Analysis of the Architecture, Technology and Advantages of AI-based Web Application Firewall

Zhou Yan

The 30th Research Institute of China Electronics Technology Group Corporation, Chengdu 610000, Sichuan, China

Abstract: ***The static defense mode of traditional firewalls is difficult to cope with rapidly changing attack methods. However, the AI-powered WAF can automatically learn traffic patterns and attack characteristics by analyzing a large amount of network data in real time, enabling dynamic policy adjustment. It can more accurately distinguish legitimate requests from malicious attacks, significantly reduce false positives and false negatives, and quickly respond to large-scale network attacks, timely block the attack link, reduce the impact of attacks on Web applications, and ensure the continuity and stability of services. By analyzing the limitations of traditional Web application firewalls, comparing the advantages of combining AI technology with traditional technology, and explaining its system architecture and key technologies, this paper aims to improve Web application security and provide a reference for building an advanced security protection system.***

Keywords: AI technology; Web application; Firewall system.

1. INTRODUCTION

With the widespread popularity of Web applications, Web applications have been deeply integrated into all aspects of social operation. They are not only applied to the refined management of smart cities but also to the real-time interaction of remote medical care. Their security has become the cornerstone of critical infrastructure and social operation. However, the network security situation has become increasingly severe and complex. Traditional Web application firewalls are mainly based on static rule libraries and are difficult to effectively respond to emerging and evolving network attacks, such as smart malware generated using artificial intelligence algorithms and advanced persistent threats (APTs) based on zero-day vulnerabilities. Currently, network attackers have started to use artificial intelligence technology to optimize their attack strategies and can automatically bypass traditional protection mechanisms. Breakthroughs in artificial intelligence technology in the fields of pattern recognition, data mining, etc. have made it possible to revolutionize Web application firewalls. Incorporating artificial intelligence technology into Web application firewall systems, enabling them to have learning, reasoning, and decision-making capabilities similar to human intelligence, and being able to perceive changes in the network environment in real time and accurately identify new attack patterns, has become a key research direction for ensuring Web application security.

Meng (2023) constructed a neural network-based evaluation system for green cabling of cables [1]; Junxi et al. (2024) proposed a graph convolutional network based on matrix factorization (GCN-MF) for recommendation [2]; Gao et al. (2026) conducted experimental geomechanical modelling of hard and soft rock masses including fault zones [3]; Han et al. (2026) developed a dual-scale model with collaborative reasoning and multi-feature fusion for robust AI-generated image detection [4]; Ya (2025) studied EDA technology in digital circuit design [5]; Sun (2025) addressed accessibility challenges and solutions in designing inclusive digital interfaces [6]; Zhang (2026) built a hybrid LSTM-GARCH model integrating volatility factors from US financial markets [7]; Ding (2025) developed a multispectral vision system for in-situ detection of pesticide residues on agricultural produce [8]; Luo (2026) analyzed the integration of computer application technology and information management [9]; Shen et al. (2025) applied the whale optimization algorithm to financial payment fraud detection [10]; Wang (2026) examined the application of computer science and technology in the big data context [11]; Ma (2025) proposed a unified framework for congestion diagnosis and dynamic mitigation in complex networks [12]; Jin (2025) optimized order allocation algorithms for industrial internet platforms [13]; Zhou (2025) designed a collaborative filtering model for digital precision distribution of social media content on private domain platforms in the automotive industry [14]; Yuan et al. (2026) introduced TA-Mem, a tool-augmented autonomous memory retrieval method for large language models in long-term conversational question answering [15]; Li et al. (2026) presented MFT, a memory-aware fine-tuning of SAM2 for efficient long-sequence video object segmentation [16]; Shan et al. (2025) rethought wine tasting for Chinese consumers through a service design approach enhanced by multimodal

personalization [17]; Liu (2025) systematically evaluated deep learning architectures for plant image classification [18]; Miao (2026) applied big data technologies for enhanced network security analysis [19]; Wang (2025) enhanced object detection in photovoltaic farm panoramic imagery using a multi-scale feature-enhanced YOLOv8 [20]; Liu (2025) researched GPU parallel computing for image processing [21]; Lu et al. (2025) employed a Faster R-CNN model for flame detection [22]; Peng et al. (2023) introduced RAIN, a regularization method on input and network for black-box domain adaptation [23]; and Peng et al. (2024) proposed a dual-augmentor framework for domain generalization in 3D human pose estimation [24].

