Iot Security Using Blockchain and Machine Learning

Vandana Dixit[1], Amritesh Bhoyar[2], Adish Gujarathi[3], Rushikesh Thakre[4], Himanish More[5]
[1]*Professor, Department of Information Technology, Progressive Education Society's Modern College of Engineering, Pune, India*
[2,3,4,5]*Department of Information Technology, Progressive Education Society's Modern College of Engineering, Pune, India*

***Abstract*—The rapid expansion of the Internet of Things (IoT) has introduced severe security vulnerabilities due to its reliance on centralized architectures and resource-constrained devices. To address these limitations, this paper proposes a hybrid, lightweight framework converging Blockchain and Machine Learning (ML) to inherently secure IoT ecosystems. The system employs an Ethereum-based distributed ledger (via Smart Contracts) to ensure immutable data logging and decentralized access control. Simultaneously, an edge-based ML engine utilizes Isolation Forests for real-time, multidimensional anomaly detection against sensor deviations and power-profiling cyber-attacks. By linking this ML-based intrusion detection directly with a blockchain-driven dynamic device trust scoring mechanism, the framework establishes an automated, self-healing network. Experimental simulations establish that this integrated approach successfully mitigates data tampering and Sybil attacks with minimal edge computational overhead, delivering a robust, scalable, and decentralized security architecture suitable for modern IoT deployments.**

***Index Terms*—Internet of Things (IoT), Blockchain, Machine Learning, Edge Computing, Anomaly Detection, Dynamic Trust Evaluation, Security Framework.**

I. INTRODUCTION

The Internet of Things (IoT) has fundamentally transformed the digital landscape by enabling physical objects to connect, collect, and exchange data autonomously. From smart home ecosystems to Industrial IoT (IIoT) pipelines, these networks provide unprecedented conveniences and operational efficiencies [1]. However, the proliferation of low-power, heterogeneous IoT devices has surfaced severe security vulnerabilities. Traditional IoT architectures rely heavily on centralized cloud servers for data processing, authentication, and access control. This centralized dependency not only creates a single point of failure but also introduces significant latency and exposes massive volumes of sensitive telemetry data to sophisticated cyber-attacks, such as Distributed Denial of Service (DDoS) and unauthorized data tampering [2].

Furthermore, typical IoT devices (e.g., ESP32, ESP8266 microcontrollers) possess severe constraints in processing power, memory, and battery life, making it computationally infeasible to run heavyweight cryptographic algorithms or complex intrusion detection systems (IDS) directly on the edge nodes [3]. Consequently, securing IoT networks requires a paradigm shift towards lightweight, decentralized, and intelligent security frameworks.

To address these challenges, the convergence of Machine Learning (ML) and Blockchain technology has emerged as a state-of-the-art solution [4]. Machine Learning offers the capability to intelligently analyse massive, high-velocity data streams to identify anomalies and zero-day threats in real-time. Simultaneously, Blockchain provides a decentralized, immutable ledger that guarantees data integrity, secure peer-to-peer communication, and transparent auditability without reliance on a central authority [5].

This research proposes a novel, hybrid 8-layer architecture that integrates Edge Computing, Machine Learning, and a Blockchain-based smart contract to secure IoT sensor networks. The core contributions of this paper are:

1. Lightweight Edge Validation: The implementation of an edge-gateway service that offloads heavy processing from resource-

constrained nodes, providing robust replay-attack protection and schema validation.
2. Behavioural Threat Detection: A robust ML engine utilizing Isolation Forests for zero-latency anomaly detection, encompassing sensor anomalies, power-profiling (e.g., detecting crypto-mining botnets), and behavioural checks.
3. Dynamic Trust Evaluation: A decentralized smart contract layer that maintains an immutable audit trail and dynamically adjusts device trust scores based on ML insights, autonomously revoking access for compromised nodes.

