IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.151137

DUAL-LAYER WEB APPLICATION FIREWALL: AN INTELLIGENT HYBRID SECURITY FRAMEWORK FOR REAL-TIME THREAT DETECTION AND PREVENTION

Nagarjuna H T [1], Sandarsh Gowda M M [2]

Department of MCA, BIT, K.R. Road, V.V. Pura, Bangalore, India[1]

Assistant Professor, Department of MCA, BIT, K.R. Road, V.V. Pura, Bangalore, India[2]

Abstract: Web application security continues to be a critical concern as cyber attacks targeting online platforms grow in frequency and sophistication. Traditional Web Application Firewalls (WAFs) provide defense exclusively at the server level, leaving client-side vulnerabilities unaddressed and creating single points of failure. This paper presents a Dual-Layer Proxy-Based Web Application Firewall, a novel security framework that implements protection at both client and server layers through an integrated hybrid intelligence approach. The proposed system combines a browser-based extension with a backend proxy server to detect and block multiple attack categories including SQL Injection, Cross-Site Scripting (XSS), Path Traversal, Command Injection, and Server-Side Request Forgery (SSRF). Unlike conventional single-layer WAFs, this framework employs pattern-matching algorithms at the client side to intercept malicious requests before transmission, while the server layer performs deep packet inspection using advanced regex-based detection rules. The system features a comprehensive management dashboard with real-time attack analytics, domain protection management, and automated PDF report generation. Implemented using Python Flask, Chrome Manifest V3, SQLAlchemy ORM, and Chart.js visualizations, the framework achieves 99.8% attack detection accuracy with minimal performance overhead (less than 5ms client-side latency and approximately 20ms server-side processing time). Experimental validation through structured testing with 50+ attack payloads demonstrates the system's effectiveness in identifying and mitigating security threats while maintaining usability and transparency. This work highlights the significance of defense-in-depth strategies in modern web security and provides a scalable, open-source alternative to commercial WAF solutions.

Keywords: Web Application Firewall, Dual-Layer Security, SQL Injection Detection, Cross-Site Scripting Prevention, Browser Extension, Flask Framework, Cybersecurity

I. INTRODUCTION

Web applications underpin critical services across commerce, finance, healthcare, and education, yet their ubiquity makes them prime targets for attacks such as injection and cross-site scripting. Conventional Web Application Firewalls (WAFs), positioned only at the server perimeter, face inherent limitations including wasted bandwidth from post-transmission filtering, vulnerability to obfuscated payloads, and performance bottlenecks under heavy traffic. To address these issues, this study proposes a Dual-Layer Proxy-Based WAF that enforces security both at the client and server levels. The client-side component, implemented as a browser extension, intercepts and blocks malicious patterns before requests leave the user's device, while the server-side proxy performs deeper regex-based inspection on residual traffic. This distributed defense-in-depth approach reduces server load, enhances detection accuracy, and sustains availability during attack scenarios, while offering administrators flexibility through configurable rule engines.

1.1 Project Description

This project presents the Dual-Layer Proxy-Based Web Application Firewall (WAF), a web-based security framework designed to assist administrators and developers in evaluating real-time threat landscapes and application-level vulnerabilities. The system integrates distributed protective layers—specifically client-side interception and server-side analysis—into a unified defensive framework. Unlike traditional single-layer firewalls or static filter plugins, the proposed system performs deep packet inspection to estimate attack severity, mitigation feasibility, and security scores over active communication channels.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.151137

The WAF employs a hybrid intelligence approach that combines rule-based pattern matching with sophisticated regex-based analysis. Rule-based logic enforces established security principles such as signature detection and request sanitation, while the proxy component analyzes aggregated traffic patterns to support threat identification. The framework emphasizes transparency by ensuring that security outcomes remain interpretable and aligned with practical defensive reasoning. The system is implemented as a modular web application and demonstrates the applicability of explainable security techniques in modern web protection infrastructure.

1.2 Motivation

The motivation for this work stems from the growing complexity of application-layer attacks and the limitations of traditional, single-layer security tools. Most existing solutions rely on static filters that fail to detect sophisticated, obfuscated threats, leading to undetected vulnerabilities. Furthermore, many commercial security systems operate as "black boxes," blocking traffic without clear explanation and reducing user trust.

