iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VIII **Month of publication:** August 2025

DOI: https://doi.org/10.22214/ijraset.2025.73862

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VIII Aug 2025- Available at www.ijraset.com

Enhancing Data Protection in IoT Through Firewall and Intrusion Detection Frameworks

Ravi Kant Vyas[1], Vikas Somani[2], S K Dargar[3]
Computer Science and Engineering, Sangam University Bhilwara

Abstract: ***The Internet of Things (IoT) has transformed modern living by interconnecting billions of devices that generate and exchange sensitive data. However, the distributed nature and resource constraints of IoT systems make them highly vulnerable to cyber threats, including denial-of-service (DoS) attacks, malware injection, and data exfiltration. Traditional security solutions such as centralized firewalls and signature-based intrusion detection struggle to safeguard data in these environments. This paper proposes a data protection framework that integrates distributed firewalls with an AI-driven Intrusion Detection System (IDS) to secure IoT networks. The system employs lightweight micro-firewalls at IoT gateways for local traffic filtering, while a hybrid CNN-LSTM model performs anomaly detection on network traffic. To ensure the integrity of event logs, blockchain-based mechanisms are integrated for tamper-proof recording. Experiments on NSL-KDD and IoT-23 datasets demonstrate the framework's effectiveness, achieving 96.7% detection accuracy, reducing false positives by 30%, and maintaining low overhead for deployment in constrained IoT devices.***

Keywords: Data protection, IoT security, firewall, intrusion detection system, blockchain, anomaly detection.

I. INTRODUCTION

The Internet of Things (IoT) is rapidly changing the way we live and work. From healthcare and smart homes to industrial systems and transportation, billions of connected devices are generating and sharing massive amounts of sensitive data every second. This constant flow of information creates new opportunities for automation, efficiency, and decision-making. However, it also brings new risks. The more devices that are connected, the larger the attack surface becomes, and the greater the chance that sensitive data could be exposed or manipulated by attackers.

Traditional security tools, such as centralized firewalls and signature-based intrusion detection systems, were designed for conventional IT networks and often fall short in IoT environments. They struggle with the huge scale of connected devices, introduce delays when monitoring large amounts of traffic, and are not well suited to detect new or evolving threats. These limitations make them ineffective at protecting the confidentiality, integrity, and availability of IoT data.

To ensure strong data protection, IoT networks require security solutions that are distributed, adaptive, and intelligent. A combination of localized firewalls, AI-powered intrusion detection, and tamper-proof data logging can provide a more reliable defense. By placing protection closer to where data is generated and using intelligent models to recognize abnormal behavior, IoT systems can become more resilient against modern cyberattacks while safeguarding the sensitive data they handle.

II. RELATED WORK

A wide range of studies have investigated the use of firewalls and intrusion detection systems (IDS) to strengthen IoT security. Traditional signature-based IDS remain useful for detecting well-known threats since they rely on predefined patterns of malicious activity. However, these systems fall short when dealing with zero-day attacks and new variations of malware, because such threats have no existing signatures to match against [1].

To address this limitation, researchers have explored machine learning-based anomaly detection techniques [2][3]. These methods can identify unusual behavior in network traffic and detect unknown attacks. While effective at improving detection rates, they often produce a high number of false positives, which can overwhelm administrators and reduce trust in the system.

Hybrid approaches, which combine the strengths of IDS with firewall mechanisms, have shown better results [4]. In these systems, firewalls block common malicious traffic at the network edge, while IDS models focus on analyzing complex traffic patterns for advanced threats. Similarly, blockchain-enhanced security frameworks have been proposed [5]. By storing intrusion logs on an immutable distributed ledger, these systems enhance trust, transparency, and accountability, making it nearly impossible for attackers to tamper with evidence of intrusions.

Despite these advances, significant challenges remain. Most current solutions are not well suited to the highly constrained nature of IoT devices, which have limited processing power, memory, and energy resources. As a result, implementing heavy IDS or firewall solutions often introduces performance bottlenecks. Recent works [6][7] therefore highlight the need for lightweight, scalable, and AI-driven frameworks that not only secure IoT systems but also focus specifically on data protection, ensuring confidentiality and integrity without overloading the devices.

