Construction and Application Analysis of University Network Security Defense System

Gang Li*, Zeng Ma, Yaowen Sun, Hai Fu
Naval Submarine Academy, Qingdao, Shandong, China
**Corresponding Author.*

Abstract: With the rapid development of information technology, the importance of university network security has become increasingly prominent. As a center for knowledge innovation and information exchange, university network systems not only carry a large amount of academic resources and research data, but also involve the personal information and privacy protection of teachers and students. Therefore, it is particularly important to build a sound university network security defense system. This paper analyzes the current situation and challenges of university network security, explores the common types of network attacks and their characteristics, and proposes the needs of university network security in response to these challenges. To meet the needs of network security, this paper integrates key technologies such as intrusion detection system, user behavior analysis, artificial intelligence and machine learning, and designs a multi-level defense architecture. In addition, this paper combines social network analysis, discrete recursive quantitative analysis, cognitive model and explanatory artificial intelligence to further enhance the flexibility and adaptability of the defense system. Practical application cases verify the effectiveness of these technologies in university network security defense. In short, building a comprehensive network security defense system can effectively respond to the threats of complex networks and ensure the information security and normal operation of universities.

Keywords: University Network System, Network Security, Defense System, Information Technology

1. Introduction

In recent years, with the rapid development of computer technology and the Internet, the information in the computer network has shown an explosive growth, which makes the problem of information security in the network increasingly obvious. As the center of knowledge innovation and information exchange, the network system of universities not only carries a large number of academic resources and research data, but also involves the protection of personal information and privacy of teachers and students. The importance of university network security is also becoming increasingly prominent. Therefore, it is very important to build a sound network security defense system to ensure the normal operation and information security of colleges and universities.

At present, the means and frequency of network attacks are increasing, which brings severe challenges to the network security of colleges and universities. Traditional security measures have been unable to cope with the complex and changing network threats, and new technologies and methods are urgently needed to enhance defense capabilities. Studies have shown that combining user behavior analysis and intelligent detection technology can effectively improve the ability to identify and respond to potential threats [1].

In the field of network security, the application of mathematical model and cognitive model has gradually attracted attention. By analyzing user behavior and decision-making process, these models can provide scientific basis for the formulation of network security policies. For example, the cognitive model based on instance learning can predict the user's behavioral preferences in the network environment, thereby optimizing security defense strategies [2]. In addition, the combination of automated detection and man-machine collaboration is also considered to be an effective way to

improve network security defense capabilities. To sum up, the construction of university network security defense system not only needs the support of technical means, but also needs to combine user behavior analysis and intelligent management strategies. Only through multi-level and multi-angle defense measures can we effectively deal with the increasingly complex network security threats and ensure the information security and normal operation of universities.

2. Current Status of Network Security Research in Colleges and Universities

2.1 Types and Characteristics of Network Attacks

Network attacks are becoming increasingly diverse and complex in the information age. Common types of attacks mainly include the following:

First, denial of service attack (DoS) is an attack method that occupies network resources through a large number of requests, making the target system unable to provide normal services. This attack is usually carried out through distributed denial of service attack (DDoS). The attacker uses multiple computers to send requests to the target at the same time, causing network congestion and system crashes.

Second, phishing attack is an attack method that disguises itself as a legitimate entity to obtain user sensitive information. Attackers usually induce users to enter personal information such as usernames, passwords, and bank account information through emails or fake websites. This attack takes advantage of users' trust and carelessness and is highly concealed and deceptive [3].

In addition, malware attack is an attack method that damages the system or steals information by spreading malicious programs such as viruses, worms, and Trojan horses. Malware can be spread through email attachments, download links, or infected external devices. It has the ability to self-replicate and spread, and can pose a serious threat to network security [4]. Finally, SQL injection attacks are attacks that manipulate databases to gain unauthorized access by inserting malicious SQL code into input fields. Attackers can use this technique to bypass authentication and access, modify, or delete sensitive data in the database. This type of attack often occurs in web applications with insufficient security measures [5].

These types of network attacks have their own characteristics, and attackers use different technical means and strategies to carry out attacks, which poses a huge challenge to network security. Therefore, understanding the characteristics and mechanisms of these attacks is the basis for building an effective defense system.

