

Distributed IoT Security with Blockchain, Privacy-Preserving Techniques, and Predictive Maintenance Models

Haitham A. Mahmoud

Haitham_mah@outlook.com

Industrial Engineering, College of Engineering

Ahmed T. Soliman

Industrial Engineering, College of Engineering

Mohammed El-Meligy

Industrial Engineering, College of Engineering

Azhar Imran

Industrial Engineering, College of Engineering

Abdelaty Edrees Abdelgawad

Industrial Engineering, College of Engineering

Research Article

Keywords:

Posted Date: August 25th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-8236805/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Distributed IoT Security with Blockchain, Privacy-Preserving Techniques, and Predictive Maintenance Models

^{1*}Haitham A. Mahmoud, ²Ahmed T. Soliman, ³Mohammed El-Meligy, ⁴Azhar Imran, ⁵Abdelaty Edrees Abdelgawad

¹Department of Industrial Engineering, College of Engineering, King Saud University, Riyadh 12372, Saudi Arabia, Haitham_mah@outlook.com, hmahmoud@ksu.edu.sa

²Department of Industrial Engineering, College of Engineering, King Saud University, Riyadh 12372, Saudi Arabia, Asoluman@ksu.edu.sa

³Jadara University Research Center, Jadara University, PO Box 733, Irbid, Jordan, Applied Science Research Center, Applied Science Private University, Amman, Jordan, mohammedali2000@gmail.com

⁴School of Software Engineering, Beijing University of Technology, Beijing, 100124, China, azharimran63@gmail.com

⁵Department of Industrial Engineering, College of Engineering, King Saud University, Riyadh 12372, Saudi Arabia, Abdelatysayed84@Gmail.com

Abstract

Modern digital ecosystems rely mostly on blockchain technology, such as decentralized and immutable ledger systems. This technology avails guarantees of secure transaction and data administration in keeping with the privacy of consumers. Thus, the blockchain systems often suffer in resource-constrained environments to experience considerable computational overhead along with low scalability and issues in handling real-time data. To overcome these restrictions, this research incorporates federated learning, decentralized storage using IPFS, and lightweight cryptographic methods to deliver secure, scalable, and real-time analytics in the IoT system. This research has proposed a novel framework based on blockchain, privacy-preserving techniques, and predictive maintenance models to address some of the security, scalability, and reliability challenges observed in IoT ecosystems. The framework guarantees secure data management, efficient real-time analytics, and robust anomaly detection by using the most advanced technologies such as federated learning, decentralized storage, and lightweight cryptographic methods. The suggested technique exceeds traditional methods by means of accuracy and error reduction with the astonishingly low FPV value of 0.005954% and FNR value of 0.000274% while giving extraordinary performance metrics that reach 99.88% accuracy, 99.89% precision, 99.97% recall, and 99.93% F1-score. This solution establishes secure, scalable, and tamper-proof infrastructure for all the applications from industrial automation, healthcare to vehicular networks, hence enabling smart and sustainable IoT governance for these applications.

1. Introduction

The rapid expansion of IoT has essentially transformed transportation, healthcare, industrial, and other vital infrastructures with unprecedented levels of data generation, communication, and service automation. The reason is that billions of approaches operate in widely dispersed locations and often resource-constrained locations, so protection for the security, privacy, and integrity of IoT ecosystems has become one of the top concerns of researchers and medical professionals alike. Conventional centralized systems that need the aggregation and processing of data at a single

location clearly pose security risks, raise operational delay, and expose users to high danger of cyberattacks and cyber intrusions (Chen et al., 2021). As such, current research has shifted toward blockchain-enabled and distributed privacy-preserving architectures that address these issues broadly.

Blockchain and other circulated ledger technologies (DLTs) provide a clear and unbreachable situation for safely transmission data between geographically detached Internet of Things devices (Alabadi et al., 2024). IoT systems can stop unwanted access, verify data integrity and improve reliability without relying on a central authority by using blockchain's holistic data design. By combining blockchain technology and high-performance computing platforms such as IPFS, it allows a sophisticated method to safely and effectively handle the massive amounts of time series data generated by IoT devices. Such collaborative solutions can lower the challenges affiliated with single points of failure, which characterize centralized IoT infrastructures; scalability; and resolve difficulties caused by delay.

Methods like homomorphic encryption and federated learning (FL) have appeared to be integral components of the next-generation frameworks for IoT. FL guarantees user privacy and reduces risks of exposing data by letting the distributed training of a model across several devices instead of sharing raw data (Singh et al. This method, combined with homomorphic encryption algorithms, enables calculations on gradients as well as encrypted data, that is, protecting sensitive data against inference attacks while maintaining correctness in models (Chen et al., 2021).

