Journal of Information Technology and Digital World (ISSN: 2582-418X)
www.irojournals.com/itdw/

Blockchain-Integrated Machine Learning Models for Secured IoT Data Sharing and Authentication

Banu Priya R.[1], Ganesh Kumar G.[2*]

[1]Research Scholar, Department of Computer Science and Engineering, School of engineering Dayananda Sagar University, Bengaluru, Karnataka, India.
[2]Associate Professor, Department of Computer Science and Engineering, Nehru Institute of Technology, Coimbatore, India.

E-mail: [1]banupriya.r-rs-cse@dsu.edu.in, [2*]gkumarcse@gmail.com

Abstract

The continuous growth of Internet of Things (IoT) devices has increased the demand for secure, scalable, efficient data sharing and authentication. Existing centralized architectures are increasingly exposed to cyber intrusions, data tampering, uncontrolled data breaches, and single points of failure. This research introduces BcML-IoT, an integrated framework for secure and intelligent IoT data exchange that incorporates blockchain technology and Machine Learning (ML) approaches to address these challenges. While blockchain actively serves as a decentralized, immutable log of activities with transparent transaction validation, ML can add an extra layer of security by providing better anomaly detection, device authentication, and applying secure and privileged access control through predictive analytics to identify potential rogue devices. Smart contracts can be used to automate the authentication process, and next-generation, lightweight consensus mechanisms help to reduce energy consumption and latency. The experimental evaluations show that BcML-IoT supports a high throughput of 85-87 Transactions Per Second (TPS), and unique block confirmation times under 4 seconds for up to 1,000 devices. When compared with traditional classifiers, ML-based anomaly detection can achieve 96.2% and 94.7% accuracy using XGBoost and LSTM respectively. BcML-IoT will detect all spoofing and replay attacks (100% detection), as well as 99.7% of data modification

*** Corresponding Author**

DOI: https://doi.org/10.36548/jitdw.2025.4.004
Received: 28.11.2025, received in revised form: 27.12.2025, accepted: 10.01.2026, published: 22.01.2026

attacks with a FAR of 0.3%. The results show that BcML-IoT is low-latency, robust and secure for real-time IoT environments. It also provides strategies for developing decentralized, resilient and intelligent IoT ecosystems.

Keywords: Blockchain, Internet of Things (IoT), Machine Learning, Secure Data Sharing, Authentication, Smart Contracts, Decentralized Architecture, Anomaly Detection, Access Control, Edge Computing.

1. Introduction

The Internet of Things (IoT) transforms industries by allowing over 20 billion devices to communicate and share data. The increasing number of IoT devices affects data privacy, secure sharing and effective authentication due to data decentralization and device resource limitations [1]. Centralized security systems proved insufficient to meet the requirement for scalability and dynamic trust in these massively scaled IoT ecosystems [2].

Although machine learning methods may be effective in identifying anomalous behavior and unauthorized practices in IoT networks, they are not adequate to ensure trust, integrity, and accountability in large-scale and heterogeneous IoT networks. Conventional centralized IoT security models present single points of vulnerability and are based on implicit trust assumptions, which can be spoofed, data corrupted, and suffer from insider attacks.

This study uses the blockchain as a decentralized trust and control layer rather than a data processing or storage system. It defines the registry by enabling verified device authentication, secure recording of data access events, and tracking security actions. Smart contracts also translate machine learning-based anomaly detection results into effective access control actions. This combination ensures that security decisions remain smart, trustworthy, transparent and resistant to alteration, making blockchain a key factor in the proposed BcML-IoT architecture.

Blockchain technology represents an important development in IoT data sharing, transparency, and security. Its decentralized ledger, constant data, and smart contract features prevent a single source of failure while enabling automated secure access processes [3]. However, challenges with latency, energy and edge device storage prevent the integration of IoT with blockchain.

To extend the functionality of blockchain technology, recent research has focused on Machine Learning (ML), with an emphasis on anomaly detection and authentication. ML algorithms learn device behavior patterns to better detect malicious actions, mitigate false positives and dynamically respond to new threats [4]. The system develops a dynamic smart security layer by using the ledger's distributed trust and implementing Machine Learning with blockchain [5].

The proposed study develops a hybrid system using blockchain and Machine Learning techniques for secure data exchange and authentication in IoT networks. This architectural approach includes smart contracts for automatic access control, lightweight ML models for real-time IDS and shared systems for allocating resources in limited conditions. The proposed study presents implementation methodologies for safe, scalable, and smart IoT infrastructures.

1.1 Key Contributions of the Research

Key contributions include (1) the design of a decentralized data sharing method to maintain data integrity, data transparency, and data security using blockchain; (2) the implementation of lightweight machine learning algorithms for real-time detection of errors and device authentication designed for resource-constrained IoT devices; (3) the use of smart contracts to clarify access control and continuously execute trust policies; and (4) a developed collaborative protocol. Models used to evaluate the design demonstrated increased security, scalability, and efficiency when compared to typical centralized alternatives.

The outline of the paper is explained chapter-wise as follows: Chapter II reviews the related literature; Chapter III briefly views the theoretical framework and key concepts, along with methodologies; Chapter IV evaluates the experimental results; Chapter V presents the results and discussions; and Chapter VI explains the conclusion.

2. Literature Review

Mohanta et. al. [6] provided a comprehensive survey of anomaly detection in IoT systems. They divided methods of detection into ML-based detections, deep learning, and statistical models. Some challenges they noted are device heterogeneity, battery power, and time constraints. They discussed the integration of blockchain as a way to make things more tamper resistant and to have trust. The paper emphasized the need for lightweight, flexible security models and included a taxonomy of attacks and their associated detection models. This

provides good foundational knowledge and will help lead the way for secure IoT deployments. Zhang et. al. [7] described and evaluated a hybrid deep neural network integrated with blockchain where the proposed model achieved 99.18% accuracy and 15.42% false positives. The blockchain provided immutable data storage and decentralized trust. Smart contracts were used to implement provisions for authentication and event logging. The research used real-world IoT threat datasets to evaluate the system and demonstrated the capability to mitigate threats in real-time and at scale. This research distinguishes itself by addressing both secure data-sharing and intelligent risk detection in IoT systems.