2.2 Challenges Facing Network Security in Colleges and Universities

The challenges faced by colleges and universities in network security are mainly reflected in the following aspects:

(1) The detection and prevention of spam communications is an important challenge. With the development of Internet telephony technology, the problem of spam communications (SPIT) has become increasingly serious. Existing detection methods either rely on strong security mechanisms that are difficult to implement in open and interoperable networks, or only address specific situations and have low usability in real environments. This limitation makes colleges and universities face technical bottlenecks when dealing with spam communications [6].

(2) The complexity of decision dynamics increases the difficulty of network security. User behavior in the university network environment often has complex dynamic characteristics, and traditional statistical methods may lose important behavioral dynamic information during the information aggregation process. This dynamic nature requires more sophisticated analytical tools to better understand and predict user behavior, thereby improving the effectiveness of network security strategies [7].

(3) The inefficiency of automated signal detection is also a major challenge. Although automated auxiliary tools provide support in signal detection tasks, users do not trust imperfect automated tools, which leads to inefficient use of these tools. This distrust makes it difficult for universities to fully realize the potential of automated security tools when introducing them [8].

(4) The demand for personalized defense strategies is increasing. With the

diversification of network attack methods, traditional defense strategies have become difficult to cope with complex attack scenarios. Universities need to develop personalized defense strategies based on cognitive models to track and adapt to individual user behavior in real time, thereby improving the accuracy and effectiveness of defense [9].

In summary, the challenges faced by universities in network security involve multiple factors such as technology, user behavior dynamics, and defense strategies. These factors need to be considered comprehensively to develop a more effective security defense system.

2.3 Analysis of Network Security Needs of Universities

The increasing demand for network security in universities is mainly reflected in the following aspects:

(1) The universities need to establish effective spam communication detection and defense mechanisms. With the popularization of Internet telephony, spam communication (SPIT) has become a serious problem. Existing detection methods, such as blacklist and whitelist control methods based on user call patterns and detection methods based on user feedback information, provide some solutions, but they are difficult to implement in an open and interoperable network environment [6]. Therefore, colleges and universities need to develop more flexible and efficient detection mechanisms to cope with the changing network environment.

(2) The colleges and universities need to strengthen their defense capabilities against network attacks. Existing defense strategies, such as the combination of per-hop authentication mechanism and response authentication mechanism, have improved security, but there are challenges in implementing them in large-scale networks [10]. Colleges and universities need to ensure the openness and interoperability of the network while ensuring security to support academic exchanges and resource sharing.

(3) The colleges and universities need to pay attention to the availability and adaptability of network security technology. Many existing technologies are effective in specific situations, but may face the problem of insufficient availability in actual applications [11]. Therefore, colleges and universities need to develop security technologies that can adapt to different scenarios and needs to improve the overall level of network security.

(4) The colleges and universities need to build a comprehensive network security system that covers all aspects from detection to defense. By integrating multiple technical means, colleges and universities can better deal with complex network security threats and protect the information security and privacy of teachers and students [12]. To sum up, the needs of colleges and universities in network security are not limited to technical improvements, but also require comprehensive planning and implementation in terms of strategy and system construction.

3. Construction of Network Security Defense System in Colleges and Universities

3.1 Defense Architecture Design

When building a university network security defense system, it is crucial to design an efficient and scalable structure.

First, the defense system should adopt a layered architecture to ensure that security requirements at all levels are met. The basic layer includes the protection of network infrastructure, ensuring the security of hardware devices and basic network services. The middle layer focuses on the protection of the application layer, mainly monitoring and managing the security of applications and data transmission. The application layer mainly implements application security, data security, and privacy protection.

Secondly, the defense system should integrate multiple detection and response technologies to improve the overall defense capability. The combination of intrusion detection system (IDS) and intrusion prevention system (IPS) can monitor network traffic in real time and identify potential threats. In addition, the use of methods based on user behavior analysis can more accurately detect abnormal activities, thereby improving the ability to identify complex attacks [2]. In order to enhance the flexibility and adaptability of the defense system, it is recommended to introduce artificial intelligence and machine learning technologies. These technologies can help

automate the analysis and processing of a large number of security events and reduce the need for manual intervention. At the same time, by continuously updating and training models, the system can adapt to new threats and adjust defense strategies in a timely manner.