PdM models have equally gained relevance in the context of Industrial IoT. As cited by Alabadi and Habbal (2023), sensor data can be taken to predict machine faults along with optimizing maintenance plans in advance with deep learning techniques. This automatically decreases the operational costs and, at times, even the downtime. With PdM's blockchain and privacy-preserving frameworks, the growth in volume and diversity of IIoT data, though tremendous, does ensure that training data and models for predictions are safe, scalable, and effective.

This combination of distributed security, privacy-preserving techniques, and predictive analytics represents a fundamental paradigm shift in the governance of IoT. These resultant frameworks provide diverse stakeholders of IoT with increased levels of trust, enhanced data integrity, confidentiality, and availability, and increased resilience to cyber threats. Blockchain integration with privacy-preserving technologies and predictive maintenance models will become highly important in ensuring sustainable, safe, and intelligent ecosystems as IoT solutions are gradually taken up by industrial, healthcare, and automotive networks.

1.1. Problem Statement

The usage of IoT appliances has produced massive amounts of sensitive data, and these are often handled by centralized platforms that are prone to single points of failure, data breaches, and cyberattacks. With traditional centralized solutions failing to provide strong protections against malicious tampering and unauthorized access, it is becoming increasingly challenging to ensure data security, privacy, and integrity across heterogeneous IoT settings. In addition, IoT systems require scalable techniques to handle constant data streams and enable effective data sharing without compromising confidentiality. It is essential to integrate privacy-preserving strategies to save user data while retaining the precision and dependability of predictive maintenance and machine learning models. Current systems face difficulty in ensuring reliability among distributed devices and handling the overhead and complexity of cryptography techniques. Additionally, it still remains a work in progress to improve

system resilience, latency, and scalability of extremely resource-constrained, dynamic IoT networks. Therefore, urgent comprehensive frameworks are required, which synergistically integrate blockchain, decentralized storage, privacy-preserving strategies, and predictive analytics for the fortification of the security and functionality of modern IoT infrastructures.

1.2. Objectives

- To design decentralized IoT systems using blockchain for secure and immutable data.
- To enhance distributed machine learning with privacy-preserving techniques and encryption.
- To use efficient consensus protocols for scalable, low-latency IoT environments.
- To implement predictive maintenance models for reliable and continuous industrial IoT insights.

2. Literature Survey

Alabadi et al. (2024) proposed a centralized system to manage data and security threats by using a deep learning framework for IIoT for predictive maintenance. Interplanetary file system (IPFS) manages data on a large scale in a decentralized way; the blockchain in the framework is used to enhance data security, ensuring constant transactions. The performance of the framework has data privacy, model accuracy, accuracy, execution time, and computing cost. So, the integration of blockchain, IPFS, DL and predictive maintenance. It is good at handling the huge data and data security. Amjad et al. proposed a new blockchain technology to overcome the privacy and security issue called Hyperledger Fabric for the IoT devices using federated learning. Their proposed solution enhances model accuracy and scalability and protects user privacy while providing secure communication. The paper combines weighted average approaches with Directed Acyclic Graphs (DAGs) for effective model updates and integration. The system ensures secure and dependable communication inside the federated learning process, based on Hyperledger Fabric for promoting trust and coordination among heterogeneous IoT devices. Therefore, the project aims to improve the security and model performance of offering an IoT system with scalable, privacy-preserving solution.

Liu et al. propose BP-DSP, a blockchain-based architecture designed for privacy-preserving IoT data service provisioning. The mechanism allows data owners to participate in services without revealing their personal information. BP-DSP uses lightweight homomorphic encryption to secure gradients from inference attacks and federated learning to enable privacy-preserving data sharing. The framework also utilizes a reputation-based incentive system to enhance model integrity and ensure high-quality contributions. According to experimental results, BP-DSP offers a scalable solution for safe and effective data-driven IoT services while protecting privacy, increasing operational efficiency by more than 40%.

Kashif et al. present blockchain architecture named EPIoT. The architecture solves problems in privacy to the end where IoT devices handle the data. So, a streamlined consensus algorithm along with low-computation cryptography serves for safe transaction purposes besides allowing data owners to gain control over preference in using privacy. For extensive validation as well as conducting security analyses the tool AVISPA used through simulations illustrates that how efficiently EPIoT functions. This method in the context of IoT guarantees a "private by design" solution which lowers processing demands and raises privacy.

Singh et al. (2022) uses Blockchain technology along with Federated Learning to create a secure architecture that helps in preserving the privacy of IoT data for smart healthcare. It thus addresses the ever-growing necessity to protect the privacy of the patients related to health care data, especially within the smart cities. This way, Federated Learning allows scalable machine learning applications without revealing users' personal information. The integration of blockchain will give an additional layer of security for IoT healthcare data. This framework is creating a distributed, secure environment that is crucial for smart city settings and intelligent healthcare systems.