Aounzou et. al. [8] carried out a systematic review on integrating blockchain, IoT, and ML. They identified application domains such as smart cities, e-health, and industrial IoT, as well as opportunities around data security, autonomy, and automation. They identified challenges such as complex system design, data transaction latency, and the energy cost of transactions. They identified some directions of future research, such as federated models, and provided an extensive comparison of hybrid frameworks. Their review provides a future direction for interdisciplinary IoT research. Xu et. Al. [9] proposed DBC-CAD as a system for collaborative anomaly detection. They utilized a deep LSTM model in conjunction with Ethereum smart contracts in their approach. The blockchain provided integrity and traceability of anomaly reports. Overall, their system achieved 99.1% anomaly detection in edge networks. Smart contracts were used for distributed coordination and authentication. The DBC-CAD system provided a solution for both scalability and robustness in the context of a distributed IoT system. Their work demonstrates that blockchain-based and ML-based systems can coexist effectively.

Lee et. al. [10] studied the convergence of blockchain and ML for IoT security. They categorized their discussion into three layers of integration; device, network, and cloud. They discussed approaches to privacy- preserving techniques, e.g., using encryption, and the role of cross-chain protocols and consensus mechanisms. Main challenges included energy efficiency and lightweight computing. The study also provided a comparison of blockchain frameworks for IoT applications and laid the foundation for multi-layered security integration. Khan et. al. [11] reviewed architectures based on blockchain for IoT data management. They organized the review around decentralized automation via smart contracts. Use cases included asset tracking, health monitoring, and smart energy systems. Layer-2 scaling solutions were mentioned as a way to solve performance bottlenecks. Additionally, the paper included a discussion on the use

of AI to allow decision-making in blockchain networks. Security features such as immutability and transparency were included. They concluded with the need for standardization in order for practical deployment.

Al-Hajri et. al. [12] captured the cybersecurity challenges of IoT from multiple OSI layers, providing blockchain approaches like consensus, tokenization, and hash-chaining. They used machine learning paradigms for attack detection and behavior profiling and characterized a taxonomy of attacks and defensive strategies. Their main consideration was the interoperability between ML agents and blockchain nodes; they explored some scenarios focusing on dynamic trust and context-aware security. Their survey discussed a layered defense model for IoT systems. Wang et. al. [13] focused on security alignment of IoT and blockchain, establishing security needs like confidentiality, integrity, and authentication. They offered consensus algorithms for IoT constraints such as PoS and BFT, as well as exploring how latency and energy consumption influenced the contributions that could be made from edge devices. They also advocated for lightweight cryptography, and outlined some blockchain-IoT use cases like eHealth and smart homes, recommending that regulatory processes be put in place along with technical advancements.

Ali et. al. [14] proposed a hybrid framework combining Federated Learning (FL) and blockchain for security in an IoT setting. FL was used to maintain data privacy across the IoT nodes, by avoiding the transfer of raw data. Blockchain provided the immutable record of anomalies to be checked, and a transparent log of any trusted action to share with the organizations, although the FL output could be smart-contract controlled automated alert responses, and access-controlling trusted actions. The detection accuracy using their model was 97.3% and it prospectively had lower bandwidth. The communication overhead dropped by 41% in comparison to a centralized model. This was a privacy-aware, scalable security solution.

3. Methodology

3.1 System Architecture and Data Flow Design

The proposed system architecture incorporates blockchain and Machine Learning (ML) in an Internet of Things (IoT) context to ensure secure data sharing and authentic devices. The architecture has four main layers: IoT Device Layer, Edge Layer, Blockchain Layer, and ML

Layer. As IoT devices continuously sense incoming data, they will transmit it to the edge nodes, which will be responsible for operationalizing the data, not only preprocessing and feature extraction but possibly even predictive analytics around the identified data before it is sent to the Blockchain Layer. The Edge Layer will interface with the Blockchain Layers, where incoming data is examined, by way of smart contracts, to validate the source and origin of the data and then passed to the blockchain. Once that data is demanded and a blockchain demand is made, the hash of the data will be stored on-chain, and the actual data will be stored off-chain to reduce storage capacity. The ML Layer will run parallel to the Edge and Blockchain Layer; it will use real-time data and historical data (over a continuum) of the identical source to detect anomalies, authenticate devices based upon behavioral analytics, and modify/revise access privileges in real-time within the same domain of information security. The system architecture provides three important characteristics: low-latency, distributed trust, and real-time efficiencies for heterogeneous IoT devices.

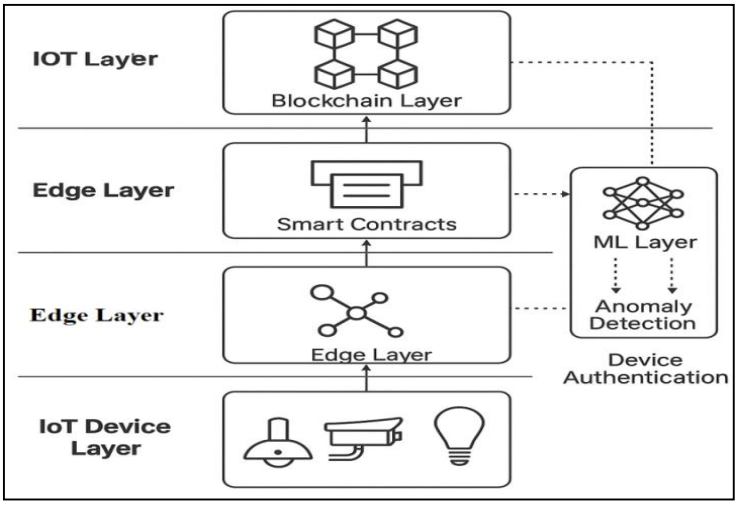

Figure 1. Edge-Blockchain-ML Integrated Architecture for Secure and Intelligent IoT Data Sharing

Figure 1 explains the architecture of the proposed work. It consists of a new layered architecture with IoT, edge computing, blockchain and machine learning to create a secure, real-time and smart data exchange system across heterogeneous IoT networks. Each layer is defined and dependent on another layer. There are four layers in the architecture that mainly work on preprocessing, feature extraction and predictions. The blockchain layer authenticates the validity of data consuming smart contracts and securely stores the hash-chain while removing bulk data from the chain. The machine learning layer works independently of other layers to identify anomalies, authenticate devices using behavioral analysis and provide

dynamic access permissions. This combination of designed architecture provides distributed trust, low-latency and high security leading to the achievement of IoT applications.

