2025 International Journal of Management Science Research, Vol.8, Issue 6, (Jun)
ISSN 2536-605X
DOI: 10.53469/ijomsr.2025.08(06).06

Application of Artificial Intelligence Technology in Cyberspace Security Defense

Jun Wang

Weicheng District, Xianyang City, 712082
2145324770@qq.com

Abstract: ***The application of artificial intelligence technology in cyberspace security defense is helpful to improve network information security. Based on this, this paper takes the overview of cyber defence and artificial intelligence technologies as the point of departure, and compares and analyzes the advantages of artificial intelligence technologies over traditional cyber defence technologies. We explored the application practices of relational rule mining technology, neural network technology, and intelligent firewall technology in network security defense. In network security defense, deepening the application and promotion of artificial intelligence technology can fully tap the value of artificial intelligence technology in information security protection, effectively resist various security threats, and provide guarantee for cyberspace security.***

Keywords: Artificial intelligence technology; Cybersecurity defense; Application.

1. INTRODUCTION

At present, China's economic development is becoming more and more rapid, and the corresponding development speed of network and computer technology is also accelerating, which has promoted the development of artificial intelligence technology and made this technology widely used in many industries, and people attach more and more importance to it. The development potential of artificial intelligence technology is great, it is a new type of technology that is widely used in cybersecurity defense and has high security, which plays a very important role in reducing the incidence of security incidents. This paper analyzes the application of artificial intelligence technology in data network security defense. Zeng et al. (2025) examined how education investment and social security influence household financial market participation, emphasizing socioeconomic implications[1]. In the educational domain, [2] Wang et al. (2024) proposed an AI-powered framework for early identification of learning difficulties, while [3] Wang (2025) developed a joint training model for recommendation systems with non-random missing data. AI's role in empathy evaluation was explored by [4] Chen et al. (2024), who introduced "Emotionqueen," a benchmark for assessing large language models' empathy. Healthcare applications feature prominently, with [5] Ding and Wu (2024) conducting a systematic review of self-supervised learning for biomedical signal processing, and [6] Restrepo et al. (2024) presenting a multimodal deep learning approach for low-resource healthcare settings. [7] Yang et al. (2025) demonstrated IoT-driven skin cancer detection using active learning, while [8] Jiang et al. (2025) developed a meta-attention-enhanced model for AI-generated news detection. Sustainability is addressed by [9] Wu et al. (2025), who analyzed supply chain digitalization's impact on energy efficiency and carbon neutrality. Technical innovations include [10] Peng et al. (2022)'s domain adaptation framework, [11] Zheng et al. (2025)'s motion-aware diffusion model for human mesh recovery, and [12] Zhang et al. (2025)'s machine learning-based anomaly detection in biomechanical data. [13] Zhou et al. (2024) investigated LSTM-based UAV path planning, and [14] Tu (2025) introduced an intelligent log analysis system for network optimization.

2. OVERVIEW OF NETWORK SECURITY DEFENSE AND ARTIFICIAL INTELLIGENCE TECHNOLOGY

2.1 Overview of Network Security Defenses

Network security defense refers primarily to the application of various technologies and methods to protect and defend computer networks from viruses and Trojans threats and intrusions. There are many defense methods and technologies for cybersecurity defense, generally using surveillance and detection methods for defense, and the effectiveness of defense is inconsistent. At present, the most widely used technologies for network security defense are passive information protection technology, intrusion detection technology, and active deception technology. With the widespread and deepening of cyberspace applications, cyberspace security defense also puts

new requirements on traditional network technologies, and artificial intelligence technology is one of the key technologies.

2.2 Overview of Artificial Intelligence Technology

Artificial Intelligence is about the intelligent behavior of artificial objects, and intelligent behavior includes perception, reasoning, learning, communication, and behavior in responsible environments. (Nilsson, 1998). Artificial Intelligence (AI) is a new technology in the field of modern computer science and technology. With the continuous development of modern science and technology, it can simulate human thought activities for system protection, and when the network is subjected to external threats and attacks during use, it can implement system defense protection autonomously. When applying artificial intelligence technology in practice, it requires the coordination and integration of various disciplines, so that it can achieve the mutual penetration and integration of the theory and technology to form intelligent technologies that mimic the activities of the human brain.