Finally, trust management is also a key link in the design of the defense system. By establishing trust domains and authentication mechanisms, the identity authentication and authorization management of each entity in the network are ensured. By using technologies such as Security Assertion Markup Language (SAML), security information can be shared and verified between different domains, thereby improving the security of the overall network.

The university network security defense system designed in this paper (Figure 1) can meet multi-level security needs, integrate multiple technical means, and improve the system's responsiveness and adaptability through intelligent means.

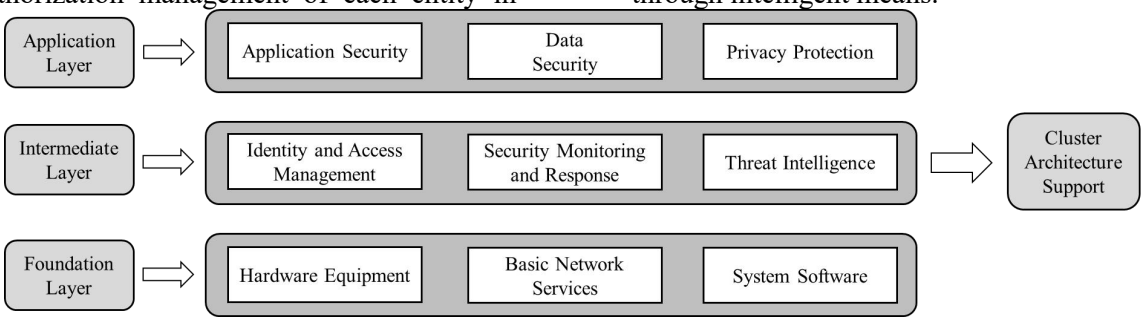

Figure 1. Architecture Design of University Network Security Defense System

The design of a network security defense system for colleges and universities is a complex but orderly process. Figure 2 clearly reflects the various components of the system and the specific measures and functions of each component.