Zhou et al. (2022) presents a novel privacy-preserving approach for improving data privacy of IoT devices by using blockchain technology and the privacy set intersection. In this strategy, the user data privacy is protected with the introduction of a new homomorphic encryption PSI method based on 0-1 encoding that hides the basis of the set. The system increases the data sharing ability by allowing storage of shared data on a blockchain through the integration of smart contracts and blockchain structure. When compared to other pertinent alternatives, security analysis shows that it offers little communication and computing overhead, excellent influence individual information, and guarantees both safety and privacy.

Alabadi and Habbal (2023) proposed a decentralized predictive maintenance model. The paper addresses crucial barriers to the adoption of traditional deep learning for predictive maintenance, such as dependence on the domain, constant model updates, and central model security issues. The proposed system outperforms state-of-the-art models as validated by performance, effective scalability through smart contract gas utilization, and improved prediction accuracy as indicated by the RMSE score. A detailed CIA (confidentiality, integrity, availability) analysis confirms that the system's security measures are indeed robust, with flaws in model storage and data orchestration successfully resolved.

3. Methodology

This diagram illustrates a comprehensive data processing and management framework integrating multiple technologies. It begins with User Interaction, where web and mobile dashboards enable notifications, alerts, and access control. Data Collection & Sensors gather real-time information from various sensors, processed through Edge Computing for immediate analytics and decision-making. Data Preprocessing involves cleaning, feature engineering, and time-series analysis, preparing data for storage and further use. Decentralized Storage ensures data redundancy and confidentiality using IPFS. The Blockchain Layer guarantees immutable records, secure data handling, and automated operations with smart contracts. Privacy-Preserving techniques like federated learning and encryption ensure secure collaboration, while Predictive Maintenance uses deep learning models for anomaly detection. Finally, Security & Performance safeguards system integrity through audits, stress tests, and performance monitoring.

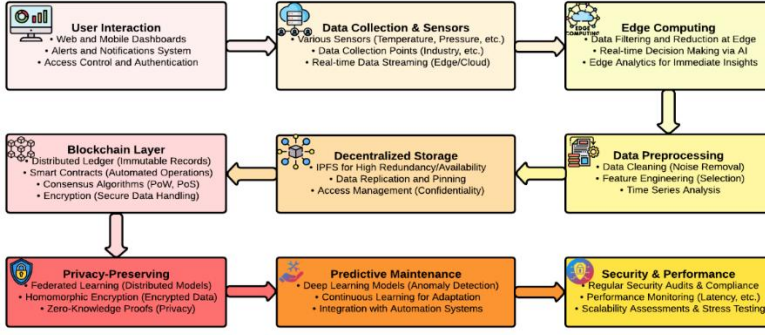


Fig. 1. Architecture Diagram

3.1. Dataset Description

The DNN-EdgeIoT-dataset consists of 157,801 rows of data that have different traffic data in the network with capture attributes such as source IP address, destination IP address, HTTP, MQTT, TCP flags, ARP, ICMP, DNS, and metadata. It has different attacks such as DDoS_ICMP, DDoS_UDP, DDoS_TCP, DDoS_HTTP, normal, MITM, XSS, backdoor, vulnerability scanner, port scanning, password, SQL injection, uploading, ransomware, and fingerprinting. It also consists of various protocol-specific fields. The dataset structure allows for an extensive analysis of network behavior in IoT environments.

3.2. User Interaction

3.2.1. Web and Mobile Dashboards

Web and mobile dashboards present real-time data, analytical results, and status indicators via user-friendly interfaces accessible on various devices. They help end-users (operators, analysts, managers) quickly understand the system state and make informed decisions.

- Let $x(t)$ be the data vector displayed on the dashboard at time t .
- Data refresh intervals Δt ensure up-to-date information:

$$x(t + \Delta t) = x(t) + \delta \quad (1)$$

represents new incoming data increments.

3.2.2. Alerts and Notifications System

When abnormalities are found or important metrics surpass thresholds, this system immediately alerts users. Alerts guarantee prompt action, cutting down on downtime and averting expensive malfunctions.

For a monitored variable $x(t)$ and threshold θ :

$$\text{Alert}(t) = \begin{cases} 1 & \text{if } x(t) > \theta \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

3.2.3. Access Control and Authentication

It is, therefore, important to guarantee that only licensed people can approach sensitive information or features of the system. For this purpose, role-based or access control based on attribute systems restrict data access to only those who are allowed in order to preserve confidentiality and integrity.

Let U be the set of users, $R(u)$ the role of user $u \in U$, and d a data resource:

$$A(u, d) = \begin{cases} 1 & \text{if } R(u) \in \text{AuthorizedRolesFor}(d) \\ 0 & \text{otherwise} \end{cases} \quad (3)$$

3.3. Data Collection & Sensors

3.3.1. Sensors

Physical parameters including temperature, pressure, vibration, and humidity are measured using a network of sensors.

