International Journal of
Science and Engineering Research 2025 Volume 4, Issue 5
High-Tech Science Press, USA
Available online at https://starscipress.com

Exploration of AI-Driven Automatic Identification and Protection Strategies for Computer Network Security

Fukuan Li*

Haikou Yuanhong Publishing Co., Ltd., Haikou 570100, Hainan, China
**Author to whom correspondence should be addressed.*

Abstract: ***In the face of the rapid advancement of computer network technology and the increasingly complex cybersecurity threats, traditional protection measures are proving inadequate. The integration of artificial intelligence (AI) technologies has brought revolutionary changes to the field of cybersecurity. This study systematically expounds the core application strategies of AI in automatic identification and protection for computer network security, deeply analyzes its significant advantages in threat detection, anomaly recognition, and intelligent defense, and constructs an AI-based cybersecurity protection framework. At the same time, the paper objectively points out the challenges faced by AI applications in cybersecurity and looks ahead to future development directions, providing theoretical support for building a more intelligent and efficient cybersecurity system.***

Keywords: Artificial intelligence; Computer network security; Automatic identification; Protection strategies.

1. Introduction

As the core infrastructure of the information age, computer networks not only carry massive data exchange and transmission tasks but also underpin the smooth operation of various business activities. However, with the popularization and increasing complexity of networks, cybersecurity threats have become more severe, with frequent security incidents such as virus infections, hacker attacks, and data leaks, causing significant impacts on individual privacy, corporate interests, and even national security. Traditional cybersecurity protection methods, such as signature database updates and rule matching, once played an important role but are now inadequate in the face of increasingly complex and ever-changing new threats. Against this backdrop, the rapid development of artificial intelligence technology offers new perspectives and solutions. By introducing advanced technologies like machine learning and deep learning, the cybersecurity field is gradually shifting from passive defense to proactive identification and intelligent protection, laying a solid foundation for building a safer and more stable network environment. Zhou (2025) developed a swarm intelligence-based multi-UAV cooperative system for precision pesticide spraying in irregular farmlands[1]. Large language model optimization has seen multiple innovations: Wen et al. (2025) created a dynamic adaptive data filtering framework for fine-tuning[2], Weng et al. (2025) enhanced security in text-to-image generation[3], Wang & Bi (2025) introduced hierarchical adaptive fine-tuning for multi-task learning[4], and Liu et al. (2025) proposed hybrid-grained structured pruning[17]. Computer vision and image processing witnessed substantial progress with Zhang et al. (2025)'s dynamic cross-attention approach for fine-grained image captioning[5], Peng et al. (2023)'s source-free domain adaptive human pose estimation[11], Pinyoanuntapong et al. (2023)'s self-aligned domain adaptation for mmWave gait recognition[12], and Zheng et al. (2025)'s motion-aware diffusion framework for human mesh recovery[13]. Natural language processing and text analysis advanced through several specialized applications: Zhao et al. (2025) developed LLaMA-based automated text quality assessment[6], Zhang et al. (2025) created meta-attention networks for automated essay assessment[7], Huang et al. (2025) enhanced document-level QA via multi-hop retrieval-augmented generation[8], and Zhang et al. (2025) reviewed innovative applications of large models[9]. Financial technology and risk management applications include Wang et al. (2025)'s AI-enhanced financial risk control system for multinational supply chains[14], Su et al. (2025)'s WaveLST-Trans model for financial anomaly detection[20], Zhang et al.

(2025)'s MamNet for network traffic forecasting[21], Zhang et al. (2025)'s deep learning approach for carbon market forecasting[22], Tong et al. (2024)'s integrated framework for credit card approval prediction[23], and Cheng et al. (2025)'s study on executive human capital and stock volatility[30]. Recommendation systems and user modeling were enhanced by Han & Dou (2025)'s integration of hierarchical graph attention with multimodal knowledge graphs[25], Yang et al. (2025)'s optimization of parallelism methods for LLM-based recommendation systems[27], and Yang (2025)'s application of prompt-based models for intelligent consultation[26]. Additional significant contributions include Fang (2025)'s cloud-native architecture for cross-border logistics[10], Wang (2025)'s transformer-augmented survival analysis for clinical trials[15], Miao et al. (2025)'s authentication protocol for IoT supply chains[18], Li et al. (2025)'s intelligent recruitment system with GPT and GNNs[19], Zhuang (2025)'s analysis of real estate marketing strategies[24], Zhang et al. (2025)'s AI-driven sales forecasting for gaming[28], and Yang (2025)'s SEO optimization using Dijkstra algorithm[29].

