International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2 (2026)



ijerst.editor@gmail.com

editor@ijerst.com

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 2, 2026
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

ADAPTIVE CYBER DEFENCE FOR WEB APPLICATIONS USING BLOCKCHAIN AND ADVERSARIAL LEARNING TECHNIQUES

[1] Mr. P. China Babu, [2] Yerra Meghana Hari Sai Sree,[3] Maridi Deekshitha,[4] Jogi Sunitha,[5] Doddi Sai Charan Teja

[1] Assistant Professor, Department of Computer Science & Engineering (Artificial Intelligence & Data Science),
ELURU COLLEGE OF ENGINEERING AND TECHNOLOGY:: ELURU.

[1] Email : chnbbpnglt@gmail.com

[2,3,4,5] Students, Department of Computer Science & Engineering (Artificial Intelligence & Data Science),

ELURU COLLEGE OF ENGINEERING AND TECHNOLOGY:: ELURU
[2]yerrameghana485@gmail.com,[3]deekshideekshi531@gmail.com,
[4]sunithajogi04@gmail.com,[5] dscharan2498@gmail.com

Abstract:

The increasing reliance on web applications for digital services has significantly expanded the attack surface for cyber threats, making web security a critical concern for organizations. Traditional cybersecurity mechanisms often struggle to respond effectively to evolving and sophisticated cyberattacks such as distributed denial-of-service (DDoS), SQL injection, cross-site scripting (XSS), and automated bot attacks. To address these challenges, adaptive cyber defense systems that incorporate advanced technologies are required. This study proposes an adaptive cyber defense framework for web applications that integrates blockchain technology with adversarial learning techniques to enhance security, transparency, and resilience against cyber threats. Blockchain provides a decentralized and tamper-resistant platform for securely recording security events, maintaining audit trails, and ensuring data integrity within the defense system. At the same time, adversarial learning techniques are employed to train machine learning models capable of detecting malicious activities and adapting to evolving attack patterns. The proposed system continuously monitors web traffic, analyzes behavioral patterns, and identifies suspicious activities using adversarially trained models that improve detection accuracy and robustness against evasion attacks. By combining the decentralized trust model of blockchain with the adaptive capabilities of adversarial machine learning, the framework enhances the ability of web applications to detect, respond to, and mitigate cyber threats in real time. The proposed approach aims to create a secure, intelligent, and scalable cyber defense system capable of protecting modern web applications from increasingly complex cyberattacks.

Keywords: Adaptive Cyber Defense, Web Application Security, Blockchain Technology, Adversarial

Learning, Machine Learning in Cybersecurity, Intrusion Detection, Cyber Threat Detection, Decentralized Security Systems, Network Security, Secure Web Applications.

I.INTRODUCTION

The rapid growth of web applications has transformed the way organizations deliver digital services, enabling online banking, e-commerce, social networking, and cloud-based platforms. However, the increasing dependence on web applications has also exposed them to a wide range of cyber threats such as SQL injection, cross-site scripting (XSS), distributed denial-of-service (DDoS) attacks, and automated bot attacks. Traditional cybersecurity mechanisms, including firewalls, signature-based intrusion detection systems, and rule-based monitoring tools, often struggle to detect new and evolving attack patterns. As cyber threats continue to become more sophisticated and adaptive, there is a growing need for intelligent and dynamic security solutions capable of responding to emerging vulnerabilities in real time.

In recent years, advanced technologies such as blockchain and machine learning have gained significant attention in the field of cybersecurity. Blockchain technology provides a decentralized and tamper-resistant platform that ensures data integrity, transparency, and secure record keeping. By maintaining immutable logs of security events and transactions, blockchain can enhance trust and accountability in cyber defense systems. On the other hand, machine learning techniques enable systems to analyze large volumes of network traffic data, identify suspicious patterns, and detect potential cyberattacks automatically. Among these techniques, adversarial learning has emerged as a powerful approach for improving the robustness of machine learning models against malicious attacks designed to evade detection.

Adversarial learning focuses on training models that can recognize and defend against adversarial inputs generated by attackers. By simulating attack scenarios and exposing models to adversarial examples during training, these systems become more resilient to evolving cyber threats. Integrating adversarial learning with blockchain-based security infrastructures offers a promising approach for developing adaptive cyber defense systems that can continuously monitor web application activities, detect anomalies, and respond to attacks in real time.

