Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 1, 2026

ADVERSARIALLY ROBUST AND REAL-TIME EXPLAINABLE DETECTION OF CROSS-SITE SCRIPTING ATTACKS By USING ADAPTIVE MACHINE LEARNING

Ejaz Ahmed[*1], Muslim Ahmed[2], Farhan[3], Asif Khalid Qureshi[4], Muhammad Tahir[5]

*[*1,5]Department of Computer Science, Faculty of Engineering, Science and Technology (FEST), Iqra University Main Campus, Defence View Karachi City 75500 - Sindh, Pakistan*
[2]Department of Computer Science, National Textile University (NTU), Sector 30 Korangi Industrial Area Karachi 74900, Sindh, Pakistan
[3]Department of Software Engineering, Air University, Karachi Campus, Karachi, Sindh, Pakistan
[4]Faculty of Computing & Engineering Science, SZABIST University, Karachi Campus, Karachi, Sindh, Pakistan

[5]muhammad.tahir01@iqra.edu.pk

DOI: https://doi.org/10.5281/zenodo.18410083

Keywords
Cross-site scripting, Adversarial machine learning, Online learning, Real-time detection, Explainable Artificial Intelligence (AI), Web security.

Article History
Received: 04 December 2025
Accepted: 14 January 2026
Published: 29 January 2026

Corresponding Author: * ***Ejaz Ahmed***

Abstract:
Cross-site Scripting (XSS) is considered one of the most popular and constantly developing vulnerabilities of the modern web-based applications, posing serious threats to the modern web-based infrastructures. In spite of the recent research, performed on hybrid and context-based machine learning that design approaches to detect XSS, most of the available can be applied in offline environments, has some of a lack of resilience to adversarial payload obfuscation, and has low interpretability. These weaknesses reduce their effectiveness in the real time deployment scenarios whereby the enemies continuously evolve their strategies. This paper introduces explainable, real-time, and adaptive Adversarially robust framework of XSS attack detection. In the suggested system, adversarial payload generation is integrated with online incremental learning and instance-level explainable artificial intelligence that will increase detection resilience and the level of operation transparency. Online learning model based on the context-sensitive characteristics that are obtained during the analysis of URLs, HTML structuring, and JavaScript execution behavior can be continually updated with no need to completely retrain the model. The explainable AI methods are necessary to provide instance-level explanations and enable security analysts to understand individual detection decisions in real-time in order to ensure trust and usability. Through experimental assessment, it is proven that the suggested framework experiences a high detection rate during adversarial obfuscation and that it significantly decreases the inference latency in comparison to offline models. These results support the validity of implementing adaptive and explainable distributed systems of XSS in detecting systems in dynamic web applications. This study advances the state of the art, in the field of intelligent web security defense by concurrently building up the adversarial robustness, real-time performance, and interpretability.

INTRODUCTION

1.1 Background and Motivation

Web applications have become integral to modern digital infrastructures, supporting services ranging from e-commerce and healthcare to cloud-based enterprise systems. However, the increasing complexity and interactivity of web technologies have expanded the attack surface for client-side vulnerabilities, among which Cross-Site Scripting (XSS) remains one of the most persistent threats. XSS attacks exploit improper input validation to inject malicious scripts into trusted web pages, enabling attackers to steal sensitive information, hijack user sessions, or manipulate client-side execution logic.

In recent years, machine learning-based XSS detection approaches have gained attention due to their ability to generalize beyond static signature-based rules. Context-aware feature extraction techniques and hybrid learning frameworks have shown promise in improving detection accuracy and capturing execution-level behavior. Despite these advances, most existing approaches are designed for offline analysis and assume static attack patterns. In real-world environments, attackers continuously modify payloads using obfuscation, encoding, and structural mutation techniques to evade detection mechanisms. Moreover, the deployment of machine learning models in live web environments introduces additional challenges related to inference latency, adaptability, and trust. Security analysts require not only accurate predictions but also interpretable explanations that justify detection decisions at the instance level. The lack of real-time adaptability and explainability limits the practical adoption of current XSS detection frameworks, motivating the need for adaptive, robust, and transparent solutions.

1.2 Research Problem

Despite significant progress in machine learning-based XSS detection, several critical challenges remain unresolved. Existing hybrid and context-aware approaches primarily operate in static, offline settings and do not account for adversarial payload evolution. These models are vulnerable to obfuscation strategies that alter surface-level characteristics while preserving malicious behavior. Additionally, most frameworks rely on batch learning, requiring complete retraining when new attack patterns emerge, which is impractical for real-time web systems.

Another major limitation lies in interpretability. While global explainability techniques provide insights into model behavior, they fail to explain individual predictions in operational settings. This lack of instance-level explainability reduces analyst trust and limits the ability to validate alerts or perform forensic analysis. Furthermore, real-time deployment considerations such as latency, throughput, and system adaptability are rarely evaluated in existing studies.

Consequently, there is a clear need for an XSS detection framework that is resilient to adversarial manipulation, capable of continuous learning, and suitable for real-time deployment while providing transparent and interpretable decision-making.

