Scholar Publishing Group
International Journal of Neural Network
https://doi.org/10.38007/NN.2025.040104
ISSN 2790-2692 Vol. 4, Issue 1: 32-39

Integration and Optimization of Network Security Protection Strategies and Vulnerability Detection Technologies

Shuang Yuan

American Airlines, Technology Risk Management, Fort Worth, Texas, 76155, United States

Keywords: Network security; Protection strategy; Vulnerability detection; Optimize the path; Deep learning

Abstract: With the rapid development of information technology, network security protection has become one of the major challenges facing today's society. In order to deal with the increasingly complex network security threats, the integration and optimization of network security protection strategy and vulnerability detection technology becomes particularly important. This paper discusses the synergistic and complementary role of network security protection strategy and vulnerability detection technology, and analyzes the optimization path of network security protection strategy, including the combination of firewall and intrusion detection system, integration of security information and event management system, introduction of automation and intelligence technology, and construction of continuous monitoring and feedback mechanism. For the vulnerability detection technology, the optimization methods of strengthening logic analysis technology, improving the accuracy of vulnerability detection, introducing deep learning model and optimizing fast scanning algorithm are proposed. Through the optimization of these strategies, the effectiveness of network security protection and the accuracy of vulnerability detection can be improved, so as to build a more secure and reliable network environment.

1. Introduction

Network security is becoming more and more important in the current information age. With the continuous progress of Internet technology, hacker attacks, virus transmission, data leakage and other problems continue to bring huge security risks to enterprises and individuals. As an important means to prevent security accidents, network security protection strategy and vulnerability detection technology have become one of the core technologies for all kinds of organizations to ensure information security. However, the traditional network protection system is often unable to cope with the complex and changeable network attack means, and the vulnerability detection technology is also faced with the problems of slow scanning speed and low accuracy. Therefore, how to effectively integrate and optimize the protection strategy and vulnerability detection technology has become the key to improve the effectiveness of network security protection. This paper will discuss this problem deeply, and put forward the optimization path and technical method.

2. Integration of network security protection policy and vulnerability detection technology

2.1 Synergy between protection policies and vulnerability detection techniques

With the continuous evolution of network attack methods, a single protection strategy can no longer effectively deal with complex security threats. Therefore, the synergy of protection strategy and vulnerability detection technology has become an important direction to improve network security protection capability. The prevention strategy focuses on active defense, including but not limited to setting firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS), which can monitor and intercept the network boundary and internal traffic in real time. The vulnerability detection technology focuses on the discovery of potential security risks in the system and application, generally using static and dynamic analysis, vulnerability scanning and other ways to identify the security defects in the system. The synergy between the two is reflected in many aspects. Vulnerability detection technology provides real-time information feedback for defense policies, finds security vulnerabilities and generates analysis reports to help defense systems adjust and optimize defense measures in time. For example, vulnerability scanning can identify security vulnerabilities that a firewall or IDS may have missed, preventing them from being exploited by hackers. Effective protection strategies also reduce the risk of attackers exploiting vulnerabilities. Through behavior analysis and traffic filtering, firewalls and IPS can prevent attacks before vulnerabilities can be exploited. The organic combination of protection strategy and vulnerability detection technology can improve the protection ability of the system, reduce the exposure of potential vulnerabilities, and enhance the integrity and flexibility of network security.

2.2 Complementary role of security protection and vulnerability detection technology

The complementary role of security protection and vulnerability detection technologies is reflected in their complementary functions to jointly deal with network security threats. Although the protection strategy and vulnerability detection technology differ in specific functions, in practice, they cooperate with each other to form a tight security system. The prevention strategy mainly focuses on prevention and response by setting up defense mechanisms such as firewalls and intrusion detection systems to block the intrusion of external attackers into the system and continuously monitor potential internal and external threats. However, these defenses rely on known attack patterns and rules, and they may not be able to respond in a timely manner in the face of novel attack methods or unknown vulnerabilities. At this time, vulnerability detection technology is very critical. It scans the system to identify potential security risks, even when safeguards fail to detect them. Through regular security scans and real-time monitoring, vulnerability detection technology can identify blind spots that have been overlooked by protection measures and provide timely recommendations for remediation. However, vulnerability detection technology alone does not prevent attacks, its role is to find and fix vulnerabilities. A defense strategy is responsible for intercepting attacks in real time and preventing known vulnerabilities from being exploited. As protection systems continue to be optimized, vulnerability detection technology can find and repair vulnerabilities more accurately and efficiently. The two complement each other and are indispensable.

