DOI: 10.53469/wjimt.2025.08(05).06

Application of Artificial Intelligence Technology in Cyber Security Defense

Hailong Guo

Guangzhou City Planning Exhibition Center, Guangdong 510000, Guangzhou, China

Abstract: ***The development of the internet has brought unprecedented convenience, but due to its open nature, the use of the internet also faces both internal and external network security challenges. Strengthening cybersecurity defense capabilities and effectively safeguarding network security during the digital transformation in the internet age is a significant challenge. The development of artificial intelligence technology has driven the emergence of new types of network cybersecurity defense techniques. Leveraging artificial intelligence, network cybersecurity defense is shifting from traditional passive security response to active security defense. This paper primarily explores the application of artificial intelligence technology in network cybersecurity defense.***

Keywords: Artificial Intelligence; Cyberspace; Network Security Defense.

1. INTRODUCTION

With the continuous deepening of globalization, rapid development of information technology, and rapid changes in the international situation, China's cyberspace security is facing severe challenges, and cyberspace security issues have seriously affected national security. How to effectively resist external network attacks and quickly identify internal network security risks has become an urgent problem to be solved in the current development of network security technology. Where should we start breaking the deadlock? Reasonably utilizing artificial intelligence technology may be a crucial step. The use of artificial intelligence technology can mimic the technical characteristics of human thinking, making it possible to independently carry out network security defense, system maintenance, and other work. The application of artificial intelligence technology is of great significance in promoting the development of network protection technology.

2. ARTIFICIAL INTELLIGENCE TECHNOLOGY

2.1 Introduction to Artificial Intelligence Technology

Artificial intelligence technology is a cutting-edge technology in current information science. In recent years, artificial intelligence technology has become a popular research direction, with applications such as ChatGPT frequently entering our field of vision, bringing qualitative changes to production and life. Academically speaking, artificial intelligence technology is divided into two categories: "strong" and "weak". Weak artificial intelligence "refers to machine learning algorithms based on mathematical technology. Designers need to predict various situations that will be encountered in practical use and use computers to determine their feasibility. Once the preset range is exceeded, weak artificial intelligence will be unable to cope. Strong artificial intelligence has stronger "thinking ability". It has the same thinking ability as humans and a certain degree of self-learning ability. Even when faced with things beyond the preset program scope, it can make autonomous decisions, make judgments, and issue specific operational instructions. In GPU-accelerated neural networks, Xie et al. [1] proposed RTop-K, an ultra-fast row-wise top-K selection algorithm, optimizing computational efficiency for deep learning workloads. Parallelly, applications in healthcare and behavioral sciences have emerged: Lin et al. [2] demonstrated the efficacy of intelligent physical exercise monitoring in enhancing executive function among ADHD children, while Peng et al. [3] explored how aerobic exercise intensity influences executive function and sleep. In logistics robotics, Luo et al. [4] developed a path-planning algorithm integrating Transformer and GCN networks, improving autonomous navigation. Consumer-centric AI tools have also gained traction. Xu et al. [5] designed experience management systems for electric vehicles using perceived-value metrics, and Shan et al. [6] analyzed cross-cultural implications of LLMs in human-computer interaction. Clinical AI advancements include Shen et al. [7]'s LSTM-based anesthetic dose management system for cancer surgery and Xu et al. [8]'s analysis of adversarial attacks in cybersecurity. Autonomous systems are further explored by Wang et al. [9], who outlined an end-to-end AI framework for self-driving cars. Privacy and model robustness remain critical. Liu et al. [10] introduced a hybrid ensemble model for anomaly detection with privacy preservation, and Guo et al. [11] addressed imbalanced

data challenges via focal loss. Weng et al. [12] proposed adaptive weighting for multi-task model fusion, enhancing scalability. Sentiment analysis, as studied by Dai et al. [13], aids enterprise service optimization, while Xing et al. [14] improved traffic forecasting via fuzzy spatiotemporal GNNs. Differential privacy in NLP was surveyed by Wu et al. [15], complementing their work on origin-destination flow prediction [16]. Financial forecasting advancements were reviewed by Fang et al. [17], and Yu et al. [18] optimized intersection management using social-value algorithms. Finally, Gao et al. [19] enhanced retrieval-augmented generation by combining ScaNN and Gemma with LLMs, showcasing AI's evolving versatility.