3. THE ADVANTAGES OF ARTIFICIAL INTELLIGENCE TECHNOLOGY IN NETWORK SECURITY DEFENSE

3.1 Advantages of fuzzy data reasoning capabilities

Artificial intelligence technology can realize fuzzy information reasoning for ambiguous and nonlinear information, allowing it to effectively discern the source and type of information, especially in the detection and defense of unknown viruses, and the defense capability of artificial intelligence technology is stronger. The application of artificial intelligence in fuzzy information processing can effectively defend network information and improve the security and certainty of network information.

3.2 Advantages of learning to reason

The application of artificial intelligence technology can rely on its powerful learning, reasoning and other capabilities to compensate for the shortcomings of traditional security defense technology, and achieve effective identification and defense of different network resources and attacks through the establishment of network security systems and databases. Therefore, the learning and reasoning capabilities of artificial intelligence technology can effectively improve cyberspace security defense capabilities, and make up for the shortcomings of traditional defense systems through the continuous generation of elements of security prevention mechanisms. At the same time, in the face of a large database, the query, reasoning analysis and other functions of artificial intelligence technology can discover effective information in a timely manner, establish security defense responses, and better improve the effectiveness of cyberspace security defense.

4. IMPORTANT ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN CYBER SECURITY DEFENSE SYSTEMS

4.1 Association Rule Mining Techniques

In the transmission and processing of huge amounts of complex network information, it is necessary to adopt a rules-given association technology, comprehensively analyze the operation of equipment and data transmission within the network system, and grasp the relationship existing between network security hazards, alarm events, and existing log data. The process mainly matches the sequence template after the network security attack and alarm event, with the corresponding rule sequence of the security event, and verifies the data information and digital signatures being passed, so as to reduce the illegal control of the network security system. Therefore, the planning department of AIS mainly establishes the collection interface of public incident information resources, and uses relational data mining, Expert evaluation and other methods extract code data related to network security attacks and alarm events from the huge data resources of the backend database, accurately identify various intrusion risks, form a set of security resource categories for the associated engine, and store them in the backend data.

4.2 Neural Network Techniques

Stable neural networks are usually built based on a number of simple processing elements, have good compatibility and excellent learning capabilities, and can accomplish distributed storage of various types of information in a very short time. In the process of using ANN, it can meet the actual needs of various information processing, and accomplish the automatic organization of relevant knowledge. In addition, the neuron computation in the neural network is generally independent and can complete the parallel processing work. At present, the existing software and hardware can ensure its value and advantage. The application of neural network technology to computer network security defense work is generally reflected in the detection of network intrusion. This is because neural network technology can accurately identify unwanted information, bad software, etc. in computer networks, thereby assisting in the analysis and processing of computer network information. In addition, agent decision algorithm is an important means in network monitoring and management, and the integration of neural network technology can effectively strengthen network monitoring efficiency and quality, on the one hand, and also protect against the generation of various small monitoring errors. When conducting network worm virus detection work, neural network technology can also meet the detection requirements well. Unlike previous detection methods, neural network technology has a high degree of efficiency and accuracy, while also being able to accurately identify various types of worms. At present, the field of computer science attaches great importance to the research of neural network technology and has promoted the continuous progress of related fields, and the application of neural networks technology to cyberspace security defense has gradually increased, laying the foundation for promoting the improvement of cyberspace security and defense capabilities.