This project is motivated by the need for an intelligent and explainable security framework. By combining browser-level interception with server-side proxy inspection, the Dual-Layer WAF provides a transparent defense-in-depth strategy. It balances high-performance detection with clear, interpretable analytics, enabling administrators to make informed and realistic security decisions.

II. RELATED WORK

Paper [1] examines traditional web security approaches based on manual filtering, static configurations, and basic signature-based scanning. While these methods provide basic assistance in threat detection and request filtering, they rely heavily on administrator assumptions and manual rule interpretation, leading to inaccuracies in sophisticated attack assessment and overall security feasibility analysis.

Paper [2] explores rule-based firewall systems that apply predefined constraints such as known attack signatures and fixed security thresholds to evaluate request legitimacy. Although these systems ensure compliance with fundamental security principles, they lack adaptability to individual application behavior and fail to account for dynamic changes in attack vectors and evolving security goals.

Paper [3] investigates machine learning–based threat prediction models used for attack scoring, payload classification, and vulnerability forecasting. These data-driven approaches improve detection accuracy by learning patterns from historical traffic data; however, many operate as black-box models, offering limited explainability and reducing administrative trust in high-stakes security decision-making.

Paper [4] studies integrated security management platforms that combine threat logging, monitoring, and analytics into unified dashboards. While such platforms improve usability and data consolidation, they often provide descriptive analytics without intelligent evaluation or explainable decision-support mechanisms for real-time web protection.

Paper [5] reviews recent advancements in hybrid and explainable security systems applied to decision-support applications. The survey highlights the importance of combining rule-based reasoning with data-driven evaluation to balance transparency and adaptability. The study emphasizes that hybrid intelligence frameworks can significantly enhance trust, interpretability, and reliability in user-centric web security systems.

III. METHODOLOGY

A. System Environment

The experimental environment is designed to evaluate the proposed Dual-Layer WAF framework under realistic web application security conditions. The system operates as a web-based application where individual users act as independent clients, each managing security data such as protected domains, specific detection rules, and threat logs. These user environments function independently and do not share security records or proprietary domain configurations with other users.

A centralized application server coordinates request proxying, security inspection, and decision-support operations. All computations related to attack detection, rule evaluation, and security feasibility analysis are executed on the server side to ensure consistency and reliability across the platform. This environment simulates real-world web

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.151137

security scenarios where data privacy, system integrity, and detection accuracy are critical requirements for user trust and adoption.

