HiLL PUBLISHING

Cybersecurity and Information Assurance, 2026, 1(1), 6-9
https://www.hillpublisher.com/Journals/cia/
ISSN Online:

Application of Artificial Intelligence in Network Security Defense

Shaoxiong He[1,*], Zhibin Liu[2], Zhiyue Xie[3]

[1]School of Management Science and Engineering, Dongbei University of Finance and Economics, Dalian 116025, Liaoning, China.
[2]College of Computer and Control Engineering, Qiqihar University, Qiqihar 161006, Heilongjiang, China.
[3]College of Computer and Big Data, Fuzhou University, Fuzhou 350116, Fujian, China.

How to cite this paper: Shaoxiong He, Zhibin Liu, Zhiyue Xie. (2026). Application of Artificial Intelligence in Network Security Defense. *Cybersecurity and Information Assurance*, 1(1), 6-9.
DOI: 10.26855/cia.2026.06.002

Received: November 22, 2025
Accepted: December 16, 2025
Published: January 22, 2026

***Corresponding author:** Shaoxiong He, School of Management Science and Engineering, Dongbei University of Finance and Economics, Dalian 116025, Liaoning, China.

Abstract

The application value of artificial intelligence technology is more prominent in all walks of life. It can not only facilitate various operations, but also help to meet the expected management requirements. In network security defense management, more and more technical personnel integrate artificial intelligence technology to quickly cope with the security risks in the system, reduce the occurrence of security problems, reduce the cost of network security work, reduce the workload of network security staff, meet the requirements and standards of network security operation, Through the implementation of AI cybersecurity defense systems will be able to improve detection and response speed, and more actively anticipate and deal with emerging threats. Highlight the advantages of artificial intelligence technology itself.

Keywords

Artificial intelligence; Network security; Defensive measures; Safety inspection

1. Introduction

With the increasing prevalence of artificial intelligence (AI) in society, it has also entered the field of cybersecurity. AI can help improve cybersecurity in many ways, including automatically detecting and responding to threats, improving network efficiency, and helping to identify vulnerabilities. Computers are increasingly used in people's daily learning and lives, becoming essential tools for both work and life. With the rapid development of China's network technology, the openness of the network itself is becoming increasingly apparent. Security issues are becoming more diverse. To achieve effective security protection, it is necessary to fully leverage the advantages of AI technology and ensure comprehensive maintenance of network operations, while also integrating innovative technological solutions to ensure the stability and security of computer networks. Summarizing rich experience and building a more mature security defense mechanism will promote the sustainable development of China's network technology industry.

2. The Role of Artificial Intelligence in Cybersecurity Defense

2.1 Well-developed learning and reasoning abilities

The advantages of integrating artificial intelligence technology into network security defense are more prominent. First, the reasoning ability of artificial intelligence technology itself can be used to judge other security risks, meet the needs of network security defense work in multiple directions, and reduce the occurrence of various security

Note: The article was originally published in *Advances in International Computer Science*, and this is an authorized translation of it.

problems. In terms of network environment management, advanced protection technology should be the main support, and the functions of artificial intelligence technology itself should be used to effectively coordinate various control modules and infer other security risks based on reasoning ability, thereby solving past security problems. Improve the problems existing in defense and improve the overall management level. In the past network security defense process, due to the limitations of technical means, there are many uncertainties in the processing of insecure information, and some omissions will also occur. Therefore, it is necessary to make full use of artificial intelligence technology in actual work. Based on its own advantages, network defense management should be done well, and the learning and reasoning ability of artificial intelligence technology itself should be used to effectively manage and supervise various data (Liu, 2020). Using a certain data as the main reason for inferring other security systems, the hidden dangers in the system can be discovered in time, further ensuring the processing efficiency of the data itself, maintaining the security of China's current network environment, and highlighting the advantages of artificial intelligence technology itself.

