The Application of Artificial Intelligence in Computer Network Technology

Wanglong Xiao

Liuyang Vocational College Hunan Liuyang 410300

Abstract: ***This article explores the multifaceted application value of artificial intelligence in computer network technology, including assisting network administrators in efficiently managing networks, significantly improving network security protection capabilities, and enhancing the intelligence and adaptability of networks. By analyzing the application examples of artificial intelligence in network management, intelligent firewalls, intrusion detection, facial recognition, information recognition, and agent technology, this paper reveals how AI technology promotes the innovation and development of computer network technology, providing strong support for building a more secure, intelligent, and efficient network environment.***

Keywords: Computer network technology; Artificial intelligence; Applications in.

1. INTRODUCTION

With the rapid development of information technology, computer networks have become an indispensable infrastructure in modern society. Faced with an increasingly complex network environment, traditional management and security protection methods seem inadequate. As the core driving force of the new round of technological revolution, artificial intelligence's powerful data processing, learning, and decision-making capabilities have brought new development opportunities for computer network technology. This article aims to explore the extensive application of artificial intelligence in computer network technology, analyze its positive role in improving network management efficiency, ensuring network security, and enhancing network intelligence, in order to provide reference for research and practice in related fields. In the foundational realm of public health and systems analysis, Su et al. (2025) structurally assessed family and educational influences on student health behaviors [1], while Yang (2025) investigated site reliability optimization technologies based on synthetic monitoring in cloud environments [2]. Understanding complex user behavior has progressed through models like that of Wang, Dong, and Zhou (2025), who applied multimodal temporal modeling and reinforcement learning to analyze user decision-making on short-video platforms [3]. The development of trustworthy autonomous systems represents a major frontier. Tang et al. (2026) proposed SVD-BDRL, an autonomous driving decision framework enhanced by blockchain for trustworthiness [4]. Concurrently, generative AI has seen innovations such as NeuroDiff3D by Lu et al. (2025), a diffusion-based method for optimizing viewpoint consistency in 3D generation [5]. To govern and secure such complex systems, Zhang (2025) designed a neuro-symbolic and blockchain-enhanced multi-agent framework for fair cross-regulatory audits [6], and Bi and Su (2025) developed a secure access method for education networks leveraging edge computing [7]. Enhancing data perception and completion is crucial. Xie et al. (2025) introduced MARNet, a multi-scale adaptive relational network for robust point cloud completion via cross-modal fusion [8]. This focus on data-driven physical systems has early roots in cyber-physical integration, exemplified by the camera-based triggering system for bridge health monitoring proposed by Hou et al. (2017) [9]. Finally, cutting-edge applications in business intelligence, control systems, and collaborative learning are emerging. Tian et al. (2025) presented a cross-attention multi-task learning approach for ad recall in digital advertising [10], while Zhang, Tian, and Hua (2025) designed an autonomous vehicle speed control system based on a PID controller [11]. The critical challenge of privacy in decentralized learning is being addressed through enhanced defenses, as seen in the multi-layer strategies against membership reasoning attacks in federated learning proposed by Deng and Yang (2025) [12], and the robust, privacy-conscious framework FedGuard for collaborative anti-money laundering introduced by Sultan et al. (2026) [13].

2. THE APPLICATION VALUE OF ARTIFICIAL INTELLIGENCE IN COMPUTER NETWORK TECHNOLOGY

The application of artificial intelligence in computer network technology has greatly improved the work efficiency and management ability of network administrators. Traditional network management tasks are tedious and complex, requiring a large amount of manual monitoring, analysis, and optimization work. And artificial

intelligence automates these tasks, such as monitoring network traffic, identifying and solving network problems, optimizing network performance, etc., allowing network administrators to focus more on strategic tasks such as network planning and upgrades. This not only improves the normal operation time of the network, but also reduces the possibility of errors or negligence. With the increasing complexity and frequency of cyber attacks, traditional security defense methods are no longer sufficient to meet the demands. Artificial intelligence, through applications such as intelligent firewalls and intrusion detection systems, can analyze network data in real-time, identify potential security threats, and take corresponding defense measures. In addition, artificial intelligence can continuously optimize its defense strategies through machine learning algorithms, improve its ability to respond to new types of network attacks, and ensure the safe and stable operation of network systems. Artificial intelligence endows computer networks with stronger intelligence and adaptability. Through real-time analysis and processing of network data, artificial intelligence can automatically adjust network parameters, optimize network performance, and respond to different network environments and business needs. Meanwhile, artificial intelligence can also provide personalized online services based on users' usage habits and needs, enhancing the user experience. The improvement of intelligence and adaptability enables computer networks to better adapt to complex and changing network environments, meeting the diverse needs of users.

