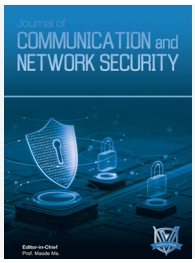
Journal of Communication and Network Security (JCNS)

DOI:http://doi.org/10.65098/jcns.01.2026.01.04



RESEARCH ARTICLE

RESEARCH ON THE APPLICATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGY IN NETWORK INFORMATION SECURITY

Dongyu Gao

Yancheng Kindergarten Teachers College, Yancheng 224005, China
Corresponding Author E-mail: estherwu5712@gmail.com

This is an open access article distributed under the Creative Commons Attribution License CC BY 4.0, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ARTICLE DETAILS

Article History:

Received 12 Sep 2025
Accepted 27 Dec 2025
Available online 9 Feb 2026

Online Article Code

ABSTRACT

Background and Purpose: With the rapid advancement of information technology, cyber threats have become increasingly complex, rendering traditional network security mechanisms insufficient. Artificial intelligence (AI), with its strong computational power and pattern recognition capabilities, has emerged as a promising approach for enhancing network information security. This study aims to examine the core applications of AI in network information security and to explore strategies for improving its effectiveness and adaptability in practical defense scenarios.
Methods: This paper reviews and analyzes existing AI-based security technologies applied to threat detection, attack defense, data security, and privacy protection. Key challenges in real-world applications are identified, and optimization strategies are proposed, including algorithm enhancement, intelligent counterattack mechanisms, improvements in computational efficiency, and the implementation of automated security policies.
Results: The analysis indicates that AI-based approaches can significantly improve the accuracy and timeliness of threat detection and response. Optimized algorithms and automated defense strategies enhance system adaptability, reduce false alarms, and strengthen overall security performance against emerging and sophisticated cyberattacks.
Conclusion: AI has substantial potential to transform network information security. Through targeted optimization of algorithms, defense strategies, and system efficiency, AI-driven security systems can achieve higher resilience and adaptability, providing effective technical support for modern network security challenges.

KEYWORDS

Artificial Intelligence, Network Security, Deep Learning, Anomaly Detection, Algorithm Optimization

With the in-depth development of the digital society, the intelligence level of network attacks continues to improve. Traditional security defense methods are struggling to deal with new attack types, such as Advanced Persistent Threats (APT), zero-day attacks, and adversarial attacks. The introduction of AI technology has provided new ideas for network information security: it can enhance threat detection capabilities through autonomous learning, pattern recognition, data analysis, and other means, and improve the intelligence level of network security systems. However, the application of AI technology in network security still faces many challenges, such as issues related to model robustness, adversarial sample attacks, and computing resource consumption. Therefore, this paper conducts a technical analysis on the application of AI in network information security, explores its core application scenarios and current challenges, and proposes targeted optimization solutions.

1. MAIN APPLICATIONS OF ARTIFICIAL INTELLIGENCE TECHNOLOGY IN NETWORK INFORMATION SECURITY

The application of AI technology in network information security covers multiple aspects and plays a key role in fields such as threat detection, defense strategy optimization, malware analysis, and data security protection. AI-driven threat detection systems identify abnormal network behaviors based on big data analysis, enabling Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to achieve higher accuracy. Deep learning algorithms can automatically learn the characteristics of malicious traffic and dynamically adjust strategies during the detection process, reducing false positives and false negatives and improving overall protection effectiveness. In addition, the application of intelligent defense technology allows security systems to adapt to evolving attack methods. Reinforcement learning technology is used in intelligent firewalls and DDoS protection systems, enabling them to adjust interception rules according to changes in attack behaviors. Combined with threat intelligence analysis, AI systems can predict potential attacks and make preventive adjustments to security policies, thereby improving response speed. In the field of malware analysis, deep learning models are widely used for static and dynamic detection. Neural network models such as CNN (Convolutional Neural Network) and RNN (Recurrent Neural Network) extract feature patterns of malicious code, enabling detection systems to accurately identify potential threats

(Zhang et al., 2024). Furthermore, Generative Adversarial Networks (GAN) are used to simulate attack behaviors, equipping AI security systems with stronger adaptability and enhancing the robustness of defense mechanisms. Moreover, the application of AI technology in data security and privacy protection is gradually deepening (Huang, 2024). The optimization of data encryption algorithms makes key management more efficient, improving the security of storage and transmission. The adoption of privacy computing technology allows data to be used for computational analysis without direct access; federated learning architectures provide a more secure method for cross-organizational data collaboration, effectively reducing the risk of data leakage.

