International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

# Recent Advances in Web Application Firewall Detection: A Comparative Survey of Signature-Based, Machine Learning-Based, and Hybrid Techniques

**Pranav Kaluram Shinde**
Department of Computer Engineering
JSPM's JSCOE, Pune

**Yash Ranjit Ingole**
Department of Computer Engineering
JSPM's JSCOE, Pune

**Neha Pintu Tikore**
Department of Computer Engineering
JSPM's JSCOE, Pune

**Gaurav Sanjay Gosavi**
Department of Computer Engineering
JSPM's JSCOE, Pune

**Dr. S.B. Chaudhari**
Department of Computer Engineering
JSPM's JSCOE, Pune

***Abstract*** **- The rapid growth of web applications has significantly increased the attack surface for cyber threats such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), server-side request forgery (SSRF), command injection, and other sophisticated web-based attacks. Web Application Firewalls (WAFs) have emerged as a critical security mechanism for protecting web applications by monitoring, filtering, and blocking malicious HTTP and HTTPS traffic. Traditional WAF solutions primarily rely on signature-based detection techniques that provide efficient protection against known attack patterns; however, their effectiveness is limited when dealing with zero-day exploits, polymorphic attacks, and obfuscated payloads. To address these limitations, machine learning-based approaches have been introduced to identify anomalous behaviors and previously unseen attack vectors through data-driven analysis. More recently, hybrid detection frameworks combining signature-based rules with machine learning and artificial intelligence techniques have gained considerable attention due to their ability to balance detection accuracy, adaptability, and computational efficiency.**

**This survey presents a comprehensive review of recent advances in Web Application Firewall detection techniques, focusing on signature-based, machine learning-based, and hybrid approaches. The study analyzes the working principles, strengths, limitations, and performance characteristics of each category while examining their effectiveness against modern web application threats. Furthermore, a comparative analysis is conducted to highlight key differences in detection capability, false-positive rates, scalability, and deployment complexity. The survey also identifies current research challenges, including encrypted traffic inspection, adversarial attacks against machine learning models, explainable security mechanisms, and real-time adaptive detection. Finally, emerging research directions and future opportunities for intelligent WAF architectures are discussed to support the development of next-generation web application security solutions.**

***Keywords - Web Application Firewall (WAF), Cybersecurity, Signature-Based Detection, Machine Learning, Hybrid Security Systems, Anomaly Detection, Web Application Security, Intrusion Detection, Artificial Intelligence, Threat Detection.***

## I.INTRODUCTION

The rapid growth of web applications has transformed the way organizations deliver services, conduct business transactions, and communicate with users. Applications such as online banking systems, e-commerce platforms, healthcare portals, educational systems, and cloud-based services have become essential components of modern digital infrastructure. However, this increasing dependence on web technologies has also expanded the attack surface available to cybercriminals, making web applications one of the most attractive targets for security attacks [5].

According to the OWASP Top 10 report, web applications frequently face threats such as SQL Injection (SQLi), Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Remote Code Execution (RCE), and Server-Side Request Forgery (SSRF) [5]. These attacks can result in data breaches, unauthorized access, financial losses, and service disruptions. As cyberattacks continue to evolve in complexity and sophistication, traditional security mechanisms alone are often insufficient to provide comprehensive protection.

To address these security concerns, Web Application Firewalls (WAFs) have emerged as an important layer of defense. A WAF acts as an intermediary between users and web servers, monitoring incoming HTTP and HTTPS requests to identify and block malicious traffic before it reaches the target application [18]. By analyzing request headers, URLs, cookies, parameters, and payloads, WAFs help organizations mitigate a wide range of web-based attacks while maintaining service availability.

Traditional WAF solutions primarily rely on signature-based detection techniques. These approaches compare incoming requests against predefined rules and known attack patterns to identify malicious activity. Signature-based detection provides fast response times and low computational overhead, making it effective for

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

detecting well-known threats [18]. However, such systems are highly dependent on continuously updated rule sets and often struggle to detect zero-day attacks, obfuscated payloads, and previously unseen attack vectors [10].

