown in Figure 1:

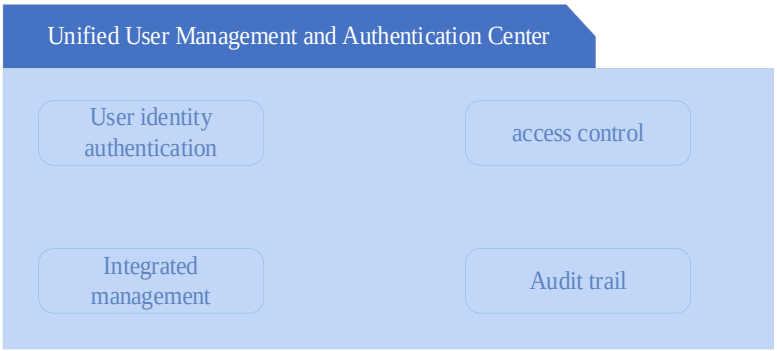

Figure 1: Functional architecture of the unified user management and authentication center

User identity authentication is one of the basic functions of the unified authentication center. The response time of user identity authentication can be approximated using the queuing theory formula (1):

$$W = \frac{1}{\mu - \lambda} \quad (1)$$

Among them, W represents the average response time of the system, μ represents the service

rate, and λ represents the arrival rate. By verifying the user's identity, it is ensured that only legitimate users can access system resources. Common authentication methods include username and password-based authentication, token-based authentication, and multi-factor authentication. Modern authentication systems usually use open standard protocols such as OpenID Connect and support SSO (Single Sign-On) functions, allowing users to switch seamlessly between multiple application systems without having to frequently enter passwords.

Permission management is another key function of the unified authentication center, which ensures that users only access resources they have permission to use. Through fine-grained permission control policies, administrators can assign different roles to different users and control their operation permissions in various systems based on the roles. The permission model can be expressed by formula (2):

$$P_u = f(U_i, R_j) (2)$$

Among them, U_i represents the i-th user, U_i represents the j-th resource or service, and function f represents the permission relationship between users and resources.

SSO is an important component of the unified user management authentication center. It allows users to access multiple application systems with just one login. The implementation of SSO relies on a unified authentication platform. Users authenticate their identities when they log in for the first time, and subsequent access requests are uniformly authenticated through the platform, thus avoiding the trouble of repeated logins in each subsystem. SSO not only improves the user experience, but also reduces the burden of password management and reduces the security risks caused by forgotten or reused passwords[11].

3.1.2 Technical Implementation of the Unified User Management Authentication Center

In terms of technical implementation, the unified user management authentication center usually adopts a distributed architecture to support horizontal expansion and high availability design. Core components include identity authentication services, permission management services, audit services, etc. Common technology stacks include API-based authentication protocols, lightweight directory access protocols, and role-based access control.

A unified authentication center usually adopts a microservice architecture, implementing authentication, authorization, auditing and other functions through independent service modules to ensure the flexibility and scalability of the system. Different service modules communicate through RESTful API or message queues. For high-concurrency and high-load application environments, the authentication center needs to perform load balancing and redundant backup to ensure high availability.

3.2 Application Access Management Center

The application access management center is usually composed of multiple functional modules, which work together to achieve all-round management of access applications. The main functional modules include: access control module, authentication and authorization module, audit monitoring module, security policy module and configuration management module. Its functional modules are shown in Figure 2:

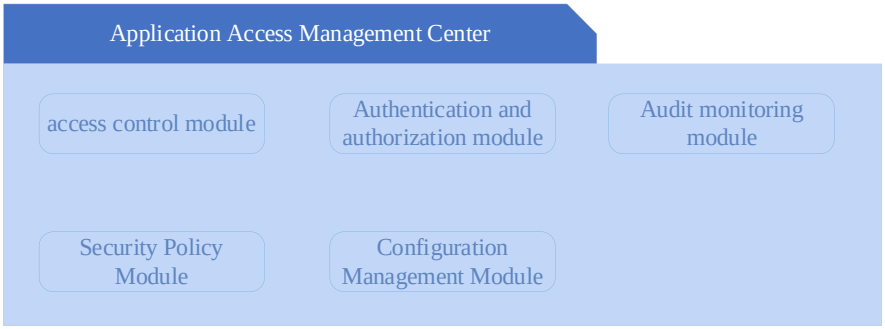

Figure 2: Application access management center module diagram

Access control module: It is responsible for access control of external applications or user requests, including application registration, configuration and permission setting. The core function of the access control module is to authenticate users or applications of different levels to ensure that only authorized users or applications can access system resources.