3. EXPLORATION OF THE APPLICATION OF ARTIFICIAL INTELLIGENCE IN COMPUTER NETWORK TECHNOLOGY

3.1 Applications in Network Management

Artificial intelligence can achieve comprehensive and all-weather monitoring of network environments by integrating advanced algorithms and models. This type of monitoring is not limited to traditional basic indicators such as network traffic and bandwidth utilization, but can also delve into finer grained levels such as packet content and protocol behavior. With the help of machine learning technology, artificial intelligence can automatically identify and classify normal traffic and abnormal behavior in the network, providing administrators with intuitive monitoring views and real-time alerts. This automated monitoring capability greatly reduces the workload of administrators and improves the timeliness and accuracy of monitoring. When a network failure occurs, traditional manual troubleshooting methods are often time-consuming, labor-intensive, and prone to omissions. Artificial intelligence, through its powerful data processing and analysis capabilities, can quickly locate the source of faults and provide preliminary solutions. Specifically, artificial intelligence will first analyze multi-source information such as network logs and performance data, and combine historical fault cases and expert knowledge bases to perform fault pattern recognition and diagnostic reasoning. Once a potential fault point is identified, artificial intelligence will immediately trigger an alarm mechanism and generate detailed fault reports and repair suggestions to help administrators quickly restore normal network operation. In addition to real-time troubleshooting, artificial intelligence can also perform predictive maintenance on network status through big data analysis technology. Through in-depth mining and pattern recognition of historical network data, artificial intelligence can detect early signs of network performance degradation or failure, and predict future development trends. Based on these predicted results, administrators can take preventive measures in advance, such as adjusting network configurations, upgrading hardware devices, or optimizing software algorithms, to avoid potential network problems from causing significant impact on business. In network management, resource allocation is a crucial step. Artificial intelligence, through its intelligent decision support system, can automatically adjust resource allocation strategies based on various factors such as network load and business requirements. For example, automatically increasing bandwidth resources during peak periods to meet user demands; Reduce resource consumption during low peak periods to lower costs. At the same time, artificial intelligence can continuously optimize network performance by adjusting routing strategies, load balancing parameters, and other methods to improve the overall performance and user experience of the network.

3.2 Applications in Intelligent Firewalls

The core capability of an intelligent firewall lies in its powerful real-time traffic analysis ability. By deploying advanced machine learning models, it can continuously monitor and analyze data packets entering and leaving the network, identifying abnormal behavior patterns. These models continuously learn and adapt to changes in the network environment, accurately distinguishing between normal traffic and potential malicious traffic, such as DDoS attacks, SQL injection, ransomware, etc. Compared to traditional firewalls that rely on fixed rule sets for detection, intelligent firewalls can detect and respond to unknown threats earlier, effectively reducing the occurrence of security incidents. Faced with rapidly evolving network threats, intelligent firewalls have demonstrated a high degree of flexibility and adaptability. It can dynamically adjust security policies based on

real-time analysis results, automatically block suspicious IP addresses, ports, or services, while maintaining unobstructed access to legitimate traffic. In addition, intelligent firewalls also have self-learning capabilities and can continuously optimize their detection algorithms and defense strategies to cope with new attack methods. This dynamic adjustment and adaptive defense mechanism ensures that intelligent firewalls remain efficient and effective in complex and ever-changing network environments. The introduction of deep learning technology has further enhanced the threat recognition capability of intelligent firewalls. By constructing deep neural network models, intelligent firewalls can gain a deeper understanding of the intrinsic characteristics and structure of network traffic, thereby more accurately identifying subtle anomalies hidden within normal traffic. This data-driven anomaly detection method not only improves the accuracy and sensitivity of detection, but also reduces false positives and false negatives. At the same time, deep learning models can automatically extract key features of network traffic, providing strong support for subsequent security analysis and response. Intelligent firewalls also have intelligent response mechanisms that can automatically trigger corresponding security response measures based on the severity and urgency of threats. For example, when a DDoS attack is detected, an intelligent firewall can quickly activate a traffic cleaning mechanism to redirect malicious traffic to a cleaning center for processing; When internal network infiltration is detected, infected devices can be immediately isolated and the administrator notified for disposal. In addition, intelligent firewalls can also achieve collaborative defense with other security devices and systems, jointly building a comprehensive and multi-level network security protection system.

3.3 Application in Intrusion Detection

Firstly, AI can deeply analyze the multidimensional characteristics of network traffic, including packet size, transmission time interval, protocol type, etc., by integrating complex deep learning networks such as convolutional neural networks and recurrent neural networks. These may be considered redundant information under traditional methods, but in the eyes of AI, they have become key clues to reveal potential threats. This deep analysis capability enables intrusion detection systems to identify more covert and complex attack patterns, effectively compensating for the shortcomings of traditional rule-based or signature based methods.