2. CHALLENGES FACED BY THE APPLICATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGY IN NETWORK INFORMATION SECURITY

The application of AI technology in network security is continuously deepening, but there are still various technical and practical difficulties during actual deployment. The stability of models directly affects detection accuracy. Biases in training data or incomplete information may lead to misjudgments or missed detections. The diversity of attack patterns makes it difficult for AI models to maintain consistent recognition capabilities across different environments; especially when data distribution changes, the effectiveness of defense may decline. Adversarial sample attacks are another major issue. Attackers can construct carefully designed inputs to cause AI systems to make incorrect judgments, thereby bypassing detection mechanisms. Additionally, the risk of data poisoning cannot be ignored: the inclusion of malicious data during the training phase may weaken the reliability of AI models, rendering them ineffective in defense during practical application. The consumption of computing resources imposes pressure on the performance of AI systems. The training and inference of deep learning models require high-performance computing equipment; when processing large-scale data or real-time detection tasks, limitations in computing capabilities may affect system response speed. Especially in high-concurrency environments, the operational efficiency of AI models determines the timeliness of security protection; reliance on cloud computing may also introduce additional network latency, affecting the effectiveness of real-time defense (Lu, 2024). Furthermore, data privacy and compliance requirements are also factors affecting AI applications. AI security systems rely on large amounts of data for training, and data involving sensitive information must comply with privacy protection regulations during collection, storage, and sharing. The complexity of cross-regional data management further increases the difficulty of building security systems. Striking a balance between data protection and network security needs has become an unavoidable issue in the implementation of AI applications.

3. OPTIMIZATION STRATEGIES OF ARTIFICIAL INTELLIGENCE TECHNOLOGY IN NETWORK SECURITY

3.1 Enhancing the Robustness of Artificial Intelligence Security Models

Optimizing the robustness of security models requires efforts from multiple aspects, including data training, algorithm optimization, and multi-model fusion, to enhance the system's adaptability in different environments. To build a more robust AI security model, dynamic training methods should be adopted to ensure that it can accurately identify abnormal behaviors even in complex network environments. Adjusting the model's training strategy is a key measure to improve stability. Online learning and incremental training technologies should be used to enable AI systems to continuously update based on the latest threat intelligence, avoiding ineffectiveness due to changes in attack patterns. During the model training phase, diverse datasets should be introduced, including traffic data from different regions, different business types, and different attack methods, enabling the model to recognize a wider range of attack patterns. Data augmentation technology should be used to generate variant attack samples, allowing the model to learn more attack variants and improve its generalization ability in real-world environments. Additionally, adversarial training should be performed regularly to ensure that the model can maintain stable decision-making capabilities when facing abnormal inputs, thereby reducing the possibility of misjudgments and missed detections. Optimizing the algorithm structure is also an effective way to enhance model stability. Adaptive neural networks should be adopted to enable dynamic adjustment of model parameters in different environments, ensuring that the model maintains efficient detection capabilities when dealing with different types of attacks. Combined with deep learning architectures based on attention mechanisms, the model can prioritize key features and avoid interference from noisy data. For complex attack behaviors, a hierarchical detection model should be built to gradually screen abnormal data, reducing computational burden and improving detection accuracy. Furthermore, in response to data distribution drift, an adaptive feedback mechanism should be established to enable the model to adjust its parameters based on real-time analysis results, reducing the decline in detection capabilities caused by changes in the data environment. Multiple detection methods should be integrated to ensure that AI security models can operate efficiently in different scenarios. Traditional rule-based detection methods should be combined with deep learning algorithms to enable security systems to function effectively against both known and unknown attacks. Expert knowledge bases should be used to establish prior rules, improving the recognition speed of common attacks; at the same time, deep learning methods should be used to explore potential attack patterns, enhancing detection capabilities. Additionally, in enterprise-level applications, federated learning mechanisms should be deployed to allow different organizations to share threat intelligence while protecting data privacy, thereby improving the adaptability and robustness of the overall detection model.