2. LIMITATIONS OF TRADITIONAL WEB APPLICATION FIREWALLS

2.1 Lag in Rule Matching

Traditional web application firewalls mainly rely on pre-set rule sets to detect various attack behaviors. In the current context where network attack methods are becoming increasingly diverse and evolving rapidly, this detection method based on fixed rules has significant lag. Security teams need to invest a large amount of effort in collecting and analyzing new attack samples and updating the firewall's rule base accordingly. However, this process often takes a long time. Before the rules are updated, the web application is actually in a state of lacking effective protection. Take the example of new SQL injection variant attacks. Such attacks can cleverly bypass traditional rules. In the case where the firewall fails to identify them in a timely manner, attackers can easily obtain sensitive information in the database, thereby increasing the risk of data leakage and causing losses to enterprises and users.

2.2 Difficult to Defend Against Unknown Attacks

The detection mechanism of traditional Web application firewalls is based on known attack patterns. The characteristics of unknown attacks are not in the existing rule base, and the firewall often misjudges them as normal traffic, making it impossible to effectively identify and prevent them. When an attacker launches an attack using newly discovered Web application vulnerabilities, the traditional firewall cannot detect this attack behavior in a timely manner due to the lack of corresponding rule matching, resulting in the Web application being exposed to risks and being easily attacked, leading to consequences such as service interruption and data loss.

2.3 High False Positive Rate

To ensure comprehensive coverage of various potential attack behaviors, traditional Web application firewalls usually set relatively broad rules. Although this approach increases the detection probability of attacks to a certain extent, it also brings serious false positive problems. A large number of false positive messages will increase the workload of security operation and maintenance personnel, who need to spend a lot of time to distinguish these false positives, thus distracting their attention from real security threats. The normal requests of some legitimate users may be misjudged as attack behaviors because they match the broad rules, which will not only affect the normal user experience, but may also cause economic losses to enterprises due to customer churn.

3. ADVANTAGES OF THE COMBINATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGY AND TRADITIONAL TECHNOLOGY

3.1 Improve Detection Accuracy

Combining artificial intelligence technology with traditional rule matching technology can achieve complementary advantages and improve the detection accuracy of web application firewalls. With the help of pre-set precise rules, traditional rule matching technology can quickly identify and block common attack behaviors. For example, for common SQL injection attacks, traditional rules can react instantly and effectively prevent attackers from illegally accessing the database.

3.2 Enhanced Adaptability and Flexibility

The integration of artificial intelligence technology enables the Web application firewall to automatically adapt to changes in the network environment and attack methods. In the ever-changing network environment, new attack methods emerge in an endless stream, and traditional firewalls often struggle to keep up with these changes quickly.

However, the artificial intelligence model can continuously update and optimize its detection algorithm by learning new traffic data in real time, thereby promptly enhancing its detection ability for new types of attacks. In this combined mode, the AI engine can serve as a supplement to the rule engine. When a new Web application framework or business model appears, the AI engine can quickly learn the new normal traffic characteristics and adjust the detection strategy. The traditional rule engine then provides basic protection on this basis to ensure that the system can operate stably in various situations and effectively resist various security threats. The two work together, making the entire system show stronger flexibility when facing complex situations.

3.3 Reduce Operation and Maintenance Costs

Although there are certain technology investment and personnel training costs in the initial stage of introducing artificial intelligence technology, in the long run, this combination method can reduce the operation and maintenance costs of the Web application firewall. The artificial intelligence model has powerful automatic processing capabilities and can automatically detect and process a large number of security incidents, greatly reducing the workload of security operation and maintenance personnel in manually analyzing and processing security alerts. In specific implementation, the AI engine can be used as a pre-filter to initially screen and analyze traffic data, filter out most normal traffic, and pass the traffic that may pose a threat to the rule engine for further judgment. Due to broad rules, traditional firewalls often generate a large number of false alarms, resulting in operation and maintenance personnel spending a lot of time and energy to identify and process these false alarms. The firewall combined with artificial intelligence technology has a lower false alarm rate, enabling operation and maintenance personnel to focus more on dealing with real security threats, thereby improving work efficiency. For example, traditional firewalls may generate thousands of false alarms daily, while the firewall combined with artificial intelligence technology can reduce the false alarm rate to dozens, effectively reducing the burden on operation and maintenance personnel and the operation and maintenance costs of enterprises.