2. Artificial Intelligence and Network Security

2.1 Overview of Artificial Intelligence

Artificial Intelligence (AI) is a cutting-edge interdisciplinary field whose core goal is to simulate, extend, and even surpass human intelligence. AI technologies encompass multiple subfields, including machine learning, deep learning, and natural language processing. As an important branch of AI, machine learning automatically extracts knowledge from large amounts of data to build models with predictive or decision-making capabilities [1]. These models can make corresponding judgments or predictions based on new data inputs, thereby achieving intelligent processing.

Deep learning is a subset of machine learning that draws on the working principles of the human brain's neural networks. By constructing multi-layer neural networks, it enables in-depth mining and analysis of complex data. Deep learning has achieved remarkable results in image recognition, speech recognition, natural language processing, and other fields, driving the rapid development of AI technology.

2.2 Overview of Cybersecurity

Cybersecurity encompasses a series of activities aimed at protecting computer network systems and their information resources from unauthorized access, use, disclosure, destruction, alteration, or destruction. With the popularization of the Internet and the advancement of information technology, cybersecurity threats have become increasingly diverse, including computer viruses, Trojan programs, phishing attacks, distributed denial-of-service (DDoS) attacks, and more. These threats can not only lead to the leakage of personal privacy and economic losses for enterprises but may also have serious impacts on national security. Therefore, cybersecurity has become an indispensable part of modern society, requiring a variety of technical and managerial measures to ensure the secure and stable operation of network systems.

2.3 The Integration of AI and Cybersecurity

The deep integration of AI technology and cybersecurity is leading a revolutionary transformation in the cybersecurity field. The introduction of AI has significantly improved the efficiency and accuracy of threat identification, judgment, and protection. It can delve into massive amounts of network data, automatically extracting subtle features that human experts might miss, and analyze them through machine learning or deep learning models to precisely identify potential threats. Moreover, leveraging its powerful predictive capabilities, AI combines historical data with real-time information to forecast future threats, laying a solid foundation for proactive defense. What's more, AI systems can continuously learn and self-optimize, dynamically adapting to new threats and achieving intelligent security protection. In short, the combination of AI and cybersecurity provides innovative solutions for addressing complex and ever-changing cybersecurity threats, and as technology continues to advance, its application prospects will become even broader.

3. Automated Identification Applications of Artificial Intelligence in Cybersecurity

3.1 Threat Detection

In the field of cybersecurity, threat detection is the primary task. Traditional threat detection methods often rely on signature libraries and rule matching, but these approaches struggle when facing new or mutated threats. AI-

based anomaly detection methods offer a new solution to this problem.

By deeply learning from vast amounts of normal network behavior data, AI accurately constructs models of legitimate activity, offering a fresh perspective for cybersecurity defense. The moment any anomalous behavior deviates from these patterns, the AI system can swiftly identify it and issue an immediate alert, enabling real-time monitoring and response [2]. This behavior-based detection method breaks free from the traditional constraints of relying on specific signatures or rules, demonstrating remarkable flexibility and adaptability. In the face of ever-evolving cyber threats—especially unknown ones—AI behavioral analysis can effectively uncover their true nature, erecting a solid line of defense for cybersecurity and significantly elevating overall security levels.

Deep learning technology demonstrates outstanding performance in malware identification. By training deep learning models, they can learn to recognize the characteristics of malicious code. These characteristics include not only static features such as instruction sequences and imported functions, but also dynamic features like system call sequences and network behavior. Deep learning models can accurately identify both known and unknown malware, providing strong protection for network security.

3.2 Behavioral Analysis

In the field of cybersecurity, AI's behavioral analytics capabilities are equally indispensable. One of its core applications is user behavior modeling and anomalous behavior identification. AI systems construct detailed models of normal user behavior by deeply analyzing historical user data such as login times, visited websites, and applications used. This model acts like a mirror, accurately reflecting the user's behavioral patterns under normal conditions.

When user behavior deviates significantly from this model, the AI system can quickly make a judgment and identify anomalous behavior. This anomaly-detection mechanism not only effectively detects external malicious actions such as hacking attacks and virus infections, but also sensitively uncovers internal threats. For example, an employee who inadvertently leaks sensitive information or deliberately engages in sabotage will exhibit patterns that starkly diverge from normal behavior, making it nearly impossible to escape the AI system's "all-seeing eyes." By issuing timely alerts and taking action, AI behavioral analysis adds a crucial layer to cybersecurity defense.