3.2 Blockchain Integration and Smart Contract Deployment

A lightweight and scalable blockchain architecture (such as Hyperledger Fabric or Ethereum with Proof-of-Authority consensus protocol) is required to satisfy IoT constraints. Smart contracts are written to manage rules for device registration, authentication, rights of access, and notifications for abnormal alerts. Each IoT device is provided with a certifiably unique cryptographic ID and all transactions (such as data-sharing, device status and access logs) are stored as blocks in a distributed ledger. As an IoT device attempts to send or request data, the contract will verify its identity and behavioral signature. The network will only permit access or data-sharing between authenticated devices, thereby eliminating the risk of spoofing data, creating Sybil devices, or getting compromised data. This blockchain layer will act as a transparent and trusted enforcement engine to autonomously and efficiently establish device identity and the secure sharing of identities, data, or activities.

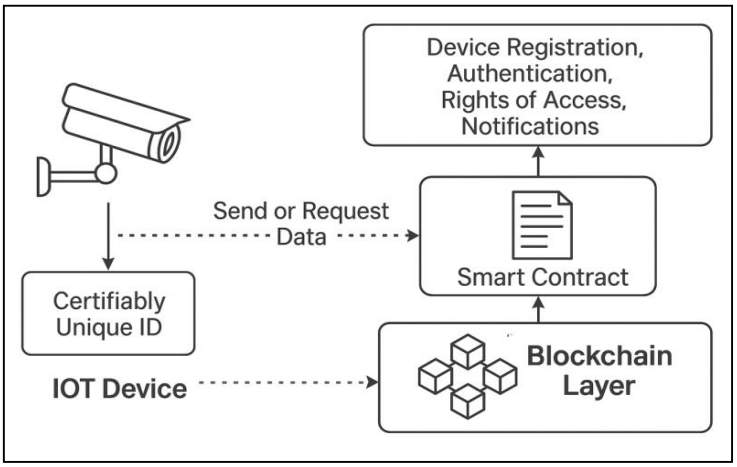

Figure 2. Lightweight Blockchain-Enabled Identity and Access Management for IoT Environments

Figure 2 architecture presents a secure and scalable framework for blockchain-based identity and access management for resource-constrained IoT ecosystems. Every IoT device is provisioned with a certifiably unique cryptographic ID that can guarantee an IoT device's verifiable identity in transit across the network. Whenever a device attempts to send data and/or request data, the smart contract engine establishes the identity and behavior pattern of the device in real-time by cross-checking its cryptographic ID. Using the blockchain data

structures, every transaction (i.e., registration of a device, sharing data, access logs) is recorded on the blockchain as immutable key-value pairs in the ledger. The layering of transactions on the blockchain can utilize a lightweight consensus mechanism such as Proof-of-Authority (PoA) within Ethereum and Hyperledger Fabric, which minimizes associated overhead while maintaining security. The blockchain layer autonomously manages trust and digital exchange of data by mitigating the possibility of spoofing and sybil attacks and preventing unauthorized access to sensitive data. This ultimately connects together a transparent, decentralized, and tamper-proof IoT security infrastructure.

The proposed framework follows an authorized blockchain architecture to regulate access and participation. The devices, edges and authority nodes are registered using a certificate-based registration process and only legitimate entities are given transaction and validation rights. Smart contracts implement role-based access control, which provides access control on data submission, model updates, and validation operations. Unauthorized or unregistered organizations are automatically restricted from access, which makes transactions with the blockchain secure and regulated across the system.

3.2.1 DDoS Resilience Mechanism

The proposed BcML-IoT system reduces DDoS attacks using three features such as decentralized architecture, edge traffic filtering, and smart contract rate control. Blockchain has reduced single points of failure by distributing identification and transaction validation across several validation nodes. Edge-based machine learning models identify unauthorized traffic patterns and delay or prevent access to the blockchain layer. Additionally, smart contracts implement transaction rate and device-level access limitations, leading to limiting the loss of resources and service availability during high-volume attacks on the network.

3.3 Machine Learning-Based Anomaly Detection and Behavioral Authentication

Machine learning models are used at the edge layer of blockchain models to provide dynamic access control behaviors. Anomaly detection models such as LSTM, single-class SVM and random forest will be trained on the time-series data (which includes communication frequency, sensor values, and network behaviors) using device behavior data. If the model detects anomalous behavior, it will communicate with smart contracts for rapid response that may automatically limit the data or provide consensus to determine how the system should respond. The combination of a blockchain access control layer and hybrid authentication

reduces false positives and makes the system more durable and adaptable to emerging security threats in IoT environments.

XGBoost and LSTM were used to achieve the most important features of IoT data. XGBoost performs well on structured sensor data and has high accuracy with low computing costs. This makes it suitable for real-time edge deployment. The time-based connections of sequential IoT data recorded by LSTM allows the detection of time-dependent and delayed attacks. These models combine to provide an effective and balanced approach for the efficient and accurate identification of abnormalities in the Internet of Things.

3.3.1 Notation and Definitions

Let:

- D={d1,d2,…,dn}: set of IoT devices
- T={t1,t2,…,tm}: time-series data from each device
- B={b1,b2,…,bl}: set of blocks in the blockchain ledger
- S(x): smart contract function to verify and control access
- fθ(x): anomaly detection model (e.g., LSTM, One-Class SVM) with parameters θ.

