Construction of a Unified Network Security Protection System for Headquarters and Branch Offices (Postprint)

Authors: Li Da Fan Jingsong

Date: 2025-07-09T00:00:00+00:00

Abstract

[Purpose] In the context of digital transformation, enterprise cybersecurity is facing unprecedented challenges. This paper aims to explore the construction of a unified, efficient, and reliable cybersecurity protection system to adapt to the constantly evolving network environment and meet the collaborative needs between headquarters and branch offices. [Methods] By analyzing the key factors affecting enterprise cybersecurity, a comprehensive solution is proposed, encompassing unified identity authentication and access control, distributed threat detection and response, centralized management and monitoring, as well as end-to-end encryption and data protection. [Results] Through the implementation of these strategies, enterprises can build a more robust and responsive cybersecurity protection system, effectively countering network threats and safeguarding data and assets. Conclusion Constructing a unified cybersecurity protection system for headquarters and branch offices requires not only technological innovation and application, but also corresponding adjustments and optimizations at the management level to address continuously evolving cyber threats.

Full Text

Preamble

Building a Unified Cybersecurity Defense System for Headquarters and Branch Offices

Li Da, Fan Jingsong
(Tongfang Knowledge Network Digital Publishing Technology Co., Ltd., Beijing 100192)

Abstract

[**Objective**] Against the backdrop of digital transformation, enterprise cybersecurity faces unprecedented challenges. This paper aims to explore the construction of a unified, efficient, and reliable cybersecurity defense system that adapts to the evolving network environment and meets the collaborative needs between headquarters and branch offices. [**Method**] By analyzing the key factors affecting enterprise cybersecurity, this paper proposes a comprehensive solution encompassing unified identity authentication and access control, distributed threat detection and response, centralized management and monitoring, and end-to-end encryption and data protection. [**Results**] Through the implementation of these strategies, enterprises can build a more robust and responsive security defense system that effectively counters cyber threats and safeguards data and assets. **Conclusion** Constructing a unified cybersecurity defense system for headquarters and branch offices requires not only technological innovation and application but also corresponding adjustments and optimization at the management level to address evolving cyber threats.

Keywords: enterprise cybersecurity; cybersecurity system; data protection; organizational collaboration; cyber threats
Classification Code: G202
Document Code: A
Article ID: 1671-0134(2025)03-132-05
DOI: 10.19483/j.cnki.11-4653/n.2025.03.029
Citation Format: Li Da, Fan Jingsong. Building a Unified Cybersecurity Defense System for Headquarters and Branch Offices [J]. China Media Technology, 2025, 32(3): 132-136.

Introduction

Building upon existing research, this paper further explores the key factors affecting enterprise cybersecurity and proposes strategies and measures for constructing a unified cybersecurity defense system. Through a comprehensive analysis of existing literature, this paper clarifies the necessity of building a unified cybersecurity defense system for headquarters and branch offices, analyzes the challenges it faces, and proposes corresponding solutions to provide theoretical guidance and practical reference for enterprises.

In today' s digital era, enterprises are experiencing rapid development in information technology construction. The widespread application of information technology has greatly enhanced operational efficiency and market competitiveness. However, with continuous advancements in network technology and innovations in business models, the enterprise network environment has become increasingly complex, and cybersecurity issues have become more prominent. Enterprises must not only protect critical data from external attacks but also ensure the security and compliance of internal data flows [1-2]. Particularly for large enterprises with multiple branch offices, achieving efficient collaboration

between headquarters and branches while ensuring data security has become an urgent issue to address.

The core of cybersecurity lies in protecting the confidentiality, integrity, and availability of data, which directly affects the stability and continuity of business operations. Once cybersecurity defenses are breached, it can lead not only to the leakage of sensitive data but also to business disruption, reputational damage, and even legal liability. Therefore, establishing a unified cybersecurity defense system is crucial for maintaining overall enterprise cybersecurity. This system must adapt to the constantly changing network environment while meeting the needs of data sharing and business collaboration between headquarters and branch offices [3-4].

In recent years, research in the cybersecurity field has been increasing, with scholars exploring enterprise cybersecurity issues from different perspectives. At the macro level of enterprise cybersecurity, Duan Junyi et al. (2024) analyzed the challenges faced by enterprise cybersecurity in the context of large-scale application of commercial software, emphasizing the importance of building unified cybersecurity strategies. They pointed out that as enterprises expand and business becomes standardized, cybersecurity is no longer a problem for a single entity but a complex issue requiring cross-regional and cross-organizational collaboration [11].

