Research on Network Security and Prevention in Higher Education Based on Artificial Intelligence

Renmao Zhao

School of Information and Intelligence Engineering, University of Sanya, Sanya, Hainan, China

Abstract: In today's information age, the rapid development of artificial intelligence and big data technologies is driving transformation and innovation across various industries. However, with the widespread application of artificial intelligence and big data, network security issues have become increasingly prominent. As an important venue for information technology construction, network security significantly impacts the stable operation of schools and their teaching and research activities. Additionally, the openness and diversity of the network environment in higher education institutions make the protection of network security even more challenging. Only by taking proactive measures to address the various threats posed by network security can we create a better campus environment and promote the healthy growth of students. While advancing information technology construction, higher education institutions also need to continuously enhance their network security protection levels to create a safe and trustworthy online environment for teachers and students, thereby facilitating the smooth progress of teaching, research, and management work.

Keywords: Artificial Intelligence; Big Data; Network Security; Countermeasures

1. Introduction

In the era of artificial intelligence and big data, the maintenance of cybersecurity has become particularly important[1]. With the rapid development of digitalization, data exchange between individuals and institutions has become more extensive and frequent. However, this also provides cyber attackers with more opportunities to obtain and misuse sensitive information, threatening personal privacy, financial security, and national security. Therefore, protecting cybersecurity is crucial for safeguarding people's interests and maintaining social stability. The proliferation of big data and artificial intelligence has equipped individuals and institutions with greater data storage and processing capabilities. This data contains a wealth of sensitive information, such as personal identification information, financial data, and trade secrets. If this data is inadvertently leaked, it could lead to breaches of personal privacy, economic losses, and a decline in competitiveness[2]. By maintaining cybersecurity, we can ensure that this valuable data is adequately protected, preventing irreversible damage. Furthermore, the development of artificial intelligence has also introduced new security challenges, as AI systems can be used to automate attacks, such as malware and phishing. At the same time, malicious actors can leverage AI to crack passwords, identify security vulnerabilities, and launch attacks on networks. Only through continuous innovation and updating of cybersecurity measures can we address these new threats and protect the security of the cyber ecosystem. Thus, in the context of artificial intelligence and big data, the importance of maintaining cybersecurity cannot be overlooked.

2. Existing Issues

2.1 Insufficient Awareness of Cybersecurity

With the increasing level of information technology in higher education institutions, the threat of cyberattacks is continuously growing. However, many universities have relatively weak awareness regarding cybersecurity management and lack understanding of cyber threats and security risks. This leads to inadequacies in cybersecurity strategies, training, and awareness education, making universities easy targets for cyberattacks[3].

2.2 Incomplete Cybersecurity Management System

Cybersecurity requires a comprehensive and systematic management framework to ensure the safety and stability of networks. However, many universities exhibit deficiencies in preventive network management, lacking robust cybersecurity strategies and policies, clear division of responsibilities, and management processes. Additionally, there is a lack of professional cybersecurity teams and technical support, which renders universities ill-equipped to respond to cyberattacks and security incidents, making it difficult to cultivate specialized cybersecurity talent and effectively address increasingly complex cybersecurity challenges.

2.3 Weak Cybersecurity Maintenance Capabilities

2.3.1 Existence of Security Vulnerabilities in Systems

With the widespread application of big data and artificial intelligence systems, the complexity of systems and software has significantly increased, providing hackers with more opportunities to discover and exploit system and security vulnerabilities, thereby infiltrating networks and obtaining sensitive information. Universities, which possess a large amount of research data and intellectual property, often become targets of attacks. If system vulnerabilities are not promptly patched, the risk of being attacked increases.

2.3.2 Virus and Trojan Infections

The rapid development of big data and artificial intelligence technologies has provided hackers with more opportunities to spread computer viruses and Trojan programs. These malicious software can propagate through networks, infecting and damaging university computer systems. Once infected, computer systems may be controlled, and data may be stolen or destroyed, severely impacting the normal operations of universities and the protection of research outcomes[4].

2.3.3 Network Junk

In the era of big data, the quantity and variety of network junk (such as spam emails, advertisements, and fraudulent information) are continuously increasing, posing challenges to the normal operation of university networks and user experience. Network junk not only wastes network bandwidth and storage resources but may also contain malicious links and fraudulent information, threatening user safety and privacy. If universities lack effective mechanisms for spam filtering and content filtering, the impact of network junk will further expand, continuously polluting the network environment and affecting students' awareness of cybersecurity, potentially even having a negative impact on their values.

