Theory and Practice of Science and Technology
2025, VOL. 6, NO. 3, 34-39
DOI: 10.47297/taposatWSP2633-456906.20250603

Research on Network Security Based on Artificial Intelligence—On How Artificial Intelligence is Reshaping the Landscape of the Network Security Industry

Jian Yu

College of Computer Science and Electronic Engineering, Hunan University, Changsha, China, 410006

ABSTRACT
Artificial intelligence (AI) technologies have made the network security system more complete and enhanced its ability to withstand security risks. In view of the characteristics of network security in the AI - era, such as increasingly intelligent, diversified, highly concealed, and extremely harmful network attacks, a functional requirements analysis is carried out on the basic layer, intermediate layer, and application layer of network security. A network security defense system is established from aspects such as AI - based network security early warning, firewalls, data encryption, and machine learning to improve network security protection.

KEYWORDS
Artificial Intelligence; Cybersecurity; Deep Learning; Threat Detection; Defense Strategy

1 Introduction

The rapid development of artificial intelligence (AI) technology has provided a new paradigm for cybersecurity defense. For example, deep learning is used to identify abnormal traffic, and reinforcement learning is utilized to optimize dynamic access control strategies. However, as AI technology permeates the field of network security, its double - edged sword effect is gradually emerging: attackers begin to use generative adversarial networks (GANs) to forge legitimate traffic to bypass detection systems, or launch adversarial sample attacks to cause misjudgments in security models. Most existing research focuses on enhancing the effectiveness of AI in threat detection, but seldom systematically analyzes the secondary risks caused by the vulnerabilities of AI itself (such as model backdoor attacks and data poisoning) , and there is an even greater lack of a global defense mechanism designed for AI - empowered attack chains. Therefore, this study proposes a cybersecurity framework that integrates adversarial training and multi - modal feature interpretation, aiming to solve two core problems: (1) how to reduce the sensitivity of AI models to adversarial perturbations through adaptive feature distillation; (2) how to build a closed - loop feedback system to achieve the dynamic evolution of defense strategies. This research has important theoretical value for enhancing the reliability and interpretability of AI - based security systems, and provides technical support for dealing with the next - generation of AI - driven cyberattacks.

2 Applications of AI-Based Cybersecurity Defense

2.1 Deep Learning Intrusion Detection System (DeepIDS)

DeepIDS utilizes deep learning technology to conduct real-time analysis of network traffic, automatically learning normal behavior patterns and detecting abnormal traffic. By comparing known attack signatures with real-time network traffic data, DeepIDS can effectively identify potential cyber-attacks and enhance cybersecurity defense capabilities. DeepIDS has strong adaptability, enabling it to promptly adjust to changes in the network environment and reduce false positives and false negatives. Additionally, DeepIDS can effectively counter zero-day attacks and emerging attack methods, thereby improving the overall security protection level of enterprise networks.

2.2 Intelligent Application Layer Firewall (IAF)

IAF integrates artificial intelligence technology to achieve automatic identification and interception of malicious traffic. Not only can IAF self-learn and self-adjust, but it can also update security policies in real-time to cope with evolving attack methods. In addition to analyzing traffic characteristics, IAF can conduct in-depth analysis of application layer protocols, providing more refined security protection. IAF can also work in conjunction with other security devices, such as intrusion detection systems, to achieve more comprehensive and efficient cybersecurity defense. This defense system provides comprehensive monitoring and protection for enterprise cybersecurity. When the honeynet captures attack commands, the data capture mechanism provided by the server can intercept these commands and generate alarm logs that match the attack characteristics, storing them in the log server. On the basis of cybersecurity defense, it is difficult for attackers to

detect.

2.3 Behavioral Analysis, Detection, and Response System (BAEDR)

BAEDR uses machine learning technology to conduct real-time analysis of network traffic and user behavior. By identifying abnormal behavior, the BAEDR system can automatically take corresponding measures, such as isolating suspicious devices or restricting their access permissions. Additionally, BAEDR can generate security reports in real-time, providing strong support for security teams. Through correlation analysis of internal and external data, BAEDR can accurately detect potential threats and improve the speed of security response. Moreover, the BAEDR system has the ability to self-learn and continuously optimize, thereby constantly improving detection accuracy.

2.4 Malware Detection and Analysis System (MDS)

The MDS system uses artificial intelligence technology to identify, analyze, and defend against malware. Through deep learning and natural language processing techniques, MDS can extract key information from a vast amount of threat intelligence, quickly identifying and classifying malware.