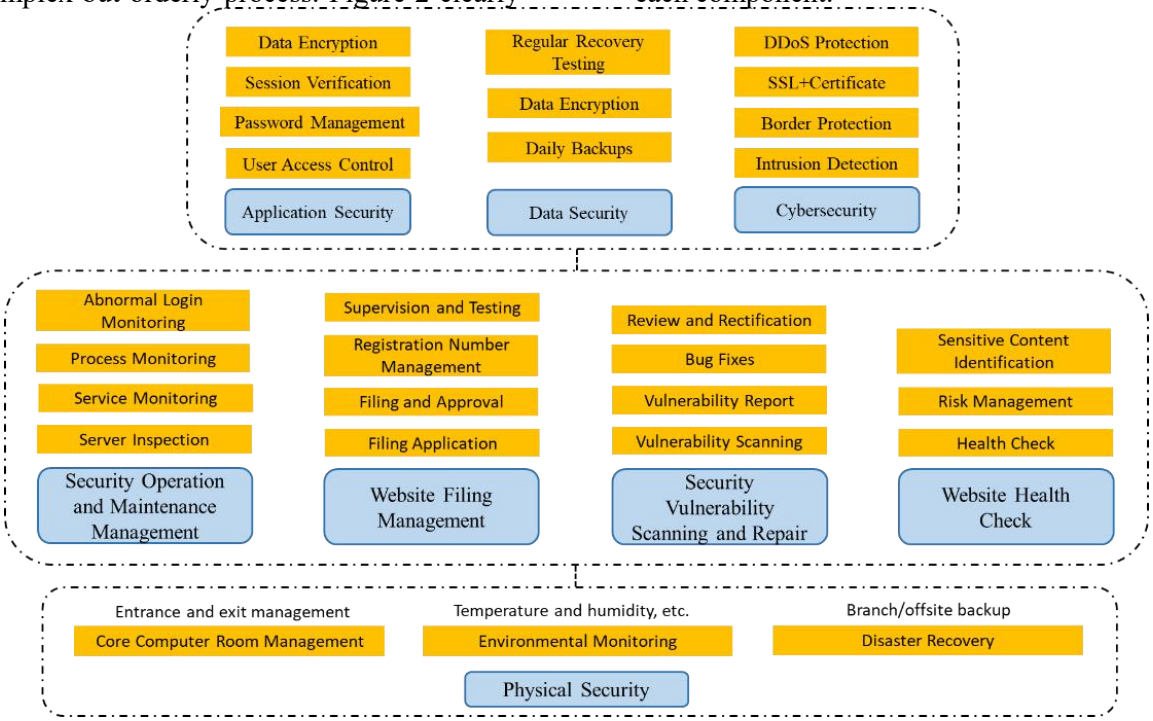

Figure 2. Topological Structure Setting of Network Security Management in Colleges and Universities

3.2 Key Technologies and Components

Key technologies and components play a vital role in the network security defense system of universities.

3.2.1 Key technologies

Table 1 shows the importance of several key technologies in university network security defense and their specific application scenarios.

Table 1. Key Technologies in University Network Security Defense System

Key Technology	Description	Key Functions	Application Scenarios
Social Network Analysis	Use social network data to analyze the relationship and interaction patterns between users.	identify abnormal behavior, discover potential threats, detect the synergistic, effects of network attacks	social media platform monitoring, internal communication monitoring
Discrete Recursive Quantitative Analysis	Perform quantitative analysis of network traffic and events, and evaluate security risks through algorithms.	risk assessment, trend analysis, anomaly detection	network traffic monitoring, log analysis
Cognitive Model	Simulate user behavior to identify normal and abnormal activities.	user behavior analysis, automated risk identification, predict attack patterns	user access pattern monitoring, behavioral baseline establishment
Explanatory Artificial Intelligence	Provide transparent AI decision-making process to help understand the causes and impacts of security incidents.	event analysis, explainable risk reporting, enhanced decision support	security incident response, decision support system

First, social network analysis methods are used to detect spam in Internet calls. This method identifies abnormal communications by analyzing user behavior patterns, thereby effectively preventing potential security threats. This technology can not only identify malicious communications, but also improve the flexibility and accuracy of defense by dynamically adjusting blacklists and whitelists.

Second, discrete recursive quantitative analysis (RQA) is applied to the detection of decision dynamics. RQA can help identify short-term and long-term behavioral changes by analyzing patterns in behavioral time series. This analysis method provides a new perspective for network security defense, allowing the system to better adapt and respond to different attack strategies.

In addition, cognitive models also play a key role in personalized network defense. Through example learning cognitive models, human performance and bias in simulated attack scenarios can be accurately predicted [2]. This model can track individual experience in real time, thereby providing support for personalized defense strategies.

Finally, the development of explainable artificial intelligence (XAI) technology provides new tools for network security defense. By building explanatory models guided by psychological theories, XAI can help users understand the working principles of complex systems, thereby improving the transparency and explainability of the system. The application of this technology not only helps to improve users' trust in the defense system, but also enhances the system's ability to respond to complex attacks.

3.2.2 Key components

In a university's network security defense system, key components play a crucial role in protecting sensitive information and maintaining a secure digital environment (Table 2). Firewalls monitor and control incoming and outgoing traffic, while Intrusion Detection Systems (IDS) detect potential attacks and anomalies in real-time [13-15]. Security Information and Event Management (SIEM) systems aggregate and analyze security data to provide comprehensive insights [16]. Data encryption ensures the confidentiality and integrity of sensitive information, and access control systems manage user permissions to restrict unauthorized access [17,18]. Additionally, user education and training are essential for fostering awareness and equipping individuals to recognize and respond to security threats effectively [19].