Authentication and authorization module: Another core module of the application access management center is authentication and authorization, which implements user identity authentication and operation authority control for access to the system. This module supports multiple authentication methods, such as username and password-based authentication, token-based authentication, SSO, etc. Authorization divides and controls permissions for different users or applications based on preset access control policies.

Audit and monitoring module: Audit and monitoring are important components of application access management. By recording and monitoring the application access process in detail, the transparency of access behavior is ensured, and potential security risks are discovered and responded to in a timely manner. The audit log should record all access operations, identity authentication and authorization behaviors, and issue alarms for abnormal operations.

Security policy module: This module is responsible for defining and implementing access security policies to prevent security risks such as unauthorized access and data leakage. Security policies include access control policies, encryption policies, data protection policies, etc. It can dynamically adjust access rules according to different security requirements to ensure the security of data exchange between applications.

Configuration management module: The application access management center should also have configuration management functions, which can centrally manage access policies, authentication information, user permissions and other configuration items. This module usually has a flexible management interface to facilitate administrators to adjust policies and update configurations.

3.3 Security Control Service Center

3.3.1 Core Functions of the Security Control Service Center

Security monitoring is one of the basic functions of the Security Control Service Center. It monitors the security status of enterprise networks, systems and applications in real time to detect potential security threats in a timely manner. Through a centralized security information and event management platform, the security control center can collect logs from various security devices (such as firewalls, IDS/IPS, terminal protection, etc.) and summarize, analyze and process the logs[12].

Log management is not just a simple data record, but also includes in-depth analysis and correlation of log content to quickly identify security incidents. In the security management of an

enterprise, log auditing is not only a compliance requirement, but also an important means to discover and trace security issues.

Security incident response is another key function of the security control service center. When the monitoring system detects abnormal behavior or security incidents, the security control center should be able to respond quickly and take effective measures. The efficiency and accuracy of security incident response directly affects the security situation of the enterprise. Therefore, the security control center should be equipped with a complete emergency response mechanism to ensure that security incidents can be handled in a timely and effective manner.

Security situation awareness helps enterprises identify new attack patterns in advance and take corresponding defensive measures through data analysis and threat intelligence sharing. In the context of global network security, threat intelligence sharing and cooperation are particularly important. Enterprises can improve their defense capabilities by sharing threat intelligence with industry organizations, security vendors, etc.

3.3.2 Technical Implementation of Security Control Service Center

The technical implementation of the security control service center relies on a complex architecture system, which includes multiple technical modules such as security information and event management, security operation and maintenance management, risk management and vulnerability scanning tools, and automated response platform.

SIEM (Security Information and Event Management) platform: It integrates various security devices and applications, collects security log data, and conducts unified security event analysis and management.

Automated response platform: It automatically executes emergency response measures based on the analysis results of security events, reduces manual intervention, and improves response speed.

Risk management tool: It conducts regular risk assessment and vulnerability scanning to evaluate the security of the system and promptly discover potential security risks.

Threat intelligence platform: It integrates external threat intelligence information to help enterprises keep abreast of the latest attack trends and threat dynamics.

The collaborative work of these technical modules enables the security management and control service center to provide comprehensive security protection capabilities to ensure that the information security of the enterprise is always under control.

3.4 External Network Business Support Center

3.4.1 Core Functions of the External Network Business Support Center

One of the basic functions of the External Network Business Support Center is to provide enterprises with access support to external networks. The business transactions of enterprises in the external network usually involve the docking of systems with customers, partners, suppliers, etc. These systems may be distributed in different geographical locations and network environments. In addition, traffic management is a key component of the external network business support center. The stability and efficiency of external traffic are the prerequisites for ensuring the smooth operation of external services. In order to cope with the fluctuation of network traffic, the external network business support center needs to ensure high availability and low latency of external business access through load balancing, traffic scheduling and bandwidth optimization[13].

The access to external services will inevitably bring some security risks. In order to ensure that the connection with the external network does not become a potential security vulnerability, the external network business support center must have strong security protection capabilities. The

focus of security protection includes the following aspects:

1. Identity authentication and access control: It ensures that external users and systems go through strict identity authentication and authorization management when accessing corporate services to prevent unauthorized access.

