Blockchain-Integrated Hybrid Intrusion Detection System for IoT Networks

Sandhya Jaiswal
MTech Scholar
CSE, Department
NIIST, Bhopal
Jaissandhya721@gmail.com

Anurag Shrivastava
Assistant Professor
Department of CSE
NIIST, Bhopal
Anilkumarprajapati1507@gmail.com

Abstract: The rapid proliferation of IoT devices has led to increased vulnerabilities in network infrastructures, making traditional centralized intrusion detection systems (IDS) insufficient to ensure security and data integrity. This study proposes an enhanced blockchain-based IDS framework that combines deep learning techniques with a decentralized ledger to detect and record network intrusions in IoT environments. The proposed system leverages a hybrid approach, integrating a Deep Neural Network (DNN) for accurate anomaly detection and a private blockchain for tamper-proof alert logging. Experimental results on a benchmark IoT intrusion dataset demonstrate significant improvements in detection accuracy, precision, and robustness against tampering. The framework ensures transparency, reliability, and resilience, providing a secure, real-time IDS solution suitable for modern IoT networks, and offering a scalable approach for future smart infrastructures.

Keywords— Blockchain, Intrusion Detection System, Internet of Things, Network Security, Machine Learning, Decentralization, Smart Contracts

I. INTRODUCTION

The rapid advancement and widespread adoption of the Internet of Things (IoT) have transformed modern networks, enabling seamless communication and automation across diverse domains, including healthcare, smart cities, industrial control systems, and home automation. Despite its benefits, the proliferation of IoT devices has introduced significant security challenges, primarily due to the heterogeneity of devices, limited computational resources, and widespread deployment in untrusted environments. IoT networks are highly susceptible to cyber attacks such as Distributed Denial of Service (DDoS), spoofing, and malware propagation, which can compromise the integrity, availability, and confidentiality of critical systems. Conventional centralized intrusion detection systems (IDS) often fail to provide effective protection due to single points of failure, scalability limitations, and susceptibility to tampering or evasion by sophisticated attackers. To address these challenges, integrating blockchain technology with intrusion detection systems (IDS) has emerged as a promising solution. Blockchain's decentralized and tamper-resistant architecture ensures secure storage and verification of network events and alerts, enabling transparent and auditable detection processes. By leveraging a distributed ledger, IoT devices and gateways can collectively validate and record intrusion alerts, thereby eliminating reliance on a centralized authority and mitigating risks associated with compromised nodes. Moreover the combination of blockchain with advanced machine learning (ML) and deep learning (DL) models enhances the accuracy of intrusion detection, allowing real-time classification of normal and anomalous network behaviour with minimal false positives.

This research proposes an enhanced deep learning-based Intrusion Detection System (IDS) framework specifically designed for IoT networks. The proposed framework integrates a hybrid CNN–LSTM architecture, where convolutional layers extract significant spatial features from network traffic data and LSTM layers capture temporal dependencies to effectively detect potential intrusions. Simultaneously, detected alerts are securely logged into a private blockchain, ensuring immutability and accountability. The proposed approach addresses critical concerns such as data integrity, decentralized decision-making, and scalability, which are essential for modern IoT deployments. Additionally, the framework incorporates feature engineering and model optimization techniques to improve detection performance while maintaining efficiency suitable for resource-constrained IoT devices.

Experimental evaluation is conducted using a benchmark IoT intrusion dataset, comparing the proposed blockchain-enabled IDS with traditional centralized ML and DL approaches. The results demonstrate enhanced detection accuracy, precision, and robustness against tampering, highlighting the practical feasibility and effectiveness of the proposed

framework. This study contributes a secure, reliable, and scalable solution for intrusion detection in IoT networks, offering a novel approach that bridges the gap between advanced detection techniques and decentralized data integrity mechanisms.