II. PROBLEM STATEMENT

The increasing dependence on IoT systems in critical infrastructures has created major security challenges due to the heterogeneous and insecure nature of IoT ecosystems. Traditional IoT architectures are mostly centralized and vulnerable to attacks targeting cloud servers, gateways, and communication channels. Additionally, IoT devices often have limited computational power, memory, storage, and battery capacity, making it difficult to implement heavyweight cryptographic techniques and conventional intrusion detection systems.

Centralized IoT infrastructures also create single points of failure, where attacks or server downtime can disrupt the entire network. These systems are more vulnerable to threats such as Distributed Denial of Service (DDoS) attacks, malware injections, replay attacks, unauthorized access, and data tampering. Existing rule-based security mechanisms are often ineffective against advanced threats like botnets, stealth malware, and zero-day attacks, which require intelligent and adaptive detection methods.

As IoT applications continue to expand across smart homes, healthcare, industrial automation, and smart cities, there is a growing need for a decentralized, scalable, lightweight, and intelligent security framework. Therefore, this research proposes a hybrid architecture integrating Blockchain, Machine Learning, and Edge Computing to enable secure communication, real-time threat detection, automated trust management, and immutable data storage in IoT environments.

III. OBJECTIVES

To realize this proposed framework, the project is guided by the following core objectives:

1. To study and analyse existing IoT security challenges and the limitations inherent in centralized cloud infrastructures.
2. To design a hybrid architecture integrating blockchain and machine learning for secure, low-latency IoT communication.
3. To develop an Ethereum-based blockchain ledger that ensures tamper-proof data storage and decentralized validation of device transactions.
4. To implement machine learning algorithms (specifically Isolation Forests) for real-time anomaly, power-profiling, and intrusion detection in multidimensional IoT data streams.
5. To evaluate the integrated system's performance, latency, and operational efficiency under simulated adversarial IoT environments.
6. To establish a scalable foundation for lightweight, intelligent, and distributed trust-management frameworks in future IoT deployments.

IV. LITERATURE SURVEY

The convergence of Internet of Things (IoT), blockchain, and machine learning (ML) has gained significant attention for securing large-scale, resource-constrained, and heterogeneous device environments. Blockchain provides decentralization, immutability, and auditability, while ML enables intelligent detection of anomalies and malicious behaviour. Together, they address critical IoT security challenges. A broad overview is presented in IoT Convergence with Machine Learning & Blockchain [1], which highlights integration approaches and trade-offs, especially between blockchain's computational overhead and IoT's limited resources. It suggests hybrid architectures where raw data remains off-chain while blockchain stores hashes and alerts.

To address resource constraints, Towards a Lightweight Security Framework [2] proposes a model where IoT devices act as light clients, offloading heavy blockchain tasks to edge nodes, supported by ML-assisted consensus for efficiency.

Focusing on data security, Machine Learning Based Data Security Model [3] combines ML-based threat detection with blockchain to ensure secure data

transmission, improving confidentiality, integrity, and availability.

In trust management, Blockchain-Driven Dynamic Trust Evaluation [4] introduces a system that assigns trust scores to IoT devices based on behaviour, enabling adaptive response to compromised nodes.

Finally, IDS in IoT Using Machine Learning and Blockchain [5] presents an intrusion detection system where ML detects attacks and blockchain securely logs alerts, improving accountability while highlighting challenges like storage and latency.

While existing literature establishes the undeniable value of lightweight blockchain deployment and ML integration, previous works largely remain limited to specific, isolated applications. Studies either focus exclusively on network-level Intrusion Detection Systems (IDS) or solely on static trust scoring models. There is a notable absence of holistic, end-to-end architectures that comprehensively integrate multi-dimensional ML analysis (spanning power consumption, sensor anomalies, and device behaviour) with a reactive, blockchain-driven dynamic quarantine system.

This project directly addresses the identified research gap by establishing a fully integrated, multi-layered framework. By combining edge-gateway validation, multidimensional ML anomaly detection, and blockchain-driven dynamic trust evaluation into a single, unified architecture, this project delivers a scalable, highly secure solution designed specifically for resource-constrained IoT environments.