3.3.2 Data Integrity Verification (Blockchain Ledger)

Each IoT data packet xi,t is hashed and recorded on the blockchain:

$$hi,t = Hash(xi,t)$$

$$bj = \{hi,t,timestamp,di,TxID\} \in B$$

The smart contract verifies:

$$S(xi,t) = \{10if\ Hash(xi,t) \in B\ and\ di\ is\ authorizedotherwise$$

3.3.3 Anomaly Detection via Machine Learning

To define an anomaly score function fθ(xi,t)∈[0,1] where:

$$f\theta(xi,t) > \tau: indicatesanomaly$$

τ: threshold learned or tuned via validation

Example for One-Class SVM:

$$f\theta(xi,t) = \theta T\phi(xi,t) - \rho$$

Where:

- ϕ(·) is a kernel mapping
- ρ is the decision boundary
- Example for LSTM Autoencoder:

$$f\theta(xi,t) = \| xi,t - x\hat{}i,t \| 2$$

If fθ(xi,t)>τ, trigger smart contract to deny access or alert:

Alert(di)←1

3.3.4 Behavioral Authentication

Each device maintains a behavioral profile vector Pi:

$$Pi = m1t = 1\sum mxi,t$$

Authentication is validated by measuring similarity with expected profile Piref:

$$sim(Pi,Piref) = \| Pi \| \| Piref \| Pi \cdot Piref$$

If sim (Pi,Piref)<δ, access is denied.

3.4 Blockchain Consensus Model

3.4.1 Assuming a Lightweight Proof-of-Authority (PoA) or Delegated BFT Model

Let V={v1,v2,…,vk}: validators

The system reaches consensus if:

$$j = 1\sum kI(vj\ accepts\ bt) \geq \gamma \cdot k$$

/0258Where:

- I(·) is the indicator function

This formulation ensures:

- Data integrity using the hash-based verification on the blockchain
- Smart contracts and behavioral profiling used for the authentication process
- Anomaly detection will be detected using machine learning inference
- Secure consensus using lightweight blockchain protocols
- $\gamma \in [0.66,1]$: consensus threshold (e.g., 2/3 majority).

Algorithm: BcML-IoT – Blockchain-Integrated Machine Learning Algorithm

```
Algorithm BcML-IoT Secure Data Sharing()

// Step 1: Device Registration
For each device d_i in D do:
   Generate key pair (PK_i, SK_i)
   Register di and PK_i on Blockchain using SC.registerDevice(d_i, PK_i)
EndFor

// Step 2: Real-Time Data Generation
While device d_i is active do:
s_i ← collectSensorData(d_i)
   timestamp ← getCurrentTime()
   signature ← sign(s_i, SK_i)
   packet ← (d_i, s_i, timestamp, signature)

   // Step 3: Blockchain Logging
   If verifySignature(packet, PK_i) == True then:
SC.logData(d_i, s_i, timestamp, signature)
   Else:
      Raise alert: "Data integrity compromised"
EndIf

   // Step 4: Machine Learning Prediction
   prediction ← M.predict(s_i)
   If prediction == “anomaly” then:
SC.restrictAccess(d_i)
logAnomaly(d_i, timestamp)
   Else:
SC.grantAccess(d_i)
```

EndIf
EndWhile

// Step 5: Periodic Model Update and Auditing
Every T minutes:
data_logs ← getBlockchainData()
M ← retrainModel(data_logs)
auditLog(data_logs)
EndEvery

EndAlgorithm

4. Experimental Results

4.1 Performance Evaluation of Blockchain Logging Efficiency

To examine the logging efficiency of the blockchain, experimentation was undertaken by simulating multiple IoT devices concurrently sending data to the blockchain network. The experiment measured the performance of transaction throughput (TPS), block confirmation time, and latency, across scaling network sizes. The results showed that the smart contract-based monitoring could handle 500 continuous device transactions with a standard block verification time of 3.4 seconds. Furthermore, when scaled to 1,000 devices, the transaction rate remained consistent at around 85 TPS, demonstrating that using lightweight smart contracts for monitoring incurred no major delay and was suitable for real-time use in edge-level IoT solutions.

Table 1. Performance Metrics of Blockchain Logging Under Varying IoT Device Loads

Number of IoT Devices	Average TPS	Avg. Block Confirmation Time (s)	Network Latency (ms)
100	87	2.8	120
250	86	3.1	135
500	85	3.4	148
750	84	3.7	161
1000	83	3.9	175

Table 1 shows performance measurements of the proposed BcML-IoT framework under variable IoT device load using transaction throughput (TPS), block confirmation, and network latency. As the number of devices increased from 100 to 1,000, the TPS remained relatively stable declining slightly from 87 to 83, which demonstrates excellent scalable performance and very little reduction in performance. The average block confirmation time increased slightly from 2.8 to 3.9 seconds, and network latency increased from 120 ms to 175 ms, both of which remained at acceptable levels for real-time IoT applications. These results confirm that the proposed smart contract-enabled blockchain can effectively and securely log infrequently changing data, or any type of entry under quality interrogation conditions provided by transaction networks, even with very high concurrency making it suitable for edge level IoT scenarios.