At the technical level, Fan Haibin explored the application strategies of zero-trust architecture in enterprise archival data protection, including identity verification and access control, data protection and encryption, and continuous monitoring and threat detection. By analyzing the advantages and challenges of these technologies, he proposed practical implementation plans [12]. Xiao Liyang et al. proposed a zero-trust-based AAA system integrating account, authentication, and auditing to address the common problems of user account management and security protection in current enterprise information systems [13]. Shu Yufeng introduced the concept and essence of zero trust from the perspective of traditional security boundary protection and existing cybersecurity situations, and proposed an enterprise security architecture based on zero-trust concepts to solve cybersecurity protection in the era of borderless networks [14]. Tong Weihua proposed a distributed intrusion detection system based on artificial intelligence technology to address the low detection accuracy and high false positive rates of traditional centralized intrusion detection systems. This system can not only adaptively learn and identify abnormal behaviors in the network, improving detection efficiency, but also achieves higher detection accuracy and stronger robustness, enabling real-time monitoring and rapid response for large-scale networks [15]. Li Chang utilized distributed storage systems and stream computing models to quickly detect malware through the analysis and processing of traffic data, providing users with more accurate and timely malware detection services, thereby improving the overall security of the system [16].

In terms of data protection, Wang Xianxuan discussed common encryption tech-

nologies and methods, such as link encryption, node encryption, and end-to-end encryption, and explored how to better apply encryption technology in network communication applications [17]. Luo Yongjian deeply examined the key elements of end-to-end encryption strategies for 5G communication technology in the Internet of Things. Based on analyzing the development background of IoT and 5G communication technology, he discussed the requirements for end-to-end encryption technology, including data security, performance efficiency, and adaptability and compatibility needs [18].

In summary, existing literature provides a rich theoretical foundation and practical guidance for building a unified cybersecurity defense system for headquarters and branch offices. However, as the network environment continues to evolve and technology develops rapidly, the construction and optimization of enterprise cybersecurity defense systems still require continuous exploration and innovation [9-10]. This paper, building upon existing research, further explores the key factors affecting enterprise cybersecurity and proposes strategies and measures for constructing a unified cybersecurity defense system.

2. Factors Affecting Collaborative Cybersecurity Systems

In today' s digital age, the importance of enterprise cybersecurity has become increasingly prominent. Organizational cybersecurity not only concerns the confidentiality, integrity, and availability of enterprise data but also directly affects operational efficiency and market competitiveness. Enterprise cybersecurity maintenance is a complex systematic project involving multiple interacting factors that collectively influence the stability and reliability of enterprise cybersecurity. This section explores the key factors affecting enterprise cybersecurity and analyzes how different factors impact the coordination between headquarters and branch offices.

Operating systems, as core components supporting enterprise IT architecture, directly affect the stability of the entire enterprise network and data security. Security vulnerabilities in operating systems can become entry points for intrusion attacks, posing serious threats to the cybersecurity of both headquarters and branch offices. These vulnerabilities may allow unauthorized access and privilege escalation. Attackers can exploit these vulnerabilities to bypass authentication mechanisms, access sensitive data, or perform malicious operations on systems. Additionally, operating system vulnerabilities may lead to denial-of-service attacks, affecting normal network operations and causing business disruption and economic losses. Furthermore, these vulnerabilities can be used to install malware, such as viruses, trojans, and ransomware, further expanding the scope of attacks and threatening the security of the entire enterprise network.

For headquarters, operating system vulnerabilities may lead to the compromise of critical business systems and data centers. Once exploited by attackers, these vulnerabilities may leak core business secrets, damage corporate reputation, and

result in legal liability and economic losses. For branch offices, security vulnerabilities in operating systems may cause communication interruptions with headquarters, affecting daily operations and data synchronization, while also increasing the risk of branch offices being used as attack springboards, threatening the security of the entire enterprise network.

In addition to operating systems, application service systems, which support core business processes and handle large amounts of sensitive data in real-time, are also critical components that cannot be ignored in today' s enterprise operating environment. If these systems lack necessary security considerations during design and deployment, they may become weak links in enterprise cybersecurity, posing serious threats to the network security of both headquarters and branch offices. Insufficient security considerations in application service systems may lead to data leakage and misuse. Without effective access control and identity verification mechanisms, unauthorized users may access sensitive data, resulting in the leakage of business secrets and customer information. Application service systems lacking security considerations may also suffer from malware attacks, such as SQL injection and cross-site scripting attacks, which may cause system crashes, data corruption or tampering, and affect enterprise network coordination and normal operations.