Secondly, AI's self-learning ability enables intrusion detection systems to dynamically adapt to changes in the network environment. With the continuous emergence of new applications and technologies, the patterns and characteristics of network traffic are also constantly evolving. AI systems can continuously monitor network traffic, automatically adjust detection models to adapt to these changes, and ensure that the system remains in optimal condition at all times. This dynamic adjustment mechanism not only improves the accuracy of detection, but also reduces the false alarm rate caused by environmental changes.

Furthermore, the integration of AI also promotes seamless integration between intrusion detection systems and emergency response systems. Once the AI system detects a potential threat, it can immediately trigger preset emergency response processes, such as automatically blocking suspicious connections, sending alerts to notify administrators, or initiating further analysis and investigation. This automated emergency response mechanism greatly shortens the time interval from detection to response, buying valuable processing time for defenders. Finally, the application of AI in intrusion detection also promotes knowledge sharing and collaborative defense in the field of security. Through the sharing and updating of machine learning models, different organizations can collectively enhance their awareness and defense capabilities against cyber threats. This cross organizational collaboration not only enhances the overall resilience of cybersecurity, but also lays a solid foundation for building a more secure and trustworthy cyberspace.

3.4 Application of facial recognition technology

Facial recognition technology, as a shining pearl in the field of artificial intelligence, has greatly promoted the process of intelligence through its integrated application in computer network technology. This technology not only revolutionizes the traditional mode of identity verification, but also significantly improves the security and convenience of access control. Users do not need to carry physical keys or memorize complex passwords, and can quickly complete identity verification based solely on facial features. Whether unlocking smartphones, access control systems, or conducting financial transactions, seamless integration and efficient security are achieved. In the field of security monitoring, the application of facial recognition technology has demonstrated unprecedented value. Through high-definition surveillance cameras and advanced algorithm analysis, the system is able to capture and analyze facial images in real-time in video streams, compare them with preset information in the database, and quickly identify specific individuals, such as suspicious individuals or important protected objects.

This ability greatly enhances the security and prevention capabilities of public places, helping the police to respond quickly and track criminal clues, while also providing strong technical support for enterprise management, large-scale event security, and more. In addition, combined with big data analysis, facial recognition technology can further explore the behavioral patterns behind facial data, providing scientific basis for security warning, trend prediction, and opening a new chapter in intelligent security.

3.5 Application of Artificial Intelligence Recognition Information Technology

In today's information explosion, artificial intelligence recognition technology is penetrating into every corner of the social economy with unprecedented depth and breadth, becoming a key force in promoting industrial upgrading and enhancing social efficiency. This technology is not limited to basic data recognition and classification tasks, but utilizes cutting-edge technologies such as deep learning, natural language processing, and computer vision to achieve deep parsing and intelligent reasoning of complex information structures, opening a new chapter in information processing.

In the medical field, the application of artificial intelligence recognition information technology has greatly promoted the precision process of medical diagnosis. By using deep learning algorithms to automatically analyze and recognize medical imaging data, AI systems can assist doctors in detecting small lesions, warning potential diseases in advance, and even in some cases, their diagnostic accuracy has exceeded that of senior experts, buying valuable treatment time for patients. At the same time, AI can also combine multiple sources of data such as patient medical records and genetic data to provide scientific basis for the design of personalized treatment plans.

The financial sector has also witnessed the enormous value of artificial intelligence in identifying information technology. Faced with massive and complex financial statements, market research reports, and various financial data, AI systems can quickly capture key information, conduct deep mining and intelligent analysis, reveal market trends for investors, evaluate investment risks, and provide accurate investment strategy recommendations. In addition, AI has demonstrated outstanding capabilities in anti fraud, credit approval, and other areas, effectively improving the risk prevention and control level and operational efficiency of financial institutions.

The widespread application of intelligent customer service systems is another example of artificial intelligence recognition information technology in improving user experience. With the help of NLP technology, these systems are able to accurately understand users' natural language input, and receive immediate and personalized responses to any inquiries, expressions of needs, or feedback. This humanized interaction method not only greatly reduces the work pressure of manual customer service, but also significantly improves the speed and satisfaction of problem solving, enhancing the stickiness and trust between enterprises and users.