2.2 The significance of applying artificial intelligence technology in cyberspace

The security defense of cyberspace has become an indispensable task, and to do a good job in security defense, network security monitoring is often the most critical part. Timely "discovery" of dangers is the foundation for ensuring network security. In today's era of information explosion and data explosion, network security defense is aimed at enhancing the anti attack capability of network systems, preventing false and harmful information from spreading in cyberspace, providing reliable information transmission for ordinary users who lack network security defense capabilities, and ensuring data security. With the development and popularization of information technology, people have gradually realized the importance of network defense efficiency and network security, and have conducted more research on them. Especially at present, with the increasingly severe problems of cybercrime and cyber attacks, in order to ensure the information security of users, network systems must have high emergency response capabilities and security defense capabilities. Introducing artificial intelligence technology into the field of cybersecurity defense can improve defense efficiency, effectively reduce incidents such as information system failures caused by attacks, and is of great significance for enhancing the security and overall performance of information systems. Artificial intelligence technology can be applied to various network information processing tasks. It can not only analyze and identify unknown network information, but also perform tracking and other processing operations to ensure the security of network systems.

3. THE SUPERIORITY OF USING ARTIFICIAL INTELLIGENCE TECHNOLOGY FOR SECURITY PROTECTION IN CYBERSPACE

3.1 Ability to analyze ambiguous messages

Compared with other types of network security defense technologies, artificial intelligence technology can efficiently detect unknown information and process fuzzy information systematically, comprehensively, and efficiently, thus improving the overall security defense efficiency and capability. When using the Internet, users are often attacked by some unknown viruses. If these viruses cannot be accurately identified, it is difficult to develop targeted prevention strategies. Failure to prevent virus attacks may cause various losses to users. By utilizing the fuzzy information processing capability of artificial intelligence technology, a series of complete identification can be carried out on fuzzy information in the network. If it has threat characteristics, artificial intelligence defense technology can respond to it in a timely manner, block or intercept its attack behavior, thereby reducing the harm caused and improving the security level of the network.

3.2 Strong adaptability to nonlinear problems

At present, domestic networks have high complexity, and the probability of unknown events occurring in the network is relatively high, which greatly increases the nonlinear effects faced by devices within the network. Conventional security protection techniques cannot provide complete and effective protection for the network. How to effectively apply artificial intelligence technology to the security defense of cyberspace can greatly enhance the computer's ability to process and control nonlinearity, thereby effectively controlling network threats, preventing devices from being attacked by various types of attacks on the network, and further improving the security defense capability of cyberspace, providing users with a better user experience.

3.3 Possess good teamwork spirit

With the continuous development of information technology, the number of information technology infrastructure is constantly increasing, the scale of networks is also constantly growing, and the structure of networks has become more complex, which puts higher demands on the security protection of cyberspace. To enhance the overall network security, it is necessary to strengthen the efficient connections between various systems, and effectively control various attack events by adopting corresponding hierarchical management methods, keeping their

probability of occurrence within a reasonable range. The use of artificial intelligence technology can enhance cooperation among different network security defense managers, ensuring that the security defense measures adopted by each level of security managers can work closely together, gradually establishing a complete network security defense system and providing better protection capabilities for network security.

4. THE SPECIFIC APPLICATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGY IN CYBERSPACE SECURITY DEFENSE SYSTEM

4.1 Artificial Neural Network Technology

Trusted neural networks are typically composed of a series of simple processing elements, with good fault tolerance and self-learning capabilities, and can effectively perform distributed data storage. Neural networks can adapt to various specific information processing needs and achieve the goal of knowledge self-organization. At the same time, the neuron operations of neural networks are relatively independent and can perform parallel operations, and existing software and hardware can ensure their computational efficiency. Neural network technology is mainly used for network intrusion detection, which can discover and process junk information or malicious programs existing in the network. Introducing neural network technology into intelligent decision-making algorithms for network monitoring can significantly enhance the effectiveness of network monitoring and avoid many error phenomena that may occur during the monitoring process. Compared to conventional detection methods, neural network technology has significant advantages in efficiency and accuracy, and can even detect new worm viruses.