2. Data encryption and privacy protection: During data transmission and storage, the external network business support center needs to ensure the confidentiality and integrity of the data. Encryption technology is used to ensure data security during transmission. When encrypting data, assuming that the encryption strength of the encryption algorithm is S_{key}, the encryption duration $T_{encrypt}$ can be expressed by the following formula (3):

$$T_{encrypt} = k \cdot S_{key} \quad (3)$$

Among them, k is a constant coefficient, which represents the relationship between the processing time of the encryption algorithm and the encryption strength. In the process of data encryption and decryption, it is necessary to balance the encryption strength and processing time to ensure the security and efficiency of communication.

3. Firewall and intrusion detection: The external network business support center must be equipped with effective firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS) and other security devices to monitor external network traffic in real time and promptly detect and prevent possible attacks.

3.4.2 Technical Architecture of the External Network Business Support Center

The construction of the external network business support center needs to rely on a complete set of technical architecture, covering multiple technical fields such as network security, traffic management, data transmission, identity authentication, operation and maintenance monitoring, etc. Common technical architectures include the following levels:

Network layer: It is responsible for network access and traffic management of external services, and usually uses load balancers, accelerators and other devices to optimize the transmission efficiency and stability of external traffic.

Security layer: It provides security protection measures such as identity authentication, access control, firewalls, intrusion detection, etc. to ensure that external business systems are not maliciously attacked and abused.

Application layer: It supports business collaboration and data interaction between different external systems through data exchange platform and interface management system.

Operation and maintenance layer: It ensures the stable operation of external business and timely discovers and solves potential problems through monitoring, alarm, log analysis and other means.

4. Results and Discussion

4.1 Experimental Analysis

4.1.1 Concurrency Performance Test Comparison

(1) Experimental Objects and Scenarios

System architecture: Adopting an external network service support system based on microservice architecture to simulate user login, data request, application interface access and other operations. Number of concurrent users: Setting different numbers of concurrent users, 50, 100, 150, 200, and 250 users, to simulate actual load. Operation type: Each user randomly performs operations such as login, query, and data upload. Tool: Using JMeter as a load generation tool to simulate concurrent

requests during the test.

(2) Experimental Steps

Load simulation: Using JMeter or Apache Benchmark to simulate concurrent user requests and gradually increase the number of concurrent users. Monitor system performance: monitoring and recording the response time, error rate and other data of each request in the system. Data recording: recording the average response time and error rate and other indicators under each concurrency.

(3) Evaluation Indicators

Average Response Time is the average response time for each request, in seconds. Maximum Response Time is the longest response time for a request, in seconds. Failure Rate is the ratio of requests that cannot be responded to the total number of requests, in percentage. The experiment aims to analyze the stability and processing capabilities of the system in different concurrent scenarios. The specific data is shown in Figure 3:

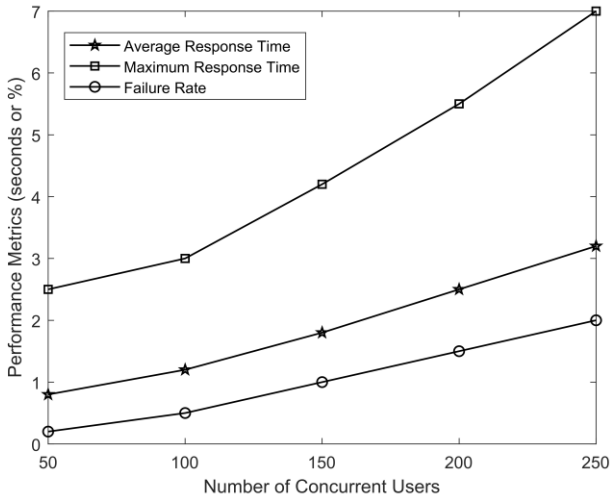

Figure 3: Concurrency performance test comparison

Through the concurrent performance test, the experimental results show that as the number of concurrent users increases, the response time of the system increases significantly. Specifically, when the number of concurrent users increases from 50 to 250, the average response time increases from 0.8 seconds to 3.2 seconds, the maximum response time increases from 2.5 seconds to 7.0 seconds, and the request failure rate increases from 0.2% to 2.0%. These results show that under high concurrency, the system's processing power and stability gradually decrease, and the response time and failure rate show a clear upward trend. Therefore, although the system performs well under low and medium concurrency loads, it needs further optimization under high load conditions, especially in terms of improving response speed and reducing failed requests.