3.6 Application of Artificial Intelligence Agent Technology

The deep application of artificial intelligence agent technology is leading computer network technology into a new era of intelligence. These agents are not just simple automation tools, they are more like intelligent assistants in the network, able to deeply understand every detail of network operation and make optimal decisions based on it. For example, in monitoring network traffic, agents can analyze packet content in real-time, identify and block potential malicious traffic, and effectively resist network attacks; In terms of resource allocation, they can dynamically adjust bandwidth, cache and other resource allocation based on the current network load situation, ensuring the efficient operation of the network. The collaboration mechanism between agents is the highlight of this technology. By building an intelligent network ecosystem, different agents can share information, coordinate actions, and form a strong synergy. This collaboration is not limited to the same network domain, but can also cross different networks and platforms to achieve global optimization and management. For example, in cross domain network management, multiple agents can work together to solve problems such as cross domain routing and data synchronization, enhancing the overall network's interconnectivity. With the continuous advancement of artificial intelligence technology and the increasing maturity of agent technology, we can foresee a more intelligent, autonomous, and flexible network environment. In this environment, agents will not only be tools for executing tasks, but also become an important component of network intelligence, working together with human users to build, maintain, and manage networks. They will have stronger learning abilities, higher autonomy, and broader collaboration capabilities, and can quickly adapt and flexibly respond to complex and changing network environments, providing more convenient, efficient, and secure network services for human society.

4. CONCLUSION

In summary, the application of artificial intelligence in computer network technology not only greatly improves the efficiency and accuracy of network management, but also significantly enhances the security protection capability and intelligence level of the network. With the continuous advancement of technology and the deepening of applications, artificial intelligence will demonstrate its unique advantages and value in more fields, promoting computer network technology towards a new stage of intelligence, efficiency, and security. In the future, the deep integration of artificial intelligence and computer network technology will usher in a new era of networking, contributing more important forces to the informationization process of human society.

REFERENCES

[1] Su, Z., Yang, D., Wang, C., Xiao, Z., & Cai, S. (2025). Structural assessment of family and educational influences on student health behaviours: Insights from a public health perspective. Plos one, 20(9), e0333086.

[2] Yang, Y. (2025). Research on Site Reliability Optimization Technology Based on Synthetic Monitoring in Cloud Environments.

[3] Wang, J., Dong, J., & Zhou, L. (2025). Research on Short-Video Platform User Decision-Making via Multimodal Temporal Modeling and Reinforcement Learning: Deep Learning for User Decision Behavior. Journal of Organizational and End User Computing (JOEUC), 37(1), 1-24.

[4] Tang, Z., Feng, Y., Zhang, J., & Wang, Z. (2026). SVD-BDRL: A trustworthy autonomous driving decision framework based on sparse voxels and blockchain enhancement. Alexandria Engineering Journal, 134, 433-446.

[5] Lu, K., Sui, Q., Chen, X., & Wang, Z. (2025). NeuroDiff3D: a 3D generation method optimizing viewpoint consistency through diffusion modeling. Scientific Reports, 15(1), 41084.

[6] Zhang, T. (2025). A Neuro-Symbolic and Blockchain-Enhanced Multi-Agent Framework for Fair and Consistent Cross-Regulatory Audit Intelligence.

[7] Bi, Y., & Su, T. (2025). A secure access method in English education network based on edge computing. Alexandria Engineering Journal, 128, 1125-1133.

[8] Xie, J., Zhang, L., Cheng, L., Yao, J., Qian, P., Zhu, B., & Liu, G. (2025). MARNet: Multi-scale adaptive relational network for robust point cloud completion via cross-modal fusion. Information Fusion, 103505.

[9] HOU, R., JEONG, S., WANG, Y., LAW, K. H., & LYNCH, J. P. (2017). Camera-based triggering of bridge structural health monitoring systems using a cyber-physical system framework. Structural Health Monitoring 2017, (shm).

[10] Q. Tian, D. Zou, Y. Han and X. Li, "A Business Intelligence Innovative Approach to Ad Recall: Cross-Attention Multi-Task Learning for Digital Advertising," 2025 IEEE 6th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), Shenzhen, China, 2025, pp. 1249-1253, doi: 10.1109/AINIT65432.2025.11035473.

[11] Y. Zhang, Z. Tian and H. Hua, "Design of an Autonomous Vehicle Speed Control System Based on a PID Controller," 2025 International Conference on Advances in Electrical Engineering and Computer Applications (AEECA), Dalian, China, 2025, pp. 491-495, doi: 10.1109/AEECA65693.2025.00092.

[12] Deng, X., & Yang, J. (2025, August). Multi-Layer Defense Strategies and Privacy Preserving Enhancements for Membership Reasoning Attacks in a Federated Learning Framework. In 2025 5th International Conference on Computer Science and Blockchain (CCSB) (pp. 278-282). IEEE.

[13] Sultan, N., Patwar, N., Wei, X., Chew, J., Liu, J., & Du, R. (2026). FedGuard: A Robust Federated AI Framework for Privacy-Conscious Collaborative AML, Inspired by DARPA GARD Principles. International Academic Journal of Social Science, 2, 1–16. https://doi.org/10.5281/zenodo.18253151