3 The Threats of Artificial Intelligence to Cybersecurity

Artificial intelligence (AI) technology has brought new opportunities to cybersecurity defense, but it has also posed threats to cybersecurity. These threats are mainly reflected in the following aspects: Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

3.1 Intelligent Attack Methods

With the help of AI technology, attackers can implement automated and intelligent attack methods, such as automated vulnerability discovery and exploitation, and intelligent password cracking. These attack methods are difficult to detect and prevent in traditional defense systems, significantly increasing the risk of cybersecurity.

3.2 Generative Adversarial Networks (GANs)

GANs can be used to generate highly realistic fake content, such as forged text, images, audio, and video. This false content can be used for the dissemination of misinformation, cyber fraud, and other malicious activities, posing a serious threat to cybersecurity.Some Common Mistakes.

3.3 Enhanced Concealment with AI

Using AI technology, malicious cyber attackers can more easily cover their tracks, making it more difficult for law enforcement agencies to trace and gather evidence. AI can also help malicious attackers more precisely target and focus on specific targets, thereby increasing the efficiency and accuracy of their attacks.

3.4 Legal and Ethical Challenges

The application of AI technology in the field of cybersecurity has brought many unresolved legal and ethical issues. For example, AI systems in cybersecurity may generate discrimination and bias based on the data they have learned, leading to unfair decision-making and treatment.

In the face of the increasingly complex cyber threats brought about by the rapid advancement of AI technology, it is crucial to develop more intelligent cybersecurity defense strategies using AI. This not only saves human resources and costs but also enables efficient responses to cybersecurity threats.

4 AI-Based Cybersecurity Defense Strategies

4.1 Intelligent Defense Strategies and Human-Machine Collaboration

Application of Intelligent Defense Tools: Deploying AI-driven defense tools enables real-time monitoring of network traffic and system activities, quickly identifying abnormal behaviors and potential threats. For example, machine learning

algorithms can analyze vast amounts of data to detect both known and unknown threats comprehensively.

Importance of Human-Machine Collaboration: Although AI can automate many security tasks, the experience and intuition of human security experts remain crucial. Security teams need to collaborate with AI systems, leveraging the data and analysis provided by AI to make more accurate decisions., and “table head” for your table title. Run-in heads, such as “Abstract”, will require you to apply a style (in this case, italic) in addition to the style provided by the drop down menu to differentiate the head from the text.

4.2 Security Alerting and Risk Assessment

Real-Time Monitoring and Threat Detection: Establish real-time monitoring systems using AI technology to perform large-scale parallel computing and in-depth correlation detection of network traffic, user behavior, and system logs, promptly identifying abnormal activities and potential threats.

Risk Assessment and Prediction: Analyze collected data using AI models to predict the nature and severity of threats, and develop preemptive measures. For example, supervised and unsupervised machine learning techniques, combined with generative AI, can comprehensively detect and defend against known and unknown threats.

Intelligence Sharing and Collaboration: Share intelligence on emerging AI-driven threats with industry partners to collectively address cybersecurity challenges.

4.3 Establishing Robust Security Mechanisms

Multi-Layered Defense System: Choose and apply various types of AI technologies based on specific needs and risk profiles to build a multi-layered and multi-dimensional defense system. For example, adopting a zero-trust architecture to continuously verify all entities, regardless of their location or network, and implementing least-privilege access policies.

Enhanced Identity and Access Management: Implement multi-factor authentication (MFA) across all systems, continuously monitor user activities for anomalies, and adopt Identity-as-a-Service (IDaaS) solutions for centralized identity management.

Security Policy and Regulation Improvement: Organizations should strengthen internal security management measures, regulate employees' use of AI tools, and effectively guard against potential security risks associated with "shadow AI". Continuous Monitoring and Optimization of Defense Strategies.

4.4 Continuous Monitoring and Dynamic Adjustment

Given the constantly evolving cybersecurity landscape and increasingly sophisticated attack methods, continuous monitoring of network and system security status is essential to promptly detect new threats and vulnerabilities. Defense strategies should be dynamically adjusted based on monitoring results to ensure their effectiveness.

Model Optimization and False Positive Reduction: Strengthen the training and optimization of AI models to improve their accuracy and stability, reducing false positives to maximize the effectiveness of AI technology in practical applications.

Emergency Response and Backup Strategies: Improve tiered response mechanisms and develop automated containment strategies for escalating attack scenarios. Implement advanced backup and disaster recovery strategies to ensure rapid recovery in the event of an attack.

