

An Intelligent Framework for Secure IoT Communication Using Machine Learning-Based Intrusion Detection and Blockchain Authentication

Assistant Prof. Kaustav Samal

Department of Computer Science and Engineering
Gandhi Institute For Technology (GIFT), Bhubaneswar, Odisha, India

Abstract - The exponential growth of Internet of Things (IoT) devices has introduced significant security challenges due to resource constraints and heterogeneous communication protocols. Traditional security mechanisms are inadequate to handle sophisticated cyber-attacks such as Distributed Denial of Service (DDoS), spoofing, and data tampering in IoT networks. This paper proposes a novel hybrid framework that integrates Machine Learning-based Intrusion Detection System (ML-IDS) with Blockchain-based authentication to enhance security, integrity, and scalability in IoT communication. The ML-IDS module employs Random Forest and Deep Neural Network classifiers trained on the UNSW-NB15 and IoT-23 datasets to detect anomalous traffic with 98.2% accuracy. Simultaneously, a lightweight blockchain consensus mechanism ensures decentralized device authentication and tamper-proof data logging. Experimental results demonstrate that the proposed framework reduces detection latency by 32% and improves throughput by 18% compared to existing approaches, while maintaining low computational overhead suitable for edge devices. The framework provides a robust solution for secure IoT deployments in smart cities, healthcare, and industrial automation.

Keywords: IoT Security, Intrusion Detection System, Machine Learning, Blockchain, Smart Devices, Cybersecurity, Edge Computing

1. INTRODUCTION

The Internet of Things (IoT) has revolutionized modern computing by interconnecting billions of heterogeneous devices that collect, process, and exchange data without human intervention. According to recent estimates, over 30 billion IoT devices are expected to be active by 2027, spanning domains such as smart homes, healthcare, industrial IoT (IIoT), and intelligent transportation systems. However, this rapid proliferation has exposed critical security vulnerabilities. Most IoT devices are resource-constrained in terms of processing power, memory, and energy, making them unsuitable for conventional cryptographic and security protocols.

Cyber-attacks targeting IoT networks have increased by 300% in the last three years, with attacks like Mirai botnet, DDoS, and ransomware causing severe disruptions. Existing solutions such as traditional Intrusion Detection Systems (IDS) suffer from high false-positive rates and lack adaptability to zero-day attacks. Blockchain technology, with its decentralized and immutable ledger, offers promising potential for secure authentication, but its high computational cost limits direct adoption in IoT.

To address these challenges, this paper presents a hybrid framework combining Machine Learning-based IDS and lightweight blockchain authentication. The major contributions of this work are:

- Design of a two-tier security framework for IoT networks.
- Implementation of an optimized ML-IDS using Random Forest and DNN for real-time anomaly detection.
- Development of a lightweight blockchain-based device authentication mechanism using Proof-of-Authority (PoA).
- Performance evaluation on real-world IoT datasets demonstrating improved accuracy and efficiency.

2. LITERATURE REVIEW

Several researchers have proposed security solutions for IoT networks. Zhang et al. (2022) proposed a deep learning-based IDS using CNN-LSTM achieving 96.5% accuracy on NSL-KDD dataset, but the model was computationally intensive for edge devices. Kumar and Singh (2023) introduced a blockchain-based access control framework that ensures data integrity but suffers from high latency due to Proof-of-Work consensus.

Al-Garadi et al. (2021) surveyed ML techniques for IoT security and highlighted the effectiveness of ensemble learning methods like Random Forest for anomaly detection. S. Roy et al. (2023) proposed a lightweight authentication protocol using ECC, which reduced overhead but failed to address insider attacks.

Recent works by Li et al. (2024) combined federated learning with blockchain for privacy-preserving IDS, showing improved scalability. However, gaps remain in integrating real-time detection with decentralized trust management without compromising resource constraints. Our work bridges this gap by proposing a hybrid, lightweight, and scalable framework.

3. PROPOSED METHODOLOGY

The proposed architecture consists of three layers: Perception Layer, Edge Security Layer, and Application Layer.