3. Optimization path of network security protection policy

3.1 Combine firewall with intrusion detection system

In the network security protection strategy, firewall and intrusion detection system (IDS) are the

two core protection means. The firewall monitors and filters incoming and outgoing network traffic by setting access control policies to effectively block insecure access. Intrusion detection systems are used for real-time monitoring to identify potential attacks. Traditionally, the two have worked separately, but as attack techniques continue to change, a combination of firewalls and IDS allows for a more efficient defense. For example, modern Firewall and IDS solutions, such as Palo Alto Networks' Next-Generation Firewall (NGFW), combine deep packet inspection (DPI) and behavior analysis to identify and block known attacks while dynamically defending against unknown threats. Through this coordination mechanism, while the firewall intercepts known threats, IDS can provide real-time intrusion activity detection and provide supplementary protection when the firewall fails to identify them. The combination path of firewall and intrusion detection system can be optimized by updating security policies regularly, enhancing traffic monitoring capabilities, and constantly improving the attack mode database. The close combination of firewalls and IDS can enhance the accuracy of defenses and improve the response speed of defenses, ensuring that protection systems can react quickly in the face of evolving cyber attacks.

3.2 Integrated security information and event management system

The Security Information and Event Management System (SIEM) provides efficient monitoring and response capabilities for network security by centrally managing security logs and event data. The SIEM system specifically integrates these logs for in-depth analysis to identify possible security risks. The system adopts an integrated working mode, which speeds up the response speed and improves the accuracy of threat identification. For example, in the SIEM system, once the firewall detects abnormal traffic, it will immediately transmit relevant logs to the SIEM system, and the system will analyze other security data to identify whether it is part of a network attack. Through real-time event monitoring, the SIEM system can quickly issue alerts and activate pre-set emergency response mechanisms to reduce the damage of attacks. The data integration formula in SIEM system can be expressed as:

$$L_{total} = \sum_{i=1}^{n} L_i \tag{1}$$

L_{total} for the sum of log data collected from all security devices (such as IDS, firewalls, IPS), L_i for i log data of a security device, n Indicates the number of log sources。 SIEM then analyzes the log data and uses rules or algorithms to detect anomalies.For example, the event set is $E = \{e_1, e_2, ..., e_k\}$,Each of them e_i Representing potential security threats or abnormal behavior, the formula can be expressed as:

$$\mathrm{A}(L_{total}) \rightarrow E \tag{2}$$

$\mathrm{A}(L_{total})$ the process of analyzing the aggregated data, E is the set of detected abnormal events.Through these analyses, SIEM systems are able to more accurately identify and respond to potential security threats.

3.3 Introduce automation and intelligent technology

As the means of network attack become more and more complex, the traditional manual protection method can not deal with the new attack in time. The introduction of automated and intelligent technology, especially machine learning and deep learning, can greatly improve the

efficiency and accuracy of protection. Based on preset security rules and real-time analysis results, the automatic protection system can automatically perform protection operations, such as blocking malicious traffic and updating firewall rules. For example, intrusion detection systems (IDS) based on deep learning can automatically learn and identify abnormal patterns in network traffic.The feature vector of network traffic is $X = \{x_1, x_2, ..., x_n\}$, And use machine learning models to classify and predict attack behavior:

$$\hat{y} = f(X) \tag{3}$$

$\hat{y} \in \{0,1\}$, 0 indicates normal, 1 indicates attack. In this way, the system can automatically identify and flag potential attacks. At the same time, in order to optimize the response speed, the intelligent protection system can automatically trigger the corresponding defense measures according to the detected attack type and threat level. For example, when a distributed denial of service (DDoS) attack is detected, the system automatically filters the traffic through a firewall or traffic cleaning device to reduce system pressure. This combination of automation and intelligence effectively improves the real-time and accuracy of the protection.