4.2 Intelligent Firewall Technology

In network security protection, the most common defense device is the firewall, which can identify and control security risks in the network, effectively protecting devices inside the wall. Generally speaking, various firewalls have been deployed in traditional cyberspace, but their deployment and use cannot achieve ideal defense effects, making it difficult to completely and effectively resist security risks. However, artificial intelligence firewall technology is different. It has significant advantages, as it can statistically analyze and judge various security risks in the network, efficiently intercept potential risks, and solve them, thereby avoiding malicious attacks or potential malicious attacks. Compared with traditional firewalls, intelligent firewall technology has improved and enhanced defense capabilities, with more comprehensive functions and more obvious security protection effects. In addition, it can optimize security access control defense mechanisms to ensure network security.

4.3 Intrusion detection technology

In the process of security protection in cyberspace, it is also necessary to monitor intrusion viruses or other risk hazards. It is necessary to have a clear understanding of the destructive power caused by these risk factors after entering the network or system, and to control them before threats appear to avoid harm to the network or system. Although traditional cybersecurity defense measures also include some monitoring methods and technologies, these methods may have some defects or unclear monitoring objects. Therefore, artificial intelligence technology must be used to improve these problems and achieve more reliable monitoring and control effects. The use of artificial intelligence intrusion detection technology can intelligently identify all information, find whether there are security risks, and use effective control methods to solve them, thereby ensuring the safe operation of cyberspace. At present, intelligent intrusion detection technology has been widely applied in the network security defense of enterprises or industry organizations, which can effectively avoid security risks caused by various intrusion factors from the outside world.

4.4 Network security defense technology for spam emails

In the security protection of cyberspace, the use of artificial intelligence technology can also effectively prevent spam information. Spam has caused a lot of trouble and interference to the Internet, and some spam will also bind viruses or other bad files to the Internet. If they are not disposed of in a timely manner, they may lead to poisoning. In this situation, it is crucial to effectively identify and control spam information, and it must be taken seriously in network security protection. The use of artificial intelligence technology can effectively solve the problem of spam information. It can achieve complete interception of this information. The spam network security defense technology has high application value. On the Internet, through the establishment of a set of anti-counterfeiting

system for various electronic information on the Internet, so as to provide reference for future spam identification and interception, so that electronic information on the Internet will no longer be polluted.

4.5 Multi agent system technology

Multi agent systems are a type of distributed artificial intelligence with autonomous capabilities that can perceive the surrounding environment and interact with it in response. At present, multi-agent systems have developed maturely, so their application in security protection in cyberspace is becoming increasingly common. This technology has the functions of environmental perception and planning. In network security protection, it is mainly applied to the perception of network trends and network intrusion detection. At present, multi-agent systems have been widely applied in various cybersecurity exercises, such as DECODE, which is a distributed environment supporting cybersecurity decision-making exercises in China. Through multi-agent system technology, we can simulate virtual opponents and achieve realistic interaction with humans. The agent platform JIAC is centered around services and has established a network security simulation environment. After a network intrusion event occurs, it can evaluate the event and find corresponding protective measures. The application of agent technology can effectively solve many problems in cyberspace, thereby improving the level of security protection in cyberspace.

4.6 Expert System Technology

As an early developed artificial intelligence technology, expert systems are commonly used in the construction of knowledge bases and inference engines. They can infer knowledge in a field, mimic the thinking patterns of human experts, analyze and solve problems, and provide specialized answers. However, in the process of expert system inference, it is also necessary to establish a relatively complete knowledge base as the operational basis for the system. Because artificial intelligence expert systems can only achieve their reasoning within existing knowledge, their reasoning behavior cannot exceed the scope of existing knowledge. At present, there is still a lot of room for development in the application of expert systems in cybersecurity defense. It is a key component of the development process of the cybersecurity defense system and can provide more specialized knowledge support for the actions of cybersecurity defense. Through expert systems, inference can be carried out on the information detected by intrusion monitoring systems, thereby analyzing whether there will be security risks in the operation of network systems. In recent years, with the development of technology, expert systems have also been continuously upgraded. They can apply various statistical methods to analyze users, construct behavior description models for various authorized user groups, and then monitor user behavior through subsystems to identify intrusion behaviors in the network.

5. CONCLUSION

In the information age, the security scope of cyberspace is constantly expanding. The security of the internet is not only related to the daily lives of the people, but also to the development of industries and social stability. Introducing artificial intelligence technology into network security defense is an inevitable trend, an important step in actively adapting to the new situation and requirements of network security, and a key to further enhancing the security of cyberspace.