While maintaining hardware security, internal management practices and security training are also important factors affecting cybersecurity. On the one hand, employee security awareness and behavior are closely related to enterprise cybersecurity. In daily work, employees may violate security policies, such as using weak passwords, clicking on unknown links, and downloading unsafe files, all of which are potential risks to enterprise cybersecurity. Therefore, enterprises need to strengthen employee security training, raise security awareness, and standardize network behavior to reduce security incidents caused by human factors. On the other hand, deficiencies in enterprise cybersecurity management cannot be ignored. In the coordination between headquarters and branch offices, the lack of effective cybersecurity management mechanisms may lead to difficulties in implementing security strategies and delayed response and handling of security incidents. Enterprises need to establish a comprehensive cybersecurity management system, including developing clear security policies, implementing regular security audits, and establishing emergency response mechanisms to ensure continuous and stable cybersecurity.

The factors affecting enterprise cybersecurity are multifaceted, including operating system vulnerabilities, insufficient security considerations in application service systems, internal user security awareness and behavior, network viruses and malware intrusion, and deficiencies in cybersecurity management. These factors are interrelated and collectively constitute the complex system of enterprise cybersecurity. Enterprises must adopt comprehensive security strategies, build a collaborative cybersecurity network for headquarters and branches, strengthen the application of security technologies, improve employee security awareness, and perfect security management mechanisms to ensure enterprise

cybersecurity and protect enterprise data and assets.

3. Architecture for Unified Cybersecurity Defense System for Headquarters and Branch Offices

3.1 Unified Identity Authentication and Access Control

In modern enterprise network environments, unified identity authentication and access control are key components for ensuring network security and coordination between headquarters and branch offices. As enterprises expand and remote work becomes more prevalent, traditional security measures are no longer adequate for current needs. Therefore, implementing unified identity authentication and access control has become central to enterprise cybersecurity strategies.

In the current environment, Zero Trust Architecture (ZTA) has become a key strategy for achieving unified identity authentication and access control. The fundamental concept of this architecture is to trust no user or device by default, requiring verification for both headquarters and branch users. This section explores the implementation details of unified identity authentication and access control, including the introduction of zero-trust architecture, deployment of multi-factor authentication, implementation of role-based access control, and continuous monitoring and auditing.

When introducing a zero-trust framework, enterprises must clearly define identity verification and authorization policies. This process involves identifying users and devices that can access network resources and specifying which resources can be accessed by headquarters and branch departments. To effectively manage user identity verification and authorization, centralized identity providers (IdP) such as Active Directory Federation Services (AD FS) or OAuth 2.0 services should be deployed. Before users and devices request access to network resources, identity verification must be performed using Multi-Factor Authentication (MFA) to ensure that only verified legitimate users and devices obtain corresponding access permissions. Additionally, the network should be divided into multiple small, isolated segments, each with its own security policies and access control lists (ACLs) to limit lateral movement and potential attack surfaces. Notably, zero-trust architecture requires continuous monitoring and evaluation of network activities to ensure the effectiveness of implemented strategies and to promptly detect and respond to abnormal behaviors.

Multi-Factor Authentication (MFA) is a strategy for enhancing network security, and its effectiveness lies in requiring users to provide two or more different forms of credentials during the authentication process. These credentials may include knowledge factors (such as passwords), possession factors (such as smart cards or mobile phones), and inherent factors (such as biometric information). The key to deploying MFA lies in selecting solutions that match enterprise security needs and resources, covering different forms such as hardware tokens, software tokens, SMS verification codes, or biometric technology. During MFA implementation,

users should be educated and trained to ensure that users at all levels fully understand the importance of MFA and are familiar with the operation processes of various authentication methods. At the same time, MFA deployment should adopt a gradual strategy, prioritizing implementation on high-risk applications and resources in headquarters or core branches, and then gradually extending to the entire enterprise network. This phased approach helps reduce disruption to users' daily workflows during deployment and allows security teams to fine-tune and optimize the system before full deployment. After MFA deployment is completed, continuous monitoring and evaluation are required, involving real-time tracking of user authentication activities and regular review of system performance and user feedback. Through continuous evaluation, problems that arise during implementation can be identified and resolved in a timely manner, and MFA strategies can be adjusted as necessary based on actual usage to improve overall user experience and system security.