This study focuses on the development of an adaptive cyber defense framework for web applications by combining blockchain technology with adversarial learning techniques. The proposed approach aims to enhance the detection of cyber threats, ensure secure and transparent event logging, and improve the overall resilience of web applications against sophisticated cyberattacks. By leveraging these advanced technologies, the framework provides a scalable and intelligent security solution for protecting modern web-based systems.

II.LITERATURE SURVEY

Recent research in cybersecurity has focused on developing intelligent and adaptive defense mechanisms to protect web applications from increasingly sophisticated cyber threats. Traditional security systems such as firewalls and signature-based intrusion detection systems have been widely used to monitor network activities and detect known attack patterns. However, these systems often struggle to identify new or evolving threats due to their dependence on predefined rules and signatures. As a result, researchers have explored the use of machine learning techniques to improve the detection and prevention of cyberattacks in web-based environments. Machine learning models such as Support Vector Machines, Decision Trees, Random Forest, and Neural Networks have been applied to analyze network traffic and identify anomalies that may indicate malicious activities.

Several studies have also investigated the use of deep learning methods for cybersecurity applications. Techniques such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) have shown promising results in detecting complex attack patterns by analyzing large volumes of network data. These approaches enable systems to automatically learn patterns from historical data and identify previously unseen cyber threats. However, machine learning-based security systems are vulnerable to adversarial attacks, where attackers intentionally manipulate input data to evade detection models. To address this limitation, adversarial learning techniques have been introduced to improve the robustness of machine learning models by training them with adversarial examples.

In parallel, blockchain technology has gained attention as a secure and decentralized platform for enhancing cybersecurity systems. Blockchain provides features such as immutability, transparency, and distributed trust, which can be used to maintain tamper-proof logs of security events and transactions. Researchers have proposed blockchain-based frameworks to improve secure data sharing, authentication, and threat intelligence in distributed systems. By recording security events on a blockchain network, organizations can ensure data integrity and prevent unauthorized modifications.

Recent studies have begun exploring the integration of blockchain with machine learning to create more secure and adaptive cyber defense systems. In such frameworks, blockchain ensures secure storage and verification of security data, while machine learning models analyze the data to detect malicious behavior. Additionally, adversarial learning techniques help strengthen these models against evasion attacks and improve detection accuracy. Although these approaches show significant potential, challenges such as computational complexity, scalability, and integration with existing web application infrastructures remain active areas of research. Overall, the literature indicates that combining blockchain technology

with adversarial machine learning offers a promising direction for developing advanced cyber defense solutions for web applications.

III.EXISTING SYSTEM

The existing systems for protecting web applications mainly rely on traditional cybersecurity mechanisms such as firewalls, rule-based monitoring systems, intrusion detection systems (IDS), and intrusion prevention systems (IPS). These security solutions are designed to detect known threats by using predefined rules, signatures, or pattern-matching techniques. Web Application Firewalls (WAFs) are commonly used to monitor HTTP traffic and block malicious requests such as SQL injection, cross-site scripting (XSS), and other common web-based attacks. Although these systems provide an initial layer of security, they are primarily reactive and depend heavily on previously known attack signatures. As a result, they often fail to detect new, unknown, or evolving cyber threats that do not match existing patterns.

In some modern systems, machine learning techniques have been introduced to improve the detection of anomalies and malicious behavior in web traffic. These systems analyze network data and identify unusual patterns that may indicate cyberattacks. However, traditional machine learning models can still be vulnerable to adversarial attacks, where attackers manipulate input data to bypass detection mechanisms. Additionally, many existing security systems rely on centralized architectures for storing security logs and managing threat data, which can create single points of failure and increase the risk of data tampering. These limitations reduce the overall effectiveness of existing cyber defense systems in protecting modern web applications against sophisticated and adaptive cyber threats. Therefore, there is a need for more advanced security frameworks that combine decentralized technologies and adaptive learning techniques to improve the resilience of web application security systems.

IV.PROPOSED SYSTEM

The proposed system introduces an adaptive cyber defense framework for web applications that integrates blockchain technology with adversarial learning techniques to enhance security and resilience against modern cyber threats. In this system, web application traffic and user activities are continuously monitored and analyzed to detect suspicious behavior. Incoming requests to the web application are first processed through a monitoring layer that collects security-related data such as login attempts, request patterns, access logs, and network traffic information. This data is then forwarded to a machine learning-based analysis module that uses adversarial learning techniques to detect anomalies and malicious activities. By training models with adversarial examples, the system becomes more robust and capable of identifying sophisticated cyberattacks designed to bypass traditional detection mechanisms.