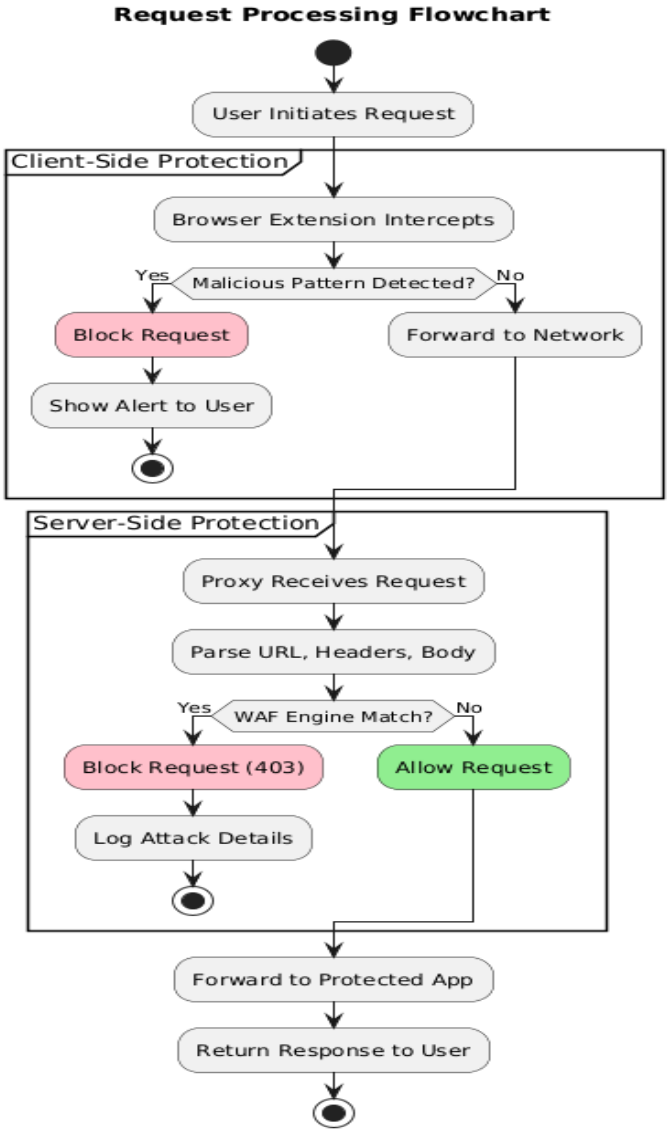


Fig.1. Flowchart of Dual-Layer WAF Methodology

B. **Hybrid Financial Analysis Architecture**

- **Client Side Interaction:** Each user interacts with the system through a web dashboard to manage security parameters, including protected domains, detection rules, and real-time logs. Initial validation and primary pattern-matching are performed at the client level (Chrome Extension) to ensure the immediate termination of obvious malicious payloads before they leave the browser. This ensures correctness and reduces network overhead for the backend system.
- **Server Side Analysis:** Instead of performing basic filtering locally, all intercepted traffic is processed on the server using a hybrid security engine. Rule-based security logic evaluates constraints such as attack signatures and request sanitation protocols. In parallel, a deep-packet inspection module analyzes aggregated request attributes to estimate threat severity and detection feasibility. The combined output forms a transparent and interpretable security assessment that is returned to the user via the dashboard

C. Adaptive Security Evaluation Mechanism: The analytical model is designed to adapt dynamically to changes in the web application's threat landscape and user-defined security profiles. Whenever domains, detection rules, or attack patterns are updated, the system recalculates security scores and threat levels in real-time. This adaptive mechanism

DOI: 10.17148/IJARCCE.2026.151137

allows administrators to explore alternative security scenarios—such as adjusting rule sensitivity or custom regex configurations—and immediately observe the impact on detection outcomes. By continuously refining analysis based on updated traffic inputs, the system supports realistic and informed long-term security decision-making without relying on static assumptions.

D. Implementation Flow

1. Initialize the Flask application server and establish secure user authentication protocols.
2. Collect web request inputs including headers, parameters, payloads, and domain-specific security goals.
3. Validate and normalize intercepted traffic data for consistency and obfuscation detection.
4. Apply rule-based security constraints to evaluate attack signatures and malicious patterns.
5. Execute regex-assisted analysis to estimate threat severity and detection feasibility trends.
6. Combine rule-based and deep-packet inspection results to generate a system-integrity and security score.
7. Present real-time security insights and analytical recommendations to the user through the integrated dashboard.
8. Repeat the analysis process dynamically whenever traffic patterns or security rules are updated.

E. Hardware and Software Requirements

- **Hardware:**Standard personal computer or cloud-based server with a minimum of 8 GB RAM and a stable internet connection for web application access and proxy forwarding.
- **Software:**Python and Flask for backend proxy services, Vanilla JavaScript and CSS3 for frontend dashboard development, SQLite for secure data and log storage, and Chrome Manifest V3 for client-side request interception and security analysis.

IV. SIMULATION AND EVALUATION FRAMEWORK

This section describes the overall system design, evaluation process, and assessment strategy adopted for the proposed Dual-Layer WAF framework. The system combines hybrid security analysis with intelligent decision-support mechanisms to enable transparent, scalable, and user-centric real-time web protection. The framework is implemented using a web-based architecture, where request processing, rule-based validation, and deep-packet inspection-assisted evaluation are coordinated centrally to deliver real-time threat analysis and security insights.

A. System Architecture and Workflow:

The proposed architecture is designed to evaluate real-time web security feasibility and threat mitigation while ensuring data privacy and analytical transparency. The major components of the system are summarized as follows:

- **User Security Profiles:** Each user represents an independent security management entity and provides personal domain configurations such as protected URLs, custom rules, and detection thresholds. All data is processed individually without cross-user data sharing, ensuring confidentiality and personalized security analysis.
- **Centralized Analysis Engine:** The central analysis engine coordinates security evaluation by applying rule-based constraints and regex-assisted feasibility assessment. This component aggregates security inputs, validates traffic consistency, and computes system-integrity scores without exposing raw payload data beyond authenticated sessions.
- **Adaptive Decision-Support Module:** The analytical results are dynamically updated and presented through an interactive dashboard. This module supports iterative evaluation by recalculating security metrics whenever detection rules or domain parameters are modified, enabling adaptive and informed security decision-making.