2.2 Powerful fuzzy information processing capabilities

When artificial intelligence technology is integrated into network security defense, it can also make full use of the fuzzy information processing capability of artificial intelligence technology, which has a strong ability to respond to unpredictable security risks and emergencies, and reduces the impact on system operation (Lan, 2020). In the process of modern network development, the openness of the network operation process is more prominent, which will lead to the gradual increase of information types and the continuous acceleration of the spread speed. In addition, with the functions of Internet communication and interconnection, some information security is difficult to be effectively determined, which in turn affects the effectiveness of information security management (Wu, 2017). Therefore, in practical work, it is necessary to make basic judgments on information by using the fuzzy information processing capability of artificial intelligence technology itself, eliminate the impact of various uncertain factors on network security management, and also integrate different network security management resources to process the corresponding information. For example, in the process of technology implementation, based on the content collected by fuzzy information processing, summarize rich work experience, formulate a special security management model, and reduce the impact of various security risks on network system operation. Comprehensively strengthen the overall security management effect and avoid the occurrence of various emergencies.

2.3 Strong network defense cooperation capabilities

Strong network defense collaboration capability is also an important function of integrating artificial intelligence technology into network security defense. With the development of network technology in China, the application functions are becoming more and more complex, which also increases the probability of problems to a certain extent. In the process of optimizing the technical model, it is gradually developing towards a systematic trend. Against this background, many requirements are put forward for network security defense capabilities. Therefore, in practical work, it is necessary to realize the innovative development of technical models and use artificial intelligence technology to complete the current security defense tasks. In practical work, different levels of intelligent management systems can be established to realize effective supervision of each link, and then run through each link. Mutual cooperation and connection, build a complete working system, and fully guarantee the effect of network security defense (Jiang, 2019).

2.4 Low cost of working defense

Traditional network security systems consume a lot of resources during the calculation process and have low security efficiency, resulting in high overall network security defense costs, which is not conducive to the relevant departments to achieve economic and social benefits. Using artificial intelligence technology in network security defense can effectively avoid the high cost of traditional defense methods. This is because artificial intelligence technology can use a large number of advanced algorithms to achieve accurate data development, calculate the accuracy of relevant data, and realize intelligent security management. It greatly improves the utilization efficiency of various resources and realizes the optimized configuration of network data. This effectively reduces the development cost of software and hardware systems in cost calculation and lays a solid foundation for the in-depth promotion of artificial intelligence technology (Qin & Zhang, 2018).

3. Specific Applications of Artificial Intelligence Technology in Cybersecurity Defense

3.1 Intelligent Firewall Technology

When integrating artificial intelligence technology into network security defense, it is necessary to continuously innovate and adjust on the basis of the original technical solutions, and then innovate the existing management system according to the requirements and standards of network security defense, which is more in line with the development direction of modern networks. For example, in actual work, artificial intelligence technology can be integrated into firewalls to achieve good protection effects. Firewalls belong to the category of isolation control technology, which includes filtering technology and state detection technology. In the process of using artificial intelligence technology, corresponding data packets can be transmitted at the network layer, making the firewall's protection and control more accurate. Then, according to the requirements of security protection, the data packet address should be analyzed, and external information should be checked one by one to reduce the occurrence of security risks (Ma, 2020). In addition, artificial intelligence technology can also be integrated into state monitoring. Different data packets need to be constructed to comprehensively supervise various security risks and effectively maintain the security factors of the network environment itself.

3.2 Automatic Detection Technology

The first step in protecting a company's network is threat detection. Rapidly detecting unreliable data is ideal, protecting the network from permanent damage. Combining artificial intelligence (AI) with cybersecurity is the best way to detect and respond to threats in real time. AI examines the entire system for risks. Unlike human intelligence, cyber AI can detect risks earlier, generating faster and more accurate security alerts, thus improving the efficiency of cybersecurity professionals.

Automatic detection technology is mainly used for scientific protection of email. Email has become an important item in people's daily life. Although it has facilitated every work behavior, people will be affected by different types of spam in this process. Not only will the amount of information received gradually increase, but if the security awareness is not strong, clicking on the link in the spam email may lead to the computer being invaded by the virus. Therefore, in actual work, it is necessary to use artificial intelligence technology to improve the existing detection mode and avoid serious impact on network security management (Yu, 2020). In the process of system application, the received information can be effectively detected, and then quickly analyzed to see if it contains a virus. It can be compared with the virus database data, and the threat factors should be deleted immediately. This can introduce the impact of various cumbersome information on security management, build a more stable network information security environment for people, and improve the use effect of artificial intelligence technology itself.