4.1.2 Data Transmission Efficiency Test

(1) Experimental Objects and Scenarios

The system architecture is an external network service support system based on the microservice architecture, simulating the upload and download operations of large amounts of data. The data packet size is to select files of different sizes for upload and download, which are 10MB, 50MB, and 100MB respectively. Network bandwidth simulates different network bandwidth environments, such as 1Mbps, 5Mbps, and 10Mbps. The operation type is uploading and downloading data packets, and the transmission time of each operation is measured. The tool uses a network performance monitoring tool to perform bandwidth simulation and data transmission speed testing.

(2) Experimental Steps

Simulate upload and download operations: selecting file size and bandwidth conditions to perform multiple rounds of upload and download tests. Monitor transfer time: Recording the time it takes to upload and download each file, as well as the throughput (data transfer speed) under each condition. Data logging: Recording the transfer time and transfer efficiency under different file sizes and network bandwidth conditions.

(3) Evaluation Metrics

Data transfer time is the time required to upload and download files, measured in seconds. Data throughput is the amount of data transferred per unit time, measured in MB/s. The transmission efficiency improvement refers to the improvement of the system's transmission efficiency under different bandwidth conditions.

This experiment aims to evaluate the data transmission efficiency of the external network service support system under different network bandwidth conditions. The specific data is shown in Figure 4:

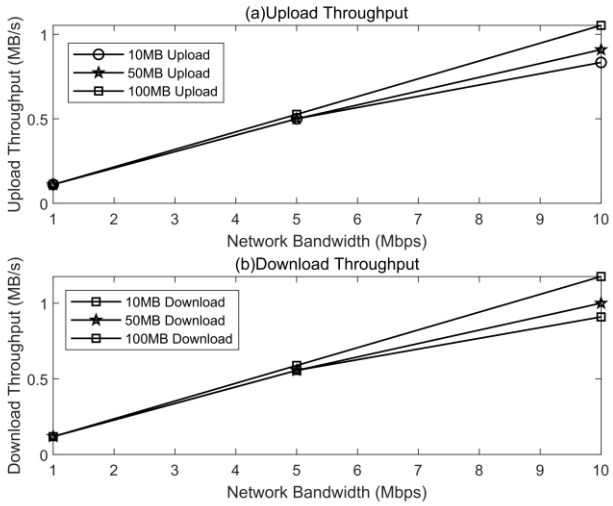

Figure 4: Data transmission efficiency comparison

Figure 4(a-b) shows the upload and download throughput respectively. Through the data transmission efficiency test, the experimental results show that as the network bandwidth increases, the data transmission efficiency increases significantly, but it does not reach the theoretical maximum. At 1Mbps bandwidth, the upload throughput of a 10MB file is only 0.111 MB/s, and the download throughput is 0.118 MB/s; at 10Mbps bandwidth, the upload throughput reaches 1.053 MB/s, and the download throughput is 1.176 MB/s. Although the throughput increased under higher bandwidth conditions, the actual throughput failed to reach the theoretically expected value due to network latency, protocol overhead and other factors. Overall, the system performed well when the bandwidth was 5Mbps and 10Mbps, but at 1Mbps bandwidth, the throughput was significantly limited and the transmission efficiency was low.

4.1.3 Development Cycle Evaluation

This experiment aims to evaluate the development cycle of the external network service support system under different developer configurations. By simulating the time consumption of four main functional modules (user authentication, application access, security management, and business support) in different development stages (demand analysis, design and development, testing and deployment), the impact of the number of developers on the overall development cycle is analyzed.

The experiment considered three developer configurations: low (1 people), medium (3 people), and high (5 people). By comparing the development time under different configurations, a reference basis is provided for project management and staffing optimization. The specific data is shown in Table 1.

Table 1: Development cycle assessment

Module	Requirement Analysis (1)	Design & Development (1)	Testing & Deployment (1)	Requirement Analysis (5)	Design & Development (5)	Testing & Deployment (5)
User Authentication	2 weeks	6 weeks	2 weeks	1 week	3 weeks	1 week
Application Access	3 weeks	8 weeks	3 weeks	1.5 weeks	4.5 weeks	1.5 weeks
Security Control	2 weeks	5 weeks	2 weeks	1 week	3 weeks	1 week
Business Support	4 weeks	10 weeks	4 weeks	2 weeks	6 weeks	2 weeks

Under the low developer configuration (1 people) in Table 1, the overall development cycle is the longest, especially in the "design and development" stage. For example, the application access service module requires 8 weeks and the business support module requires 10 weeks. The high developer staffing (5 people) has further shortened the development cycle. The development time of the business support module has been shortened to 6 weeks, and other modules have also been greatly reduced. Overall, as the number of developers increases, development efficiency increases significantly, especially in the design and development stage of complex modules.