3. Cybersecurity Strategies in the Context of Artificial Intelligence

3.1 Enhancing Awareness of Cybersecurity Management

In the context of artificial intelligence and big data, enhancing awareness of cybersecurity management is crucial. First, universities should strengthen cybersecurity education and training by organizing cybersecurity training courses to impart basic knowledge and skills related to cybersecurity to faculty, students, and staff. The training content should include methods for identifying cyber threats and attacks, the use of secure passwords, and prevention of malware, among other topics. Special attention should be given to the applications and challenges of artificial intelligence and big data technologies in cybersecurity to help individuals better understand and address related issues. Additionally, universities should focus on conducting cybersecurity awareness campaigns, utilizing channels such as bulletin boards, posters, websites, and social media to convey the importance of cybersecurity and relevant information to faculty, students, and staff. The promotional content should include successful case studies, practical security tips, and common types of cyber attacks, enabling individuals to better recognize the significance of cybersecurity for both personal and organizational safety[5]. Furthermore, universities should strengthen collaboration and communication with the fields of artificial intelligence and big data. These technologies play a vital role in cybersecurity, and universities and organizations can partner with relevant research institutions, experts, and companies to engage in joint research, project collaboration, and knowledge sharing. This approach can further enhance understanding of the role of artificial intelligence and big data technologies in cybersecurity and explore new cybersecurity solutions.

3.2 Establishing a Comprehensive Security Management System

Establishing a comprehensive security management system is of great significance for maintaining campus network security. Higher education institutions should formulate clear security strategies and policies, which serve as the foundation of the security management system, providing unified guidance and standards for the organization. Institutions should further develop regulations for network usage, data protection policies, and procedures for addressing security vulnerabilities. These policies should align with the organization's business needs and risk tolerance, and they must receive support and promotion from senior management.

Higher education institutions can utilize big data technology to conduct comprehensive risk assessments and analyses of their network systems, applications, and data. This approach can help identify potential security risks and threats, as well as assess their impact on the organization and potential losses. Based on the results of the risk assessment, institutions can implement corresponding security measures, prioritizing high-risk issues to ensure the effective use of security resources.

Additionally, it is essential to develop comprehensive plans to address cybersecurity incidents. To this end, institutions should establish mechanisms for responding to and managing security incidents, including reporting, investigation and analysis, recovery, and remediation. By leveraging big data technology, they can monitor and analyze security incidents in real-time, providing rapid warning and response capabilities. Through the use of big data analytics and artificial intelligence algorithms, it is possible to automate the identification and response to security incidents, thereby accelerating the speed and accuracy of incident resolution.

3.3 Emphasizing Virus Prevention on Campus Networks

Virus prevention is crucial for creating a positive online environment, and universities should establish robust firewalls and intrusion detection systems. Firewalls serve as the first line of defense in protecting university networks from unauthorized access and malware intrusions. Universities should adopt advanced firewall technologies, integrating artificial intelligence and big data to achieve intelligent intrusion detection and defense. By utilizing AI algorithms and big data analysis, it is possible to monitor and analyze network traffic in real-time, identify abnormal behaviors and potential virus attacks, and respond promptly.

Additionally, universities should install and use reliable antivirus software, ensuring timely updates to virus definitions and patches to recognize and prevent new viruses. The application of artificial intelligence and big data technologies can facilitate deep learning and analysis of virus samples, enhancing the accuracy and efficiency of virus detection. To strengthen network security, universities must formulate clear security policies, including restrictions on external access and prohibiting unauthorized devices from connecting to the network[6]. By integrating AI technology, intelligent access control systems can be implemented, which automatically identify and block suspicious network access behaviors based on user behavior and data analysis, thereby reducing the chances of virus transmission.

Finally, universities should conduct regular comprehensive security checks and vulnerability scans of their network systems to promptly identify and rectify system vulnerabilities, minimizing the risk of virus attacks. Artificial intelligence technology can be applied in vulnerability scanning and risk assessment, automatically identifying and evaluating security vulnerabilities within network systems, and providing accurate security remediation recommendations for universities.