3.2 Defense Against Adversarial Attacks

Optimizing defense strategies requires efforts from aspects such as model training, threat tracking, and detection methods, equipping AI security systems with stronger recognition capabilities and adaptability when facing adversarial attacks. Adversarial training can be used to enhance the model's defense capabilities: adversarial samples are proactively generated during the training process and added to the dataset, enabling the model to learn how to recognize malicious inputs that have been interfered with. Methods such as PGD (Projected Gradient Descent) should be used to adjust training strategies, ensuring that the model remains stable under different perturbation conditions. Combined with optimization algorithms such as TRADES (Trade-off Between Robustness and Accuracy), the model can improve detection accuracy while enhancing its ability to distinguish abnormal inputs. Furthermore, during the model deployment phase, online training should be conducted continuously to enable the model to adapt to new adversarial samples and improve the effectiveness of the detection system. Blockchain technology can be combined for data traceability, enhancing the traceability of attack behaviors. Using the distributed storage mechanism of blockchain to record network security events ensures that every suspicious access or abnormal behavior is fully retained. Smart contracts should be used to automatically analyze threat intelligence, detect abnormal access patterns, and provide real-time early warnings. During the data auditing process, tamper-proof blockchain storage methods should be used to prevent attackers from deleting or forging attack records. Combined with a security alliance chain shared across organizations, different enterprises and institutions can collaboratively analyze adversarial attacks, improving overall security defense capabilities. Multi-modal detection technology should be adopted to enhance the comprehensiveness of attack recognition. Traditional security detection models often rely on a single data source, and attackers can forge data for specific dimensions to bypass detection systems. Multiple data sources such as network traffic, log behaviors, and device fingerprints should be integrated, enabling AI systems to make comprehensive judgments based on multiple features rather than relying on a single indicator when analyzing threats. Through in-depth fusion of different types of data, potential forgery behaviors can be identified, reducing the risk of single-point failure. Additionally, a detection optimization mechanism based on reinforcement learning should be established to enable AI systems to continuously adjust detection strategies, making defense more flexible.

3.3 Improving the Real-Time Response Capability of Artificial Intelligence in Network Security

Optimizing real-time response capabilities requires efforts from aspects such as computing architecture, attack detection strategies, and inference efficiency, enabling AI systems to quickly identify threats and implement defense measures when facing network attacks. Edge computing can be used to reduce data transmission latency and improve analysis speed. AI models should be deployed on local devices or distributed nodes, enabling data to be processed at the source rather than relying on cloud servers for centralized computing. In high-sensitivity scenarios such as industrial control and financial transactions, edge computing can reduce the response time of security events, enabling the system to make rapid defense decisions. Furthermore, in distributed environments, federated learning technology should be used to optimize AI models, enabling different nodes to collaboratively update defense strategies without centralized data processing, thereby further reducing latency and improving overall defense effectiveness. Attack detection strategies should be adjusted to enable the system to automatically adapt to changes when facing new threats. Reinforcement learning should be used to optimize detection models, enabling them to dynamically adjust based on attackers' behavior patterns. In DDoS attack defense, an adaptive traffic management system combined with reinforcement learning should be used, enabling the model to quickly adjust traffic filtering rules, identify abnormal requests, and dynamically adjust response strategies when an attack occurs. For Intrusion Detection Systems (IDS), deep reinforcement learning should be used to enhance the recognition of unknown threats, enabling the system to make optimized decisions based on historical data when facing new attack methods, without relying on preset rules. Additionally, in Security Information and Event Management (SIEM) systems, reinforcement learning should be used to adjust alert levels, reducing false positives and allowing security teams to focus their efforts on the most urgent security events, improving overall response efficiency. AI inference efficiency should be optimized to reduce resource consumption and accelerate decision-making speed in complex computing tasks. Model pruning technology should be used to reduce unnecessary computing nodes, enabling deep learning models to perform fewer computing steps during inference and improving the response capability of detection systems. Furthermore, model quantization technology should be applied to convert floating-point computing into low-bit integer computing, enabling models to run faster on the same hardware resources (Zheng & Guo, 2024). On edge devices, lightweight AI models based on Transformer architecture should be deployed, enabling security systems to complete efficient threat detection with limited computing resources. Moreover, asynchronous inference methods should be combined to achieve more efficient allocation of computing resources for different detection tasks, avoiding system response delays caused by resource competition.