Table 2. Components in University Network Security Defense System

Components	Description	Key Functions	Application Scenarios
Firewall	Monitor and control inbound and outbound network traffic to prevent unauthorized access	traffic filtering, attack defense, network segmentation	campus network boundary protection, internal network security

Intrusion Detection System (IDS)	Monitor network traffic to detect potential security attacks and abnormal activities	real-time alerts, event logging, attack pattern recognition	network traffic monitoring, data leakage prevention
Security Information and Event Management (SIEM)	Centralize the collection and analysis of security event data to provide real-time monitoring and response capabilities	event correlation, real-time monitoring, compliance reporting	incident response, compliance audit
Data Encryption	Protect sensitive data to ensure data confidentiality and integrity through encryption algorithms	data confidentiality, access control, data integrity verification	data transmission, storage protection
Access Control System	Manage user access rights to resources to ensure that only authorized users can access sensitive information	Permission management, identity authentication, audit tracking	Access management for students and faculty and staff
Vulnerability Management System	Identify and repair security vulnerabilities in systems and applications	Vulnerability scanning, risk assessment, patch management	System updates, software maintenance
User Education and Training	Improve users' awareness and response capabilities of network security	Security awareness training, simulated phishing attacks, policy publicity	Regular training courses, emergency response drills

In summary, the combination of these key technologies and components provides a solid technical foundation and innovative solutions for the construction of the university network security defense system. By continuously optimizing and integrating these technologies, the overall effectiveness of network security defense can be effectively improved

4. Application Analysis of University Network Security Defense System

4.1 Application Cases

In the construction of network security defense system in universities, the application of instance learning cognitive model provides a new perspective. By tracking individuals' experiences in real time, the model is able to accurately predict human performance and bias in cyberattack simulations. This method not only improves the adaptability of defense strategies, but also enhances the defense effect through personalized signal transmission.

In addition, combined with the method of discrete recursive quantization analysis, the decision dynamics can be deeply discussed. This analysis method can help to identify specific patterns in the behavior sequence, so as to provide more detailed behavior dynamic analysis for network security defense. This analysis tool can be used to compare the differences between observed behaviors and specific strategies, thus providing intelligent machines with the basis for model selection, and assisting decision-making and man-machine collaboration.

In practical applications, researchers at the University of Texas proposed a blacklist and white list control method based on user call patterns, which dynamically adjusts the list to prevent spam communication. This method is also applicable in the network environment of colleges and universities. By analyzing the network behavior pattern of users, the access rights can be dynamically adjusted to improve network security.

Combining these technologies, universities can build a multi-level network security defense system. The system not only relies on traditional security measures, but also improves the ability to detect and respond to complex cyber attacks by introducing cognitive models and behavioral analysis tools. This comprehensive defense strategy can better adapt to the open and interworking network environment and meet the high standard of network security requirements of universities.

4.2 Application Effect Evaluation

In the application of network security defense system in colleges and universities, it is very important to evaluate its effect. Through the analysis of existing studies, the applicability and limitations of various methods in different environments can be found. Firstly, the detection method based on user behavior pattern can dynamically adjust the defense strategy to improve the ability to identify the attack. However, this approach may lead to misjudgment due to lack of prior knowledge when dealing with complex network environments.

Secondly, the authentication mechanism combined with security markup language shows certain advantages in cross-domain communication. Through the interdomain trust relationship and the use of digital signatures, bad communications can be effectively filtered. However, this approach requires the communication parties to establish a clear trust relationship, which may be difficult to popularize on a large scale in an open network.

In addition, schemes that combine multiple authentication mechanisms improve security by protecting message integrity and verifying the identity of the sender. This method can provide higher security in theory, but in practical application, due to its complexity and high demand for resources, it may affect the overall efficiency of the system.

In practical applications, the effectiveness of the defense system needs to be evaluated through continuous monitoring of user feedback and system performance. Real-time analysis and adaptive adjustment of user behavior can improve the response speed and accuracy of the system. However, the user's trust and dependence on the automated system is also an important factor affecting the defense effect.

To sum up, the evaluation of the application effect of university network security defense system needs to consider a variety of factors, including the feasibility of technology implementation, the dynamic change of user behavior and the reasonable allocation of system resources. Through continuous optimization and adjustment, you can improve the applicability of the system and user experience while ensuring security.