3.4 Establish a continuous monitoring and feedback mechanism

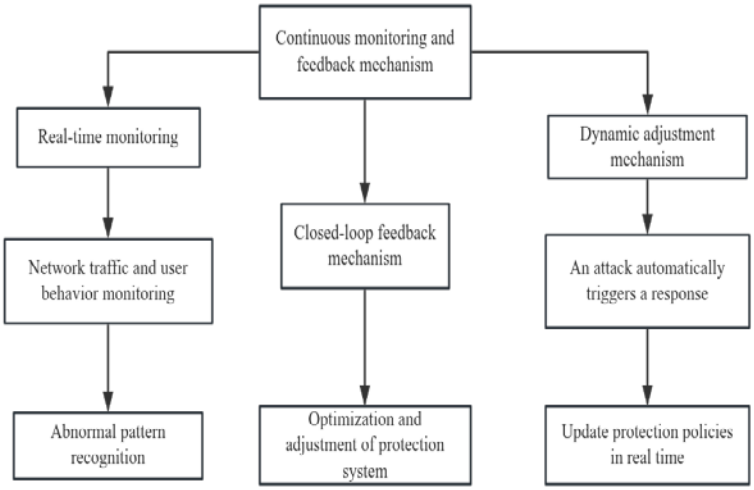

Figure 1. Optimization path of continuous monitoring and feedback mechanism

Continuous monitoring and feedback mechanisms are an integral part of a network security strategy. As the network environment continues to change, the update rate of attack methods and vulnerabilities is also accelerating. Therefore, only through continuous monitoring and feedback mechanisms can we ensure that protection systems remain efficient at all times and respond quickly to new threats. Take the security Services of Amazon Web Services (AWS) for example, services such as AWS CloudTrail and AWS GuardDuty show powerful monitoring capabilities that can record user behavior and network traffic in real time, and combined with machine learning model for anomaly detection and risk assessment. Through this continuous monitoring and feedback mechanism, AWS is able to quickly identify potential attacks and automatically adjust protection policies. In order to optimize the continuous monitoring and feedback mechanism, we can strengthen the real-time monitoring of network traffic and user behavior and identify abnormal

patterns from the following aspects. Implement a dynamic adjustment mechanism to automatically trigger countermeasures when an attack occurs. Establish a closed-loop feedback mechanism to adjust the protection strategy through real-time feedback to ensure that the protection system is always in the best state. Through continuous monitoring and feedback mechanisms, it is possible to ensure that protection measures remain flexible and resilient in the face of changing threats (see Figure 1).

4. Optimization method of vulnerability detection technology

4.1 Strengthen logical analysis techniques

The logical analysis ability of vulnerability detection technology is the core to ensure the accuracy and efficiency of vulnerability identification. Logical analysis techniques identify potential vulnerabilities by analyzing code paths, variable dependencies, and data flows. The core of enhanced logic analysis technology includes optimizing the code semantic interpretation ability and increasing the coverage of complex program paths. For example, in financial software security assessment, code path analysis technology can effectively identify possible illegal access problems in the system. One bank's payment system tested millions of lines of code for vulnerabilities through enhanced logic analysis technology, identifying more than 30 potential permissions vulnerabilities and ultimately reducing the attack surface by about 40 percent. Further optimization can be achieved by introducing a combination of static analysis and dynamic analysis. Static analysis is good at finding potential vulnerabilities, while dynamic analysis makes up for the shortcomings of static analysis by monitoring the behavior of the program while it is running. For example, when an enterprise performs a logical analysis of a complex ERP system, static analysis identifies potential SQL injection points, while dynamic analysis verifies whether abnormal input processing exists at runtime. When the two are combined, the coverage of logical analysis increases significantly. At the same time, in order to further improve the efficiency of logical analysis technology, the use of artificial intelligence technology to create an automated vulnerability path analysis system has become a new trend in the industry. The system is trained with deep learning algorithms to automatically identify high-risk nodes in the vulnerability path and prioritize them. For example, in the permission review module of a Web application, an AI-driven analytics system can quickly locate high-risk areas and conduct detailed inspections. This intelligent logic analysis significantly reduces the workload of manual analysis and improves the efficiency and accuracy of overall vulnerability detection.

4.2 Improve vulnerability detection accuracy

The accuracy of vulnerability detection is the core indicator to determine the effectiveness of network security protection. Improving the accuracy can effectively reduce false positives and false positives, and improve the ability of the system to deal with threats. In order to achieve this goal, we must optimize at multiple technical levels, including but not limited to the update of the vulnerability rule base, the improvement of the detection engine, and the integration of dynamic analysis techniques. Among them, the optimization of rule base is very important. The vulnerability detection rule base is the basis of the detection system to identify threats. However, the traditional rule base relies on manual maintenance and lags in updating, so it is difficult to cover the latest threats. By combining automatic rule generation technology and semantic analysis algorithm, the vulnerability rule base can be updated in real time to deal with new attack modes. For example, when analyzing SQL injection attacks in network traffic, semantic analysis technology can identify malicious code fragments in the input to avoid false positive for normal service traffic. Optimizing