3.3 Intelligence Processing

In cybersecurity, intelligence is crucial. Timely intelligence enables organizations to proactively defend against potential threats and minimize losses. However, cybersecurity intelligence is often vast and diverse, making manual processing extremely difficult. AI technology has also demonstrated powerful capabilities in this field.

AI can automatically collect, organize, and analyze cybersecurity intelligence. Through natural language processing, AI can understand key information in the intelligence, such as threat types, attack methods, and impact scope. Based on this information, AI can build a threat-intelligence database to support security decision-making [3]. In addition, AI-based threat-intelligence analysis can monitor the network-threat landscape in real time. By analyzing intelligence from various sources, AI can predict future threats and provide early warnings and response recommendations. This helps organizations prepare defenses in advance and reduce security risks.

In summary, AI applications in cybersecurity cover threat detection, behavioral analysis, and intelligence processing. These applications not only improve the efficiency and accuracy of cybersecurity protection but also provide new solutions for coping with increasingly complex threats. As AI technology continues to advance and cybersecurity needs grow, AI will be applied more broadly and deeply in the cybersecurity field.

4. AI Defense Strategies in Cybersecurity

As cybersecurity threats become more complex and diverse, traditional protection methods can no longer meet modern network-security needs. The integration of artificial intelligence (AI) has brought revolutionary changes to cybersecurity defense, demonstrating great potential in intelligent defense, adaptive protection, security drills, and assessments.

4.1 Intelligent Defense

Intelligent defense is the core of cybersecurity protection, aiming to identify and block malicious attacks in real time to ensure the security and stability of network systems. AI-driven intelligent defense systems, such as AI-powered intrusion detection systems (IDS), play an important role in this area.

AI-driven IDS uses deep-learning algorithms to analyze massive network-traffic data in real time. It can not only recognize known attack patterns but also detect unknown attacks through anomaly detection. The system automatically learns the characteristics of normal network traffic and builds a normal-behavior model. Once traffic deviates significantly from the normal model, the system immediately issues an alert and takes corresponding blocking measures [4]. In addition, AI is applied in intelligent defense to malicious-code detection and phishing-attack identification. Through machine-learning algorithms, AI can automatically extract features of malicious code and build efficient detection models. Similarly, AI can accurately identify phishing attacks by analyzing email content, sender behavior, and other information, effectively preventing data breaches and fraud.

4.2 Adaptive Protection

The network environment is dynamic, and traditional static defense strategies struggle to keep up. Integrating AI breathes new life into adaptive protection. AI can analyze network posture in real time, accurately identify potential threats, dynamically adjust defense policies, and evolve in sync with the network environment.

Firewalls based on AI are a prime example of adaptive protection. Beyond the basic functions of traditional firewalls, they automatically tune rules according to real-time threat conditions. For instance, when a certain type of attack is detected repeatedly, the AI firewall will automatically strengthen the relevant rules to safeguard the network. Moreover, AI enables intelligent traffic scheduling and load balancing. By analyzing traffic data and real-time performance metrics, AI can predict congestion and failures, pre-emptively reroute traffic, and allocate resources to keep the network running smoothly.

4.3 Security Drills and Assessment

Security drills are the core means of improving network defense capabilities. With the introduction of AI technology, both the efficiency and realism of drills are greatly enhanced. AI can simulate complex and ever-changing attack scenarios, providing a highly realistic training environment that allows security teams to test and sharpen their emergency response capabilities more effectively.

Security-drill platforms built on AI can emulate a wide range of sophisticated attacks, including Distributed Denial of Service (DDoS) and Advanced Persistent Threats (APT). Through these simulated attacks, security teams can evaluate their incident-response skills and the effectiveness of their defense strategies [5]. In addition, AI can be used for security assessment. Traditional methods rely heavily on human experience and static rules, making it hard to uncover all hidden risks. AI-driven assessment, however, leverages machine-learning algorithms to automatically analyze security logs, configuration files, and other data, revealing latent vulnerabilities and risks. This approach is not only efficient but also comprehensive, providing a full picture of the network's security posture. Furthermore, AI can generate targeted improvement recommendations based on assessment results, helping organizations elevate their overall cybersecurity defenses.