To overcome these limitations, researchers have increasingly explored machine learning-based approaches for web attack detection. Early studies demonstrated that learning-based systems could identify abnormal traffic patterns and detect attacks that were difficult to capture using static signatures [1], [2]. Machine learning algorithms such as Decision Trees, Support Vector Machines (SVM), K-Nearest Neighbors (KNN), Random Forests, and Artificial Neural Networks have been widely applied to classify web requests as legitimate or malicious [11], [15]. Among these techniques, Random Forest models have gained significant attention due to their high accuracy, robustness, and ability to handle complex feature sets.

Recent advancements in artificial intelligence and deep learning have further enhanced the capabilities of Web Application Firewalls. Deep learning architectures, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have shown promising results in automatically learning attack patterns from large-scale datasets without extensive manual feature engineering [6], [9]. These approaches improve the detection of sophisticated and previously unseen threats but often require significant computational resources and large volumes of labeled training data.

In response to the strengths and weaknesses of individual detection methods, researchers have proposed hybrid WAF architectures that combine signature-based detection with machine learning and anomaly detection mechanisms. Hybrid approaches aim to leverage the efficiency of traditional rule-based systems while benefiting from the adaptability and intelligence of machine learning models [16], [17]. Several studies have reported improved detection accuracy, reduced false-positive rates, and enhanced resilience against modern attack techniques through the adoption of hybrid frameworks [19].

Despite considerable progress in Web Application Firewall technologies, several challenges remain unresolved. Issues such as encrypted traffic inspection, adversarial machine learning attacks, model interpretability, dataset limitations, and protection of cloud-native applications continue to impact the effectiveness of existing solutions [7], [8], [19]. Furthermore, the increasing adoption of APIs, microservices, and containerized environments has introduced new security requirements that are not fully addressed by many current WAF implementations.

Motivated by these challenges, this survey presents a comprehensive review of recent advances in Web Application Firewall detection techniques. The paper focuses on three major categories: signature-based, machine learning-based, and hybrid detection approaches. A comparative analysis is conducted to evaluate their strengths, limitations, and applicability in modern web security environments. Additionally, current research gaps and future directions are discussed to provide insights into the development of next-generation intelligent Web Application Firewall systems.

.

## II. LITERATURE SURVEY

The development of Web Application Firewalls (WAFs) has evolved significantly over the years in response to the growing number of web-based attacks. Researchers have proposed various techniques ranging from traditional signature-based detection systems to advanced machine learning and hybrid frameworks. This section reviews the major contributions reported in the literature and categorizes them based on their detection methodologies.

### A. Signature-Based Detection Approaches

Signature-based detection is one of the earliest and most widely adopted techniques in Web Application Firewalls. These systems identify malicious requests by comparing incoming traffic against predefined attack signatures and security rules. Due to their simplicity and efficiency, signature-based approaches continue to be extensively used in commercial and open-source WAF solutions.

Valeur et al. [1] introduced one of the early approaches for detecting web application attacks through the analysis of HTTP request characteristics. Their work demonstrated the effectiveness of identifying malicious patterns in web traffic and highlighted the importance of request inspection in web security systems. Similarly, Robertson et al. [2] proposed an anomaly characterization technique that complemented traditional rule-based mechanisms for web attack detection.

ModSecurity has emerged as one of the most widely used open-source Web Application Firewalls. Trustwave SpiderLabs [18] demonstrated how predefined security rules can effectively mitigate common web threats such as SQL Injection (SQLi), Cross-Site Scripting (XSS), and Directory Traversal attacks. The primary advantage of signature-based detection lies in its fast execution and low computational overhead. However, these systems require continuous rule updates and often struggle to detect zero-day attacks and obfuscated payloads [10].

Although signature-based WAFs remain effective against known threats, researchers have identified limitations related to adaptability and evolving attack patterns. As a result, alternative detection mechanisms have been explored to address these shortcomings.