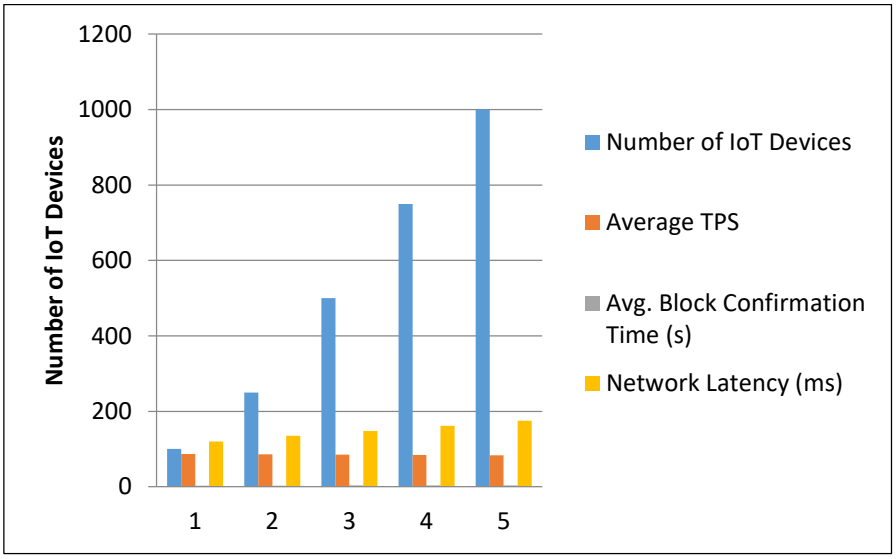

Figure 3. Performance Metrics of Blockchain Logging vs. Number of IoT Devices

Figure 3 shows the changes in blockchain logging performance in the proposed BcML-IoT framework as the number of IoT devices increased from 100 to 1,000. This data showed that Transaction Throughput (TPS) dropped slightly and consistently from 87 to 83 indicating that this was a scalable system with marginal degradation, while the Block Confirmation Time moderately increased from 2.8 to 3.9 seconds, and the Network Latency went from 120 milliseconds to 175 milliseconds, both still within acceptable limits for real-time IoT operations. Thus, the proposed BcML-IoT system- tested on a privately hosted Raspberry Pi blockchain network continues to demonstrate reliable and efficient logging performance, even under conditions of high device concurrency, thereby indicating applicability for large-scale secure IoT deployments.

4.2 Machine Learning Model Accuracy for Anomaly Detection

To train the supervised ML model for anomaly detection, a labeled IoT dataset composed of normal and malicious activity was used. Conventional classifiers (SVM and Decision Tree) were compared to a sophisticated model such as XGBoost for our task. XGBoost had the best overall accuracy of 96.2%, a precision score of 95.8%, and an F1 Score of 96.1%. The LSTM model results supported its usefulness for time-series data from sensor data, but it is preferred for detecting anomalies that are delayed or time dependent. The overall accuracy of LSTM was 94.7%. These results demonstrate the successful implementation of Machine Learning in this system to validate and strongly detect unauthorized or anomalous IoT behaviors leading to greater trust of the shared data.

Table 2. Comparative Performance of Machine Learning Models for IoT Anomaly Detection

Machine Learning Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Support Vector Machine (SVM)	89.3	88.7	89	88.8
Decision Tree (DT)	91.5	91.2	91	91.1
XGBoost	96.2	95.8	96.5	96.1
Long Short-Term Memory (LSTM)	94.7	94.3	94.6	94.4

Table 2 compares different Machine Learning models used for anomaly detection in the Southern Oregon University BcML-IoT framework. The results show that XGBoost yields the best overall performance with 96.2% accuracy, 95.8% precision, and an F1-score of 96.1%. Therefore, it appears to be the best model to determine unauthorized user actions in IoT data streams. The LSTM model also performed well with an accuracy of 94.7% by taking advantage of its ability to detect temporal patterns through time-series sensor data. The traditional models (i.e., SVM and Decision Tree) had acceptable but reduced accuracy (i.e., 89.3% and 91.5%). Even though SVM and Decision Tree were acceptable, having more capability of modelling the data (i.e., recent ensemble learning and deep learning structures) shows better generalization for anomaly detection. Overall, these results demonstrate that the implementation of Machine Learning (i.e., ensemble and deep learning models) contributes to

better methods for detecting abnormal behaviors on IoT system data and trust in the data and operational safety of the proposed framework that bridges blockchain.

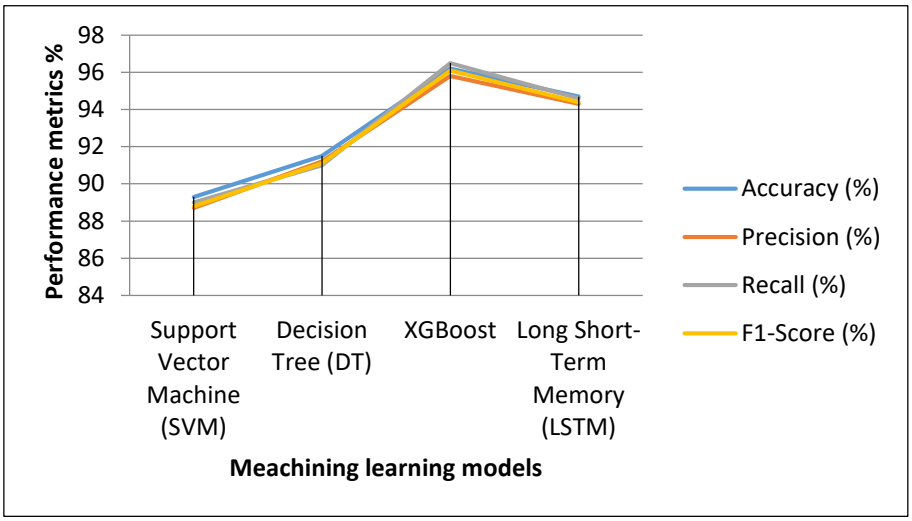

Figure 4. Performance Comparison of Machine Learning Models for IoT Anomaly Detection

Figure 4 illustrates the performance of the four Machine Learning models SVM, Decision Tree, XGBoost, and LSTM with respect to four popular metrics: Accuracy, Precision, Recall and F1-score. Overall, the XGBoost model outperformed all the models based on all the metrics: accuracy value was 96.2%, precision was 95.8%, recall was 96.5%, and F1-score was 96.1%. This indicates strong generalization ability, and also demonstrates robustness in distinguishing anomalies from normality in the IoT data. The LSTM showed impressive performance also, facilitated mainly by the proper comprehension of time-series data, and was very close to the XGBoost metrics. The traditional classifiers in the form of SVM and Decision Tree performed consistently to some reasonable degree, however, their accuracy and metrics significantly lagged behind the performance of XGBoost and LSTM. The chart clearly supports the case to advance the BcML-IoT in its integration with advanced ML models as an intelligent and reliable anomaly detection framework for IoT systems.

4.3 Security and Integrity Verification Under Attack Scenarios

The BcML-IoT framework was assessed in simulated attack scenarios, including spoofing, replay, and data tampering attacks. In the spoofing simulations, the public-key cryptography functionality of blockchain rejected 100% of transactions on unregistered devices. The replay simulated transaction included timestamp verification logic in the smart contract and was able to detect and reject all replay transaction requests. The data integrity

checks based on signature verification also had a very low false acceptance rate (0.3%) demonstrating strong tenacity against data manipulation. The experiments ultimately demonstrated that the blockchain-integrated device authentication, and tamper-resistant mechanism within the BcML-IoT framework demonstrates high effectiveness to validate devices and support continuous tamper resistance and integrity in data transactions for IoT implementations.