In addition to machine learning-based threat detection, the proposed framework utilizes

blockchain technology to store security logs and threat intelligence in a decentralized and tamper-resistant manner. Each detected event, transaction, or security alert is recorded as a block in the blockchain network, ensuring data integrity, transparency, and protection against unauthorized modification. The decentralized nature of blockchain eliminates single points of failure and provides secure sharing of threat information among different nodes in the network.

The system also includes a real-time response mechanism that automatically triggers defensive actions when malicious activity is detected. These actions may include blocking suspicious IP addresses, alerting administrators, updating firewall rules, or isolating compromised components of the web application. By combining the secure data management capabilities of blockchain with the adaptive detection capabilities of adversarial machine learning, the proposed system creates an intelligent and dynamic cyber defense solution. This framework enhances the ability of web applications to detect, prevent, and respond to evolving cyber threats while maintaining secure and transparent security records.

V.SYSTEM ARCHITECTURE

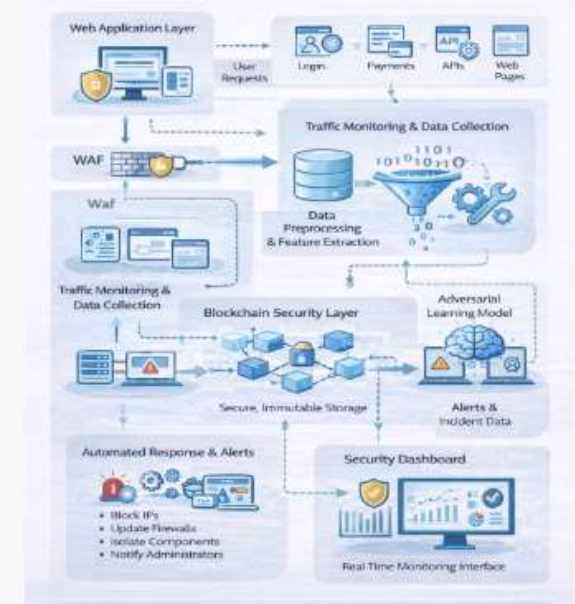


Fig 5.1

The system architecture for "Adaptive Cyber Defense for Web Applications Using Blockchain and Adversarial Learning Techniques" is designed to detect, prevent, and respond to cyber threats in real time by combining machine learning and blockchain technology. The architecture consists of multiple modules that work together to monitor web traffic, analyze threats, and maintain secure and tamper-proof security records.

1. Web Application Layer

This layer represents the web-based platform where users interact with services such as login systems, payment gateways, APIs, and web pages. All user requests first pass through the security monitoring components before reaching the application server. This layer acts as the entry point for all incoming traffic to the system.

2. Web Application Firewall (WAF)

The Web Application Firewall provides the first line of defense by filtering incoming HTTP

requests and blocking known malicious traffic. It protects the application from common attacks such as SQL injection, cross-site scripting (XSS), and other web-based vulnerabilities.

3. Traffic Monitoring and Data Collection Module

This module continuously monitors network traffic, user requests, and application logs. It collects data such as IP addresses, session behavior, access patterns, request frequency, and system activity logs. The collected data is then forwarded for further analysis and threat detection.

4. Data Preprocessing and Feature Extraction Module

The collected data is cleaned and processed to remove irrelevant information and noise. Important features related to user behavior, network activity, and request characteristics are extracted. These features are then prepared for analysis by machine learning models.

5. Adversarial Learning Model

This module uses machine learning models trained with adversarial learning techniques to detect anomalies and cyber threats. By training models with adversarial examples, the system becomes more resilient to attackers attempting to bypass detection mechanisms. The model analyzes patterns in the data and identifies suspicious activities or potential attacks.

6. Blockchain Security Layer

All detected security events, alerts, and threat information are stored in a blockchain network. Blockchain ensures secure, decentralized, and tamper-proof storage of security logs. This prevents unauthorized modification of security data and provides transparency and trust in the cyber defense system.

7. Automated Response and Alert Module

When a potential threat is detected, this module automatically triggers defensive actions such as blocking suspicious IP addresses, updating firewall rules, isolating compromised system components, or notifying system administrators.

8. Security Dashboard and Monitoring Interface

The final module provides a visualization interface for security administrators. It displays real-time alerts, attack patterns, system logs, and security analytics through dashboards and reports, enabling administrators to monitor system health and respond to security incidents efficiently.