### B. Machine Learning-Based Detection Approaches

The increasing sophistication of cyberattacks has encouraged researchers to investigate machine learning techniques for web application security. Unlike traditional rule-based systems, machine learning models learn patterns from historical traffic data and can identify previously unseen attack behaviors.

Several classification algorithms, including Decision Trees, Support Vector Machines (SVM), K-Nearest Neighbors (KNN), Random Forests, and Naïve Bayes, have been applied to web attack detection. Almseidin et al. [15] evaluated multiple machine learning algorithms for intrusion detection and demonstrated their effectiveness in distinguishing malicious traffic from legitimate requests.

Shaheed et al. [11] proposed a machine learning-based WAF that utilized feature engineering techniques to analyze HTTP requests. Their study showed that machine learning models could significantly improve attack detection performance compared to traditional rule-based systems. The research highlighted the importance of selecting relevant features such as request length, special character frequency, URL structure, and payload characteristics for accurate classification.

Recent studies have further explored deep learning architectures for web attack detection. Berman et al. [9] presented a comprehensive survey of deep learning applications in cybersecurity, demonstrating the ability of neural networks to automatically learn complex attack patterns. Similarly, LeCun et al. [6] emphasized the effectiveness of deep learning models in handling large-scale security datasets and extracting meaningful representations from raw data.

Despite their advantages, machine learning-based WAFs face several challenges, including dependency on high-quality datasets, computational overhead, feature selection complexity, and false-positive generation [8]. Furthermore, model interpretability remains a concern in practical deployment environments.

### C. Hybrid Detection Approaches

To overcome the limitations of individual detection techniques, researchers have increasingly focused on hybrid WAF architectures that combine signature-based detection with machine learning and anomaly detection mechanisms.

Applebaum et al. [10] highlighted the complementary strengths of signature-based and machine learning-based approaches, suggesting that integrating both techniques could improve overall detection performance. Their survey demonstrated that hybrid systems are capable of identifying both known and previously unseen attacks while maintaining acceptable operational efficiency.

Vitor et al. [16] introduced a machine learning-assisted virtual patching framework that enhanced traditional web protection

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

mechanisms through intelligent traffic analysis. The proposed approach demonstrated how machine learning could be integrated into existing security infrastructures without replacing established rule-based systems.

More recently, Choudhary and Kesswani [17] proposed ModSec-Learn, a framework that combines ModSecurity rules with machine learning classification models. Experimental results showed improvements in detection accuracy and reductions in false-positive rates compared to standalone signature-based systems. Similarly, Rigaki and Garcia [19] investigated adversarial machine learning attacks against WAFs and emphasized the importance of developing robust hybrid architectures capable of resisting evasion attempts.

The literature indicates that hybrid detection frameworks represent one of the most promising directions for modern Web Application Firewall development. By combining the speed of signature-based detection with the adaptability of machine learning techniques, hybrid systems provide a balanced approach to protecting web applications against both known and emerging cyber threats.

Based on the reviewed studies, it is evident that each detection technique offers unique advantages and limitations. Signature-based approaches remain effective for known attack patterns, machine learning techniques improve adaptability and zero-day attack detection, while hybrid frameworks attempt to combine the strengths of both methodologies. These observations motivate the comparative analysis presented in the following section.

## III.COMPARATIVE ANALYSIS

Web Application Firewall (WAF) technologies have evolved from traditional rule-based systems to intelligent machine learning and hybrid security frameworks. Each detection technique offers unique advantages and limitations in terms of attack detection capability, computational complexity, adaptability, and deployment requirements. Signature-based approaches are highly effective against known threats but struggle with zero-day attacks. Machine learning-based systems improve adaptability and anomaly detection but require quality datasets and computational resources. Hybrid approaches attempt to combine the strengths of both methods to achieve better detection performance while minimizing false positives.

To better understand the characteristics of each detection methodology, Table I presents a comparative analysis of representative studies discussed in the literature.