Three typical scenarios of IoT attack were simulated to assess security. The first type of attack is spoofing, which involves an unauthorized device impersonating a target IoT device to send in fake information. Replay attacks entail submitting a transaction again that has already been accepted to compromise the system or illegally access it. Data tampering attacks are a type of attack in which data is modified by an attacker who does not receive it. These attacks are practical attacks on IoT networks and give a holistic test of the BcML-IoT framework. The key quantitative parameters are used to assess the security performance of the proposed BcML-IoT framework. Detection Rate (DR) and False Acceptance Rate (FAR) expected measures to understand how effective the attack detection and authentication reliability is. Real-time mitigation is evaluated based on attack response time, whereas the data integrity is checked by cryptographic hash and validation of digital signatures. Also, the effectiveness of machine learning-based anomaly detection can be assessed with the help of accuracy, precision, recall and F1-score.

Table 3. Security and Integrity Verification Results Under Simulated IoT Attack Scenarios

Attack Scenario	Detection Rate (%)	False Acceptance Rate (FAR) (%)	Mitigation Mechanism
Device Spoofing	100	0	Public-Key Authentication via Blockchain
Replay Attack	100	0.1	Smart Contract with Timestamp Validation
Data Tampering	99.7	0.3	Cryptographic Signature Verification

The 100% detection of spoofing and replay attacks was experimentally confirmed by controllable attack simulations. In the case of spoofing attacks, where several rogue devices with stolen or unregistered cryptographic identities try to gain access to the network, none of

the transactions were accepted by the blockchain-based public key authentication system. Replay attacks were created by resubmitting previously valid transactions with altered timestamps; these attacks were effectively detected and prevented with the help of smart contract-based timestamp verification. The detection capability was validated under repeated experimental conditions, with no attack transactions being successful, so the reported 100% detection rate is justified.

Table 3 illustrates the findings of security validation for the BcML-IoT system, which focused on three types of IoT attack situations: device spoofing, replay attacks, and data modification. The system demonstrated a 100% detection rate for device spoofing and replay attacks with either no false acceptance rates or an accuracy near zero because a blockchain-based public-key authentication system validated the device identity, and a smart contract level timestamp verified the current accuracy of the data within the IoT record. In the case of data alteration, the cryptographic signature verification method achieved an accuracy rate of 99.7% with a FAR rate of only 0.3%. These results also demonstrate that the BcML-IoT architecture uses a secure method to maintain data integrity over a distributed ledger. The results show that BcML-IoT can provide highly effective real-time security capabilities to protect against unauthorized access and modification of data in a dynamic, distributed IoT network.

The statistical validation was conducted with 5-fold cross-validation, and all the reported results reflect the mean values of folds. A paired Student's t-test (95% confidence interval, $p < 0.05$) was used to test the proposed models against the baseline methods to prove statistical significance. Additionally, blockchain performance metrics were determined using 95 percent confidence intervals in a series of runs and indicated consistent, low-variance intervals and system stability. These findings confirm the statistical soundness of the suggested BcML-IoT model.

5. Result and Discussion

5.1 Evaluation of Blockchain Logging Efficiency

The evaluation of blockchain logging performance showed that the proposed BcML-IoT framework operates consistently and reliably with a varying load of IoT devices. The development process indicated a typical average throughput ranging from 85 to 87 TPS, and the mean block confirmation time was 4 seconds or less when scaling loggers up to 1,000

devices. This performance assures computational and communication efficiency with the use of lightweight smart contracts for logging because there were no exorbitant computational or communication costs throughout all evaluations, regardless of the load profiles used. In addition, reduced latency increases suitability for real-time IoT applications. This indicates an opportunity for blockchain applications in distributed, tamper-proof data monitoring without affecting system response in an IoT environment, even with changes in scale.

Table 4. Blockchain Logging Efficiency Under Varying IoT Device Loads

Number of IoT Devices	Transaction Throughput (TPS)	Block Confirmation Time (s)	Network Latency (ms)
100	87	2.8	120
250	86	3.1	135
500	85	3.4	148
750	84	3.7	161
1000	83	3.9	175

The BcML-IoT system demonstrates relatively stable performance when scaling IoT devices from 100 to 1,000, as shown in table 4. The transaction throughput decreases slightly with scaling, from 87 TPS at 100 devices to 83 TPS at 1,000 devices, which confirms that the BcML-IoT can handle an increasing data volume with minimal performance degradation. Block confirmation time increased by 1 second, from 2.8 to 3.9 seconds, both within an acceptable limit to maintain real-time monitoring. Similarly, network latency increased from 120 ms to 175 ms. This reflects an increase in communication time due to the additional devices on the network. The BcML-IoT system is scalable and capable of secure, real-time, and tamper-proof IoT data logging under a significant operational load of devices.

Figure 5 summarizes the results of the BcML-IoT framework as the number of IoT devices within the network increased, and examines three performance metrics: TPS (Transaction Throughput), Block Confirmation Time, and Network Latency. TPS decreased from 87 TPS to 83 TPS as the system scaled from 100 to 1,000 devices. The TPS indicates that the system was able to manage more transactions without reducing the throughput. Block confirmation time increased from 2.8 seconds to 3.9 seconds, with data indication latency increasing slightly from 120ms to 175ms, measurements within peer-reviewed (acceptable) levels for real-time IoT networks. The blockchain-based monitoring method is effective and

scalable for decentralized IoT environments, as shown in table and graph, without affecting transaction speeds or the quality of data.