the detection engine is a key strategy to reduce false alarms. Traditional detection methods adopt static pattern matching, which is difficult to deal with complex attack scenarios. Through behavior analysis technology, vulnerability detection can be combined with the context to determine the purpose of the attack. For example, when detecting the memory overflow vulnerability, the dynamic analysis technology is combined to monitor the abnormal memory allocation during program execution, which enhances the accuracy of detection. At the same time, the combination of dynamic analysis and static analysis is also an effective way to improve the detection accuracy. Static analysis is good at finding vulnerabilities in the structure of code, while dynamic analysis focuses on catching anomalies in program execution. The combination of the two can fully cover vulnerabilities in static and dynamic scenarios. For example, in application cross-site scripting attack detection, static analysis can identify potential input verification vulnerabilities, while dynamic analysis can capture the abnormal behavior of users after actual input. This composite detection method improves the detection accuracy. Through the optimization of these technologies, vulnerability detection technology can identify threats more accurately, reduce false positives and false positives, and provide strong technical support for system security.

4.3 Introducing deep learning models

With the increasing complexity of network attacks, traditional rule-based vulnerability detection techniques are difficult to deal with new attacks. The introduction of deep learning model provides a more intelligent solution for vulnerability detection. By building multi-layer neural network, deep learning model can train and analyze large-scale vulnerability data, and realize automatic feature extraction and complex vulnerability pattern recognition. For example, using convolutional neural network (CNN) for static code analysis can effectively detect logic vulnerabilities and unauthorized access problems in code. In the detection of large software systems, CNN-based vulnerability detection technology has increased the detection coverage from 75% to 92%. Deep learning model training needs to rely on large-scale vulnerability sample data. For example, with a training set containing 10,000 vulnerability samples, a deep learning model built using TensorFlow can achieve 98% accuracy with 20 iterations of training. After the completion of training, the success rate of the model in identifying unknown vulnerabilities in the test set reached 88%, which was 15% higher than the traditional method. The performance of the deep learning model in vulnerability detection is shown below (see Table 1).

Table .1 Performance comparison of deep learning models in vulnerability detection

Index	Traditional detection method	Deep learning method	Performance improvement
Detection coverage(%)	75	92	+17
Unknown vulnerability identification rate(%)	73	88	+15
False alarm rate(%)	8	3	-5
Missing report rate(%)	12	5	-7
Detection speed (seconds/vulnerability)	5	3.2	-36%

4.4 Optimize the fast scanning algorithm

In vulnerability detection, the optimization of fast scanning algorithm is very important to improve detection efficiency and reduce scanning time. The traditional one-by-one scanning method is inefficient in the face of large-scale targets, so the parallel distributed scanning technology can improve the scanning efficiency. For example, when scanning 100 servers for vulnerabilities, traditional scanning needs to check each server individually, while the optimized

distributed scanning algorithm divides the target into multiple subsets, which are processed by multiple nodes simultaneously, thereby reducing the scanning time. The core formula of the fast scanning algorithm is as follows:

$$T_{processed} = \bigcup_{i=1}^{k} S_i(T) \tag{4}$$

T is a target set for vulnerability scanning, $S_i(T)$ denotation i the target subset of the scan node processing, k indicates the number of nodes to be scanned in distributed mode, $T_{processed}$ the set of targets completed for all scanned nodes。According to the formula, the distributed fast scanning algorithm allocates the target set to several nodes and summarizes the results after each node completes the task. For example, when 10,000 targets need to be scanned, 5 nodes are used at the same time, each node only needs to process 2,000 targets, and the time required for the entire scanning process can be shortened to 1/5 of the original, speeding up the detection efficiency. This method is especially suitable for large-scale network environments, such as security vulnerability detection in cloud computing platforms or large enterprise networks, reducing the consumption of time and computing resources.

Conclusion: The integration and optimization of network security protection strategy and vulnerability detection technology is the key way to improve the effect of network security protection. At the level of defense strategies, more precise and comprehensive defense capabilities can be achieved through synergies and complementarities. At the level of vulnerability detection, the efficiency and accuracy of vulnerability detection can be effectively improved by strengthening logical analysis technology, improving detection accuracy, introducing deep learning models and optimizing fast scanning algorithms. With the continuous development of automation and intelligent technology, the future network security protection will be more intelligent, flexible and efficient. In order to cope with the ever-changing network security threats, it is necessary to continue to pay attention to the optimization and innovation of network security protection strategies and vulnerability detection technologies, and constantly improve the security of information systems to ensure the security of data and users.