**Table I. Comparative Analysis of Existing WAF Detection Techniques**

| Ref. | Author(s) | Year | Detection Technique | Key Contribution | Advantages | Limitations |
|---|---|---|---|---|---|---|
| [1] | Valeur et al. | 2005 | Learning-Based Detection | Early web attack detection using HTTP request analysis | Detects anomalous behavior | Higher false positives |
| [2] | Robertson et al. | 2006 | Anomaly-Based Detection | Behavioral profiling for web attack detection | Can detect unknown attacks | Complex profile generation |
| [10] | Appleabum et al. | 2023 | Survey of Signature and ML WAFs | Comparative study of WAF technologies | Comprehensive analysis | Limited experimental validation |
| [11] | Shaheed et al. | 2022 | Machine Learning-Based WAF | Feature engineering for web attack classification | High detection accuracy | Dataset dependency |
| [15] | Almseidin et al. | 2017 | Machine Learning Classification | Evaluation of multiple ML algorithms | Good classification performance | Requires extensive training |
| [9] | Berman et al. | 2019 | Deep Learning Security Models | Survey of deep learning in cybersecurity | Learns complex attack patterns | High computational cost |
| [16] | Vitor et al. | 2018 | ML-Assisted Virtual Patching | Integration of ML with web protection mechanisms | Improved adaptability | Increased implementation complexity |
| [17] | Choudhary and Kesswani | 2024 | Hybrid WAF Framework | Combines ModSecurity and ML models | Reduced false positives | Requires continuous optimization |
| [19] | Rigaki and Garcia | 2020 | Adversarial ML Analysis | Evaluation of WAF evasion techniques | Highlights security weaknesses | Focused on attack scenarios |
| [18] | Trustwave SpiderLabs | 2012 | Signature-Based WAF | ModSecurity rule-based protection | Fast and efficient detection | Ineffective against zero-day attacks |

The comparison demonstrates that no single detection technique is capable of addressing all web security challenges. Signature-based systems remain effective for identifying known attack patterns with minimal computational overhead, whereas machine learning-based approaches offer improved adaptability and enhanced detection of previously unseen threats. Hybrid frameworks provide a balanced solution by integrating rule-based and intelligent detection mechanisms, making them one of the most promising directions for next-generation Web Application Firewall development. As web attacks continue to evolve, future WAF solutions are expected to incorporate adaptive learning, threat intelligence integration, and explainable artificial intelligence to improve both security effectiveness and operational transparency.

## IV. RESEARCH GAPS AND LIMITATIONS

Although significant progress has been made in the development of Web Application Firewall (WAF) technologies, several challenges continue to limit their effectiveness against modern web-based threats. The literature reviewed in this survey highlights a number of technical, operational, and research-related issues that remain unresolved. These gaps provide opportunities for future improvements in intelligent web application security systems.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

### A. Limitations of Signature-Based Detection

Traditional signature-based WAFs remain highly effective for detecting known attack patterns. However, their performance depends heavily on predefined rules and continuously updated signature databases. As cyberattacks evolve rapidly, maintaining comprehensive and up-to-date rule sets becomes increasingly difficult. Furthermore, signature-based systems are generally ineffective against zero-day attacks, polymorphic malware, and heavily obfuscated payloads that do not match existing attack signatures.

Another challenge is the increasing use of encoding and evasion techniques by attackers. Simple modifications to malicious payloads may allow attackers to bypass static detection rules, reducing the overall effectiveness of traditional WAF deployments.

### B. Challenges in Machine Learning-Based Detection

Machine learning has significantly improved the ability of WAFs to detect unknown attacks and abnormal traffic behavior. However, the success of machine learning models depends largely on the availability of high-quality datasets. Many existing studies rely on limited or outdated datasets that may not accurately represent real-world web traffic patterns.

In addition, machine learning models often require extensive feature engineering, parameter tuning, and periodic retraining. Poor feature selection or imbalanced datasets can negatively affect detection accuracy and increase false-positive rates. These challenges become more significant when deploying machine learning models in large-scale production environments.

Another important concern is model interpretability. Security administrators often need clear explanations regarding why a request has been classified as malicious. Many advanced machine learning and deep learning models operate as black-box systems, making security decisions difficult to interpret and verify.