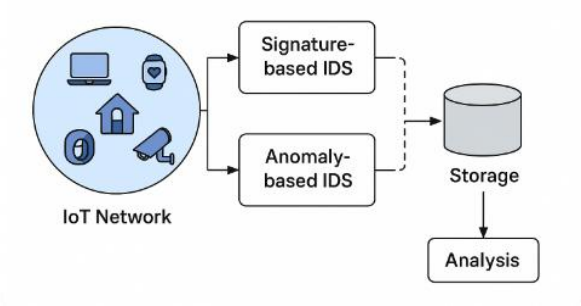

Figure 1. Intrusion Detection in IoT

II. LITRETURE REVIEW

The literature reveals extensive research on intrusion detection systems for IoT networks, focusing on signature-based, anomaly-based, and hybrid approaches. Traditional IDS methods often face limitations related to scalability, centralized trust, and vulnerability to single points of failure. Recent studies highlight the integration of machine learning and deep learning techniques to improve detection accuracy and adaptability to evolving attacks. Blockchain-based IDS frameworks have been proposed to enhance data integrity, decentralization, and secure information sharing among IoT nodes. Despite promising results, challenges such as computational overhead, latency, and real-world deployment constraints remain open research issues.

Author [1] proposes a blockchain-based hybrid intrusion detection system (BC-HyIDS) for secure signature exchange in distributed IoT networks. The framework integrates signature-based and anomaly-based detection with blockchain to enhance data security and trust. Implemented using Hyperledger Fabric v2.0 and Hyperledger Sawtooth, the system employs cryptographic techniques for secure data storage. Experimental results show improved performance in terms of accuracy, detection rate, and reduced false alarm rate, demonstrating the effectiveness of blockchain integration in intrusion detection systems.

This paper Author [2] focuses on conducting a Systematic Literature Review (SLR) on Blockchain-based Intrusion Detection/Prevention Systems in IoT Networks. We reviewed several relevant blockchain-based IDS and IPS proposed for IoT networks and their mechanisms. The most recent research articles, published between 2017 and 2022, were selected from several data.

In this work Authors [3] presents a hybrid intrusion detection approach that integrates machine learning with blockchain to detect cyber threats in resource-constrained IoT environments. The proposed hybrid decision tree (HIDT) model achieves high attack detection accuracy on benchmark datasets while maintaining low false positive and false negative rates. The system enables rapid identification of malicious nodes, reducing network delay and routing overhead. Experimental results demonstrate improved throughput, scalability, and robustness, highlighting the effectiveness of blockchain-enabled intelligent intrusion detection for securing IoT and cyber-physical networks.

Authors [4] addressed the security challenges in Internet of Medical Things (IoMT) networks, highlighting the limitations of traditional security mechanisms in highly dynamic and interconnected environments. The study emphasized that centralized machine learning–based intrusion detection systems suffer from privacy risks and single points of failure. To overcome these issues, the authors explored federated learning to enable privacy-preserving intrusion detection through local model training on end devices. Furthermore, blockchain technology was incorporated to ensure secure and trustworthy collaboration among distributed nodes. The proposed approach demonstrated high intrusion detection accuracy while effectively preserving data privacy in IoMT networks.

Authors [5] proposed a blockchain-based collaborative intrusion detection framework to address the increasing complexity of modern cyber threats. The study highlighted the importance of collaborative intrusion detection systems in improving threat detection and information sharing. To reduce alert collisions during data exchange, an efficient leader node selection mechanism was introduced. Unlike traditional node-level detection approaches, the framework employed an ensemble learning–based collaborative detection strategy, resulting in improved detection precision. Experimental evaluation using benchmark datasets demonstrated that the proposed framework outperformed conventional intrusion detection systems, confirming its effectiveness in enhancing cybersecurity defenses.

Authors [6] proposed a blockchain-enabled intrusion detection model to enhance the security of Internet of Things (IoT) networks by ensuring data integrity, decentralization, and tamper-proof logging. The study integrated blockchain consensus mechanisms with federated-style local training, lightweight cryptography, and SHAP-based explainability to improve both security and interpretability. The proposed framework combined blockchain technology with explainable artificial intelligence to enable transparent and real-time detection of various cyberattacks, including DoS, DDoS, scanning, injection, and backdoor attacks. Performance evaluations demonstrated that the blockchain-enabled IDS outperformed existing approaches, offering a robust, flexible, and interpretable cybersecurity solution for modern IoT environments.

III. PROPOSED METHODOLOGY

This research work proposes a hybrid deep learning-based Intrusion Detection System (IDS) tailored for Internet of Things (IoT) environments. The objective of the proposed methodology is to accurately detect malicious network activities by leveraging both spatial feature extraction and temporal pattern learning. To achieve this, CNN–LSTM architecture is designed, combining the strengths of Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. The CNN component automatically extracts significant traffic-related features, while the LSTM component captures sequential dependencies in network behavior, thereby enhancing detection performance.

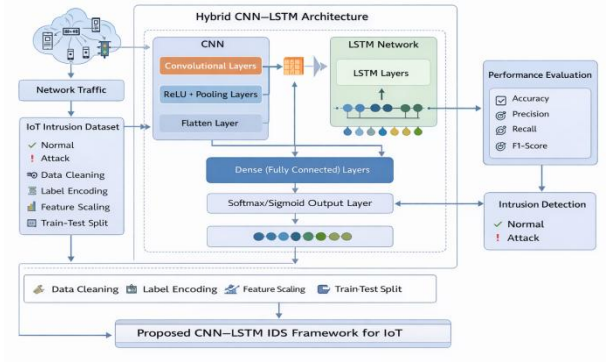

Figure 3.1: Proposed IDS Framework

Initially, the IoT intrusion dataset is collected and subjected to preprocessing to ensure data quality and model stability. Data cleaning techniques are applied to remove missing and redundant records. Categorical labels are encoded into numerical format to make them compatible with the deep learning model. Feature scaling is performed using normalization techniques to ensure uniform distribution and faster convergence during training. The dataset is then divided into training and testing subsets to enable unbiased performance evaluation. Furthermore, the input data is reshaped to match the requirements of the CNN–LSTM architecture.

The proposed hybrid architecture begins with convolutional layers that apply multiple filters to extract local feature patterns from network traffic data. These layers are followed by activation functions and pooling operations to reduce dimensionality and retain essential information. The extracted feature maps are then forwarded to the LSTM layer, which learns long-term dependencies and sequential relationships present in IoT traffic flows. This sequential learning capability allows the model to effectively distinguish between normal and malicious traffic patterns.

Ultimately, fully connected dense layers are employed to perform classification based on the learned feature representations. The output layer utilizes an appropriate activation function (sigmoid or softmax) depending on whether the classification task is binary or multi-class. The model is trained using the Adam optimizer and cross-entropy loss function, ensuring efficient weight updates and convergence. Performance evaluation is conducted using standard metrics including accuracy, precision, recall, F1-score, and confusion matrix analysis.

The integration of CNN for automated feature extraction and LSTM for temporal dependency modeling significantly improves intrusion detection capability compared to traditional machine learning approaches. The proposed methodology provides a robust and scalable solution for securing IoT networks against evolving cyber threats.

IV. RESULTS AND DISCUSSION

The proposed CNN–LSTM-based intrusion detection model was evaluated using the IoT intrusion dataset to assess its effectiveness in detecting malicious network activities. The dataset was divided into training and testing subsets to ensure unbiased evaluation. The model was trained using the Adam optimizer with cross-entropy loss, and performance was measured using standard classification metrics including accuracy, precision, recall, and F1-score.

After training, the proposed model achieved an overall accuracy of 94.1% on the test dataset. The weighted precision, recall, and F1-score were observed to be 0.95, 0.94, and 0.95 respectively, indicating strong classification capability across majority classes. However, due to class imbalance within the dataset, the macro-averaged metrics were comparatively lower, reflecting the challenges in detecting minority attack classes. Despite this imbalance, the confusion matrix analysis demonstrates that the model effectively distinguishes between benign and malicious traffic with minimal misclassification.

Table 4.1: Performance Comparison with Existing Methods

Model	Accuracy (%)	Precision	Recall	F1-Score
LSTM	92.3	0.93	0.91	0.92
Proposed CNN–LSTM	94.1	0.95	0.94	0.95

The integration of convolutional layers enabled efficient extraction of discriminative spatial features from network traffic data, while the LSTM layer successfully captured temporal dependencies within traffic flows. This hybrid architecture significantly improved detection performance compared to traditional machine learning models and standalone deep learning

approaches. To further validate the effectiveness of the proposed framework, its performance was compared with existing machine learning and deep learning-based intrusion detection approaches reported in prior studies. The comparative results are presented in Table 4.1. A lightweight blockchain mechanism was integrated to securely store detected intrusion events. Each detected attack is recorded as a block containing timestamp, prediction label, confidence score, and cryptographic hash. This ensures tamper-resistant logging and enhances trust in IoT security monitoring systems.