3.4 Integration of Artificial Intelligence and Automated Security Policies

Optimizing security policies requires integrating AI into Security Orchestration, Automation and Response (SOAR) platforms, equipping defense systems with rapid decision-making and dynamic adjustment capabilities. An intelligent alert management system should be deployed to enable AI to analyze security events in real-time in the Security Operations Center (SOC), screen high-risk alerts, and reduce interference from false positives. Combined with Natural Language Processing (NLP) technology, security logs and attack reports should be parsed, enabling AI to automatically summarize threat intelligence and correlate different security events. Automatic response rules should be configured to enable the SOAR platform to immediately implement appropriate defense actions (such as blocking malicious IPs, adjusting access permissions, or triggering isolation mechanisms) after identifying threats, thereby shortening response time. The defense rule adjustment mechanism should be optimized to enable AI to dynamically update security policies based on real-time data. Machine learning algorithms should be used to analyze historical attack patterns, predict potential future risks, and automatically generate new defense rules. Reinforcement learning technology should be applied to enable AI to optimize policies through continuous interaction, reducing human intervention. Adaptive models should be used to enable defense systems to automatically adjust detection thresholds when facing new attacks, improving policy adaptability. Additionally, threat intelligence sharing platforms should be combined to enable AI systems to learn the latest attack trends and apply them to security policies in real-time, thereby reducing the risk of security lag. Log analysis capabilities should be enhanced to enable AI to accurately identify abnormal patterns and automatically push policy optimization recommendations. Deep learning-based behavior analysis models should be deployed to enable the system to detect abnormal traffic, abnormal access behaviors, or potential intrusion activities and adjust security rules in real-time. Federated learning technology should be used to enable the sharing of security policy optimization results among different enterprises or organizations, improving overall security defense capabilities while ensuring data privacy. An automated decision engine should be built to enable AI to adjust response priorities based on security risk levels and optimize protection policies before an attack occurs, improving the implementation efficiency of security policies.

3.5 Artificial Intelligence-Driven Data Security and Privacy Protection

Optimizing data security measures requires efforts from aspects such as privacy computing, access control, and encryption technology, ensuring that data remains protected during storage, transmission, and use. A federated learning architecture should be deployed to enable multiple institutions to train AI models without directly sharing raw data, realizing distributed data analysis. Secure Multi-Party Computation (MPC) and homomorphic encryption technology should be adopted to enable data to be computed in an encrypted state, preventing data leakage. Combined with differential privacy methods, AI models should be made to perturb sensitive information during the learning process, avoiding data traceability risks. The data access management mechanism should be optimized to enable AI to dynamically adjust permission control policies. Behavior analysis technology should be used to detect user access patterns in real-time, enabling the system to automatically adjust permissions when abnormal access behaviors are detected. An AI-based adaptive access control system should be configured to enable permission allocation to be adjusted based on user roles, access frequency, and data sensitivity, rather than relying on fixed rules. Combined with a zero-trust architecture, the AI system should perform identity verification for each access request, improving access security. Additionally, an AI-driven anomaly detection system should be deployed to identify and block unauthorized data access, ensuring that sensitive information remains in a secure and controllable environment. Data encryption strategies should be optimized to enable AI to dynamically adjust encryption levels based on security risks. Quantum-computing-resistant encryption algorithms should be combined to ensure that data remains secure when facing high-intensity computing attacks. An adaptive key management system should be deployed to enable AI to automatically allocate, store, and update encryption keys, reducing security risks caused by poor key management. During data transmission, AI-optimized end-to-end encryption methods should be adopted to ensure that data maintains integrity and confidentiality in different network environments. Furthermore, AI should be used to analyze data integrity, monitor data change records, identify potential tampering behaviors, and trigger automatic protection measures after anomaly detection, improving the reliability of the data security system.