### C. Limitations of Hybrid Detection Frameworks

Hybrid WAF architectures combine signature-based and machine learning-based techniques to improve detection performance. While these systems generally achieve higher accuracy and better adaptability, they introduce additional complexity in implementation and maintenance.

Integrating multiple detection mechanisms requires efficient coordination between rule-based engines, anomaly detection modules, and machine learning classifiers. As the number of security layers increases, computational overhead and deployment complexity also increase. Maintaining consistency among different detection components remains a significant challenge for hybrid frameworks.

Furthermore, many proposed hybrid systems have been evaluated in controlled laboratory environments rather than real-world production scenarios. As a result, their practical scalability and long-term operational performance remain insufficiently explored.

### D. Emerging Security Challenges

Modern web applications increasingly rely on cloud computing, microservices, APIs, containerized environments, and WebSocket communications. Many existing WAF solutions were originally designed for traditional web applications and may not provide adequate protection for these emerging architectures.

The widespread adoption of HTTPS encryption introduces additional challenges for traffic inspection and attack detection. Although encryption improves privacy and security, it also limits the visibility of network traffic, making malicious payload identification more difficult.

Additionally, recent studies have demonstrated that machine learning models can be vulnerable to adversarial attacks. Carefully crafted inputs may manipulate classification decisions and enable malicious requests to bypass security mechanisms. Research in adversarially robust WAF systems is still in its early stages and requires further investigation.

### E. Research Opportunities

Based on the identified limitations, several promising research directions can be explored. These include the development of explainable artificial intelligence (XAI) techniques for security decision-making, creation of realistic and publicly available web attack datasets, implementation of lightweight detection models for real-time environments, and the design of adaptive hybrid architectures capable of responding to evolving attack patterns.

Moreover, the integration of threat intelligence feeds, federated learning, automated rule generation, and large language model (LLM)-assisted security analysis represents a promising avenue for next-generation Web Application Firewall development. Addressing these challenges will contribute to the creation of more intelligent, scalable, and resilient web application security solutions.

## V. PROPOSED RESEARCH DIRECTION

The analysis of existing Web Application Firewall (WAF) technologies reveals that although considerable progress has been made in web attack detection, several challenges continue to affect their effectiveness in modern cybersecurity environments. Based on the research gaps identified in the previous section, a number of promising research directions can be explored to enhance the performance, adaptability, and reliability of future WAF systems.

### A. Explainable Artificial Intelligence for WAFs

One of the major challenges associated with machine learning-based security systems is the lack of transparency in decision-making. Many existing models operate as black-box systems and provide limited information regarding the reasons behind attack classification. Future research should focus on the integration of Explainable Artificial Intelligence (XAI) techniques that can generate interpretable and human-understandable security decisions. Such approaches would assist security analysts in understanding attack behavior, validating detection results, and improving trust in automated security mechanisms.

### B. Adaptive and Self-Learning Detection Systems

Traditional WAFs require frequent rule updates, while machine learning models often need periodic retraining to maintain detection performance. Future research should investigate adaptive and self-learning WAF architectures capable of continuously learning from new traffic patterns and emerging threats. Such systems could automatically adjust detection strategies based on real-time observations, reducing administrative effort and improving protection against evolving cyberattacks.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

### C. Robustness Against Adversarial Attacks

Recent studies have shown that machine learning models can be manipulated through adversarial inputs specifically designed to bypass detection mechanisms. Developing adversarially robust WAF frameworks remains an important research challenge. Future work should focus on adversarial training techniques, secure feature extraction methods, and resilient classification models that can maintain detection accuracy even when attackers attempt to evade security controls.

### D. Security for Modern Web Architectures

The increasing adoption of cloud-native applications, microservices, APIs, containerized environments, and WebSocket communications has introduced new attack surfaces that are not adequately addressed by many existing WAF solutions. Future research should focus on developing specialized security mechanisms for these emerging technologies. In particular, API security, microservice traffic analysis, and container-aware threat detection are expected to become critical areas of investigation in next-generation WAF development.