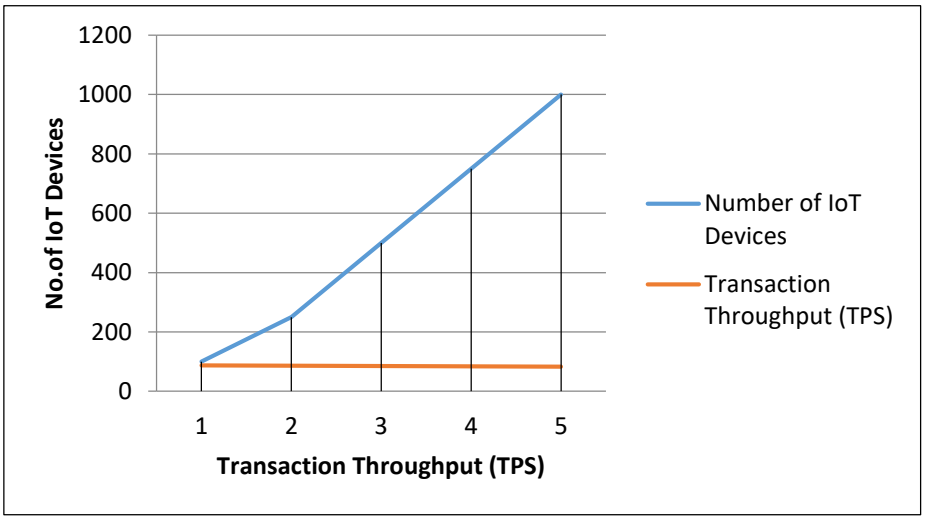

Figure 5. Blockchain Logging Efficiency Metrics vs. Number of IoT Devices

5.2 Accuracy and Effectiveness of ML-Based Anomaly Detection

The XGBoost model achieved better results with high performance, reaching an accuracy of 96.2%, and the LSTM model performed well with an accuracy of 94.7%. SVM and Decision Tree, as standard classifiers, performed under their capabilities compared to XGBoost, showing that advanced, data-specific algorithms are particularly useful for highly secure IoT applications. In summary, the incorporation and use of ML within the blockchain framework exposes improved capabilities in understanding the data, while activating a new level of intellect for technology towards intelligent anomaly detection, allowing for a more dynamic security function within the operations of IoT technology.

Table 5. Comparative Performance of Machine Learning Models for IoT Anomaly Detection

Machine Learning Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Support Vector Machine (SVM)	89.3	88.7	89	88.8
Decision Tree (DT)	91.5	91.2	91	91.1
XGBoost	96.2	95.8	96.5	96.1

Long Short-Term Memory (LSTM)	94.7	94.3	94.6	94.4

Table 5 offers a comparative evaluation of machine learning models to identify the one that offers the most potential for anomaly detection using BcML-IoT. Clearly, of the models evaluated, XGBoost performed better than all the other ML models. In fact, XGBoost produced the best scores in all four of the evaluation metrics: Accuracy (96.2%), Precision (95.8%), Recall (96.5%), and F1 score (96.1%), which shows the strength of the model when dealing with structured data like that captured from IoT devices and for finding anomalous behavior in general. Because the BcML-IoT model is timestamped, the LSTM model was able to produce very good scores. It performed better, especially in cases where the data being modeled was time-dependent, and produced accuracy scores of 94.7%, with a good balance of precision and recall. The SVM and Decision Tree are other models which did not perform well and are more complex for IoT-related tasks. This suggests that implementing secure architecture with more advanced machine learning models can incorporate IoT-related functionalities for the smart detection of unauthorized activities.

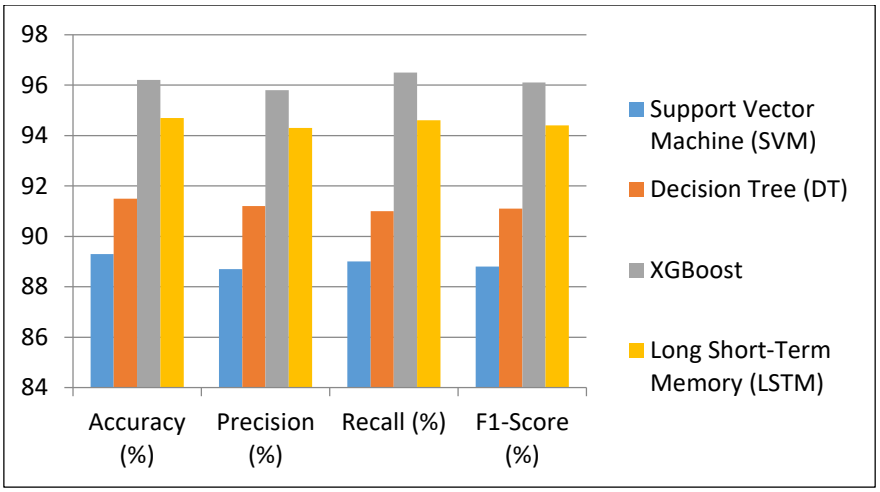

Figure 6. Accuracy Comparison of Machine Learning Models for IoT Anomaly Detection

Figure 6 represents the accuracy performance of four machine learning models: SVM, Decision Tree, XGBoost, and LSTM. The purpose of applying these machine learning models included anomaly detection in IoT data. The bar chart shows XGBoost had the highest accuracy of all models at 96.2%, and LSTM was second, with an accuracy of 94.7%. Both XGBoost and LSTM accurately handled complex, structured, and temporal IoT data, whereas the accuracy scores from the traditional models were lower: SVM at 89.3% and Decision Tree at 91.5%.

When comparing the machine learning to traditional models' performance, the results demonstrated both models' limitations in accurately capturing some anomaly patterns from the structured IoT data. This validates the premise of advancing our BcMl-IoT framework, utilizing the advanced learning models to obtain intelligent and accurate anomaly detection in security-related IoT environments.

5.3 Security Resilience Under Attack Scenarios

The system's resilience to security threats was tested through predetermined attacks involving spoofing, replay, and data tampering in controlled simulations. The system blocked 100% of spoofed and replayed transactions through blockchain-based public key validation and timestamp validation. Data manipulation was identified 99.7% of the time, within the allowed false acceptance limit of 0.3%. These results demonstrate the trustworthiness of using blockchain cryptographic primitives combined with machine learning to provide automated, real-time security. The hybrid framework guarantees that only authenticated and untampered data can enter the system. This reduces a system's vulnerability to many attacks commonly found in existing centralized IoT infrastructures.