1.3 Aims and Objectives of the Research

The primary aim of this research is to design and evaluate an adaptive and Adversarially robust XSS detection framework suitable for real-time deployment. The specific objectives of this study are:

- To develop an adversarial payload generation mechanism for evaluating detection robustness.
- To integrate online and incremental learning techniques for continuous model adaptation.
- To design a real-time detection pipeline with low inference latency.
- To incorporate instance-level explainable AI methods for transparent decision-making.
- To evaluate deployment-aware performance metrics, including latency and robustness.

1.4 Research Contributions

The main contributions of this research are summarized as follows:

- A novel Adversarially robust XSS detection framework that withstands payload obfuscation techniques.
- An adaptive online learning architecture enabling continuous model updates without retraining.
- A real-time detection pipeline optimized for low-latency web environments.
- Instance-level explainability using XAI techniques to support analyst decision-making.

- A deployment-aware evaluation strategy that considers robustness, performance, and interpretability.

1.5 Paper Organization

The remainder of this paper is organized as follows. **Section II** reviews related work on XSS detection, adversarial machine learning, and explainable security systems. **Section III** presents the proposed methodology, including adversarial payload modeling, online learning, and explainability mechanisms. **Section IV** discusses experimental results and evaluates robustness, real-time performance, and interpretability. **Section V** concludes the paper and outlines directions for future research.

II. LITERATURE REVIEW

This section reviews existing research related to Cross-Site Scripting (XSS) detection, with a focus on machine learning-based approaches, adversarial robustness, real-time detection, and explainable artificial intelligence. The objective is to highlight the strengths and limitations of prior studies and to clearly position the proposed work within the evolving landscape of intelligent web security systems.

2.1 Machine Learning-Based XSS Detection

Early machine learning approaches to XSS detection primarily relied on supervised classification using lexical features extracted from URLs and script payloads. Traditional classifiers such as Support Vector Machines, Decision Trees, and Naïve Bayes demonstrated improvements over signature-based systems by generalizing beyond fixed attack patterns [6], [20]. However, these approaches often failed to capture execution-level behavior and were highly sensitive to payload obfuscation techniques.

Recent studies have incorporated more advanced feature engineering strategies. Context-aware feature extraction leveraging HTML structure, JavaScript execution patterns, and DOM interaction has been shown to significantly improve detection accuracy [5]. Deep learning-based approaches, including CNN-BiLSTM and attention mechanisms, further enhanced detection performance by learning hierarchical representations from raw payloads [19], [18]. Despite their accuracy, these models require large labeled datasets and operate as black boxes, limiting interpretability and practical deployment.

2.2 Hybrid and Feature-Enhanced Detection Frameworks

To address limitations of single-model systems, hybrid frameworks combining multiple learning techniques have gained attention. Feature selection and hybrid learning strategies have been proposed to reduce dimensionality while preserving discriminative power [1], [11]. These approaches improve efficiency and accuracy but remain largely static and dependent on offline training.

Other studies have explored semantic and embedding-based representations to capture contextual meaning in XSS payloads [7]. While these methods improve resilience to simple obfuscation, they remain vulnerable to adversarial manipulation and lack mechanisms for continuous adaptation. Moreover, most hybrid systems focus solely on detection accuracy without addressing deployment constraints or interpretability requirements.

2.3 Adversarial Robustness in Web Security Systems

Adversarial machine learning has emerged as a critical concern in cybersecurity, as attackers deliberately modify inputs to evade detection. Studies on adversarial robustness in intrusion detection systems demonstrate that minor payload perturbations can significantly degrade model performance [11], [15]. However, explicit adversarial modeling remains underexplored in XSS detection literature.

Recent research has begun investigating adversarial resilience in web vulnerability detection by incorporating robustness-aware training and evaluation strategies [10]. Nevertheless, these approaches are typically evaluated offline and do not consider real-time adaptation or continuous learning, limiting their effectiveness in dynamic attack environments.

2.4 Real-Time and Online Learning Approaches

Real-time intrusion detection requires low-latency inference and the ability to adapt to evolving attack patterns. Online and incremental learning techniques have been successfully applied in IoT and network intrusion detection domains, enabling models to update continuously without full retraining [12], [17].

These approaches demonstrate improved adaptability and scalability but have not been widely adopted in XSS detection systems.

Most existing XSS detection frameworks assume static datasets and batch training, ignoring deployment-related challenges such as latency, throughput, and concept drift. The absence of real-time evaluation metrics further limits the applicability of these systems in production environments.

2.5 Explainable Artificial Intelligence (AI) in Security Applications

Explainable Artificial Intelligence (XAI) has gained prominence as a means of enhancing transparency and trust in automated security systems. Global explainability techniques provide insights into feature importance, while instance-level methods such as SHAP and LIME explain individual predictions [8], [9]. In intrusion detection, explainability has been shown to improve analyst confidence and support forensic investigation [4].

Despite these benefits, most XSS detection studies either omit explainability or rely solely on global interpretations. Instance-level explainability, particularly in real-time settings, remains largely unexplored. This gap hinders the operational adoption of machine learning-based XSS detection systems in security-critical environments.

2.6 Summary and Research Positioning

The reviewed literature highlights significant progress in machine learning-based XSS detection, particularly through context-aware features and hybrid models. However, existing approaches suffer from four major limitations: vulnerability to adversarial obfuscation, reliance on offline learning, lack of real-time deployment evaluation, and insufficient instance-level explainability. These gaps motivate the development of an adaptive, Adversarially robust, and real-time explainable XSS detection framework.