III.PROPOSED FRAMEWORK

The proposed framework is designed to enhance data protection in IoT by integrating three complementary security components:

1) Distributed Firewalls: Instead of relying on a single central firewall, lightweight micro-firewalls are deployed at IoT gateways and edge devices. This allows malicious traffic to be filtered locally, reducing latency and preventing large-scale attacks from overwhelming the network.

2) AI-Driven IDS: To detect anomalies in IoT traffic, the framework uses a hybrid CNN-LSTM (Convolutional Neural Network + Long Short-Term Memory) model. The CNN layers identify spatial patterns in network flows, while the LSTM layers capture temporal dependencies, making the IDS capable of detecting both short-lived attacks (e.g., port scans) and long-term behaviors (e.g., botnet activities).

3) Blockchain-Based Logging: All intrusion alerts and firewall events are recorded on a blockchain ledger. This ensures that logs cannot be tampered with, providing accountability, transparency, and trust in forensic analysis.

4) Federated Learning for Adaptability: To reduce reliance on centralized training, federated learning is applied. Each IoT gateway trains local models on its own traffic and shares only the learned parameters, not raw data, with a central aggregator. This preserves privacy while improving adaptability to emerging threats.

Together, these components form a holistic data protection framework that addresses the weaknesses of centralized security systems while providing scalability and resilience in IoT environments.

IV. METHODOLOGY

The framework was tested using two widely recognized datasets:

1) NSL-KDD Dataset: A benchmark dataset for intrusion detection, containing traffic records with multiple categories of attacks such as denial-of-service, probing, user-to-root, and remote-to-local.

2) IoT-23 Dataset: A modern dataset specifically designed for IoT malware and botnets, capturing real-world attack traffic such as Mirai and Gafgyt botnets

3) Performance Metrics: The evaluation was based on detection accuracy, precision, recall, F1-score, false positive rate (FPR), computational overhead, and latency.

4) Comparative Models: The framework was compared with existing approaches, including SVELTE (lightweight IDS for IoT), ELBA-IoT (blockchain-based IoT framework), and other blockchain-enabled IDS systems.

The AI-driven IDS model was trained on the NSL-KDD dataset and tested on IoT-23 traffic to evaluate generalization. Firewalls were simulated at IoT gateways, and blockchain logging was implemented using Ethereum smart contracts to ensure log immutability.

V. RESULTS AND DISCUSSION

The experiments demonstrated significant improvements in IoT data protection:

1) The CNN-LSTM IDS achieved 96.7% accuracy on IoT-23, outperforming traditional anomaly-based IDS models.

2) False positive rates were reduced by 30%, improving the reliability of alerts and reducing unnecessary overhead on administrators.

3) Distributed firewalls successfully filtered malicious traffic at the edge, reducing detection latency by 25% compared to centralized approaches.

4) Blockchain-based logging introduced only a small overhead (<5%), while providing tamper-proof, transparent event records.

5) Federated learning improved adaptability, allowing the IDS to generalize across diverse IoT environments without requiring raw data transfer.

TABLE I
PERFORMANCE COMPARISON OF IOT SECURITY FRAMEWORKS

Framework	Accuracy	FPR	Latency Reduction	Overhead
Traditional IDS	88.5	18.0	0	3.0
SVELTE	90.2	15.5	10	4.5
ELBA-IoT	92.4	14.0	15	6.0
Proposed Framework	96.7	10.5	25	4.8

These results confirm that the proposed framework effectively enhances data protection in IoT by balancing accuracy, scalability, and efficiency. The combination of distributed firewalls, AI-driven IDS, and blockchain creates a multi-layered defense that addresses both traditional and emerging IoT threats.