To fully leverage the effectiveness of a computer network security defense system, relevant technical personnel must strictly design the system architecture based on the system design diagram. The computer network security defense system consists of three main layers: the network infrastructure layer, the network application layer, and the network middleware layer. During the design process, AI technology serves as the core, enabling rapid data collection and analysis to enhance the proactivity of cybersecurity defense and play a significant role in improving the overall defense capabilities.

5 Optimizing Cybersecurity Strategies with AI-Driven Innovation

5.1 Cybersecurity: A Matter of Great Importance

In today's era where digitalization has permeated every aspect of life, cyberspace has become a crucial battleground for both enterprises and individuals. Cybersecurity strategies, as the key bulwark against cyber threats, cannot be overstated in their importance. They are not only the solid shield for personal privacy but also the essential safeguard for the economic interests and reputation of businesses. Once a cybersecurity breach occurs, companies may face severe consequences such as customer data leaks and business disruptions, leading to heavy economic losses and reputational

damage.

5.2 Four Principles for Building Security Strategies

Constructing cybersecurity strategies requires adherence to four fundamental principles. The principle of comprehensiveness demands that strategies cover all potential threats and system vulnerabilities without any blind spots. The principle of specificity emphasizes the need to tailor unique security strategies based on the distinct nature, business characteristics, and security needs of different organizations to achieve precise protection. The principle of flexibility takes into account the rapid evolution of network technologies and the ever-changing threat landscape, requiring strategies to be dynamically adjustable to adapt to new environments. The principle of compliance ensures that strategies strictly follow relevant laws, regulations, and industry standards, maintaining cybersecurity within a legal framework.

5.3 AI-Powered Cybersecurity Monitoring

With the rapid advancement of artificial intelligence (AI) technology, cybersecurity strategies are now presented with a new opportunity for intelligent upgrading. AI-based real-time traffic analysis systems, acting as intelligent guardians of cybersecurity, constantly monitor the transmission status of data packets in the network. By autonomously learning the characteristics of normal network traffic through AI models and precisely comparing them with real-time traffic data, these systems can quickly trigger alarms and automatically take defensive measures once they detect abnormal traffic patterns and potential malicious activities. Practice has shown that this intelligent monitoring approach can significantly reduce the success rate of cyber-attacks and effectively minimize potential losses.

5.4 AI-Driven Automated Strategy Optimization

AI-empowered optimization of cybersecurity strategies has broken through the limitations of traditional monitoring and alerting, achieving automated adjustment and optimization of strategies. By deeply mining and analyzing multi-dimensional data such as historical security incidents, vulnerability remediation records, and user feedback, AI systems can automatically optimize the configuration of protective strategies and adjust strategy parameters. Moreover, leveraging machine learning algorithms, AI continuously self-learns and evolves, constantly enhancing the adaptability and accuracy of strategies to ensure that cybersecurity protection remains highly effective.

5.5 Establish Mechanisms to Enhance Security Intelligence

To fully leverage the effectiveness of AI in optimizing cybersecurity strategies, establishing a scientific evaluation and feedback mechanism is crucial. Regular assessments of the implementation of strategies are necessary, closely monitoring key indicators such as detection rates, false alarm rates, and response times. Timely collection and analysis of user feedback from real-world applications are also essential to gain an in-depth understanding of existing issues and directions for improvement. Based on the evaluation results and feedback, continuous optimization of AI models and strategy configurations should be carried out to form a virtuous cycle of continuous improvement. This will enhance the level of intelligent cybersecurity protection and build a robust cybersecurity defense line for both enterprises and individuals.

6 Applications and Future Prospects of Automation and Response in Cybersecurity

Automation and response are key components in the field of cybersecurity, focusing primarily on the automated detection, response, and remediation of threats. In this domain, the application of artificial intelligence (AI) provides organizations with powerful support for more efficient threat management.

6.1 Security Automation

Security automation is an effective way to enhance cybersecurity levels through automated processes. AI can automatically execute a range of security tasks, from threat detection to vulnerability remediation. For example, AI-based threat detection systems can automatically trigger alerts and take measures to isolate infected systems, effectively preventing the spread of attacks. Automated vulnerability scanning tools can detect system vulnerabilities and automatically schedule remediation tasks.

Moreover, automation plays a significant role in identity and access management, ensuring dynamic adjustment of user permissions. When employees change positions or leave the company, the system can automatically revoke or adjust

their permissions, thereby reducing the risk of insider threats.