The deepening application of AI technology in cybersecurity provides new solutions for addressing increasingly complex cyber threats. Applications in intelligent defense, adaptive protection, security drills, and assessment not only enhance the efficiency and accuracy of cybersecurity but also strengthen the overall security and stability of network systems. As AI technology continues to advance and cybersecurity demands grow, AI is expected to be applied more extensively and deeply in the cybersecurity field, offering strong support for building a safer and more stable network environment.

5. Challenges and Prospects of AI in Cybersecurity

5.1 Challenges

Despite significant achievements in applying AI to cybersecurity, its development still faces many challenges. First, data quality is a fundamental issue. AI model training relies on large volumes of high-quality data, yet real-world network data often contain noise and are incomplete, affecting model accuracy and effectiveness. Second, model interpretability is another major difficulty. Many AI models, especially deep learning ones, are often seen

as "black boxes" whose decision-making processes are hard to explain—crucial in cybersecurity, where clear decision rationales are required. Additionally, adversarial attacks are on the rise. Malicious actors may exploit AI vulnerabilities to design targeted attacks that bypass AI defenses. Meanwhile, legal and ethical issues cannot be ignored, such as data privacy protection and responsibility for AI decisions, which urgently need clarification and resolution.

5.2 Prospects

Despite the challenges, the prospects for AI in cybersecurity remain broad, driven by continuous AI advances and growing security needs. In the future, AI-based zero-trust security architectures will gradually become mainstream, enabling more granular protection through continuous verification and dynamic authorization. Moreover, emerging technologies like quantum-secure computing will deeply integrate with AI, further enhancing cybersecurity capabilities to counter more complex and advanced threats. Overall, AI will play an increasingly vital role in cybersecurity, providing strong assurance for building a safer and more stable network environment.

6. Conclusion

This study systematically expounds the core application strategies of artificial intelligence in the automatic identification and protection of computer network security, revealing the significant advantages of AI technology in enhancing network security defense capabilities. The integration of AI not only improves the accuracy of threat detection and the effectiveness of behavioral analysis, but also optimizes intelligence processing and intelligent defense mechanisms. However, the article also points out the challenges faced by AI in network security applications, such as data quality, model interpretability, and legal-ethical issues. In the future, continuous attention and resolution of these challenges are needed to further advance the deep integration of AI and network security, so as to build a more intelligent, efficient, and secure network environment to address increasingly complex network security threats.

References

[1] Zhou, Dianyi. "Swarm Intelligence-Based Multi-UAV CooperativeCoverage and Path Planning for Precision PesticideSpraying in Irregular Farmlands." (2025).

[2] Wen, Hairu, et al. "A Dynamic Adaptive Data Filtering and Sampling Framework for Optimized Fine-Tuning of Large Language Models." 2025 5th International Conference on Consumer Electronics and Computer Engineering (ICCECE). IEEE, 2025.

[3] Weng, Yijie, et al. "SecureGen: A Robust Framework for Enhancing Security and Resilience in Text-to-Image Generation Models." 2025 8th International Symposium on Big Data and Applied Statistics (ISBDAS). IEEE, 2025.

[4] Wang, Yang, and Xiaowei Bi. "Hierarchical Adaptive Fine-Tuning Framework for Enhancing Multi-Task Learning in Large-Scale Models." 2025 5th International Conference on Neural Networks, Information and Communication Engineering (NNICE). IEEE, 2025.

[5] Zhang, Wenqing, et al. "Dynamic Cross-Attention and Multi-Level Feature Fusion for Fine-Grained Image Captioning in Advertising." 2025 5th International Conference on Neural Networks, Information and Communication Engineering (NNICE). IEEE, 2025.

[6] Zhao, Shihao, et al. "LLaM-ScoreNet: An Advanced Architecture for Automated Text Quality Assessment Based on LLaMA Language Model." 2025 5th International Conference on Artificial Intelligence and Industrial Technology Applications (AIITA). IEEE, 2025.

[7] Zhang, Danyang, et al. "Maximizing Scoring Divergence in Automated Essay Assessment with LLaMA-Based Meta-Attention Networks." (2025).

[8] Huang, Xinyue, et al. "Enhancing Document-Level Question Answering via Multi-Hop Retrieval-Augmented Generation with LLaMA 3." arXiv preprint arXiv:2506.16037 (2025).

[9] Zhang, Zheyu, et al. "Innovative Applications of Large Models in Computer Science: Technological Breakthroughs and Future Prospects." 2025 6th International Conference on Computer Engineering and Application (ICCEA). IEEE, 2025.