3.6 Artificial Intelligence-Driven Adaptive Optimization of Security Policies

In a dynamically changing network environment, traditional static security policies often struggle to cope with emerging threats. The introduction of AI technology, particularly reinforcement learning and adaptive algorithms, enables real-time adjustment and optimization of security policies. By continuously monitoring network traffic and user behaviors, AI systems can identify abnormal patterns and automatically adjust protection rules to respond to potential attacks (Zhong, 2024). For example, using deep reinforcement learning models, security systems can quickly learn and develop effective response strategies when facing unknown threats, thereby improving overall defense capabilities. Additionally, combined with federated learning technology, different organizations can share threat intelligence and collaboratively optimize security policies, enhancing cross-domain protection effects. To achieve adaptive optimization of policies, a feedback mechanism should be established to enable AI systems to continuously adjust and improve their policy models based on actual defense effects. This includes analyzing

false positives and false negatives, identifying deficiencies in policies, and correcting them through model training. At the same time, combined with explainable AI technology, the transparency and auditability of policy adjustments should be ensured, enhancing user trust in AI system decisions. During implementation, attention should be paid to the quality and diversity of data to ensure the comprehensiveness and representativeness of model training, thereby improving the accuracy and effectiveness of policy optimization. Furthermore, automated policy evaluation tools should be deployed to conduct regular reviews and tests of existing security policies, identifying potential vulnerabilities and areas for improvement. By simulating attack scenarios, the performance of policies under different attack methods should be evaluated to further guide the policy adjustment of AI systems. Combined with real-time threat intelligence, AI systems can predict potential future attack trends and adjust protection policies in advance to achieve proactive defense. Ultimately, a dynamic, intelligent, and collaborative security policy optimization system should be built to enhance the overall effectiveness of network security protection.

4. CONCLUSION

The application of AI technology in the field of network information security is increasingly in-depth, providing modern security systems with stronger threat detection capabilities, more precise attack defense strategies, and more flexible data protection methods. Facing an increasingly complex network environment, relying solely on traditional security protection methods can no longer meet needs; the introduction of AI has equipped security systems with stronger adaptability and real-time response capabilities. In terms of threat detection, AI models based on deep learning and behavior analysis can accurately identify abnormal activities, improving the precision of security defense. In the field of attack defense, AI combined with technologies such as adversarial training and edge computing enables security systems to more effectively resist attacker intrusions and optimize real-time protection strategies. Furthermore, in terms of data security and privacy protection, the application of AI has enhanced data encryption technologies, optimized data storage and access management, and reduced the risk of data leakage. In the future, with the continuous evolution of AI technology, network security systems will gradually move towards a more intelligent, efficient, and secure direction, providing stronger protection for the network environment in the digital era.

REFERENCES

Huang, J. (2024). Network information security issues and protection strategies in the artificial intelligence era. *Network Security Technology and Application*, (7), 124-126.

Lu, Z. (2024). Network information security issues and protection strategies in the artificial intelligence era. *Information and Computer (Theoretical Edition)*, *36*(14), 145-147.

Zhang, H., Liu, Y., & Wang, S. (2024). Research on the application of CNN-RNN algorithm in network intrusion detection and information security confidentiality technology. *Computer Knowledge and Technology*, *20*(33), 44-46.

Zheng, X., & Guo, J. (2024). Analysis of the development of network information security technology in cloud computing environment. *Digital Communication World*, (8), 119-121.

Zhong, Q. (2024). Research on computer network information security and its protection countermeasures. *Shihezi Science and Technology*, (5), 39-40.

Cite The Article: Dongyu Gao (2026). Research on the Application of Artificial Intelligence Technology in Network Information Security.
***Journal of Communication and Network Security*, 1(1): 01-04.**