The design principle of Role-Based Access Control (RBAC) is to grant corresponding access permissions based on the roles users play in the enterprise organizational structure. The prerequisite for implementing RBAC strategies requires precise definition of user roles and clear delineation of the scope of responsibilities and corresponding permission sets for each role, dividing functions between headquarters and branches while ensuring enterprise collaboration. The execution of this strategy involves detailed allocation of access permissions to files, applications, and network resources, aiming to ensure that users at different levels only obtain the minimum permission set necessary to perform their duties. RBAC strategy implementation further emphasizes the importance of the principle of least privilege, which advocates limiting user permissions to the minimum required to complete tasks while ensuring smooth business processes, thereby reducing potential security risks. Additionally, given the dynamic nature of enterprise operations and organizational structures, RBAC strategies need to be regularly reviewed and adjusted. This process helps maintain the timeliness and adaptability of the strategy, ensuring it continues to meet enterprise security needs and reflect the latest business processes.

Continuous monitoring and auditing encompass real-time monitoring of user activities, system logs, and abnormal behaviors, as well as regular security audits. Real-time monitoring of user activities and system logs provides security teams with insights into enterprise cybersecurity posture, enabling immediate response to any abnormal behavior. At the same time, regular audits serve as a systematic review method that can reveal potential weaknesses in security strategies and ensure that security measures remain aligned with current business needs and security objectives. Through these continuous assessments and adjustments, enterprises can ensure the adaptability and forward-looking nature of their security strategies, thereby maintaining competitiveness in the constantly evolving cyber threat environment.

3.2 Distributed Threat Detection and Response

Distributed Threat Detection and Response (DTDR) aims to achieve rapid identification, analysis, and response to potential threats through coordinated efforts across multiple network nodes at headquarters and branches, thereby improving the overall defense capability against cyber attacks. This section analyzes the implementation of distributed threat detection and response based on threat intelligence collection and sharing, security monitoring deployment, construction of automated response mechanisms, and the importance of cross-organizational collaboration.

Threat intelligence is the foundation of the DTDR system, involving the collection, analysis, and sharing of information about potential threats. Effective threat intelligence comes from multiple channels and levels, including but not limited to open-source intelligence, commercial threat intelligence, and enterprise' s own security logs and event data. Implementing threat intelligence collection first requires establishing a centralized intelligence platform that integrates intelligence from different sources and provides unified analysis and reporting functions. After obtaining threat intelligence, relevant enterprise departments need to utilize advanced analysis tools, such as machine learning and artificial intelligence, to identify and understand threat patterns, helping security teams mine valuable information from large amounts of data and predict potential attack behaviors. Additionally, sharing threat intelligence is key to improving the security level of the entire industry. By sharing intelligence with industry partners and the security community, enterprises can not only obtain a broader threat perspective but also improve response speed to new threats.

Security monitoring is another important component of the DTDR system, involving the deployment of monitoring devices at key nodes of the network to capture network traffic, system logs, and user behavior data in real time. The deployed monitoring devices need to have advanced detection capabilities to identify various complex attack patterns, such as zero-day attacks, Advanced Persistent Threats (APT), and insider threats. Common monitoring devices include Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Endpoint Detection and Response (EDR), and Security Information and Event Management (SIEM) systems. Reasonable deployment of these devices can not only provide real-time alerts and reports but also integrate with other enterprise security measures to achieve automated threat response and mitigation.

After potential threats are detected in a timely manner, rapid and effective response becomes the decisive factor for successful attack defense. The establishment of automated response mechanisms, relying on predefined playbooks and workflows, can ensure that security incidents are handled quickly and orderly. This includes but is not limited to the isolation of infected systems, blocking of malicious traffic, removal of malware, and recovery of damaged data. To build an efficient automated response system, enterprises must conduct detailed analysis and optimization of their existing security operation processes. This process

involves not only the clear definition of incident response procedures but also the establishment of cross-departmental collaboration mechanisms and the development of automated tools and scripts. Through these comprehensive measures, enterprises can significantly improve the response speed and handling efficiency of security incidents, thereby taking the initiative in cybersecurity defense.

On the basis of improving hardware deployment for distributed threat detection and response, enterprises should also emphasize the importance of cross-organizational collaboration to achieve effective DTDR. Through cooperation with branch departments, industry partners, government agencies, and the security community, enterprises can share threat intelligence, coordinate response actions, and jointly improve the security level of the entire industry. Additionally, cross-organizational collaboration needs to be built on trust and transparency. Enterprises need to establish clear communication channels and collaboration agreements with partners and ensure that all participants follow the same security standards and best practices. Finally, enterprises need to invest in personnel training and culture building to promote cross-organizational collaboration and knowledge sharing.