4. WEB APPLICATION FIREWALL SYSTEM BASED ON ARTIFICIAL INTELLIGENCE TECHNOLOGY

4.1 System Architecture Analysis

The architecture of the Web application firewall system based on artificial intelligence technology is a complex and precise system. Each module works in coordination to provide comprehensive security protection for Web applications.
as follows.

1) Data collection and preprocessing module. This module is responsible for collecting various types of traffic data of Web applications, including HTTP request data, response data, and user behavior data, etc. During the collection process, the system will face a large amount of complex data, which may include invalid information, duplicate requests, and noise data, etc. Therefore, preprocessing operations are crucial. The data cleaning process will remove invalid and duplicate data to ensure the accuracy and integrity of the data; the denoising operation can eliminate interference factors in the data and improve the quality of the data; the format conversion will unify the data into a format suitable for subsequent analysis and model training to ensure data consistency, lay a solid data foundation for subsequent analysis and model training, and improve the availability of the data. For example, in a Web application of a large e-commerce website, a large amount of user request data is generated every day. Through the data collection and preprocessing module, effective request data can be screened out, duplicate and invalid requests can be removed, and high-quality data support can be provided for subsequent security protection.

2) Artificial intelligence model training module. This module uses a variety of advanced machine learning and deep learning algorithms. In terms of machine learning algorithms, the system uses multiple algorithms such as support vector machine (SVM), decision tree, and random forest, which can accurately capture feature patterns from a large amount of normal and attack traffic data. For example, the SVM algorithm will deeply learn key features such as parameters and URLs in HTTP requests, and accurately distinguish normal requests from attack requests by constructing a classification boundary. In practical applications, the SVM algorithm can identify SQL injection attacks disguised as normal requests and provide a reliable judgment basis for the firewall. Deep learning models such as convolutional neural network (CNN), recurrent neural network (RNN) and its variants (such as LSTM) are constructed to deeply analyze Web application traffic. The CNN model can automatically extract features of the structure and content of Web pages and can identify potential XSS attack codes in the pages. Through large-scale data training, the parameters of these models are continuously optimized, making the detection

accuracy of attacks continuously improve. In a Web application in the financial industry, the deep learning model can accurately identify abnormal login behaviors by analyzing users' operation behaviors and traffic patterns, and timely discover potential security threats.

3) Real-time Detection and Response Module. This module is the front line of the system. A well-trained artificial intelligence model is deployed in this module to constantly monitor Web application traffic. Once the model detects suspected attack traffic, it will immediately trigger an efficient response mechanism. The corresponding measures include blocking the attack traffic to prevent the attack from spreading further, recording the attack information in detail to provide a basis for subsequent security analysis and traceability, and quickly sending an alert to the security administrator so that the administrator can timely understand the situation of security incidents. For example, when the system detects a SQL injection attack, it will instantly block the relevant HTTP requests to prevent the attacker from performing illegal operations on the database. The system will send a report containing detailed information such as the attack source IP to the administrator, and the administrator can take timely measures to handle the security incident based on this information to ensure the secure and stable operation of the Web application.

4.2 Explanation of Key Technologies

1) Anomaly detection technology. The core of the artificial intelligence-based anomaly detection technology lies in learning the normal Web application traffic patterns and characteristics to build an accurate normal behavior model. When building the normal behavior model, the system collects a large amount of historical traffic data, which covers various normal operation scenarios. Through in-depth analysis of this data, the characteristics representing normal behavior are extracted, and machine learning algorithms are used to integrate and model these characteristics to form a model that can describe the normal behavior pattern. When real-time traffic data enters the system, it is compared with the built normal behavior model. If the deviation between the real-time traffic data and the normal model is large and exceeds the preset threshold, the system will determine the possible potential attacks. For example, when analyzing user login behavior, the system will establish feature models such as normal login time, location, and frequency. Under normal circumstances, users may log in to the system from common locations during fixed periods on weekdays. However, if the system detects that a certain user logs in frequently from multiple different regions within a short period of time, and the login time is significantly different from the historical records, then the system will regard it as an abnormal behavior and further conduct in-depth detection to determine whether there is an attack behavior.