### E. Integration of Artificial Intelligence and Threat Intelligence

Artificial Intelligence (AI) and cyber threat intelligence have the potential to significantly enhance web application security. Future WAF systems may incorporate threat intelligence feeds, automated attack correlation, and intelligent rule generation to improve detection capabilities. The integration of Large Language Models (LLMs) can further support automated security analysis, attack interpretation, and policy generation. Such intelligent systems could provide faster responses to emerging threats while reducing the workload of security administrators.

### F. Development of Standardized Datasets and Evaluation Frameworks

Another important research direction involves the creation of realistic and publicly available datasets for training and evaluating WAF detection models. Many current studies rely on limited datasets that may not accurately represent real-world attack scenarios. Standardized datasets and benchmarking frameworks would enable fair comparison among different detection techniques and facilitate reproducible research in the field of web application security.

Overall, future Web Application Firewall technologies are expected to evolve toward intelligent, adaptive, and autonomous security platforms that combine traditional protection mechanisms with machine learning, artificial intelligence, threat intelligence, and real-time behavioral analysis. Addressing these research directions will contribute to the development of more accurate, scalable, and resilient solutions for protecting modern web applications against increasingly sophisticated cyber threats.

## VI. CONCLUSION

Web applications have become an essential component of modern digital infrastructure, supporting critical services across sectors such as finance, healthcare, education, e-commerce, and government. As the number and complexity of web-based cyberattacks continue to increase, the need for effective Web Application Firewall (WAF) solutions has become more important than ever. Over the years, WAF technologies have evolved from traditional signature-based systems to intelligent machine learning and hybrid detection frameworks capable of addressing increasingly sophisticated attack techniques.

This survey presented a comprehensive review of recent advances in Web Application Firewall detection techniques, focusing on signature-based, machine learning-based, and hybrid approaches. Signature-based WAFs remain effective for detecting known attack patterns with low computational overhead and fast response times. However, their dependence on predefined rules limits their ability to identify zero-day attacks and evolving threats. Machine learning-based approaches have demonstrated significant improvements in detecting anomalous behaviors and previously unseen attacks by learning patterns from web traffic data. Despite their advantages, these methods face challenges related to dataset quality, feature engineering, model interpretability, and false-positive generation.

Hybrid detection techniques have emerged as a promising solution by combining the strengths of signature-based and machine learning-based approaches. These systems provide improved detection accuracy, enhanced adaptability, and better resistance against modern attack strategies while maintaining practical deployment capabilities. Nevertheless, challenges such as encrypted traffic inspection, adversarial machine learning attacks, scalability, and protection of cloud-native applications continue to present significant research opportunities.

Based on the comparative analysis conducted in this survey, hybrid WAF architectures appear to offer the most balanced approach for modern web application security. Future research should focus on explainable artificial intelligence, adversarially robust machine learning models, intelligent threat intelligence integration, and adaptive security mechanisms capable of responding to rapidly evolving cyber threats. The continued advancement of these technologies will play a crucial role in developing next-generation Web Application Firewall solutions that are more accurate, scalable, and resilient in protecting web applications against emerging security challenges.

## VII. REFERENCES

[1] F. Valeur, D. Mutz, and G. Vigna, “A Learning-Based Approach to the Detection of Web Application Attacks,” in *Proceedings of the Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, Vienna, Austria, pp. 251–272, 2005. [Online]. Available: https://link.springer.com/chapter/10.1007/11506881_13

[2] W. Robertson, G. Vigna, C. Kruegel, and R. A. Kemmerer, “Using Generalization and Characterization Techniques in the Anomaly-Based Detection of Web Attacks,” in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2006. [Online]. Available: https://www.ndss-symposium.org

[3] M. Roesch, “Snort: Lightweight Intrusion Detection for Networks,” in *Proceedings of the 13th USENIX Conference on System Administration (LISA)*, pp. 229–238, 1999. [Online]. Available: https://www.usenix.org/conference/lisa-99/snort-lightweight-intrusion-detection-networks