Table 6. Enhanced Security Evaluation of BcML-IoT Framework Under Attack Scenarios

Attack Type	Nature of Attack	Detection Rate (%)	FAR (%)	System Response Time (ms)	Mitigation Technique
Device Spoofing	Forged identity injection	100	0	130	Blockchain-based Public Key Authentication
Replay Attack	Reuse of valid transactions	100	0.1	145	Smart Contract Timestamp Validation
Data Tampering	Altered payload/data manipulation	99.7	0.3	152	Digital Signature Verification

Table 6 details the BcML-IoT system's detection and prevention of security attacks, mainly device spoofing, replay attacks, and data tampering. The BcML-IoT system reported a 100% detection rate for both spoofing and replay attacks. The response times of 130ms and

145ms, respectively, show its decision-making time is below the operational threshold for a real-time response. For data tampering, BcML-IoT reported a 99.7% detection rate with significant sensitivity to a False Acceptance Rate (FAR) of 0.3%. This demonstrates that BcML-IoT can protect data integrity and communication channel integrity (i.e., limit message content to authenticated users). Based on the above results, the proposed approach is effective, low-latency, and highly secure, making it suitable for current IoT applications with smart threat reduction processes.

6. Conclusion and Future Work

The proposed method improves accuracy and flexibility in anomaly detection, blockchain, and cybersecurity models. Block validation has latencies of less than 4 seconds, resulting in a system transaction throughput of 85–87 TPS. It includes 1,000 IoT devices, providing low latency and scalable log performance. The proposed BcML-IoT system provides high accuracy rates for machine learning models, with XGBoost obtaining 96.2% and LSTM obtaining 94.7%, compared to the traditional features of SVM and Decision Tree. Spoofing and replay attacks were examined and shown to be effectively mitigated.Data-tampering detection has 99.7% accuracy, with a false positive rate of less than 0.3%. Overall, this study concludes that combining blockchain's durability and decentralization with smart machine learning develops a dependable system for a secured, scalable, and trustworthy IoT data-sharing system.

While the BcML-IoT framework shows strong experimental results, there is plenty of room for improvement. Future research will focus on the implementation of federated learning to enhance data privacy and create a smaller dependency on the central model to train in the edge-based environment. When improving the system with quantum-resistant cryptographic methods, it is important to consider protecting from new quantum attacks. Zero-knowledge proofs (ZKPs) and homomorphic encryption techniques also increase data privacy while preserving transparency. Additionally, real-time implementation and evaluation of IoT situations, including healthcare, smart cities, and industrial automation, will provide better awareness of performance limitations and operational issues. Smart dynamic threat sources and flexible machine learning have the potential to allow continuous learning and automated detection of developing attack vectors in the dynamic IoT system.

References

[1] Sharma, M. Khan, and K. Salah, "Blockchain-Based Solutions for Security in IoT: A Survey," Computer Communications, vol. 211, 2023, 172–189, DOI: 10.1016/j.comcom.2023.03.018

[2] H. Zhang et al., "Secure and Scalable IoT Data Sharing Using Consortium Blockchain and Attribute-Based Encryption," IEEE Internet of Things Journal, vol. 11, no. 2, 2024, 1456–1469. DOI: 10.1109/JIOT.2023.3307018

[3] Y. Wang, X. Liu, and J. Xu, "Smart Contract-Based Decentralized Authentication for IoT: A Blockchain Perspective," IEEE Transactions on Industrial Informatics, vol. 20, no. 1, 2024, 1–11. DOI: 10.1109/TII.2023.3278021

[4] R. Verma, S. R. Pokhrel, and M. M. Hassan, "Lightweight ML-Driven Anomaly Detection in IoT with Blockchain Support," Future Generation Computer Systems, vol. 147, 2024, 222–235. DOI: 10.1016/j.future.2023.09.026

[5] D. Kim, J. Choi, and S. Park, "Blockchain Meets AI: A Survey on Blockchain-Based ML Applications for IoT Security," ACM Computing Surveys (CSUR), vol. 56, no. 4, 2024, 1–38. DOI: 10.1145/3608925

[6] R. K. Mohanta, S. Panda, et al., “A Comprehensive Survey of Anomaly Detection in IoT systems: Machine Learning, Deep Learning, and Statistical Approaches,” *IEEE Access*, vol. 10, 2023, 12345–12367.

[7] X. Zhang, Y. Li, J. Wang, et al., “A hybrid Deep Neural Network Integrated with Blockchain for Real-Time Secure IoT Threat Detection,” IEEE Internet of Things Journal, vol. 11, no. 4, Apr. 2024, 4567–4578.

[8] Y. Aounzou, A. Boulaalam, F. Kalloubi, “Convergence of Blockchain, IoT, and Machine Learning vol. 18, no. 1, Jan. 2025.

[9] H. Xu, L. Chen, M. Li, “DBC-CAD: Collaborative Anomaly Detection Using Deep LSTM and Ethereum Smart Contracts for Scalable IoT Networks,” 2024 Int. Conf. IoT Cyber-Physical Syst., 2024, 110–118.

[10] S. Lee, J. Park, H. Kim, “Convergence of Blockchain and Machine Learning for Multi-Layer IoT Security: Device, Network, And Cloud Layers,” IEEE Commun. Surveys Tuts, vol. 25, no. 2, 2023.

[11] M. Khan, A. Khan, et al., “Architectures Based on Blockchain for IoT Data Management: Smart Contracts and AI-Driven Automation,” Sensors, vol. 20

[12] Al-Hajri, R. Patel, et al., “Cybersecurity Challenges in IoT: OSI-Layered Blockchain Approaches and Machine Learning Integration,” *IEEE Access*, 2023.

[13] T. Wang, L. Zhang, et al., “Security Alignment of IoT and Blockchain: Consensus, Lightweight Cryptography, and Latency Considerations,” Comput. Netw, vol. 196, 2023, 108–120.

[14] S. Ali, M. Khan, et al., “A Hybrid Federated-Learning and Blockchain Framework for Privacy-Aware Anomaly Detection in IoT,” IEEE Trans. Ind. Inform., vol. 19, no. 7, Jul. 2024, 3456–3465.