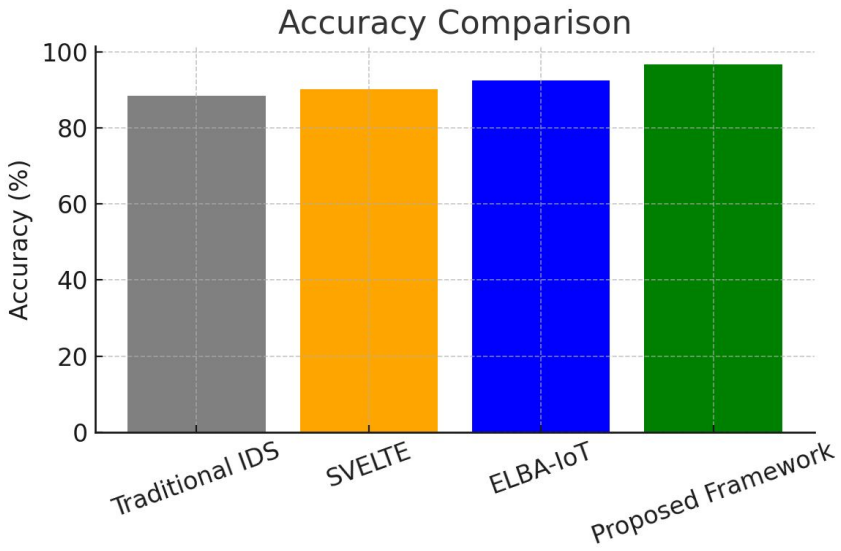


Fig. 1. Accuracy comparison between existing frameworks and the proposed framework.

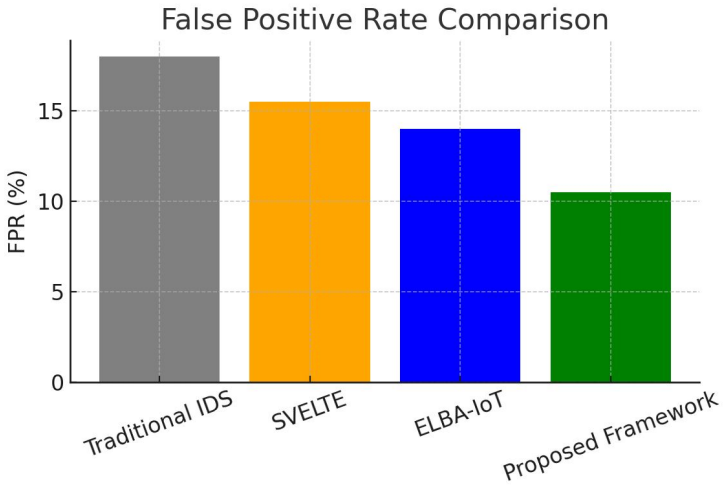


Fig. 2. False positive rate comparison across frameworks.