REFERENCES

[1] Xie, X., Luo, Y., Peng, H., & Ding, C. RTop-K: Ultra-Fast Row-Wise Top-K Selection for Neural Network Acceleration on GPUs. In The Thirteenth International Conference on Learning Representations.
[2] Lin, L., Li, N., & Zhao, S. (2025). The effect of intelligent monitoring of physical exercise on executive function in children with ADHD. Alexandria Engineering Journal, 122, 355-363.
[3] Peng, Y., Zhang, G., & Pang, H. (2025). Impact of Short-Duration Aerobic Exercise Intensity on Executive Function and Sleep. arXiv preprint arXiv:2503.09077.
[4] Luo, H., Wei, J., Zhao, S., Liang, A., Xu, Z., & Jiang, R. (2024). Intelligent logistics management robot path planning algorithm integrating transformer and gcn network. IECE Transactions on Internet of Things, 2(4), 95-112.
[5] Xu, Y., Shan, X., Guo, M., Gao, W., & Lin, Y. S. (2024). Design and application of experience management tools from the perspective of customer perceived value: A study on the electric vehicle market. World Electric Vehicle Journal, 15(8), 378.

[6] Shan, X., Xu, Y., Wang, Y., Lin, Y. S., & Bao, Y. (2024, June). Cross-Cultural Implications of Large Language Models: An Extended Comparative Analysis. In International Conference on Human-Computer Interaction (pp. 106-118). Cham: Springer Nature Switzerland.
[7] Shen, Z., Wang, Y., Hu, K., Wang, Z., & Lin, S. (2025). Exploration of Clinical Application of AI System Incorporating LSTM Algorithm for Management of Anesthetic Dose in Cancer Surgery. Journal of Theory and Practice in Clinical Sciences, 2, 17-28.
[8] Xu, J., Wang, Y., Chen, H., & Shen, Z. (2025). Adversarial Machine Learning in Cybersecurity: Attacks and Defenses. International Journal of Management Science Research, 8(2), 26-33.
[9] Wang, Y., Shen, Z., Hu, K., Yang, J., & Li, C. (2025). AI End-to-End Autonomous Driving.
[10] Liu, S., Zhao, Z., He, W., Wang, J., Peng, J., & Ma, H. (2025). Privacy-Preserving Hybrid Ensemble Model for Network Anomaly Detection: Balancing Security and Data Protection. arXiv preprint arXiv:2502.09001.
[11] Guo, X., Cai, W., Cheng, Y., Chen, J., & Wang, L. (2025). A Hybrid Ensemble Method with Focal Loss for Improved Forecasting Accuracy on Imbalanced Datasets.
[12] Weng, Y., Fan, Y., Wu, X., Wu, S., & Xu, J. (2024, November). A Multi-Layer Alignment and Adaptive Weighting Framework for Multi-Task Model Fusion. In 2024 International Conference on Intelligent Robotics and Automatic Control (IRAC) (pp. 327-330). IEEE.
[13] Dai, Yonghui, et al. "Research on image of enterprise after-sales service based on text sentiment analysis." International Journal of Computational Science and Engineering 22.2-3 (2020): 346-354.
[14] Xing, Jinming, et al. "Network Traffic Forecasting via Fuzzy Spatial-Temporal Fusion Graph Neural Networks." 2024 11th International Conference on Soft Computing & Machine Intelligence (ISCMI). IEEE, 2024.
[15] Wu, Yingyi, et al. "Recent Technologies in Differential Privacy for NLP Applications." 2024 11th International Conference on Soft Computing & Machine Intelligence (ISCMI). IEEE, 2024.
[16] Wu, Yingyi, et al. "A Survey on Origin-Destination Flow Prediction." 2024 11th International Conference on Soft Computing & Machine Intelligence (ISCMI). IEEE, 2024.
[17] Fang, Jingxing, et al. "A Comparative Study of Sequential Deep Learning Models in Financial Time Series Forecasting." 2024 11th International Conference on Soft Computing & Machine Intelligence (ISCMI). IEEE, 2024.
[18] Yu, Chenyang, et al. "A Social Value Orientation-Based Priority Swapping Algorithm for Efficient Autonomous Intersection Management." 2024 11th International Conference on Soft Computing & Machine Intelligence (ISCMI). IEEE, 2024.
[19] Gao, Min, et al. "Leveraging Large Language Models: Enhancing Retrieval-Augmented Generation with ScaNN and Gemma for Superior AI Response." 2024 5th International Conference on Machine Learning and Computer Application (ICMLCA). IEEE, 2024.