3.4 Scientific Norms for Using Computer Networks

Unreasonable applications of computer networks are more likely to lead to cybersecurity issues; therefore, universities should focus on the scientific and standardized use of computer networks. First, it is essential to enhance the security of passwords and identity authentication. Using strong passwords is a crucial measure for protecting personal accounts and data security. Individuals should choose complex passwords that include letters, numbers, and special characters, and change them regularly. Additionally, implementing two-factor authentication (such as mobile verification codes or fingerprint recognition) can provide an extra layer of security to prevent unauthorized access.

Secondly, universities should guide faculty and students to be cautious when clicking on and downloading links, especially those from unknown sources, such as untrusted emails, messages, and websites. These links may contain malware, viruses, or phishing sites, which could lead to personal information leaks or system infections. It is equally important to download software and files only from trusted sources to prevent the spread and infection of malware.

Universities should also regularly update operating systems and applications, as these updates typically include patches that fix security vulnerabilities and enhance security. This practice helps maintain the security and stability of systems, effectively preventing known vulnerabilities from being exploited by attackers. Furthermore, universities should guide faculty and students to recognize the importance of data backup, regularly backing up important personal and institutional data to guard against data loss and ransomware.

Finally, it is advisable to encourage individuals to use trusted security tools and services, selecting verified and reputable options such as antivirus software, firewalls, and virtual private networks (VPNs). These tools and services can provide real-time security monitoring and protection, safeguarding personal privacy and data security.

3.5 Emphasizing the Construction of Cybersecurity Teams

Building a strong cybersecurity team is key to ensuring the safety of the campus network environment. Professional teams should hold nationally recognized certifications, such as the "Cybersecurity Assurance Professional" certificate, to demonstrate their expertise. By participating in specialized cybersecurity training, these individuals can timely update their knowledge, grasp the latest trends, and enhance their ability to tackle complex challenges. Engaging in training and technical seminars organized by industry associations can facilitate communication with peers in the field, share best practices, and strengthen collaboration networks within the cybersecurity domain. The school should encourage team members to proactively learn from the advanced experiences of other enterprises and sister institutions in network management, improving the quality of campus cybersecurity efforts through innovative thinking and effective solutions. These measures are conducive to cultivating a professional and innovative cybersecurity team, providing a solid guarantee for the stable operation of campus networks.

3.6 Ensuring Investment in Cybersecurity Funding

Reasonable budget allocation is crucial for enhancing cybersecurity protection. Schools must ensure that cybersecurity funding is included in the annual financial budget to support the reinforcement and maintenance of existing network infrastructure, as well as the development of emerging security technologies. Regular assessments of information systems' graded protection should be conducted to identify and rectify security vulnerabilities, with at least 5% of the total funding for information construction allocated to cybersecurity, reflecting the school's commitment to protecting information assets and the integrity of academic research. Continuous financial investment is vital for promoting technological advancement and provides a foundation for cultivating and enhancing the capabilities of professional talent and teams. Through financial support, schools can attract and retain experts in the field of cybersecurity, forming a specialized team responsible for developing and implementing cybersecurity strategies to ensure a secure and continuously innovative network environment.

4. Conclusion

In the context of artificial intelligence and big data, cybersecurity issues have become more complex and urgent. By comprehensively utilizing artificial intelligence and big data technologies, universities can better address cybersecurity challenges and effectively protect the network security of universities and other organizations. However, cybersecurity is an ongoing challenge that requires continuous innovation and improvement. Therefore, it is essential to closely monitor technological developments and the evolution of threats, strengthen collaboration and information sharing, and promote advancements and applications in cybersecurity technology. Only through collective efforts can we establish a secure and reliable network environment in the context of artificial intelligence and big data, thereby fostering the sustainable development of a digital society.

References

[1] Zhao Hanqing, Duan Jingfeng, Luo Jialun. Research on Application of Artificial Intelligence Technology in Big Data Network security defense [J]. Network

security Technology and application, 2023(3):19-20.

[2] Quan Bin, Wang Chen. Application of artificial Intelligence technology in Network security defense system [J]. Information Systems Engineering, 2023(2):51-53.

[3] Wang Yuli, Zhang Yiming. Research on Artificial Intelligence Technology to strengthen Network security construction [J]. Cyberspace Security, 2021(Z5):73-78.

[4] Ma Yiwei. Application of artificial Intelligence in Network security defense system [J]. Computer and Network, 2019(15):48-49.

[5] Xu Jing. "Double-edged sword" in the field of artificial Intelligence network security [J]. China Information Security, 2019(7):35-37.

[6] Beware of network security threats brought by the development of artificial intelligence technology [J]. Network Security and Informatization, 2019(4):26-27.