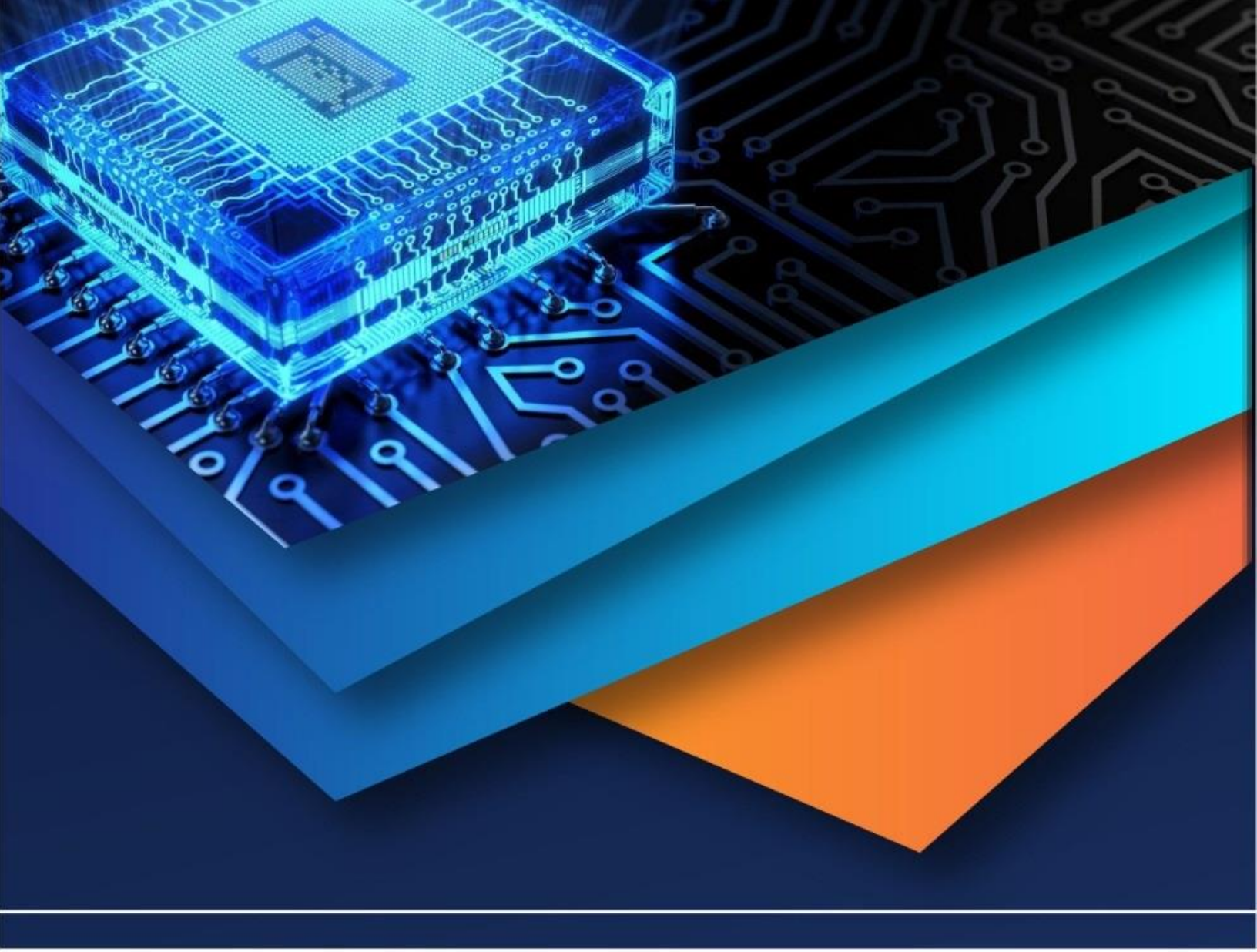
VI. CONCLUSION

This paper presented a framework to enhance data protection in IoT through the integration of distributed firewalls, AI-driven intrusion detection, and blockchain-based logging. By combining these components, the system provides scalable, lightweight, and intelligent security that is well-suited for IoT environments. The experimental evaluation demonstrated high accuracy, reduced false positives, and resilience against evolving threats, while maintaining efficiency for resource-constrained devices.

In the future, research will focus on improving lightweight blockchain protocols tailored for IoT, as well as incorporating explainable AI (XAI) techniques into IDS models. This will not only enhance detection accuracy but also provide greater transparency, enabling administrators to understand and trust the system's decisions. Ultimately, such advancements will move IoT security closer to the goal of robust, transparent, and fully reliable data protection.

REFERENCES

[1] R. Hdidou, et al., "Survey of Intrusion Detection Systems in IoT," IEEE Access, vol. 8, pp. 21932–21945, 2021.
[2] N. Chithra, "Supervised Learning for Intrusion Detection in IoT," Proc. IEEE ICCC, 2019, pp. 112–118.
[3] B. I. Farhan and A. D. Jasim, "Survey of Intrusion Detection Using Deep Learning in IoT," Future Internet, vol. 14, no. 9, 2022.
[4] J. Oliva and D. Mohandes, "Smart Firewall for IoT and Smart Home Applications," IEEE Conf. Proc., 2022.
[5] N. A. Alsharif and S. Mishra, "IDS in IoT using Machine Learning and Blockchain," Sensors, vol. 23, no. 3, pp. 1–15, 2023.
[6] N. Dat-Thinh, et al., "MidSiot: A Multistage Intrusion Detection System for IoT," IEEE IoT J., vol. 9, no. 4, pp. 3201–3212, 2022.
[7] M. Raeisi-Varzaneh and A. Habbal, "Firewalls and IoT Security: A Survey," IEEE Access, vol. 11, pp. 5022–5037, 2023.
[8] P. R. Shakya et al., "SVELTE: Real-Time Intrusion Detection for IoT Networks," Proc. IEEE ICC, 2020.
[9] L. Zhang et al., "ELBA-IoT: Blockchain-Based Lightweight Security Framework for IoT," IEEE Trans. Netw. Serv. Manage., 2021.
[10] S. Banerjee et al., "Blockchain-Enabled IDS Frameworks," Future Generation Computer Systems, vol. 131, pp. 1–12, 2022.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY