Open Access

The Application of Artificial Intelligence in Computer Network Security Management

Linlin Han

Tianjin Jinghai District First Land and Planning Management Office, Tianjin City, China

Abstract: With the rapid advancement of information technology, computer network security issues have become increasingly prominent. Against this backdrop, this paper briefly outlines the importance of computer network security management, analyzes existing challenges in this field, and discusses the application of artificial intelligence in computer network security management. It aims to provide insights for research and practice in related domains.

Keywords: Artificial Intelligence; Computer networks; Security management; Applications

1. Introduction

Traditional cybersecurity management approaches are increasingly inadequate for addressing the growing complexity and volatility of cyber threats. Consequently, seeking new technological solutions to enhance the efficiency and accuracy of cybersecurity management has become an urgent priority. The rise of artificial intelligence (AI) technology has introduced novel solutions for computer network security management. By simulating human thought and behavioral processes, AI can identify patterns and detect anomalies within vast datasets, thereby providing intelligent support for cybersecurity management.

2. The Importance of Computer Network Security Management

With the rapid advancement of information technology, computer networks have permeated every aspect of our lives. Whether in daily routines, work, or education, we rely heavily on computer network support. However, the open and shared nature of network environments also introduces numerous security risks, making computer network security management critically important. First, computer network security management is essential for protecting personal privacy. In the digital age, personal information has become a vital resource. Its leakage or misuse can inflict significant harm on individuals. For instance, the exposure of personal identity details may lead to identity theft, financial fraud, and other serious issues. Strengthening computer network security management through measures such as encryption technology and access controls can effectively safeguard personal privacy, preventing unauthorized access and exploitation by malicious actors. Secondly, computer network security management plays a vital role in maintaining national security. In modern society, computer networks have become vital infrastructure for national operations, spanning political, economic, and military domains. Attacks or disruptions to these networks could severely impact national security. Hacker attacks, for instance, may lead to critical data leaks or tampering, potentially triggering cyber warfare between nations. Strengthening cybersecurity management and establishing robust network defense systems thus form a crucial safeguard for national security. Finally, computer network security management also plays a vital role in promoting economic and social development. In the information age, computer networks have become a major driving force for economic and social progress. By strengthening cybersecurity management, we can ensure the stability and security of the network environment, providing robust support for the development of e-commerce, e-government, and other sectors. Simultaneously, cybersecurity management can drive innovation and application in network technologies, promote the deep integration of informatization and industrialization, and inject new momentum into economic and social development.

3. Issues in Computer Network Security

3.1 Openness and Shared Nature of Network Environments

With the rapid advancement of information technology, network environments—characterized by their openness and shared nature—have permeated every corner of society. This openness and shared nature not only bring unprecedented convenience to people but also pose severe challenges to computer network security. On one hand, the openness of network environments means anyone can access the internet to publish, disseminate, and exchange information[1]. This openness greatly facilitates information flow and knowledge sharing, enabling people to access needed information and resources more conveniently. However, this openness also provides opportunities for criminals. Hackers, viruses, Trojan horses, and other cyberattack methods proliferate, exploiting the network's openness to infiltrate computer systems, steal critical data, disrupt normal operations, and even cause network paralysis. These attacks not only threaten personal privacy and property security but can also impact business operations and even jeopardize national security and stability. On the other hand, the sharing nature of the network environment enables the distribution of various resources online, including software, documents, videos, and more. This sharing significantly enhances resource utilization efficiency, fostering social collaboration and innovation. However, it also introduces security risks. Malicious software or viruses may disguise themselves as legitimate shared resources, spreading through networks to infect other users and execute attacks or sabotage. Furthermore, access control for shared resources presents a critical challenge. Improper permission settings can lead to unauthorized access of sensitive information, resulting in data breaches and misuse.

3.2 Vulnerabilities in Computer Operating Systems

As the core software of a computer, the operating system shoulders the critical tasks of managing hardware resources and providing a runtime environment for software. However, due to its complexity and diversity, operating systems inevitably contain vulnerabilities and flaws. If exploited by hackers or other malicious attackers, these vulnerabilities pose serious security threats to computer systems. First, operating system vulnerabilities can be exploited by hackers to launch various attacks. Hackers may use vulnerability scanning tools to discover and exploit these weaknesses, thereby gaining access to computer systems. Once inside, attackers might implant malicious code—such as viruses or Trojan horses—to steal user information, disrupt normal system operations, or even take full control of the computer system. Additionally, hackers may leverage operating system vulnerabilities to launch denial-of-service attacks, rendering computer systems inoperable and causing substantial losses for individuals and businesses. Secondly, design flaws in operating systems can also lead to security issues. Some operating systems may have been designed without sufficient consideration for security, resulting in inherent vulnerabilities[2]. For instance, an operating system's permission management mechanism might be inadequate, allowing unauthorized users to execute sensitive operations. Furthermore, flaws in update mechanisms may prevent timely patch installation, leaving systems exposed to known vulnerabilities. Finally, the diversity of operating systems complicates security management. Different operating systems feature distinct architectures, interfaces, and security policies, requiring security administrators to develop tailored security strategies and management measures for each. However, due to human and resource constraints, it is challenging to ensure comprehensive protection for every operating system. In such scenarios, the emergence of new vulnerabilities in any operating system can be rapidly exploited by hackers, posing a threat to the entire network.

3.3 Configuration and Management of Network Devices

In the field of network security, the configuration and management of network devices are critical components. These devices—such as routers, switches, and firewalls—form the cornerstone of computer networks, responsible for data transmission, exchange, and protection. Improper configuration or inadequate management can pose serious security risks to the entire network system. (1). Network device configuration directly impacts network security. Improper configuration can degrade device performance and even trigger security incidents. Take firewalls as an example: as the first line of defense, their configuration rules determine which traffic is permitted and which is blocked. Overly permissive firewall rules may allow unauthorized access, creating opportunities for hackers. Similarly, router configuration is critical. If access control settings are not rigorously enforced, hackers may exploit vulnerabilities to attack the entire network system. (2). Network device management is another vital component of cybersecurity. This includes routine maintenance, updates, and monitoring. Poor management can lead to device failures or security vulnerabilities. For instance, firmware or software flaws in network devices may be exploited by attackers if not promptly patched. Additionally, password management is vital—overly simple or long-unchanged passwords can be guessed or cracked, granting attackers control over the entire device. (3). Human factors also play a significant role in the configuration and management of network devices. Some administrators may lack security awareness or make operational errors, leading to configuration issues. For instance, accidental operations could alter firewall rules, allowing traffic that should be blocked to pass through. Alternatively, administrators might forget to update device firmware or software, leaving devices vulnerable to known security flaws.

4. Application of Artificial Intelligence in Computer Network Security Management

4.1 Real-Time Monitoring and Analysis of Network Traffic

Traditional network security management methods often rely on fixed rules and patterns for traffic filtering and judgment. However, in the face of increasingly complex and dynamic network attack methods, this static approach to protection has proven inadequate. The introduction of artificial intelligence technology enables more precise and efficient real-time monitoring and analysis of network traffic. First, AI can perform real-time traffic analysis through algorithms like deep learning. By training on vast amounts of network traffic data, AI automatically identifies characteristics of normal versus abnormal traffic, accurately flagging potential attack vectors. This data-driven approach proves more flexible and precise than rule-based methods[3]. Second, AI can perform predictive analysis of network traffic based on historical data and attack patterns. By studying past cyberattack data, AI can identify attackers' behavioral patterns and predict future potential threats. This predictive capability enables cybersecurity administrators to develop proactive defense strategies and effectively counter potential attacks. Third, AI enables real-time monitoring and alerting of network traffic. Upon detecting abnormal traffic or potential attack activities, AI immediately triggers alerts to notify cybersecurity personnel for prompt action. This real-time monitoring and alert mechanism significantly enhances the responsiveness and accuracy of cybersecurity management, minimizing losses caused by cyberattacks.