V. PROPOSED SYSTEM ARCHITECTURE

To address the challenges identified in traditional, centralized IoT deployments, this research proposes a hybrid 8-tier architectural framework. The system integrates intelligent edge computing, real-time machine learning analysis, and an immutable blockchain ledger to create a secure, self-regulating ecosystem.

System Architecture Outline:

1. Physical Device Layer: Comprises resource-constrained sensors (e.g., ESP32, ESP8266) responsible for gathering telemetry data (temperature, humidity, motion, and system power metrics).
2. Local Communication Layer: Employs the Message Queuing Telemetry Transport (MQTT) protocol, secured via TLS encryption (Port 8883), ensuring resilient, encrypted transmission against local network sniffing.
3. Edge Validation Server (Gateway): Before data reaches the central cloud, a local gateway (Raspberry Pi) buffers the MQTT streams. The gateway performs critical security pre-checks: schema validation, cryptographic payload verification, and sequence number tracking to inherently block replay-attacks. Validated packets are batched, hashed (SHA-256), and forwarded via HTTPS.
4. Central Orchestration Server: A centralized backend (Node.js/Express) protected by JSON Web Tokens (JWT) and rate-limiting modules. It authenticates edge gateways, manages real-time socket connections for the presentation layer, and delegates security verification to the ML and Blockchain counterparts.
5. Machine Learning Threat Analysis: A continuous analysis engine utilizing Isolation Forest algorithms. By offloading this computation from the sensors to the central processing tier, the system accurately classifies incoming telemetry into Normal, Sensor Anomaly, Power Anomaly (e.g., crypto-mining or DDoS botnet signatures), or Behavioural Security Threats (e.g., unusual nighttime access).
6. Blockchain Immutable Ledger: A Smart Contract layer executing on an Ethereum-compatible network (Ganache) that maintains a tamper-proof "Cyber Incident Record System."
7. Dynamic Trust Evaluation Protocol: The Smart Contract maintains a fluid trust score (0-100) for every registered device. Malicious payloads detected by the Edge Gateway or ML engine trigger automatic penalizations. If a device's trust score drops below a minimal operational threshold, the blockchain contract autonomously blocks any remote-control commands directed at that device.
8. Real-time Visualization Dashboard: A React-based Single Page Application (SPA) offering millisecond-latency alerts, historical threat analytics, and a direct interface for verifying on-chain event hashes.

VI. SYSTEM WORKFLOW

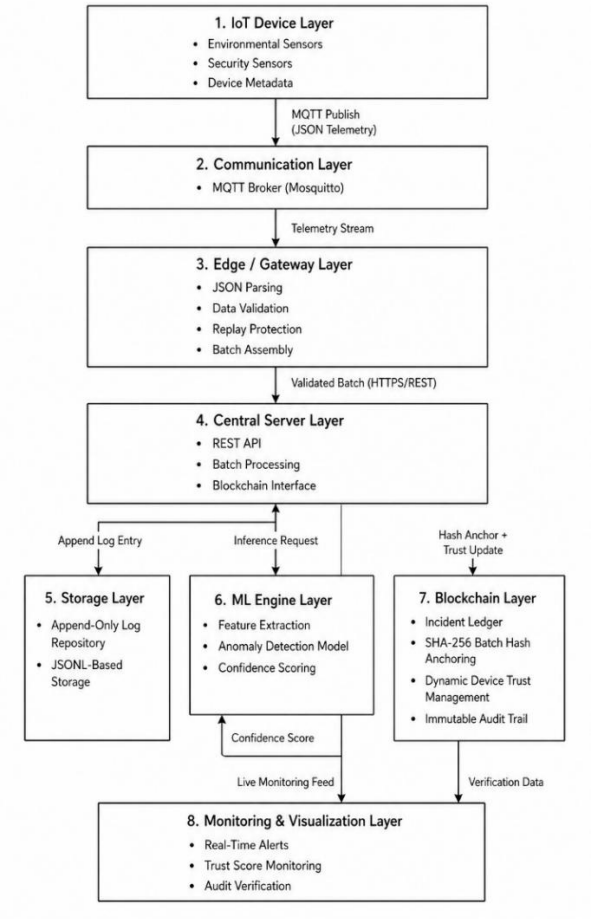
The complete workflow of the proposed system is as follows:

1. IoT sensors collect environmental and system data.
2. Data packets are transmitted securely through MQTT.
3. The edge gateway validates incoming packets.
4. Valid packets are forwarded to the orchestration server.
5. The ML engine analyzes telemetry data for anomalies.
6. If malicious activity is detected:
7. Alerts are generated.

- Blockchain records are updated.
- Device trust scores are reduced.

8. Devices with low trust scores are automatically quarantined.
9. Dashboard notifications are displayed in real time.

This workflow establishes a self-healing security architecture.



VII. THREAT DETECTION MECHANISM

The proposed framework uses a multidimensional threat detection mechanism to identify various cyber-attacks in IoT environments. Unlike traditional rule-based systems, it combines Machine Learning and behavioural analysis to detect both known and unknown threats in real time.

One major threat addressed is replay attacks, where attackers capture and retransmit legitimate packets to manipulate devices or gain unauthorized access. The Edge Validation Gateway mitigates this through sequence tracking, timestamp verification, and payload integrity checks, rejecting duplicated or suspicious packets.

The framework also performs sensor anomaly detection using the Isolation Forest algorithm. By analysing telemetry data, the system can identify abnormal readings such as unrealistic temperature changes, unusual humidity levels, or inconsistent motion patterns that may indicate cyber intrusion or device malfunction.

In addition, the framework monitors power consumption and resource usage to detect crypto-mining malware, botnet activity, and other malicious behaviour that causes abnormal CPU or energy usage. Behavioural analysis further strengthens security by examining communication frequency, access timing, and device interaction patterns to identify suspicious activities.

To mitigate Sybil attacks, the framework uses blockchain-based trust management with immutable device identities and dynamic trust scores, preventing unauthorized or fake nodes from participating in the network.

Overall, the integration of Machine Learning, Edge Computing, and Blockchain creates a proactive, adaptive, and intelligent security framework for protecting IoT environments against evolving cyber threats.

VIII. IMPLEMENTATION SETUP

Hardware Specification:

1. Sensor Nodes: ESP32 and ESP8266 Wi-Fi microcontrollers flashed with custom C++ (Arduino Core) firmware, utilizing WiFiClientSecure for TLS MQTT publishing.

2. Edge Gateway: A Raspberry Pi 4 Model B (2GB RAM) acting as the local base station. It hosts the Mosquitto MQTT Broker and a Python-based Gateway service.
3. Central Infrastructure: A standard computing server (Intel i7, 16GB RAM) hosting the Blockchain testnet, ML Engine, and Web Application securely.

Software Stack and Technologies

1. Data Transport: Eclipse Mosquitto (MQTT) configured with CA certificates.
2. Backend & ML: The gateway and ML engines are implemented in Python (Flask) using scikit-learn for the Isolation Forest training blocks and pandas for data manipulation. The primary orchestration API is built on Node.js utilizing Express.js.
3. Blockchain Network: The decentralized ledger is simulated using the Ganache local Ethereum workspace. The smart contract, DeviceLog.sol, is developed in Solidity (v0.8.0) and interacts with the Python backend via Web3.py RPC calls.
4. Presentation Layer: A dynamic dashboard built using React and Vite, featuring WebSockets (Socket.IO) for immediate threat visualization and Recharts for analytical graphing.