4.3 Intelligent firewall technology

Firewalls are commonly used defense means for computer network security, which can identify and control security hazards in the network, thus providing good protection for computer equipment. Traditional firewall technology includes data packet filtering, network address translation (NAT), protocol status checking, and VPN function, but the application of these firewalls does not achieve the expected results, and it is difficult to fully and effectively protect against security hazards. The intelligent firewall based on artificial intelligence technology has intrusion detection capabilities that can be applied to intelligent identification of external intrusion hazard elements. At the same time, the relevant analysis and control of data through computation, statistics and memory data content, realize the calculation of huge amounts of data in the network, discover the content of feature values in the network and conduct relevant security access control defense to improve the interception capability of harmful information.

5. CONCLUSION

In summary, cybersecurity defense needs advanced technology to support, and AI technology as an emerging technology with its learning capabilities and fuzzy data processing capabilities, It is more suitable for the development of cybersecurity defense, and the application of artificial intelligence technology can not only effectively improve the problems existing in cybersecurity prevention, but also improve the effectiveness and technicality of cybersecurity management, which has great advantages for promoting the development of China's cybersecurity Defense.

REFERENCES

[1] Zeng, Yuan, et al. "Education investment, social security, and household financial market participation." Finance Research Letters 77 (2025): 107124.
[2] Wang, Chun, Jianke Zou, and Ziyang Xie. "AI-Powered Educational Data Analysis for Early Identification of Learning Difficulties." The 31st International scientific and practical conference “Methodological aspects of education: achievements and prospects”(August 06–09, 2024) Rotterdam, Netherlands. International Science Group. 2024. 252 p.. 2024.
[3] Wang, Hao. "Joint Training of Propensity Model and Prediction Model via Targeted Learning for Recommendation on Data Missing Not at Random." AAAI 2025 Workshop on Artificial Intelligence with Causal Techniques. 2025.
[4] Chen, Yuyan, et al. "Emotionqueen: A benchmark for evaluating empathy of large language models." arXiv preprint arXiv:2409.13359 (2024).
[5] Ding, Cheng, and Chenwei Wu. "Self-Supervised Learning for Biomedical Signal Processing: A Systematic Review on ECG and PPG Signals." medRxiv (2024): 2024-09.
[6] Restrepo, David, et al. "Multimodal Deep Learning for Low-Resource Settings: A Vector Embedding Alignment Approach for Healthcare Applications." medRxiv (2024): 2024-06.

[7] Yang, Jing, et al. "IoT-Driven Skin Cancer Detection: Active Learning and Hyperparameter Optimization for Enhanced Accuracy." IEEE Journal of Biomedical and Health Informatics (2025).
[8] Jiang, Chenxi, et al. "LMAT-ND: A Meta-Attention-Enhanced Llama-7B Model for AI-Generated News Detection." 2025 5th International Conference on Consumer Electronics and Computer Engineering (ICCECE). IEEE, 2025.
[9] Wu, W., Bi, S., Zhan, Y., & Gu, X. (2025). Supply chain digitalization and energy efficiency (gas and oil): How do they contribute to achieving carbon neutrality targets?. Energy Economics, 142, 108140.
[10] Peng, Qucheng, et al. "RAIN: regularization on input and network for black-box domain adaptation." arXiv preprint arXiv:2208.10531 (2022).
[11] Zheng, Ce, et al. "Diffmesh: A motion-aware diffusion framework for human mesh recovery from videos." 2025 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV). IEEE, 2025.
[12] Zhang, Shengyuan, et al. "Research on machine learning-based anomaly detection techniques in biomechanical big data environments." Molecular & Cellular Biomechanics 22.3 (2025): 669-669.
[13] Zhou, Dianyi, et al. "Research on LSTM-driven UAV path planning." Fourth International Conference on Advanced Algorithms and Neural Networks (AANN 2024). Vol. 13416. SPIE, 2024.
[14] Tu, T. (2025). Log2Learn: Intelligent Log Analysis for Real-Time Network Optimization.

Author Profile

Jun Wang birth date: 1973.1, ethnicity: Han, gender: female, place of origin: Shaanxi, organization: Central Tibetan National University, position: nil, title: Senior Engineer, qualification: Master, Zip code: 712082, research interest: Computer network security.