3.3 Artificial Neural Network Technology

The application of artificial neural network technology in security defense is also quite important. It can achieve a comprehensive security effect. Artificial neural networks themselves have strong analytical capabilities, enabling them to quickly classify and select various malicious information. They can also utilize their learning and data processing capabilities to store and share information, fully leveraging their diverse advantages to establish a robust security defense system. They can build time-series-based predictive models to quickly identify viruses in computers, making security protection more accurate and meeting the requirements of modern security management. Simultaneously, users can obtain more accurate defense results based on data analysis, understand the basic operating status of their computers, and then formulate more scientific security measures, ensuring that the operation of each device has a high security level and meets daily usage requirements.

3.4 Intrusion Risk Prediction

Predictive analytics for identifying anomalous behavior or activity patterns is one of the main applications of artificial intelligence in cybersecurity. Cybercriminals are always looking for new ways to use this system. AI can help identify these new threats before they cause any damage. AI systems help determine an inventory of IT assets and provide a complete and accurate list of various systems with different access permissions for all devices, users, and applications. Now, considering asset inventory and threat exposure (as described above), AI-based systems can predict how and where they are most likely to be hacked, enabling them to plan which resources are most vulnerable. This intrusion

risk prediction will help organizations prepare, limit impact, and break attack chains. Furthermore, risk data, policies, and procedures can be developed and modified to improve network resilience through AI-based analytics.

3.5 Expert System

Expert systems are a relatively mature technology in the field of artificial intelligence. They include reasoning capabilities and knowledge bases, and after simulating and learning based primarily on expert knowledge, they can handle various problems in network security defense, comprehensively improving the overall processing effectiveness. The application of expert systems relies heavily on the quantity and expertise of the knowledge base itself. To enhance overall security protection, advanced detection systems can be integrated for auxiliary use. These systems perform in-depth detection of massive amounts of information according to system operation requirements, then integrate different security characteristics and behaviors, accurately calculate system parameter patterns, and quickly identify abnormal rules to protect against various intrusion attempts and reduce the occurrence of security problems.

4. Conclusion

Integrating artificial intelligence (AI) technology into cybersecurity defense offers significant advantages. It not only allows for flexible responses to cybersecurity challenges but also facilitates the upgrading and updating of security technology models. AI can be a powerful tool in combating cybercrime. Through automation, tasks currently performed by human security analysts can be automated, reducing false alarms and accelerating detection and response processes. More importantly, it's crucial to recognize the potential risks associated with using AI and take measures to mitigate them, creating a favorable environment for people to use the internet. Therefore, in practice, it's necessary to deepen the understanding of AI technology applications, update existing technical solutions, and enhance the effectiveness of cybersecurity defenses.

References

Jiang, F. (2019). Application of artificial intelligence technology in big data network security defense. *Computer Products and Circulation*, (4), 148-149.

Lan, F. (2020). Research on the application value of artificial intelligence technology in network security defense. *Digital Technology and Application*, *38*(10), 186-188.

Liu, Y. (2020). A brief discussion on artificial intelligence and its implementation strategies in computer network technology. *Computer Products and Circulation*, (4), 148.

Ma, Y. (2020). Design of computer network security defense system based on big data and artificial intelligence technology. *Information and Computer (Theoretical Edition)*, *32*(4), 208-209.

Qin, L., & Zhang, X. (2018). Research on the application of artificial intelligence technology in network security defense. *Journal of Chifeng University (Natural Science Edition)*, *34*(8), 55-56.

Wu, J. (2017). An exploration of the application of artificial intelligence technology in network security defense. *Computer & Network*, *43*(14), 60-61.

Yu, Z. (2020). Exploring the application of artificial intelligence technology in cyberspace security defense. *Computer Products and Circulation*, (1), 146.