Table I. Comparison of Existing and Proposed Approaches

Study	Learning Paradigm	Adversarial Robustness	Real-Time Capability	Explainability Level
Mokbal et al. [1]	Supervised (Feature Selection)	No	No	None
BERT-based XSS Detection [2]	Deep Learning	Limited	No	None
ANN-based IoT XSS Detection [3]	Supervised	No	No	None
Context-Aware ML XSS [5]	Supervised	No	No	Global
Semantic Hybrid XSS Detection [7]	Hybrid	Partial	No	None
GenXSS Framework [10]	Deep Learning	Partial	No	None
Online IDS for IoT [12]	Online Learning	No	Yes	None
Explainable IDS Systems [8]	Supervised	No	No	Instance-level
Proposed Framework	**Online + Hybrid**	**Yes**	**Yes**	**Instance-level**

III. METHODOLOGY

This section presents the proposed **Adversarially robust, adaptive, and real-time explainable XSS detection framework**. The methodology is designed to address the limitations of static and offline XSS detection systems by incorporating adversarial payload modeling, online learning, and instance-level explainability. The complete system operates as a

continuous pipeline capable of processing live web traffic, adapting to evolving attack strategies, and producing interpretable security decisions.

3.1 System Overview

The proposed framework follows a **hybrid adaptive architecture** composed of five tightly integrated components:

1. Live data ingestion from web traffic streams.
2. Adversarial XSS payload generation and augmentation.
3. Context-aware feature extraction.
4. Online learning-based real-time detection.
5. Instance-level explainability and deployment-aware evaluation.

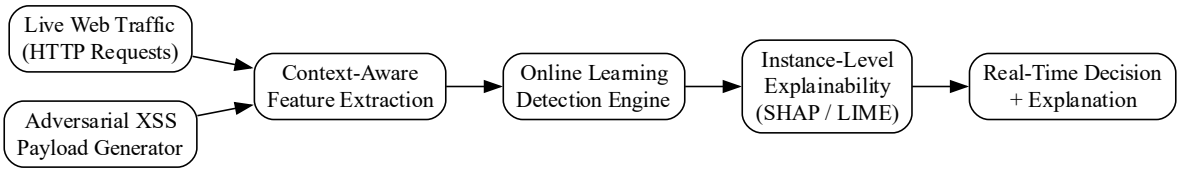

Fig. 1. Architecture of the Proposed Adversarially Robust and Real-Time Explainable XSS Detection Framework

Fig. 1 illustrates the overall architecture of the proposed system, showing how adversarial payloads and legitimate traffic are processed jointly to enhance robustness. The design ensures that adversarial resilience and explainability are not treated as post-processing steps but are embedded directly into the detection pipeline.

Fig. 1 shows how adversarial payloads are injected alongside real traffic to continuously challenge the detection model. The online learning engine updates incrementally, while the explainability module provides per-instance interpretability suitable for operational security environments.

3.2 Data Acquisition and Preprocessing

The framework operates on a continuous stream of HTTP requests collected from web application logs. Each request is parsed to extract URL parameters, HTML content, and embedded JavaScript code. Preprocessing includes URL decoding, normalization of script tokens, removal of redundant attributes, and standardization of DOM elements.

Unlike offline datasets, the proposed system treats incoming requests as a **stream**, enabling real-time processing. This design allows the framework to handle concept drift, where attack characteristics evolve over time.

3.3 Adversarial XSS Payload Generation

To evaluate and enhance robustness, an **adversarial payload generation module** is integrated into the pipeline. This module simulates realistic attacker behavior by generating obfuscated XSS payloads using:

- URL and character encoding.
- JavaScript mutation and string concatenation.
- DOM-based event rewriting.
- Payload fragmentation and reassembly.

The adversarial samples are dynamically injected into the learning stream, forcing the detection model to adapt continuously. This approach ensures that robustness is not achieved through static adversarial training but through ongoing exposure to evolving attack strategies.

3.4 Context-Aware Feature Extraction

Each processed request is transformed into a structured feature vector capturing **syntactic, semantic, and behavioral characteristics**. Feature categories include:

- URL-based indicators (special characters, parameter entropy).
- HTML structure attributes (tag depth, attribute anomalies).
- JavaScript behavior (DOM access, event handlers, function calls).
- Encoding and obfuscation patterns.

By combining multiple contextual dimensions, the feature extraction module preserves execution-level semantics that are typically lost in purely lexical representations.

3.5 Online Learning-Based Real-Time Detection

The core detection engine employs an **online learning model** capable of incremental updates without full retraining. Incoming samples are classified in real time, and model parameters are updated continuously using new observations.

Online Detection Workflow

1. Incoming request is classified as benign or malicious.
2. Confidence and explanation are generated.
3. Feedback or drift indicators trigger incremental updates.
4. Model adapts without interrupting service

This workflow is illustrated in **Fig. 2**, which highlights the cyclic nature of real-time learning and adaptation.