VI.IMPLEMENTATION



Fig 6.1



Fig 6.2



Fig 6.3



Fig 6.4



Fig 6.5



Fig 6.6

VII.CONCLUSION

The rapid growth of web applications has increased the risk of cyber threats such as SQL injection, cross-site scripting (XSS), and distributed denial-of-service (DDoS) attacks. Traditional security systems are often limited in detecting evolving and sophisticated attacks because they rely mainly on predefined rules and signature-based detection mechanisms. The proposed adaptive cyber defense framework integrates blockchain technology with adversarial learning techniques to enhance the security of web applications. By continuously monitoring web traffic and analyzing patterns using machine learning models trained with adversarial examples, the system can detect both known and unknown cyber threats more effectively. The integration of blockchain technology ensures secure, decentralized, and tamper-proof storage of security logs, which improves transparency and reliability in cyber defense operations. Additionally, automated response mechanisms enable the system to quickly block malicious activities and alert administrators in real time. Overall, the combination of blockchain and adversarial

machine learning provides a robust and intelligent approach to strengthening web application security against modern cyber threats.

VIII.FUTURE SCOPE

Future research can further enhance the proposed adaptive cyber defense framework by incorporating advanced artificial intelligence techniques such as deep learning and transformer-based models for improved threat detection accuracy. The system can also be expanded to support large-scale distributed environments such as cloud computing platforms and Internet of Things (IoT) networks, where cyber threats are becoming increasingly complex. Integrating federated learning techniques could allow multiple organizations to collaboratively improve security models without sharing sensitive data. Additionally, real-time threat intelligence sharing through blockchain networks can help create collaborative cyber defense ecosystems among organizations. Future developments may also focus on improving scalability, reducing computational overhead, and designing more efficient consensus mechanisms for blockchain-based security systems. These advancements will enable the development of more intelligent, scalable, and autonomous cyber defense solutions capable of protecting next-generation web applications.

IX.REFERENCES

[1] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning, MIT Press, 2016.
[2] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” Nature, 2015.
[3] A. Vaswani et al., “Attention is all you need,” NeurIPS, 2017.
[4] J. Devlin et al., “BERT: Pre-training of deep bidirectional transformers for language understanding,” NAACL, 2019.
[5] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
[6] M. Swan, Blockchain: Blueprint for a New Economy, O’Reilly Media, 2015.
[7] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things,” IEEE Access, 2016.
[8] W. Stallings, Network Security Essentials, Pearson, 2017.
[9] W. Stallings and L. Brown, Computer Security: Principles and Practice, Pearson, 2018.
[10] B. Schneier, Applied Cryptography, Wiley, 2015.
[11] J. Andress, The Basics of Information Security, Syngress, 2014.
[12] N. Carlini and D. Wagner, “Towards evaluating the robustness of neural networks,” IEEE Symposium on Security and Privacy, 2017.
[13] I. Goodfellow et al., “Explaining and harnessing adversarial examples,” ICLR, 2015.
[14] A. Javaid et al., “A deep learning approach for network intrusion detection system,” Bio-inspired Information and Communications Technologies, 2016.
[15] M. Ring et al., “Flow-based network traffic classification using machine learning,” Computers & Security, 2019.
[16] T. Wolf et al., “Transformers: State-of-the-art natural language processing,” EMNLP, 2020.
[17] Y. Kim, “Convolutional neural networks for sentence classification,” EMNLP, 2014.
[18] S. Hochreiter and J. Schmidhuber, “Long short-term memory,” Neural Computation, 1997.
[19] D. Jurafsky and J. H. Martin, Speech and Language Processing, Pearson, 2019.
[20] R. Feldman, “Techniques and applications for sentiment analysis,” Communications of the ACM, 2013.
[21] C. Romero and S. Ventura, “Educational data mining: A survey,” IEEE Transactions on Systems, Man, and Cybernetics, 2013.
[22] M. Peters et al., “Deep contextualized word representations,” NAACL, 2018.
[23] N. Reimers and I. Gurevych, “Sentence-BERT: Sentence embeddings using Siamese BERT networks,” EMNLP, 2019.
[24] S. Ruder, “Neural transfer learning for natural language processing,” PhD Thesis, 2019.
[25] T. Nguyen and G. Armitage, “A survey of techniques for internet traffic classification using machine learning,” IEEE Communications Surveys & Tutorials, 2008.