3.3 Centralized Management and Monitoring

In today' s enterprise network environment, cybersecurity management is gradually becoming centralized to achieve a unified view and control of cybersecurity for headquarters and branch offices. This "single network" management model emphasizes integrated management of cross-regional networks, aiming to build a coordinated and consistent security defense system through centralized management and monitoring strategies.

The implementation of centralized management and monitoring first requires enterprises to establish a unified security policy framework that covers all branch offices and remains consistent with headquarters' security policies. On this basis, enterprises should deploy centralized management platforms, such as Security Information and Event Management (SIEM) systems, to achieve centralized configuration, monitoring, and management of network-wide security devices. Such platforms can collect, correlate, and analyze logs and event data from different security devices, thereby providing comprehensive insights into potential threats.

To further improve monitoring efficiency, enterprises can utilize advanced analysis technologies, such as behavior analysis, anomaly detection, and machine learning, to identify and respond to complex security threats. These technologies can extract valuable security intelligence from massive amounts of data, helping security teams quickly identify attack patterns and take corresponding defense measures. In the process of implementing centralized management and monitoring, enterprises also need to focus on network traffic visualization. By deploying network traffic analysis tools, they can monitor data flow in real time and identify unauthorized access and data leakage behaviors. Additionally, re-

mote monitoring of branch offices is equally important, requiring enterprises to establish reliable remote access and monitoring mechanisms to ensure that the security status of branch offices can be promptly addressed and handled.

While implementing technology, enterprises also need to emphasize the role of personnel. Security teams should receive professional training to master the use of centralized management tools and be able to make accurate judgments and responses based on monitoring data. Enterprises should cultivate a security culture where all employees participate, making staff aware of their responsibilities in maintaining cybersecurity, thereby improving the entire organization' s awareness of security threat prevention.

In summary, centralized management and monitoring provides a unified cybersecurity management view for headquarters and branch offices, helping enterprises build a more robust and responsive security defense system. Through the organic combination of technology, processes, and personnel, enterprises can maintain a competitive advantage in the constantly evolving cyber threat environment and ensure the security and integrity of their information assets.

3.4 End-to-End Encryption and Data Protection

End-to-end encryption and data protection strategies ensure data security during transmission and the confidentiality, integrity, and availability of data in both static and dynamic states. The application of end-to-end encryption technology provides seamless protection for data throughout the entire transmission path from source to destination, thereby effectively defending against potential eavesdropping, tampering, and data leakage.

The implementation of end-to-end encryption requires encryption at the starting point of data transmission and decryption only after the data reaches its destination. This encryption method eliminates the need for intermediate nodes to decrypt data, thereby reducing the possibility of data being intercepted and misused during transmission. To achieve this, enterprises need to deploy strong encryption protocols, such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL), and adopt advanced encryption algorithms such as Advanced Encryption Standard (AES).

In terms of data protection, enterprises need to adopt multi-layered security measures to ensure that data is properly protected at every stage of collection, storage, use, sharing, and destruction (see Figure 1 [Figure 1: see original paper]). This includes implementing data access control to ensure that only authorized users can access sensitive data; adopting data backup and recovery strategies to prevent data loss and business interruption; and employing data masking techniques to reduce risks when data is leaked. Additionally, enterprises need to pay attention to compliance requirements for data protection. With increasingly stringent global data protection regulations, such as the EU' s General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), enterprises must ensure that their data protection mea-

sures comply with relevant laws and regulations. This involves not only the implementation of technical measures but also training employees on data protection regulations and establishing corresponding data protection policies and procedures.

Conclusion

This paper proposes a unified cybersecurity defense system for headquarters and branch offices through a comprehensive analysis of current challenges and needs in the cybersecurity field. Based on an in-depth exploration of the key factors affecting enterprise cybersecurity, it presents a comprehensive solution including unified identity authentication and access control, distributed threat detection and response, centralized management and monitoring, and end-to-end encryption and data protection.

Unified identity authentication and access control, as the foundation of cybersecurity, effectively enhances enterprise cybersecurity defense capabilities through the introduction of zero-trust architecture, multi-factor authentication, and role-based access control. Meanwhile, the distributed threat detection and response strategy improves the overall defense capability against cyber attacks through coordinated efforts across headquarters and branches, achieving rapid identification and response to potential threats. The centralized management and monitoring strategy provides a unified cybersecurity management view by establishing a unified security policy framework and deploying centralized management platforms, enabling centralized configuration, monitoring, and management of network-wide security devices. The end-to-end encryption and data protection strategy ensures data security during transmission and the confidentiality, integrity, and availability of data in both static and dynamic states.