6.2 AI-based Threat Response

Threat response is the process of taking measures to mitigate risks and repair damaged systems after a threat is detected. AI plays a crucial role in this process. Once a threat is detected, AI can automatically analyze its nature and scope, identify affected systems and data, and provide strong support for security teams to take targeted measures.

Additionally, AI can generate automated responses, such as isolating infected systems, suspending malicious activities, or automatically fixing vulnerabilities. This kind of automated response can quickly mitigate risks and reduce potential losses.

6.3 Automated Recovery and Emergency Response

Automation also holds significant value in network recovery and emergency response. When facing large-scale cyberattacks or disasters, AI can assist organizations in quickly resuming normal operations. For example, AI can automatically back up critical data and restore systems when necessary. It can also analyze network architecture to help restore network topology. Automated emergency response plans can be triggered automatically in case of network emergencies, ensuring that organizations can respond swiftly.

6.4 Summary

In summary, automation and response are core elements of cybersecurity, and the application of AI has significantly improved the speed and efficiency of threat response. Through automation, organizations can better protect their networks and data, reducing potential losses.

7 Future Trends and Challenges

In the future, the application of artificial intelligence in cybersecurity will continue to evolve, but it also faces numerous challenges and limitations.

7.1 Future Trends of AI in Cybersecurity

Future trends include deeper AI integration, smarter decision-making support, and broader automation. AI systems will become increasingly intelligent and adaptive, capable of continuous learning and adapting to emerging threats. At the same time, AI will play a more critical role in areas such as cloud security, IoT security, and 5G network security.

7.2 Ethical and Privacy Issues

The application of AI in cybersecurity has raised a series of ethical and privacy concerns. For example, AI could be used for mass surveillance, infringing on personal privacy. AI decision-making systems may also exhibit unfairness and discrimination. Therefore, it is essential to establish corresponding ethical guidelines and regulations to ensure the legal and ethical application of AI in cybersecurity.

7.3 Technical Challenges and Limitations

AI applications in cybersecurity face several technical challenges, such as adversarial machine learning attacks, model interpretability, and data quality issues. Addressing these challenges requires ongoing research and innovation.

8 Conclusion

In the context of rapid advancements in artificial intelligence (AI) technology, the development of technology also brings new challenges, with the cybersecurity landscape becoming increasingly severe. AI technology plays a significant role in cybersecurity defense. This paper introduces the threats and challenges that AI technology poses to cybersecurity defense, as well as corresponding countermeasures. It also constructs a highly practical and executable defense system by integrating multiple technologies at the application level. In cybersecurity defense, it is necessary to fully utilize AI technology in combination with traditional defense methods to jointly address cyber threats. By leveraging the synergy between AI and human efforts, the effectiveness of cybersecurity defense can be enhanced. Moreover, cybersecurity

professionals need to closely monitor technological trends, continuously optimize cybersecurity defense strategies, and constantly improve their defense capabilities to ensure the security of cyberspace.

References

[1] Ma Yiwei.(2023),Research on Cybersecurity Based on Artificial Intelligence.Cybersecurity Technology and Application, Issue 11,pp. 156–157,.

[2] Wang Ming, Sun Zhiwen, Yang Haiyan. (2024), The Threats and Countermeasures of Artificial Intelligence to Cybersecurity, Cybersecurity Technology and Application, Issue 1,pp.163–165.

[3] Hong Meixue, Bai Shigang,. (2024), Applications of Artificial Intelligence in Cybersecurity in Magnetism, Cybersecurity Technology and Application, Issue 8, pp. 115–117.

[4] Gao Junxia.(2024),Design of Cybersecurity Defense Systems Based on Artificial Intelligence.Information: Technology and Application,Volume 25, Issue 10,pp.146-148.

[5] Wang Jipeng. (2020), A Multi-layer Detection System for Android Malware Based on Deep Learning. MASTER THESIS FOR PROFESSIONAL DEGREE.

[6] Zhou Jie.(2021),Research on Android Malware Detection Methods Based on Static and Dynamic Analysis.MASTER THESIS FOR PROFESSIONAL DEGREE.

[7] Pi Xunxun, Wu Lisheng. (2023), Design of Cybersecurity Defense Systems Based on Artificial Intelligence Technology. Wireless Internet Technology,No. 18,pp.25-27.

[8] Dong Hongmeng.(2024),The Application of Artificial Intelligence Technology in Computer Network Security.Technology and Innovation, Issue 9,pp.78-80.