3.1 System Architecture

1. Perception Layer: Comprises IoT sensors and devices collecting environmental data.
2. Edge Security Layer: Core of the framework containing two modules:
 - a) ML-IDS Module: Captures network traffic, extracts 42 features (flow duration, packet size, protocol type, etc.), and classifies traffic as benign or malicious using trained models.
 - b) Blockchain Authentication Module: Each device is registered with a unique cryptographic identity stored on a private blockchain. PoA consensus is used to validate transactions with minimal energy consumption.
3. Application Layer: Provides secure data visualization and alert management for end users.

3.2 Machine Learning-based IDS

Data preprocessing includes normalization, missing value imputation, and feature selection using Information Gain. We evaluated multiple classifiers: Support Vector Machine (SVM), Random Forest (RF), and Deep Neural Network (DNN with 3 hidden layers). RF with 100 estimators and DNN with ReLU activation achieved best performance. The model is deployed at edge gateways to enable low-latency detection. If anomaly score > threshold (0.85), traffic is blocked and logged into blockchain.

3.3 Blockchain Authentication

We implement a private Ethereum blockchain with PoA consensus. Smart contracts handle device registration, authentication, and revocation. Each data packet is hashed (SHA-256) and its hash is stored on-chain, ensuring data integrity without storing entire payload on-chain, thus saving storage. The lightweight design reduces block time to 2.5 seconds and energy consumption by 60% compared to PoW.

4. EXPERIMENTAL SETUP AND RESULTS

Implementation was carried out on Ubuntu 20.04 with Python 3.9, TensorFlow 2.8, and Scikit-learn. Datasets used: UNSW-NB15 and IoT-23. Hardware: Intel i7, 16GB RAM, and Raspberry Pi 4 as edge node simulation.

Performance Metrics:

- Random Forest Accuracy: 97.4%, Precision: 96.8%, Recall: 97.9%, F1-Score: 97.3%
- DNN Accuracy: 98.2%, Precision: 98.0%, Recall: 98.5%, F1-Score: 98.2%
- Detection Latency: 45ms (proposed) vs 66ms (traditional IDS)
- Throughput: 1240 packets/sec vs 1050 packets/sec baseline
- False Positive Rate: Reduced to 1.8%

The blockchain module achieved authentication time of 120ms per device and handled 500 concurrent devices with 98% success rate. Energy consumption on Raspberry Pi was only 3.2W average.

5. DISCUSSION

The results confirm that hybrid integration provides both proactive detection and preventive authentication. Unlike standalone IDS, blockchain logging prevents log tampering and provides auditability. The use of PoA instead of PoW makes the solution viable for resource-constrained environments. However, scalability beyond 1000 devices requires sharding techniques, which will be explored in future work.

6. CONCLUSION AND FUTURE WORK

This paper presented a secure and efficient framework for IoT communication leveraging ML-based IDS and blockchain authentication. The framework achieves high detection accuracy, low latency, and decentralized trust. Future work will focus on integrating Federated Learning for privacy-preserving model training across edge nodes, implementing blockchain sharding for large-scale deployments, and testing on real-time IIoT testbeds at GIFT Bhubaneswar.

The proposed solution can be extended to smart healthcare, smart grids, and autonomous vehicles where security is paramount.

7. REFERENCES

- [1] Al-Garadi, M.A., et al. (2021). A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. IEEE Communications Surveys & Tutorials.
- [2] Zhang, Y., et al. (2022). Deep Learning-based Intrusion Detection for IoT Networks. IEEE IoT Journal, 9(12), 10200-10211.
- [3] Kumar, R., & Singh, S. (2023). Blockchain-based Secure Access Control for IoT. Future Generation Computer Systems.
- [4] Li, X., et al. (2024). Federated Learning and Blockchain for Secure IoT. ACM Computing Surveys.
- [5] Roy, S., et al. (2023). Lightweight ECC-based Authentication for IoT. Journal of Network and Computer Applications.
- [6] UNSW-NB15 Dataset, <https://research.unsw.edu.au/projects/unsw-nb15-dataset>
- [7] IoT-23 Dataset, Stratosphere Laboratory, <https://www.stratosphereips.org/datasets-iot23>
- [8] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

ACKNOWLEDGEMENT

The author would like to thank the Department of Computer Science and Engineering, GIFT Bhubaneswar for providing research facilities and support.