4.2 Vulnerability Scanning and Risk Assessment

In computer network security management, vulnerability scanning and risk assessment are indispensable critical components. The objective of these tasks is to promptly identify potential security risks within network systems and implement effective preventive measures. However, traditional vulnerability scanning and risk assessment often rely on manual processes, resulting in low efficiency and susceptibility to errors. With the continuous advancement of artificial intelligence technology, its automation and intelligence features have revolutionized vulnerability scanning and risk assessment. First, artificial intelligence enables automated vulnerability scanning. Traditional scanning tools are typically limited to detecting known vulnerabilities, proving ineffective against unknown threats. AI, however, leverages deep learning and machine learning technologies to comprehensively analyze a network system's code, configurations, and protocols, uncovering potential hidden vulnerabilities. This automated scanning approach not only significantly enhances scanning efficiency but also identifies more unknown vulnerabilities, thereby providing more comprehensive security protection for network systems. Second, risk assessment quantifies the security threats facing a network system, helping security managers understand its security posture and formulate appropriate security strategies. Traditional risk assessment methods often rely on expert experience and judgment, introducing subjectivity and uncertainty. AI, however, can learn from historical data and attack patterns to build precise risk assessment models, enabling objective and accurate evaluations of a network system's security posture. This data-driven approach provides a more accurate reflection of the system's security status, offering security administrators more valuable decision support[4]. Furthermore, AI can deliver personalized remediation recommendations. AI can generate tailored remediation recommendations based on the specific context of the network system and the characteristics of the vulnerabilities. These recommendations encompass not only concrete remediation steps and methods but also critical considerations and potential risks during the remediation process. Such personalized guidance enables security administrators to address vulnerabilities more swiftly and accurately, thereby enhancing the overall security of network systems.

4.3 Building Intelligent Firewalls and Intrusion Detection Systems

Among the numerous aspects of computer network security management, firewalls and intrusion detection systems serve as two critical lines of defense. They effectively counter external threats, safeguarding the secure and stable operation of network systems. On one hand, the implementation of intelligent firewalls renders network security protection more intelligent and dynamic. Traditional firewalls typically employ static filtering rules, unable to adapt to real-time changes in the network environment. Intelligent firewalls, however, leverage artificial intelligence to analyze network traffic in real time, identifying characteristics of both normal and abnormal traffic. Based on these analyses, they dynamically adjust protective strategies. This intelligent approach more effectively intercepts malicious traffic, preventing attackers from exploiting vulnerabilities. Additionally, intelligent firewalls perform predictive analysis using historical data and attack patterns to proactively identify potential threats. By training and learning from vast amounts of network traffic data, intelligent firewalls can summarize attackers' behavioral patterns and predict future potential network threats. This predictive analysis helps cybersecurity administrators proactively develop defense strategies and promptly address potential security risks[5]. On the other hand, intrusion detection systems (IDS) serve as another critical line of defense in cybersecurity management. Traditional IDS systems typically only detect known attack patterns and are ineffective against unknown attack methods. AI-based intrusion detection systems, however, enable real-time, comprehensive monitoring of network systems. Through technologies like deep learning and machine learning, these systems automatically identify abnormal behaviors and attack indicators within the network, promptly issuing alerts and initiating appropriate countermeasures. This intelligent intrusion detection approach significantly enhances the efficiency and accuracy of cybersecurity management, safeguarding network security. Furthermore, intelligent firewalls and intrusion detection systems can operate synergistically to form a more robust cybersecurity defense framework. Intelligent firewalls intercept malicious traffic and prevent external attacks, while intrusion detection systems monitor internal network security conditions, promptly identifying and addressing potential security risks. Complementing and collaborating with each other, they jointly construct a solid cybersecurity defense line.

5. Conclusion

In summary, the application of artificial intelligence in computer network security management has achieved remarkable results, providing robust support for cybersecurity protection. Through automation and intelligent methods, AI can effectively enhance the efficiency and accuracy of network security management while reducing security risks. Future research should continue monitoring AI technological advancements while refining and optimizing relevant algorithms and models to maximize their contribution to computer network security management. Concurrently, interdisciplinary collaboration and knowledge exchange must be strengthened to collectively drive innovation and progress in this field.

References

[1] Luo, X. Research on the Application of Artificial Intelligence in Computer Network Technology in the Era of Big Data. *Modern Industrial Economy and Informatization,* 2020, 10(12): 97–98.

[2] Feng, C. A Brief Discussion on the Application of Artificial Intelligence in Computer Network Technology under the Background of Big Data. *Computer Knowledge and Technology*, 2020, 16(36): 34–35.

[3] Zhang, Y. Research on Big Data Security and Privacy Protection Based on Cloud Computing. *Electronic Technology and Software Engineering*, 2020, 0(21): 255–256.

[4] Si, K., Fan, T., & Fan, L. Effective Application of Artificial Intelligence in Computer Network Technology under the Background of Big Data. *Computer Knowledge and Technology*, 2020, 16(33): 176–177.

[5] Guan, E. Application of Artificial Intelligence in Computer Network Technology in the Era of Big Data. *Digital Communication World*, 2020, (12): 154–155.