IX. ADVANTAGES OF PROPOSED SOLUTION

The hybrid integration of edge computing, machine learning, and blockchain in this proposed architecture offers several distinct advantages over traditional IoT security models:

1. Decentralized Trust and Immutability: By anchoring security logs and device trust scores to an Ethereum-based smart contract, the system eliminates the single point of failure inherent in centralized databases. Audit trails are mathematically verifiable and tamper-proof.
2. Zero-Latency Threat Mitigation: Unlike traditional cloud-based ML pipelines that suffer from round-trip latency, the local ML engine combined with the edge gateway allows the system to detect and quarantine compromised nodes within milliseconds before lateral movement can occur.
3. Resource Efficiency (Lightweight Design): By offloading heavy cryptographic validation and ML inference to the Raspberry Pi and Central Node.js Server, the constrained ESP32 and ESP8266 battery-powered nodes are freed to focus strictly on efficient MQTT telemetry transmission.
4. Automated Self-Healing: The system transcends passive alert generation; the Dynamic Trust Evaluation protocol on the blockchain autonomously revokes permissions for malicious nodes without requiring human administrative intervention.
5. Multi-Dimensional Threat Coverage: By fusing sensor anomaly detection with power-profiling and behavioral rules (via Isolation Forests), the system catches sophisticated threats like stealth crypto-mining malware and Sybil attacks that simple threshold-based alarms miss.

X. LIMITATIONS AND FUTURE SCOPE

1. Blockchain transaction costs and scalability issues may arise in large IoT deployments.
2. The accuracy of the Isolation Forest algorithm depends on the quality of training datasets.
3. Edge devices still require moderate computational resources for real-time threat detection.
4. Real-world implementation and integration of the framework can be complex.
5. Future improvements may include Federated Learning, lightweight blockchain technologies such as IOTA, and AI-driven adaptive threat intelligence.
6. The framework can also be expanded for 5G-enabled IoT, smart cities, healthcare IoT, and Industrial IoT (IIoT) environments.

XI. CONCLUSION

This project successfully designed and implemented a highly secure, hybrid IoT framework by converging the intelligent threat detection capabilities of Machine Learning with the decentralized trust management of Blockchain. The system effectively addressed the limitations inherent to centralized cloud dependency by introducing edge-based gateway validation, reducing the computational burden on resource-constrained IoT nodes.

The integration of an Isolation Forest algorithm permitted the accurate, real-time detection of multidimensional anomalies without requiring heavy, supervised deep learning architectures at the edge. Concurrently, the Blockchain ledger ensured that all intercepted telemetric data and resulting administrative actions remained immutable and transparent. Through its Dynamic Trust Evaluation mechanism, the framework not only detected threats but reacted autonomously to quarantine compromised network segments.

Ultimately, this integrated approach provides a robust, scalable foundation for securing future IoT deployments across smart homes, healthcare, and industrial automation. Future work may explore transitioning the Ethereum-based test net to highly scalable Directed Acyclic Graph (DAG) protocols (such as IOTA) and integrating federated learning to preserve data privacy across multiple distinct edge clusters.

REFERENCES

[1] "IoT Convergence with Machine Learning & Blockchain", Discover Internet of Things, vol. 6, 2024. [ScienceDirect, Article: S2542660524001288].

[2] Shereen Ismail, Muhammad Nouman, Diana W. Dawoud, Hassan Reza "Towards a lightweight security framework using blockchain and machine learning for IoT sensor networks", Journal of Information Security and Applications, vol. 75, 2024. [ScienceDirect, Article: S2096720923000490].

[3] Smitha Chowdary Ch, Srilakshmi Puli, Lakshmi Viveka K, M.V.B.T.Santhi, "Machine Learning Based Data Security Model Using Blockchain for Secure Data Transmission in IoT".

[4] MRagul∗, A Aloysius, V Arulkumar, "Advancing IoT Security through Blockchain-Driven Dynamic Trust Evaluation", Indian Journal of Science and Technology, Feb. 2025. [indjst.org].

[5] N. A. Alsharif, S. Mishra, and M. Alshehri, "IDS in IoT using Machine Learning and Blockchain," Engineering, Technology & Applied Science Research, vol. 13, no. 4, pp. 11197–11203, Aug. 2023. DOI: https://doi.org/10.48084/etasr.5992