2) Optimization of machine learning classification algorithms. To improve the performance of machine learning algorithms in Web application firewalls, relevant personnel need to optimize them in multiple aspects. Ensemble learning combines multiple different machine learning models to give full play to the advantages of each model, thereby improving the accuracy and stability of classification. For example, fuse the random forest and logistic regression models. The random forest model has strong anti-overfitting ability and the ability to handle high-dimensional data, and can capture complex non-linear relationships in the data, while the logistic regression model has the characteristics of simplicity and strong interpretability and performs well in dealing with linearly separable problems. Relevant personnel need to fuse these two models and combine their advantages to improve the classification accuracy of different types of attacks. Using feature selection and dimensionality reduction techniques is also an important means to optimize machine learning algorithms. In practical applications, Web application traffic data often contains a large number of features, some of which are redundant, which will not only increase the training time of the model, but also consume a large amount of computing resources. Relevant personnel can use feature selection techniques to remove those redundant features that have little impact on the classification results and retain the key features, thereby shortening the model training time and reducing the consumption of computing resources. Dimensionality reduction techniques can convert high-dimensional data into low-dimensional data, reduce the complexity of the data, while retaining the main information of the data, and enhance the training efficiency and generalization ability of the model. For example, in a Web application traffic dataset containing hundreds of features, the number of features can be reduced to dozens through feature selection and dimensionality reduction techniques, while improving the classification accuracy and generalization ability of the model. In addition, hyperparameter tuning is also an optimization method that cannot be ignored. The hyperparameters of machine learning models have an important impact on the performance of the models, and different combinations of hyperparameters will lead to great differences in the performance of the models on the training set and the test set. Relevant personnel can use methods such as grid search, random search or Bayesian optimization to systematically tune the hyperparameters of the model, find the optimal combination of hyperparameters, and further improve the classification performance of the model in Web application firewalls.

3) Applications of deep learning in traffic analysis. Deep learning models have unique advantages in Web application traffic analysis, capable of automatically learning complex features in Web application traffic without manual extraction. Recurrent neural network (RNN) is a commonly used deep learning model, especially suitable for analyzing data with time series characteristics. In Web application traffic analysis, the HTTP request sequence often has a certain time-dependent relationship, such as the consecutive operation behaviors of users. RNN can analyze the HTTP request sequence, capture the time-dependent relationship between requests, and thus better understand the user's behavior pattern. When detecting DDoS attacks, RNN can learn the request frequency and pattern of normal traffic. Under normal circumstances, the request frequency of Web applications is relatively stable, and the request pattern has a certain regularity. When a large number of abnormal requests appear, RNN can accurately identify this abnormal pattern and determine it as a DDoS attack. In addition, generative adversarial network (GAN) plays an important role in deep learning traffic analysis. GAN can generate simulated attack traffic data to expand the training dataset. By generating various types of attack traffic data, the deep learning model can be exposed to more attack scenarios during the training process, thereby enhancing the model's adaptability to various attack scenarios. For example, in an actual Web application firewall system, after training the deep learning model with the simulated attack traffic data generated by GAN, the detection accuracy of the model for new types of DDoS attacks is improved.

5. CONCLUSION

This research focuses on the Web application firewall system based on artificial intelligence technology, and elaborates in detail the system architecture, key technologies and the advantages of combining with traditional technologies. The research results show that artificial intelligence can effectively improve the detection accuracy, adaptability and flexibility of Web application firewalls, reduce operation and maintenance costs, and significantly enhance the security protection ability. Looking ahead, emerging technologies such as quantum machine learning and transfer learning will drive Web application firewalls towards higher intelligence and efficiency, but it is necessary to pay attention to the security risks brought by artificial intelligence itself and strengthen its combined application with technologies such as blockchain, which will provide new paths for building a more complete Web application security ecosystem.

REFERENCES

[1] Meng, L. (2023). Research on the Evaluation System of Green Cabling of Cables Based on Neural Network. Innovation & Technology Advances, 1(2), 25–31. https://doi.org/10.61187/ita.v1i2.37

[2] Junxi, Y., Wang, Z., & Chen, C. (2024). GCN-MF: A graph convolutional network based on matrix factorization for recommendation. Innovation & Technology Advances, 2(1), 14–26. https://doi.org/10.61187/ita.v2i1.30

[3] Gao, H., Zhao, W., Chen, W., Liu, J., Peng, W., & Zhou, S. (2026). Experimental study and geomechanical modelling of hard and soft rock masses including fault zones. Environmental Earth Sciences, 85(1), 7.

[4] Han, J., Zhong, P. & Sun, L. Dual-scale model collaborative reasoning with multi-feature fusion for robust AI-generated image detection. Multimedia Systems 32, 363 (2026). https://doi.org/10.1007/s00530-026-02425-4

[5] Ya, L. (2025). EDA Technology in Digital Circuit Design: A Study on Application Methodologies. International Journal of Advance in Applied Science Research, 4(12), 6-10.