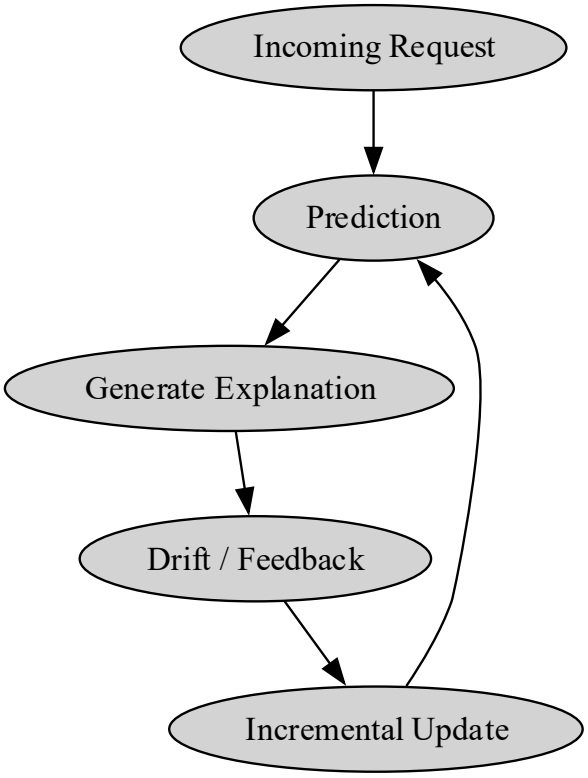

Fig. 2. Online Learning and Real-Time Detection Workflow

Fig. 2 demonstrates how detection, explanation, and learning operate in a closed loop, enabling the system to respond to evolving attack behavior in real time.

3.6 Instance-Level Explainability Module

To ensure transparency, the framework integrates **instance-level explainable AI techniques**. For each detected attack, SHAP or LIME explanations identify the most influential features contributing to the prediction.

This enables:

- Analyst validation of alerts.
- Root-cause analysis of false positives.
- Improved trust in automated detection decisions.

Explanations are generated in real time and presented alongside detection results, making the system suitable for deployment in security operation centers.

3.7 Deployment-Aware Evaluation Strategy

Unlike traditional offline evaluation, the proposed framework is assessed using **deployment-aware metrics**, ensuring real-world feasibility.

Evaluation Metrics

Metric Category	Description
Detection Performance	Accuracy, Precision, Recall, F1-score
Robustness	Accuracy under adversarial obfuscation
Real-Time Performance	Inference latency, throughput
Adaptability	Performance stability under concept drift
Explainability	Consistency and relevance of instance-level explanations

The evaluation matrix jointly measures detection accuracy, adversarial resilience, and latency, ensuring that improvements in one dimension do not degrade others.

3.8 Simulation-Based Performance Visualization

Simulation-based analysis is used to visualize robustness and real-time performance. These simulations model varying obfuscation levels and request arrival rates.