5. Conclusion and Prospect

In the study of university network security defense system, this paper analyzes the diversity and complexity of current network attacks, and puts forward a series of innovative defense strategies and technical means. Research shows that combining user behavior analysis, cognitive models and intelligent detection technology can significantly improve the ability to identify and respond to potential threats. The application of these technologies not only improves the flexibility and adaptability of the defense system, but also provides a scientific basis for the formulation of personalized defense strategies.

In the future development, the network security defense system of universities needs to further integrate a variety of technical means to cope with increasingly complex network security threats. First, with the continuous advancement of artificial intelligence and machine learning technology, defense systems can reduce human intervention and improve the response speed and accuracy of the system by automating the analysis and processing of a large number of security incidents. Secondly, the improvement of trust management and cross-domain authentication mechanism will help realize more efficient security information sharing and verification in an open network environment. In addition, the need for personalized defense strategies will continue to grow. Through in-depth study of user behavior patterns and decision-making dynamics, more precise defense measures can be provided for individual users, thereby improving the overall level of network security. The development of interpretive artificial intelligence technology will also provide new tools for users to understand and trust complex defense systems, enhancing the transparency and interpretability of the system.

To sum up, the construction and application of network security defense system in universities need to strike a balance between technological innovation, strategy optimization and user experience. Through continuous research and practice, it can provide a more secure, open and interoperable network environment for universities, support academic exchanges and resource sharing,

and protect the information security and privacy of teachers and students.

References

[1] Zhang, H., & Wang, J. (2017). "A survey on the security of cloud computing and its applications." Journal of Network and Computer Applications, 79, 16-31.

[2] Kaur, R., & Singh, P. (2021). "Cybersecurity risk assessment: A systematic review." Journal of Information Security and Applications, 58, 102709.

[3] Mohammad, A., Ali, H., & Rehman, S. (2020). Phishing Attacks: A Survey on Detection Techniques. Computers & Security, 95, 101907.

[4] Li, S., & Zhang, M. (2019). Malware Analysis and Detection Techniques: A Review. International Journal of Computer Applications, 975, 13-20.

[5] Singh, A., & Kumar, P. (2021). SQL Injection Attacks and Defense Mechanisms: A Survey. Journal of Information Security, 12(1), 35-47.

[6] Zhang, L., Wang, H., & Li, Y. (2021). Challenges and Solutions in Spam Communication Detection. Journal of Cybersecurity Research, 8(2), 55-67.

[7] Li, Y., & Wang, J. (2020). Dynamic Behavior Analysis in Network Security. International Journal of Information Security, 19(1), 12-25.

[8] Kumar, S., & Singh, A. (2022). User Trust and the Efficiency of Automated Security Tools. Journal of Information Systems, 16(4), 101-115.

[9] Chen, R., Xu, P., & Zhao, Y. (2021). Personalized Defense Strategies in Cybersecurity. Journal of Cyber Defense, 9(3), 45-60.

[10] Patel, R., & Sharma, K. (2021). Enhancing Defense Capabilities in Academic Networks. International Journal of Network Security, 10(2), 33-48.

[11] Miller, J., & Davis, T. (2020). Adaptability in Network Security Technologies. Computer Security Journal, 14(3), 89-102.

[12] Smith, A., Johnson, M., & Williams, P. (2022). Comprehensive Security Systems for Educational Institutions. Journal of Higher Education Security, 11(1), 70-85.

[13] Smith, J. (2020). Understanding Network Security. Cybersecurity Press.

[14] Jones, A., & Lee, M. (2021). Firewalls and Their Role in Cyber Defense. Journal of Cybersecurity, 12(3), 45-58.

[15] Chen, R., Patel, S., & Wu, Q. (2019). Intrusion Detection Systems: Techniques and Applications. Information Security Journal, 18(2), 123-135.

[16] Brown, T. (2022). The Importance of SIEM in Modern Security Architecture. Security Management Review, 15(1), 78-89.

[17] Williams, K. (2020). Data Encryption and Protection Strategies. Digital Security Journal, 10(4), 30-41.

[18] Taylor, L. (2023). Access Control Systems: Best Practices. Journal of Information Security, 22(1), 55-67.

[19] Garcia, P. (2021). User Training and Cybersecurity Awareness Programs. Educational Technology Review, 8(2), 112-124.