[6] Sun, Lingxin. "Designing Inclusive Interfaces: Accessibility Challenges and Solutions in Digital Products." Proceedings of the 2025 International Conference on Artificial Intelligence and Sustainable Development. 2025.

[7] Zhang, X. (2026, March). A Hybrid LSTM-GARCH Model Integrating Volatility Factors from the US Financial Markets. In Proceedings of the 2026 International Conference on AI Decision-Making and Management (pp. 183-189).

[8] Ding, G. (2025). Development and Validation of a Multispectral Vision System for In-Situ Detection of Pesticide Residues on Agricultural Produce. International Journal of Advance in Applied Science Research, 4(8), 98-102.

[9] Luo, R. (2026). The Integration Analysis of Computer Application Technology and Information Management. International Journal of Advance in Applied Science Research, 5(2), 27-30.

[10] Shen, Zepeng, et al. "Research on Application of Whale Optimization Algorithm in Financial Payment Fraud Detection." 2025 4th International Conference on Artificial Intelligence, Internet and Digital Economy (ICAID). IEEE, 2025.

[11] Wang, J. (2026). Research on the Application of Computer Science and Technology in the Context of Big Data. International Journal of Advance in Applied Science Research, 5(1), 72-77.
[12] Ma, J. (2025). A Unified Framework for Congestion Diagnosis and Dynamic Mitigation in Complex Networks. International Journal of Advance in Applied Science Research, 4(11), 36-41.
[13] Jin, L. (2025). Optimization of Order Allocation Algorithms for Industrial Internet Platforms. International Journal of Advance in Applied Science Research, 4(12), 44-48.
[14] Zhou, Z. (2025, November). Digital precision distribution strategy for social media content on private domain platforms in the automotive industry: a collaborative filtering model based on user behavior. In Proceedings of the 2025 International Conference on Digital Society and Intelligent Computing (pp. 516-521).
[15] YUAN, Mengwei, et al. TA-Mem: Tool-Augmented Autonomous Memory Retrieval for LLM in Long-Term Conversational QA. In: 2026 9th International Conference on Advanced Algorithms and Control Engineering (ICAACE). IEEE, 2026. p. 2684-2688.
[16] Li, G., Yuan, H., Chen, S., Hu, Q., Wang, J., & Jiang, K. (2026). MFT: Memory-Aware Fine-Tuning of SAM2 for Efficient Long-Sequence Video Object Segmentation. IEEE Signal Processing Letters.
[17] Shan, X., Xu, Y., Xia, T., & Lin, Y. S. (2025, October). Rethinking Wine Tasting for Chinese Consumers: A Service Design Approach Enhanced by Multimodal Personalization. In 2025 International Conference on Content-Based Multimedia Indexing (CBMI) (pp. 1-5). IEEE.
[18] Liu, Y. (2025). The Deep Learning Paradigm for Plant Image Classification: A Systematic Evaluation of Architectural Efficacy. International Journal of Advance in Applied Science Research, 4(8), 73-79.
[19] Miao, J. (2026). Big Data Technologies for Enhanced Network Security Analysis: Applications and Approaches. International Journal of Advance in Applied Science Research, 5(4), 16-20.
[20] Wang, J. (2025). Multi-Scale Feature-Enhanced YOLOv8 for Object Detection in Photovoltaic Farm Panoramic Imagery. International Journal of Advance in Applied Science Research, 4(10), 7-11.
[21] Liu, X. (2025). Research on the Application of GPU Parallel Computing in Image Processing. International Journal of Advance in Applied Science Research, 4(2), 1-7.
[22] Lu, J., Chen, J., Chen, Z., Zhang, L., & Fang, J. (2025). Flame Detection Based on Faster R-CNN Model. International Journal of Advance in Applied Science Research, 4(7), 41-45.
[23] Peng, Qucheng, et al. "RAIN: regularization on input and network for black-box domain adaptation." Proceedings of the Thirty-Second International Joint Conference on Artificial Intelligence. 2023.
[24] Peng, Qucheng, Ce Zheng, and Chen Chen. "A Dual-Augmentor Framework for Domain Generalization in 3D Human Pose Estimation." Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2024.

Author Profile

Zhou Yan (1984 -), female, from Shaoyang, Hunan, engineer, master, research direction: applied security.