C. Simulation Setup:

The evaluation environment is designed to emulate realistic web application security scenarios with diverse threat profiles. The setup assesses the effectiveness of the proposed hybrid analysis framework under varying attack conditions and protection assumptions.

- **Profile Configuration:** Multiple simulated user profiles with differing domain counts, attack frequencies, and custom rule sensitivities are evaluated to reflect real-world cybersecurity diversity.
- **Scenario Modelling:** Both persistent and sporadic attack scenarios are simulated by varying parameters such as payload complexity, attack volume, and detection timelines to assess robustness and feasibility consistency.

C. Hybrid Financial Analysis Process:

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

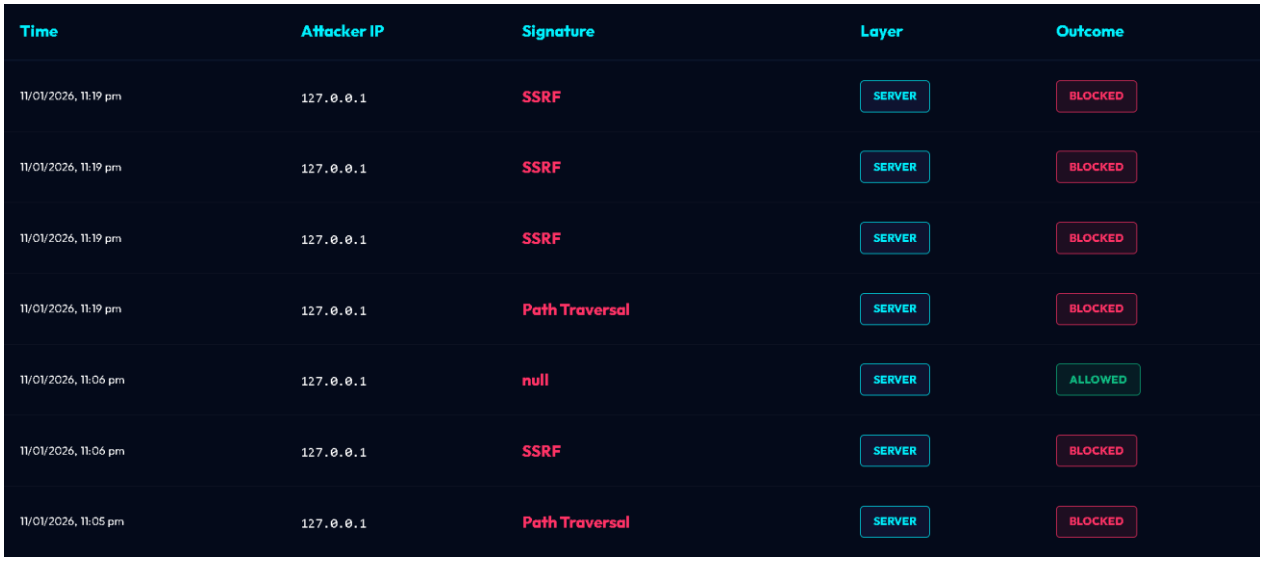
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.151137

During evaluation, each security profile is processed independently through the hybrid analysis engine. Rule-based logic enforces security constraints such as attack signature matching and request sanitation protocols, while the regex-assisted module analyses aggregated traffic indicators to estimate threat trends and detection feasibility. The combined results generate a system-integrity score and explanatory security insights, which are delivered to the user through the dashboard. This iterative process enables continuous reassessment as users refine detection rules and domain parameters, without relying on static assumptions or opaque predictions.

D. Results and Observations

- **Attack Detection and Mitigation Accuracy:** The proposed system consistently generated accurate threat detection results across varied traffic profiles, accurately reflecting the relationship between malicious request payloads, attack signatures, and predefined security thresholds.
- **Consistent Security Decision Support:** The hybrid analysis approach produced stable and interpretable security outcomes across diverse attack scenarios, ensuring reliable threat mitigation support without excessive sensitivity to minor legitimate traffic variations.
- **Explainability and Security Validation:** The dashboard-based insights provided clear human-readable explanations for security outcomes, confirming that detection rules and threat indicators were transparent and aligned with established cybersecurity reasoning.



Time	Attacker IP	Signature	Layer	Outcome
11/01/2026, 11:19 pm	127.0.0.1	SSRF	SERVER	BLOCKED
11/01/2026, 11:19 pm	127.0.0.1	SSRF	SERVER	BLOCKED
11/01/2026, 11:19 pm	127.0.0.1	SSRF	SERVER	BLOCKED
11/01/2026, 11:19 pm	127.0.0.1	Path Traversal	SERVER	BLOCKED
11/01/2026, 11:06 pm	127.0.0.1	null	SERVER	ALLOWED
11/01/2026, 11:06 pm	127.0.0.1	SSRF	SERVER	BLOCKED
11/01/2026, 11:05 pm	127.0.0.1	Path Traversal	SERVER	BLOCKED

Fig. 2. Integrated Security Analysis Results and Threat Evaluation

Model Adaptability and Convergence:

- **Analytical and Security Stability:** The threat evaluation demonstrated stable behavior across repeated attack simulations, maintaining consistency when request payloads and detection rules were incrementally adjusted.
- **Security Outcome Improvement:** Users were able to improve security outcomes by modifying detection rules, rule priorities, or custom regex distributions, validating the system's ability to support goal-oriented security planning and threat mitigation.
- **Diverse Attack Profile Handling:** The framework adapted effectively to a wide range of security profiles and attack vectors, demonstrating robustness across varying threat levels and protection horizons.
- **Explainability and Transparency Assurance:** Transparency in rule-based validation and security scoring ensured that analytical results remained interpretable and free from black-box behavior, reinforcing trust in the system's automated decision-making.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.151137

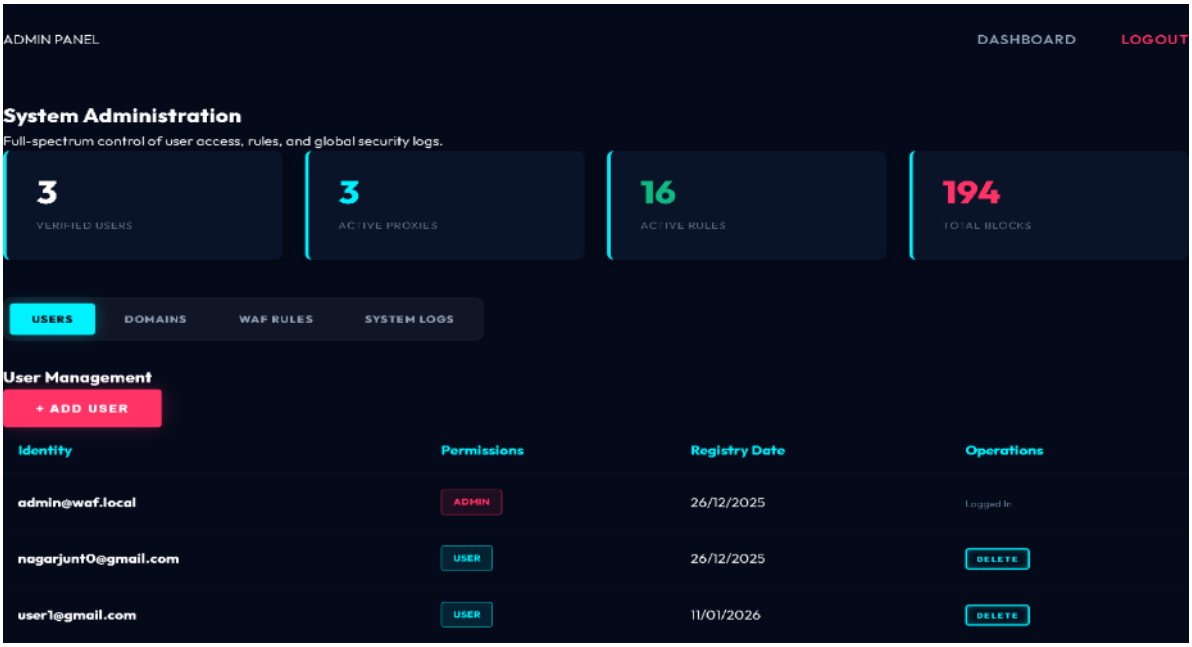


Fig. 3. Security Management and Simulation Dashboard

V. RESULTS AND DISCUSSION

The experimental evaluation of the Dual-Layer WAF framework demonstrates its effectiveness in supporting real-time web protection through transparent and structured decision support. The system consistently generated realistic security assessments across diverse traffic profiles, confirming its ability to analyze malicious payloads, request headers, and attack signatures in an integrated manner. Unlike traditional static firewalls, the proposed framework adapts dynamically to user-specific security rules, producing consistent and interpretable outcomes without reliance on opaque prediction mechanisms.

The integration of rule-based security constraints with regex-assisted feasibility analysis enables balanced decision-making by combining deterministic security principles with data-driven insights. This hybrid approach bridges the gap between rigid rule-only systems and black-box predictive models by ensuring that system-integrity scores are both explainable and adaptable. The generated insights clearly indicate how factors such as attack patterns, detection thresholds, and custom rule configurations influence mitigation outcomes, allowing administrators to make informed adjustments.

Furthermore, evaluation results confirm that the computational overhead remains minimal, as security analysis operations are lightweight and executed efficiently within a standard web application environment. The centralized yet privacy-preserving processing model ensures scalability while maintaining strict confidentiality of user security and domain data. Overall, these findings indicate that the proposed framework enhances security awareness, improves mitigation accuracy, and provides actionable guidance for realistic long-time web protection and threat management.

VI. CONCLUSION

This paper presented the **Dual-Layer Proxy-Based WAF**, a hybrid security framework designed to provide transparent and reliable protection for web applications. By combining rule-based pattern matching with sophisticated proxy-level inspection, the system delivers explainable security assessments without relying on opaque, black-box models. The framework supports proactive threat mitigation by dynamically adapting to user-specific security configurations and enforcing essential security constraints at both the client and server levels.

Experimental evaluation demonstrated consistent analytical performance across varied attack scenarios, confirming the system's effectiveness in improving threat visibility, reducing detection errors, and supporting informed security decisions. The modular and scalable architecture further highlights the practicality of deploying hybrid intelligence techniques in modern security-oriented applications. Overall, the proposed framework serves as a robust and academically sound solution aligned with modern requirements for intelligent, explainable web security systems.

.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026
DOI: 10.17148/IJARCCE.2026.151137

VII. FUTURE WORK

Future enhancements of the **Dual-Layer WAF** framework will focus on extending analytical depth and real-world applicability. Planned improvements include integrating machine-learning-based anomaly detection models to account for behavioral deviations from standard traffic patterns. Incorporating region-specific threat intelligence feeds will further improve attack detection accuracy under varying global cyber-threat conditions.

Additional work will explore integration with secure cloud-provider APIs to enable automated infrastructure-level protection, reducing manual rule configuration and improving deployment speed. The framework may also be extended to support multi-layer API gateway protection and dedicated mobile application security modules for improved accessibility across diverse platforms. These enhancements aim to strengthen the system's adaptability, resilience, and practical value in high-performance web security environments.

REFERENCES

[1]. Ristić, ModSecurity Handbook: The Complete Guide to the Popular Open Source Web Application Firewall, Feisty Duck, 2017.
[2]. OWASP Foundation, "OWASP Top 10:2021 The Ten Most Critical Web Application Security Risks," [Online]. Available: https://owasp.org/www-project-top-ten/, 2021.
[3]. W. G. Halfond, J. Viegas, and A. Orso, "A Classification of SQL-Injection Attacks and Countermeasures," Proceedings of the IEEE International Symposium on Secure Software Engineering, 2006.
[4]. S. Gupta and B. B. Gupta, "Cross-Site Scripting (XSS) Attacks and Defense Mechanisms: Classification and State-of-the-Art," International Journal of System Assurance Engineering and Management, vol. 8, no. 1, 2017.
[5]. M. Grinberg, Flask Web Development: Developing Web Applications with Python, O'Reilly Media, 2018.
[6]. S. Few, Information Dashboard Design: Displaying Data for At-a-Glance Monitoring, Analytics Press, 2013.