[4] N. Provos and T. Holz, *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*. Addison-Wesley Professional, 2007. [Online]. Available: https://www.pearson.com/en-us/subject-catalog/p/virtual-honeypots/P200000003191

[5] OWASP Foundation, “OWASP Top 10: The Ten Most Critical Web Application Security Risks,” 2021. [Online]. Available: https://owasp.org/www-project-top-ten/

[6] Y. LeCun, Y. Bengio, and G. Hinton, “Deep Learning,” *Nature*, vol. 521, no. 7553, pp. 436–444, 2015. [Online]. Available: https://www.nature.com/articles/nature14539

[7] I. Goodfellow, J. Shlens, and C. Szegedy, “Explaining and Harnessing Adversarial Examples,” in *International Conference on Learning Representations (ICLR)*, 2015. [Online]. Available: https://arxiv.org/abs/1412.6572

[8] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges,” *Cybersecurity*, vol. 2, no. 20, 2019. [Online]. Available: https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7

[9] D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, “A Survey of Deep Learning Methods for Cyber Security,” *Information*, vol. 10, no. 4, p. 122, 2019. [Online]. Available: https://www.mdpi.com/2078-2489/10/4/122

[10] A. Applebaum, M. Grossman, and N. Waisbrot, “Signature-Based and Machine-Learning-Based Web Application Firewalls: A Short Survey,” *Journal of Cybersecurity and Privacy*, vol. 3, no. 2, pp. 145–162, 2023. [Online]. Available: https://www.mdpi.com/journal/jcp

[11] A. Shaheed, M. B. B. Sharif, and A. A. Abdullah, “Web Application Firewall Using Machine Learning and Feature Engineering,” *Security*

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

*and Communication Networks*, vol. 2022, Article ID 5280158, 2022. [Online]. Available: https://www.hindawi.com/journals/scn/2022/5280158/

[12] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Dataset," in *IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 2009. [Online]. Available: https://ieeexplore.ieee.org/document/5356528

[13] G. Creech and J. Hu, "Generation of a New IDS Test Dataset: UNSW-NB15," in *Military Communications and Information Systems Conference (MilCIS)*, 2013. [Online]. Available: https://research.unsw.edu.au/projects/unsw-nb15-dataset

[14] J. Kim, H. Kim, and J. Kim, "An Intelligent Web Application Firewall Using Deep Learning," *IEEE Access*, 2020. [Online]. Available: https://ieeexplore.ieee.org

[15] M. Almseidin, M. Alzubi, S. Kovacs, and M. Alkasassbeh, "Evaluation of Machine Learning Algorithms for Intrusion Detection Systems," in *IEEE Symposium Series on Computational Intelligence*, 2017. [Online]. Available: https://ieeexplore.ieee.org/document/8285334

[16] P. M. B. Vitor, R. de Oliveira, and M. Correia, "Machine Learning-Assisted Virtual Patching of Web Applications," arXiv preprint, 2018. [Online]. Available: https://arxiv.org/abs/1803.05529

[17] A. Choudhary and S. Kesswani, "ModSec-Learn: Enhancing ModSecurity with Machine Learning for Web Attack Detection," arXiv preprint, 2024. [Online]. Available: https://arxiv.org/abs/2406.13547

[18] Trustwave SpiderLabs, *ModSecurity Handbook: The Complete Guide to the Popular Open Source Web Application Firewall*. Feisty Duck, 2012. [Online]. Available: https://www.feistyduck.com/books/modsecurity-handbook/

[19] M. M. Rigaki and S. Garcia, "WAF-A-MoLE: Evading Web Application Firewalls Through Adversarial Machine Learning," arXiv preprint, 2020. [Online]. Available: https://arxiv.org/abs/2001.01952

[20] M. Grossi, N. Ibrahim, V. Radescu, R. Loredo, K. Voigt, C. Von Altrock, and A. Rudnik, "Mixed Quantum–Classical Method for Fraud Detection With Quantum Feature Selection," *IEEE Transactions on Quantum Engineering*, vol. 3, pp. 1–12, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9915517