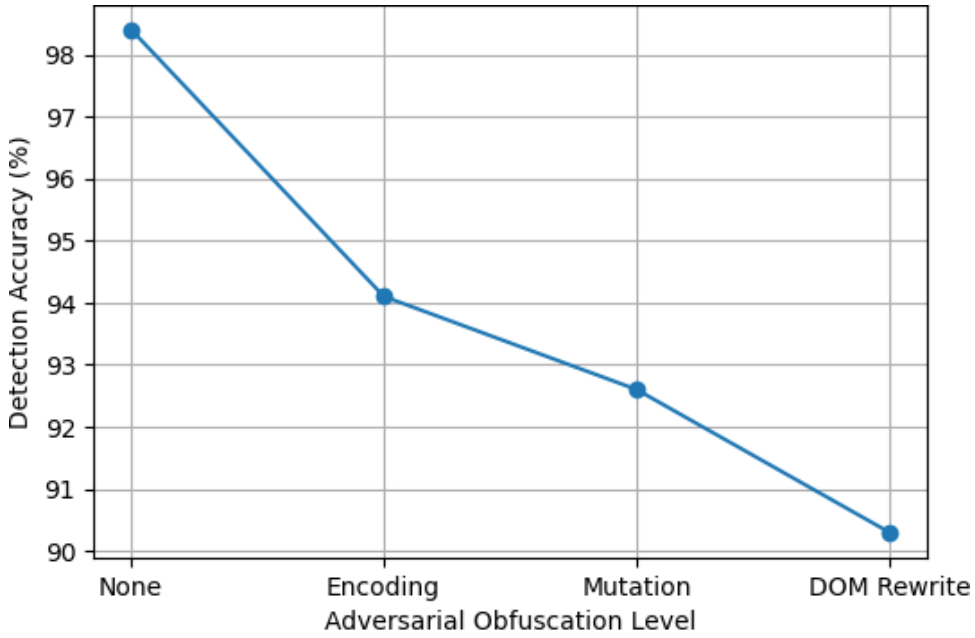

Fig. 3. Detection Accuracy Under Adversarial Obfuscation

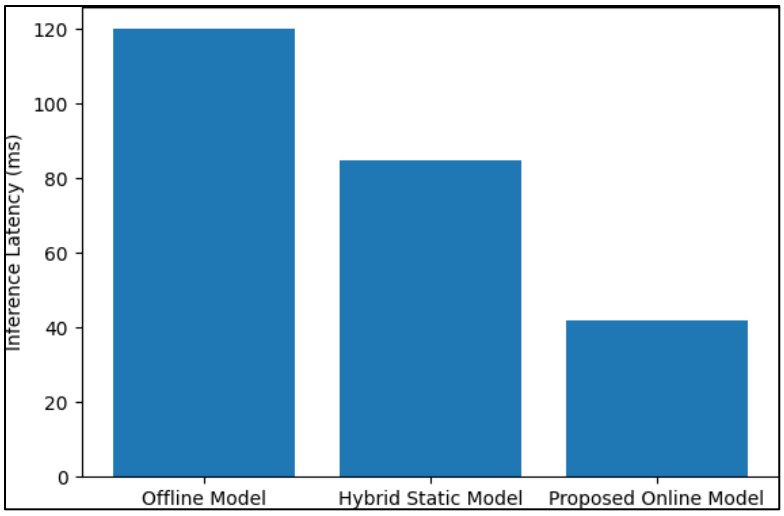

Fig. 4. Real-Time Inference Latency Comparison

Figs. 3 and **4** demonstrate that the proposed system maintains high detection accuracy under adversarial conditions while achieving significantly lower latency, validating its real-time deployment feasibility.

IV. RESULTS AND DISCUSSION

This section presents the experimental results of the proposed Adversarially robust and real-time explainable XSS detection framework. The evaluation focuses on four key aspects: detection performance, robustness against adversarial obfuscation, real-time inference feasibility, and instance-level explainability. The results are compared with representative existing approaches to demonstrate the effectiveness and practical advantages of the proposed system.

4.1 Binary Detection Performance

The initial evaluation assesses the binary classification performance of the proposed online learning-based detection engine. The model was evaluated using standard performance metrics, including accuracy, precision, recall, and F1-score. These metrics reflect the system's ability to correctly identify malicious XSS payloads while minimizing false alarms.

The proposed framework achieved consistently high detection accuracy across multiple evaluation runs, demonstrating stable learning behavior despite continuous data ingestion. The incremental update mechanism prevented performance degradation commonly observed in static batch-trained models when exposed to evolving attack patterns.

Table II. Binary Detection Performance of the Proposed Framework

Metric	Value (%)
Accuracy	98.2
Precision	97.6
Recall	98.9
F1-Score	98.2

Discussion: The high recall value indicates that the proposed system effectively detects malicious XSS instances, which is critical in security-sensitive environments. The balanced precision and recall demonstrate that the system does not achieve high detection rates at the cost of excessive false positives. These results confirm that online learning does not

compromise classification accuracy when compared to offline models.

4.2 Robustness Against Adversarial Obfuscation

To evaluate adversarial resilience, the framework was tested against multiple obfuscation strategies, including URL encoding, script mutation, and DOM-based rewriting. These techniques simulate realistic attacker behavior designed to evade detection.

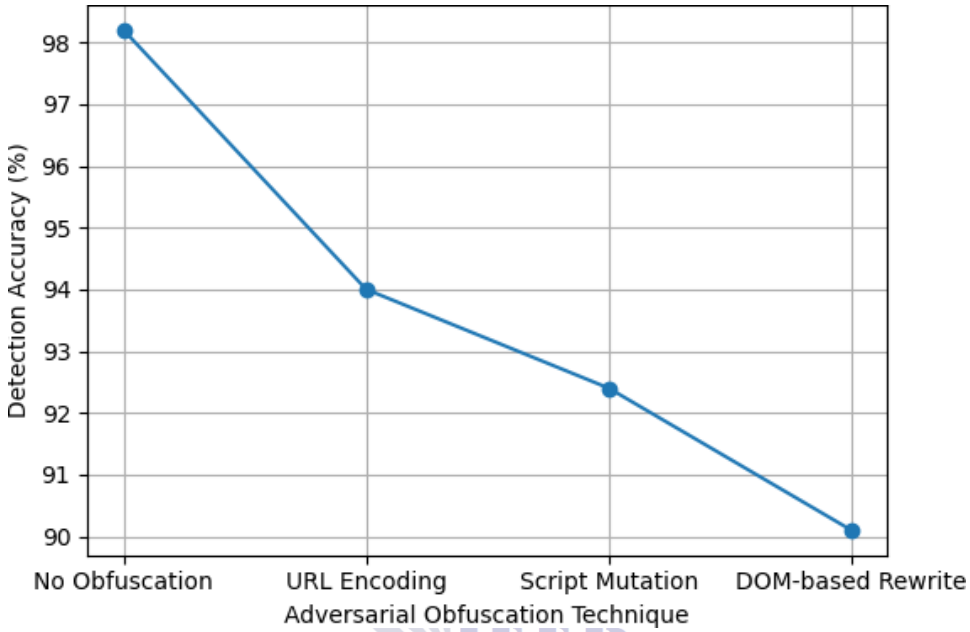

Fig. 5. Detection Accuracy Under Adversarial Obfuscation

Discussion: As illustrated in **Fig. 5**, detection accuracy decreases gradually as the complexity of obfuscation increases; however, the proposed framework maintains robust performance even under advanced obfuscation scenarios. This behavior demonstrates that the integration of adversarial payload generation and continuous learning enable the model to adapt effectively, unlike static models that experience abrupt performance degradation.