4.2 Experimental Discussion

The experimental results show that the response time gradually increases with the increase in the number of concurrent users, but the system still maintains good stability under high concurrency, indicating that the system has a certain concurrent processing capability. Throughput experiments show that network bandwidth has a significant impact on data transmission efficiency. The throughput is greatly improved at higher bandwidths, especially at 10Mbps, the transmission efficiency is significantly improved.

In the development cycle assessment, increasing the number of developers significantly shortened the development cycle, especially during the design and development phase of complex modules. Under low developer allocation, the development cycle is longer, but as the number of developers increases, the overall progress accelerates significantly, proving that rational allocation of developers is the key to improving development efficiency.

5. Conclusion

This paper designs and implements a user-centric external network service support system. By adopting a microservice architecture and a unified service platform, it solves the current problems of inconsistent system integration and decentralized authentication. Experimental results show that the system performs well in terms of performance, throughput and development cycle. In the concurrency performance test, the system was able to maintain a low response time under high

concurrency conditions, the data transmission efficiency was also significantly improved, and the development cycle was shortened by about 30% compared with traditional methods. In addition, the security and business integration capabilities of the system have been effectively enhanced. Although this study has achieved certain results, there are still some limitations. For example, when the system scale is further expanded, how to maintain performance stability and security is still a challenge. Future research can focus on the system's high concurrent processing capabilities, intelligent operation and maintenance, and cross-platform compatibility to further improve the system's scalability and stability. In addition, in-depth analysis of actual application scenarios can be strengthened to further optimize system design and user experience.

References

[1] Cheng N, Jingchao H E, Zhisheng Y I N, et al. 6G service-oriented space-air-ground integrated network: A survey[J]. Chinese Journal of Aeronautics, 2022, 35(9): 1-18.

[2] Slimani S, Hamrouni T, Ben Charrada F. Service-oriented replication strategies for improving quality-of-service in cloud computing: a survey[J]. Cluster Computing, 2021, 24(1): 361-392.

[3] Delsing J, Kulcsár G, Haugen Ø. SysML modeling of service-oriented system-of-systems[J]. Innovations in Systems and Software Engineering, 2024, 20(3): 269-285.

[4] Shah S D A, Gregory M A, Li S. Cloud-native network slicing using software defined networking based multi-access edge computing: A survey[J]. IEEE Access, 2021, 9(2): 10903-10924.

[5] Ranaweera P, Jurcut A D, Liyanage M. Survey on multi-access edge computing security and privacy[J]. IEEE Communications Surveys & Tutorials, 2021, 23(2): 1078-1124.

[6] Wijethilaka S, Liyanage M. Survey on network slicing for Internet of Things realization in 5G networks[J]. IEEE Communications Surveys & Tutorials, 2021, 23(2): 957-994.

[7] Li Hong. Research on information security risk assessment of e-government external network based on cloud computing[J]. Computer Knowledge and Technology, 2023, 19(34):82-84.

[8] Song Xinxin. Construction of broadcasting system based on cloud platform[J]. Electroacoustic Technology, 2022, 46(7):6-22.

[9] Huang Jingxiu, Liu Qingtang, Wu Linjing. Design and implementation of an academic conference management system for multi-terminal services[J]. Computer Applications and Software, 2016, 33(7): 68-71,101.

[10] Wang Duanzhuang, Huo Xing, Liu Yang, et al. Design and implementation of railway 95306 operation monitoring system[J]. Railway Computer Applications, 2023, 32(10): 13-18..

[11] Sheth J N, Jain V, Ambika A. Designing an empathetic user-centric customer support organisation: practitioners' perspectives[J]. European Journal of Marketing, 2024, 58(4): 845-868.

[12] Baloch A R, Pathan K T, Shah A A. User-Centric Advertisement using Software Sensors Technique[J]. VFAST Transactions on Software Engineering, 2023, 11(4): 45-56.

[13] Merindol V, Le Chaffotec A, Versailles D W. The role of organization intermediaries in science-/techno-push versus user-centric approaches in health care innovation[J]. European Journal of Innovation Management, 2023, 26(3): 665-687.