In summary, constructing a unified cybersecurity defense system for headquarters and branch offices requires not only technological innovation and application but also corresponding adjustments and optimization at the management level. By implementing the strategies proposed in this paper, enterprises can build a more robust and responsive security defense system that effectively counters evolving cyber threats and safeguards enterprise data and assets. In the future, as technology continues to advance and the network environment keeps changing, the construction and optimization of enterprise cybersecurity defense systems will be an ongoing process that requires enterprises to continuously engage in technological innovation and strategic adjustments to adapt to new challenges and needs.

References

[1] Cyberspace Security Situation Analysis Group, CCID Think Tank. Outlook on China' s Cybersecurity Development Situation in 2024 [J]. Cybersecurity and Informatization, 2024(2): 35-

[2] Wang Yingbo. Preliminary Study on Core Competitiveness Indicators

of Cybersecurity Enterprises [J]. Information Security and Communication Confidentiality, 2015(8): 4-455.
[3] Xu Shuang, Liu Wenbin, Li Jialong, et al. Research Progress on Data Security Governance Under Big Data Background [J]. Journal of Taiyuan University of Technology, 2024(1): 127-
[4] Chen Huoquan. Cybersecurity Strategy for Data Governance Under Big Data Background [J]. Macroeconomic Research, 2015(8): 76-84, 142.
[5] Li Zhuozhi. Research on Enterprise Cybersecurity Defense System Construction [J]. Cybersecurity Technology and Application, 2024(7): 108-110.
[6] Liu Yanhua. Research on Enterprise Cybersecurity Defense System Construction [J]. Electronic Technology and Software Engineering, 2022(11): 54-57.
[7] Zou Shuang, Luo Sirui. Research on Enterprise Cybersecurity Defense System Construction [J]. Communication and Information Technology, 2022(202): 63-67.
[8] Li Gang, Yang Wei. Construction of Cybersecurity Defense System for Large Enterprises [J]. Digital Users, 2022(41): 52-54.
[9] Semerci M, Cemgil A T, Sankur B. An intelligent cyber security system against DDoS attacks in SIP networks[J]. Computer Networks, 2018, 136(MAY8): 137-154.
[10] Liu Y, Morgan Y. Security against Passive Attacks on Network Coding System - A Survey[J]. Computer Networks, 2018, 138(JUN.19): 57-76.
[11] Duan Junyi, Xu Jin. Construction of Enterprise Application Security System Improvement [J/OL]. Journal of Tianjin University of Technology, 1-6[2024-12-27]. http://kns.cnki.net/kcms/detail/12.1374.N.20240914.1136.056.html.
[12] Fan Haibin. Enterprise Archival Data Protection Strategy Based on Zero-Trust Architecture [J]. Cybersecurity and Informatization, 2024(8): 138-140.
[13] Xiao Liyang, Bi Yubing, Liu Xiao, Zhu Bodi, Liu Di, Liu Chaofei, Cui Yiqun. Design and Implementation of Group-Level AAA System Based on Zero-Trust Architecture [J]. Thermal Power Generation, 2023(9): 171-180.
[14] Shu Yufeng. Enterprise Security Architecture Based on Zero Trust [J]. Electronic Technology and Software Engineering, 2021(17): 243-244.
[15] Tong Weihua. Design of Distributed Intrusion Detection System Based on Artificial Intelligence Technology [J]. Information Recording Materials, 2024(7): 150-152, 156.
[16] Li Chang. Malware Detection Method Based on Distributed Traffic Data [J]. Mobile Information, 2024(5): 158-160.
[17] Wang Xianxuan, Luo Yunfang, Deng Guobin. Application of Data Encryption Technology in Computer Network Communication Security [J]. Information Technology Times, 2024(8): 37-
[18] Luo Yongjian. End-to-End Encryption Strategy for 5G Communication Technology in IoT [J]. Communication Power Supply Technology, 2024(4): 155-157.

Author Information: Li Da (1979–), male, from Liaoning, bachelor' s degree, senior engineer, research direction: networks, cybersecurity, cloud computing; Fan Jingsong (1977–), male, from Liaoning, associate degree, research direction:

networks, cybersecurity, artificial intelligence.

(Responsible Editor: Li Yansong)

Note: Figure translations are in progress. See original paper for figures.