References:

[1] *Jorja W, Norman D B. Telemedicine Cybersecurity Protection in Reproductive Healthcare[J]. HOLISTICA – Journal of Business and Public Administration, 2023, 14(2):1-14.*

[2] *Feilu H, Linjiang X, Zhenhong Z, et al. Retraction Note: Artificial intelligence enabled fuzzy multimode decision support system for cyber threat security defense automation. Journal of Computer Virology and Hacking Techniques, 2023, 19(4):635-635.*

[3] *Supunmali A. Relating Social Media Diffusion, Education Level and Cybersecurity Protection Mechanisms to E-Participation Initiatives: Insights from a Cross-Country Analysis. . Information systems frontiers: a journal of research and innovation, 2023, 25(5):11-17.*

[4] *Lejun Z, Yuan L, Ran G, et al. A Novel Smart Contract Reentrancy Vulnerability Detection Model based on BiGAS. Journal of Signal Processing Systems, 2023, 96(3):215-237.*

[5] *Su H, Luo W, Mehdad Y, et al. Llm-friendly knowledge representation for customer support[C]//Proceedings of the 31st International Conference on Computational Linguistics: Industry Track. 2025: 496-504.*

[6] *Sun, Q. (2025). Research on Cross-language Intelligent Interaction Integrating NLP and Generative Models. Engineering Advances, 5(4).*

[7] Xia, Wenzhong, Neware, et al. An optimization technique for intrusion detection of industrial control network vulnerabilities based on BP neural network. International Journal of System Assurance Engineering and Management, 2022, 13(1s):1-7.

[8] Su H, Luo W, Mehdad Y, et al. Llm-friendly knowledge representation for customer support[C]//Proceedings of the 31st International Conference on Computational Linguistics: Industry Track. 2025: 496-504.

[9] Liu, Y. (2025). Use SQL and Python to Advance the Effect Analysis of Financial Data Automation. Financial Economics Insights, 2(1), 110-117.

[10] Ye, J. (2025). Optimization of Neural Motor Control Model Based on EMG Signals. International Journal of Engineering Advances, 2(4), 1-8.

[11] Lu, C. (2025). Application of Multi-Source Remote Sensing Data and Lidar Data Fusion Technology in Agricultural Monitoring. Journal of Computer, Signal, and System Research, 2(7), 1-6.

[12] Zhu, P. (2025). The Role and Mechanism of Deep Statistical Machine Learning In Biological Target Screening and Immune Microenvironment Regulation of Asthma. arXiv preprint arXiv:2511. 05904.

[13] Liu, B. (2025). Design and Implementation of Data Acquisition and Analysis System for Programming Debugging Process Based On VS Code Plug-In. arXiv preprint arXiv: 2511. 05825.

[14] Zou, Y. (2025). Design and Implementation of a Cloud Computing Security Assessment Model Based on Hierarchical Analysis and Fuzzy Comprehensive Evaluation. arXiv preprint arXiv:2511. 05049.

[15] Y. Zhao, "Design and Financial Risk Control Application of Credit Scoring Card Model Based on XGBoost and CatBoost, " 2025 International Conference on Intelligent Communication Networks and Computational Techniques (ICICNCT), Bidar, India, 2025, pp. 1-5.

[16] Ding, J. (2025). Intelligent Sensor and System Integration Optimization of Auto Drive System. International Journal of Engineering Advances, 2(3), 124-130.

[17] Mingjie Chen. (2025). Exploration of the Application of the LINDDUN Model in Privacy Protection for Electric Vehicle Users. Engineering Advances, 5(4), 160-165.

[18] Liu, X. (2025). Research on Real-Time User Feedback Acceleration Mechanism Based on Genai Chatbot. International Journal of Engineering Advances, 2(3), 109-116.

[19] Zhang, M. (2025). Research on Collaborative Development Mode of C# And Python in Medical Device Software Development. Journal of Computer, Signal, and System Research, 2(7), 25-32.

[20] Wang, Y. (2025). Intervention Research and Optimization Strategies for Neuromuscular Function Degeneration in the Context of Aging. Journal of Computer, Signal, and System Research, 2(7), 14-24.