CONCLUSION

This research study presented a hybrid CNN–LSTM-based intrusion detection framework designed for securing IoT networks against diverse cyber threats. By combining convolutional layers for automated feature extraction with LSTM networks for temporal dependency learning, the proposed model effectively captured complex traffic patterns. Experimental evaluation demonstrated superior performance compared to traditional machine learning and standalone deep learning models, achieving high accuracy and F1-score. The results confirm that hybrid deep learning architectures significantly enhance detection capability in imbalanced IoT datasets. Future work will focus on improving minority class detection, optimizing computational efficiency, and implementing the model in real-time IoT environments.

REFERENCES

[1] S. R. Khonde et. al. “Hybrid intrusion detection system using blockchain framework” Khonde and Ulagamuthalvi J Wireless Com Network (2022) 2022:58 https://doi.org/10.1186/s13638-022-02089-4

[2]Khawla Shalabi et. al “A Blockchain-based Intrusion Detection/Prevention” ScienceDirect, Procedia Computer Science 236 (2024) 410–419

[3] Shailendra Mishra et. al. “Blockchain and Machine Learning-Based Hybrid IDS to Protect Smart Networks and Preserve Privacy” https://doi.org/10.3390/ electronics12163524

[4] Khadija Begum et. al. “BFLIDS: Blockchain-Driven Federated Learning for Intrusion Detection in IoMT Networks” Blockchain-Driven Federated Learning for Intrusion Detection in IoMT Networks. Sensors 2024 https://doi.org/10.3390/ s24144591, MPDI 2024

[5] Jiachen Huang et. al. “Optimization Scheme of Collaborative Intrusion Detection System Based on Blockchain Technology” Electronics 2025, 14, 261 https://doi.org/10.3390/electronics14020261

[6] Atul Kumar1, et. al. “Secure blockchain based intrusion detection for IoT networks” Kumar et al. Discover Computing (2025) 28:226, https://doi.org/10.1007/s10791-025-09754-4 Discover 2025

[7] Shailender Kumar Vats et. al. “Securing Distributed Blockchain Ledgers: An Intrusion Detection System Powered by Advanced Smart Contracts for Enhanced Cloud-Based Big Data Storage” International Journal of Intelligent Systems and Applications in Engineering IJISAE, 2024, 12(3), 901–909

[8] Chakir O, Sadqi Y, Abdellaoui Alaoui EA. An explainable machine learning-based web attack detection system for industrial IoT web application security. Inform Secur J Glob Perspect. 2024; 1–27.

[9] Awad M, Fraihat S, Salameh K, Redhaei A, A. Examining the suitability of netflow features in detecting IoT network intrusions. Sensors. 2022;22(16):6164.

[10] Swain PK, Pattnaik LM, Satpathy S. IoT applications and cyber threats: mitigation strategies for a secure future. In: Explainable IoT applications: A demystification. Cham: Springer Nature Switzerland; 2025. p. 403–28.

[11] Abed-alguni BH, Alzboun BM, Alawad NA. BOC-PDO: an intrusion detection model using binary opposition cellular prairie dog optimization algorithm. Cluster Comput. 2024;27(10):14417–49.

[12] Doriguzzi-Corin R, Knob LAD, Mendozzi L, Siracusa D, Savi M. Introducing packet-level analysis in programmable data planes to advance network intrusion detection. Comput Networks. 2024;239:110162.

[13] Batchu RK, Bikku T, Thota S, Seetha H, Ayoade AA. A novel optimization-driven deep learning model for the detection of DDoS attacks. Sci Rep. 2024;14(1):28024.

[14] Le TTH, Kim H, Kang H, Kim H. Classification and explanation for intrusion detection system based on ensemble trees and SHAP method. Sensors. 2022;22(3):1154.

[15] Muna RK, Hossain MI, Alam MGR, Hassan MM, Ianni M, Fortino G. Demystifying machine learning models of massive IoT attack detection with explainable AI for sustainable and secure future smart cities. Internet of Things. 2023;24:100919.

[16] Fraihat S, Makhadmeh S, Awad M, Al-Betar MA, Al-Redhaei A. Intrusion detection system for large-scale IoT netflow networks using machine learning with modified arithmetic optimization algorithm. Internet of Things. 2023;22:100819.