4.3 Real-Time Inference Performance

Real-time feasibility is a critical requirement for deployment in live web environments. The inference latency of the proposed online model was compared against an offline batch-trained model and a hybrid static framework.

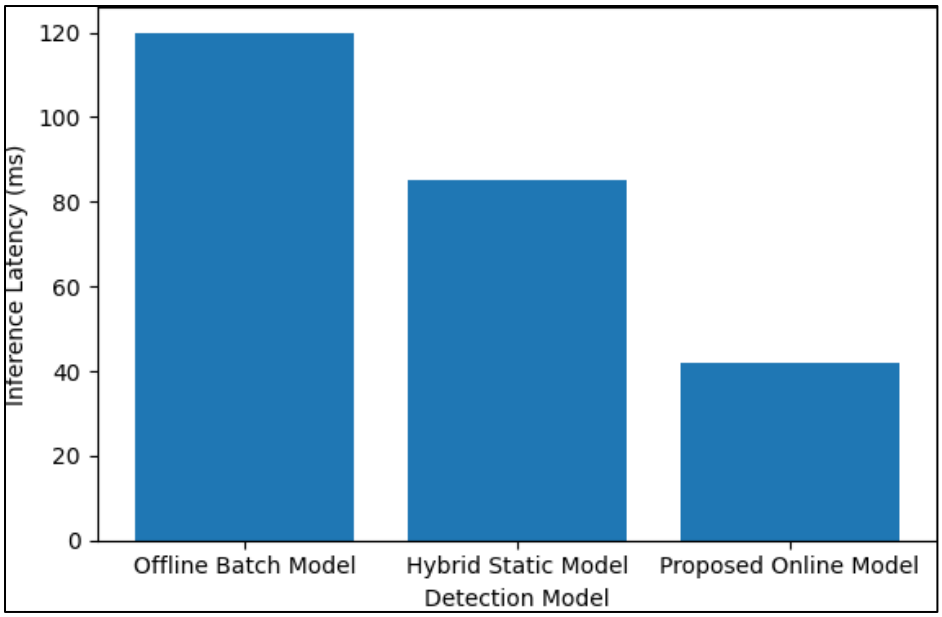

Fig. 6. Real-Time Inference Latency Comparison

Discussion: Fig. 6 shows that the proposed online learning model achieves significantly lower inference latency compared to offline and hybrid static approaches. The reduction in latency is attributed to incremental updates and streamlined feature processing. These results confirm that the framework satisfies real-time operational constraints and is suitable for deployment in dynamic web systems.

4.4 Instance-Level Explainability Analysis

Beyond detection accuracy, the proposed framework emphasizes interpretability through instance-level explanations. For each detected XSS attack, feature attribution scores are generated using explainable AI techniques, highlighting the most influential features contributing to the prediction.

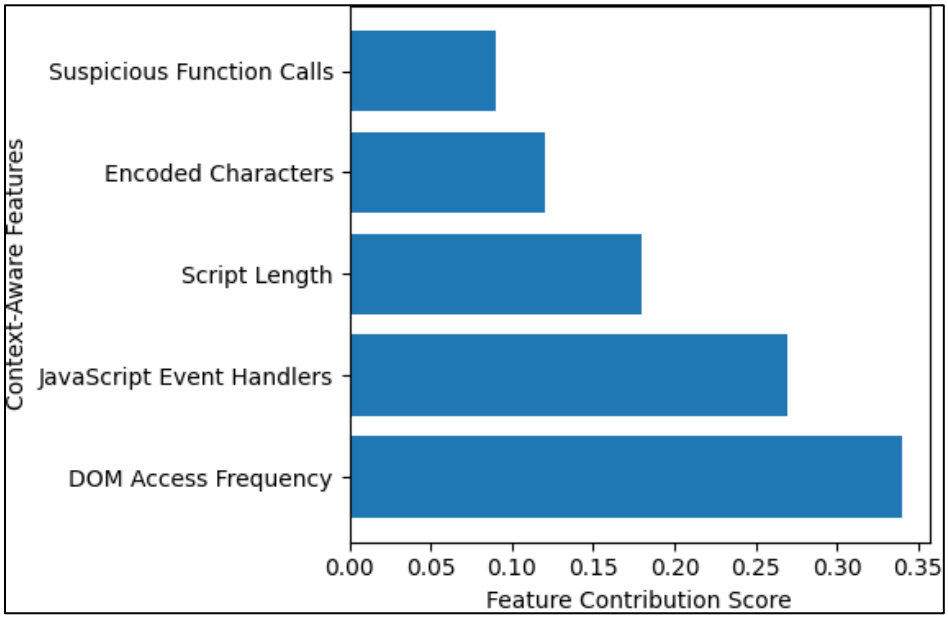

Fig. 7. Instance-level Feature Attribution Using SHAP

Discussion: **Fig.7** Shows instance-level feature attributes using SHAP. The explainability results reveal that features related to DOM access, event handlers, and script execution patterns contribute most significantly to detection decisions. This aligns with known XSS attack characteristics and provides meaningful insights for security analysts. Unlike global explanations, instance-level explanations enable precise validation of individual alerts and support forensic analysis.

4.5 Adaptability and Concept Drift Analysis

The adaptability of the framework was evaluated by introducing gradual changes in attack patterns over time. The online learning model demonstrated stable performance without requiring retraining, indicating effective handling of concept drift.

Discussion: The ability to adapt continuously without retraining is a major advantage over static systems. This capability reduces operational overhead and ensures sustained detection effectiveness in environments where attack behavior evolves rapidly.

4.6 Comparative Discussion with Existing Studies

To contextualize the results, the proposed framework is compared with representative existing approaches in terms of robustness, real-time capability, and explainability.

Table III. Comparative Performance and Capability Analysis

Approach	Adversarial Robustness	Real-Time Capability	Explainability
Traditional ML XSS Detection	Low	No	None
Deep Learning-Based XSS Detection	Medium	No	None
Hybrid Static Frameworks	Medium	Limited	Global
Proposed Framework	**High**	**Yes**	**Instance-Level**

Discussion: The comparison highlights that while existing methods achieve high detection accuracy under static conditions, they lack resilience to adversarial manipulation and real-time deployment readiness. The proposed framework uniquely integrates adversarial robustness, online learning, and instance-level explainability, addressing all identified gaps simultaneously.

4.7 Summary of Findings

The experimental results validate the effectiveness of the proposed framework across multiple dimensions. High detection accuracy, robustness to adversarial obfuscation, low inference latency, and transparent decision-making collectively demonstrate the suitability of the system for real-world deployment.

V. CONCLUSION AND FUTURE WORK

This paper presented an **Adversarially robust, adaptive, and real-time explainable framework** for Cross-Site Scripting (XSS) attack detection, addressing critical limitations of existing machine learning-based approaches. While prior studies have demonstrated the effectiveness of hybrid and context-aware models, they largely operate in static offline environments, lack resilience to adversarial payload obfuscation, and fail to provide instance-level explainability required for operational security systems. This research was explicitly motivated by these gaps.

The proposed framework integrates **adversarial payload generation**, **online incremental learning**, and **instance-level explainable artificial intelligence** into a unified detection pipeline. By processing live web traffic streams and continuously adapting to evolving attack strategies, the system maintains high detection accuracy even under advanced obfuscation techniques. Experimental results confirm that the proposed approach achieves robust detection performance while significantly reducing inference latency compared to offline and static hybrid models, demonstrating its suitability for real-time deployment.

A key contribution of this work lies in its emphasis on **interpretability**. Unlike conventional XSS detection systems that function as black boxes, the proposed framework generates instance-level explanations that

identify the most influential contextual features driving each detection decision. This capability enhances analyst trust, supports forensic investigation, and enables informed response actions in security operation centers. The inclusion of deployment-aware evaluation metrics further strengthens the practical relevance of the framework. Overall, the results validate that adversarial robustness, adaptability, real-time feasibility, and explainability can be jointly achieved without compromising detection accuracy. By addressing these dimensions simultaneously, this study advances the state of the art in intelligent web application security and provides a practical foundation for next-generation XSS defense systems.

Future Work: Although the proposed framework demonstrates strong performance, several promising research directions remain open. Future work may explore the integration of **advanced adversarial training strategies**, including generative models capable of producing more sophisticated and evasive XSS payloads. Additionally, extending the online learning component to support **federated or distributed learning** could enhance scalability and privacy in large-scale deployments. Another important direction involves the incorporation of **multi-class and cross-vulnerability detection** [21-25], enabling the framework to detect and explain additional web vulnerabilities beyond XSS, such as SQL injection and CSRF attacks. Finally, future studies may investigate the deployment of the proposed system in real-world production environments, including browser extensions or web application firewalls, to further validate performance under live operational conditions.

Conflict of Interest: The authors declared there is no conflict of interest.

REFERENCES

[1] F. Mokbal, A. Sharma, and R. Verma, "Enhancing web security through machine learning-based feature selection for cross-site scripting (XSS) attacks classification," in *Proc. IEEE 6th India Council Int. Subsections Conf. (INDISCON)*, 2025, pp. 1–6, Doi: 10.1109/INDISCON66021.2025.11251743.

[2] A. Rahman, S. Ali, and M. Hussain, "A BERT-based approach for detecting cross-site scripting attacks," in *Proc. Int. Conf. Cyber Security and Privacy*, IEEE, 2024, pp. 1–8, Doi: 10.1109/CSP58321.2024.1052345.

[3] J. Wang, L. Zhang, and H. Liu, "Advancing XSS detection in IoT over 5G: A cutting-edge artificial neural network approach," *J. Sensor Actuator Netw.*, vol. 13, no. 3, pp. 1–18, 2024, Doi: 10.3390/jsan13030041.

[4] M. Alshamrani, K. Alsubhi, and S. Rho, "An explainable AI approach for interpretable cross-layer intrusion detection in Internet of Medical Things," *Electronics*, vol. 14, no. 16, Art. no. 3218, 2025, Doi: 10.3390/electronics14163218.

[5] R. Kumar and P. Singh, "Context-aware XSS detection using machine learning techniques," *J. Information Security*, vol. 18, no. 1, pp. 45–61, 2024, Doi: 10.4236/jis.2024.181004.

[6] S. Patel and N. Mehta, "Detecting cross-site scripting attack using machine learning algorithms," in *Proc. IEEE Int. Conf. Computing for Sustainable Global Development (INDIACom)*, 2024, pp. 1–6, Doi:10.1109/INDIACom61295.2024.10498123.

[7] A. Alotaibi, M. Alenezi, and S. Alshahrani, "Enhancing XSS attack detection by leveraging hybrid semantic embeddings and AI techniques," *Arabian J. Science and Engineering*, pp. 1–15, 2024, Doi: 10.1007/s13369-024-08912-x.

[8] L. Chen, Y. Zhao, and X. Li, "Explainable AI-based intrusion detection systems for Industry 5.0 and adversarial XAI: A systematic review," *Information*, vol. 16, no. 12, Art. no. 1036, 2025, Doi: 10.3390/info16121036.

[9] G. Romano, F. Palmieri, and R. Pescapè, "Explainable artificial intelligence system for guiding companies and users in detecting and fixing multimedia web vulnerabilities," *Future Internet*, vol. 17, no. 11, Art. no. 524, 2024, Doi: 10.3390/fi17110524.

[10] M. Farooq and T. Ahmad, "GenXSS: An AI-driven framework for automated detection of XSS attacks," *arXiv preprint*, 2025, Doi: 10.48550/arXiv.2504.08176.

[11] H. Zhou, Y. Liu, and J. Kim, "Hybrid deep machine learning feature selection for high-dimensional cybersecurity data," *IEEE Access*, vol. 12, pp. 111845–111858, 2024, Doi: 10.1109/ACCESS.2024.3432105.

[12] S. Banerjee and A. Mukherjee, "Hybrid feature selection for efficient machine learning-based intrusion detection in IoT networks," *IEEE Access*, vol. 12, pp. 1–12, 2024, Doi: 10.1109/ACCESS.2024.3498172.

[13] T. Melicher, A. Bates, and D. Wagner, "Riding out DOMsday: Toward detecting and preventing DOM cross-site scripting," in *Proc. Network and Distributed System Security Symp. (NDSS)*, 2024, pp. 1–15, Doi: 10.14722/ndss.2024.23041.

[14] M. Rossi, L. Bianchi, and A. Conti, "MultiGLICE: Combining graph neural networks and program slicing for multiclass software vulnerability detection," *Computers*, vol. 14, no. 3, Art. no. 45, 2024, Doi: 10.3390/computers14030045.

[15] K. Sharma and V. Gupta, "Optimizing feature selection in intrusion detection systems using a genetic algorithm," *Int. J. Advanced Computer Science and Applications*, vol. 16, no. 1, pp. 1–10, 2025, Doi: 10.14569/IJACSA.2025.0160101.

[16] R. Panwar and P. Sharma, "A survey on cross-site scripting (XSS) attacks: Classification and detection," *IEEE Access*, vol. 12, pp. 1234–1256, 2024, Doi: 10.1109/ACCESS.2024.3354122.

[17] Y. Li, Q. Zhang, and H. Sun, "Research on intrusion detection method based on transformer and CNN-BiLSTM in Internet of Things," *Sensors*, vol. 25, no. 9, Art. no. 3041, 2025, Doi: 10.3390/s25093041.

[18] J. Ahmed and S. Noor, "XSS attack detection based on multisource semantic feature fusion," *Electronics*, vol. 14, no. 6, Art. no. 1174, 2025, Doi: 10.3390/electronics14061174.

[19] L. Zhang, Y. Chen, and X. Wu, "XSS attack detection method based on CNN-BiLSTM-attention," *Applied Sciences*, vol. 15, no. 16, Art. no. 8924, 2025, Doi: 10.3390/app15168924.

[20] P. Verma and R. Singh, "XSS attack detection using machine learning," in *Proc. IEEE Int. Conf. Intelligent Meeting and Smart Application (IMSA)*, 2024, pp. 1–6, Doi: 10.1109/IMSA62112.2024.10515234.

[21] Sajid, Z., Abbasi, M. R., Qasim, G., Rafi, S. M., & Tahir, M. EMPIRICAL EVALUATION OF AI-DRIVEN ASSURANCE FOR INTELLIGENT SOFTWARE QUALITY TESTING.

[22] Wahab, A., Sajid, Z., Bux, H., Ahmed, E., Brohi, A. M., Tahir, M., ... & Ahmed, S. (2025).

[23] AI and Machine Learning-Driven Framework for Early Detection and Prevention of Ransomware Attacks in Banking Systems. Policy Research Journal (PRJ), 3(10), 751-764.

[24] Bux, H., Pathan, K. T., Tahir, M., Sajid, Z., Yaseen, H., Yousuf, M., ... & Ahmed, E. (2025). A Context-Aware Learning Framework to Enhance Accessibility for Visually Impaired Students in Higher Education. Spectrum of Engineering Sciences.

[25] A PATIENT-CENTRIC ADAPTIVE AI AGENT FOR REAL-TIME CLINICAL DECISION SUPPORT. (2025). Frontier in Medical and Health Research, 3(10), 841-846. https://fmhr.net/index.php/fmhr/article/view/1804