[10] Fang, Zhiwen. "Cloud-Native Microservice Architecture for Inclusive Cross-Border Logistics: Real-Time Tracking and Automated Customs Clearance for SMEs." Frontiers in Artificial Intelligence Research 2.2 (2025): 221-236.

[11] Peng, Qucheng, Ce Zheng, and Chen Chen. "Source-free domain adaptive human pose estimation." Proceedings of the IEEE/CVF International Conference on Computer Vision. 2023.

[12] Pinyoanuntapong, Ekkasit, et al. "Gaitsada: Self-aligned domain adaptation for mmwave gait recognition." 2023 IEEE 20th International Conference on Mobile Ad Hoc and Smart Systems (MASS). IEEE, 2023.
[13] 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.
[14] Wang, Z., Chew, J. J., Wei, X., Hu, K., Yi, S., & Yi, S. (2025). An Empirical Study on the Design and Optimization of an AI-Enhanced Intelligent Financial Risk Control System in the Context of Multinational Supply Chains. Journal of Theory and Practice in Economics and Management, 2(2), 49–62. Retrieved from https://woodyinternational.com/index.php/jtpem/article/view/208
[15] Wang, Y. (2025). Efficient Adverse Event Forecasting in Clinical Trials via Transformer-Augmented Survival Analysis.
[16] Liu, Jun, et al. "Toward adaptive large language models structured pruning via hybrid-grained weight importance assessment." Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 39. No. 18. 2025.
[17] Miao, Junfeng, et al. "Secure and Efficient Authentication Protocol for Supply Chain Systems in Artificial Intelligence-based Internet of Things." IEEE Internet of Things Journal (2025).
[18] Li, Huaxu, et al. "Enhancing Intelligent Recruitment With Generative Pretrained Transformer and Hierarchical Graph Neural Networks: Optimizing Resume-Job Matching With Deep Learning and Graph-Based Modeling." Journal of Organizational and End User Computing (JOEUC) 37.1 (2025): 1-24.
[19] Su, Tian, et al. "Anomaly Detection and Risk Early Warning System for Financial Time Series Based on the WaveLST-Trans Model." (2025).
[20] Zhang, Yujun, et al. "MamNet: A Novel Hybrid Model for Time-Series Forecasting and Frequency Pattern Analysis in Network Traffic." arXiv preprint arXiv:2507.00304 (2025).
[21] Zhang, Zongzhen, Qianwei Li, and Runlong Li. "Leveraging Deep Learning for Carbon Market Price Forecasting and Risk Evaluation in Green Finance Under Climate Change." Journal of Organizational and End User Computing (JOEUC) 37.1 (2025): 1-27.
[22] Tong, Kejian, et al. "An Integrated Machine Learning and Deep Learning Framework for Credit Card Approval Prediction." 2024 IEEE 6th International Conference on Power, Intelligent Computing and Systems (ICPICS). IEEE, 2024.
[23] Zhuang, R. (2025). Evolutionary Logic and Theoretical Construction of Real Estate Marketing Strategies under Digital Transformation. Economics and Management Innovation, 2(2), 117-124.
[24] Han, X., & Dou, X. (2025). User recommendation method integrating hierarchical graph attention network with multimodal knowledge graph. Frontiers in Neurorobotics, 19, 1587973.
[25] Yang, J. (2025, July). Identification Based on Prompt-Biomrc Model and Its Application in Intelligent Consultation. In Innovative Computing 2025, Volume 1: International Conference on Innovative Computing (Vol. 1440, p. 149). Springer Nature.
[26] Yang, Haowei, Yu Tian, Zhongheng Yang, Zhao Wang, Chengrui Zhou, and Dannier Li. "Research on Model Parallelism and Data Parallelism Optimization Methods in Large Language Model-Based Recommendation Systems." arXiv preprint arXiv:2506.17551 (2025).
[27] Zhang, Jingbo, et al. "AI-Driven Sales Forecasting in the Gaming Industry: Machine Learning-Based Advertising Market Trend Analysis and Key Feature Mining." (2025).
[28] Yang, Yifan. "Website Internal Link Optimization Strategy and SEO Effect Evaluation Based on Dijkstra Algorithm." Journal of Computer, Signal, and System Research 2.3 (2025): 90-96.
[29] Cheng, Ying, et al. "Executive Human Capital Premium and Corporate Stock Price Volatility." Finance Research Letters (2025): 108278.