Each sensor outputs a time-series signal reflecting changing conditions over time.

- If there are n sensors, the data at time t is:

$$x(t) = [x_1(t), x_2(t), \dots, x_n(t)]. \quad (4)$$

3.3.2. Data Collection Points

These points aggregate raw sensor data from various industrial environments or facilities, serving as localized data hubs before forwarding information to the edge.

- Let $\{x(t_1), x(t_2), \dots, x(t_T)\}$ represent aggregated data samples at different times $t_1, t_2, \dots, t_T$.

3.3.3. Real-time Data Streaming

Data is continuously streamed to edge nodes, enabling real-time analytics and rapid decision-making.

- Streaming function:

$$x(t) \xrightarrow{\text{stream}} \text{Edge} \quad (5)$$

ensuring continuous data flow.

3.4. Edge Computing

3.4.1. Data Filtering and Reduction at Edge

Edge nodes preprocess data locally, removing noise, selecting relevant features, and reducing data dimensionality to optimize bandwidth and storage usage.

- A filtering operation f_{edge} :

$$y(t) = f_{\text{edge}}(x(t)) \quad (6)$$

where $y(t)$ is a reduced data vector.

3.4.2. Real-time Decision Making via AI

AI models deployed at the edge classify incoming data as normal or anomalous, enabling immediate on-site decisions without depending on cloud latency.

- Edge-based inference:

$$\hat{z}(t) = g_{\text{edge}}(y(t)) \quad (7)$$

where $\hat{z}(t)$ might be a binary indicator (0 or 1) of an anomaly.

3.4.3. Edge Analytics for Immediate Insights

Analytics tools running at the edge derive actionable insights on-the-fly, allowing near-instant responses (e.g., local control adjustments).

- Real-time analytics function h_{edge} :

$$\text{Insight}(t) = h_{\text{edge}}(y(t)) \quad (8)$$

providing immediate summaries or Key Performance Indicators (KPIs).

3.5. Data Preprocessing

3.5.1. Data Cleaning

Remove noise and outliers to ensure signal integrity. This improves data quality for subsequent modeling steps.

- Moving average filter:

$$\tilde{x}(t) = \frac{1}{k} \sum_{\tau=t}^{t-k+1} x(\tau) \quad (9)$$

3.5.2. Feature Engineering

Extracting and selecting relevant features (e.g., statistical moments, frequency components) enhances model accuracy and reduces complexity.

- Feature extraction function ϕ :

$$\phi(x(t)) = [\mu(x(t)), \sigma^2(x(t)), \dots] \quad (10)$$

3.5.3. Time Series Analysis

Decompose signals into trend, seasonal, and residual components, or apply spectral analysis to identify underlying patterns.

- Decomposition:

$$x(t) = T(t) + S(t) + R(t) \quad (11)$$

3.6. Decentralized Storage

3.6.1. IPFS for High Redundancy/Availability

InterPlanetary File System

(IPFS) uses content-addressing, distributing data chunks across multiple nodes, ensuring redundancy and fault tolerance.

- Data chunks identified by hash:

$$H(d_i) = \text{hash}(d_i) \quad (12)$$

3.6.2. Data Replication and Pinning

Critical data chunks are replicated and pinned on multiple nodes to ensure data remains available, even if some nodes go offline.

- Replication condition:

$$\forall d_i, \exists n_j: d_i \in n_j \quad (13)$$

3.6.3. Access Management (Confidentiality)

Access is controlled through encryption keys. Only permitted users who has correct key can decrypt and inspect the data stored.

- Authorization check:

$$A_{\text{storage}}(u, d_i) = \begin{cases} 1 & \text{if user } u \text{ has key for } d_i \\ 0 & \text{otherwise} \end{cases} \quad (14)$$

3.7. Blockchain Layer

3.7.1. Distributed Ledger

Transactions are stored in a chained ledger of blocks, making records tamper-evident and enhancing trust.

- Blocks chained via cryptographic hashes:

$$B_j = \{\text{Transactions}, H(B_{j-1})\} \quad (15)$$

3.7.2. Smart Contracts

Self-executing contracts encode business logic, triggering actions when predefined conditions are met.

- Smart contract function C :

$$O = C(I) \quad (16)$$

where I = inputs and O = outputs.

3.7.3. Consensus Algorithms

Consensus guarantees all nodes agree on the blockchain state. Proof of Stake protocols prevent fraud and double spending.

- Find n s.t.:

$$H(B_j, n) < \text{TargetDifficulty} \quad (17)$$

3.7.4. Encryption (Secure Data Handling)

Cryptographic methods ensure data confidentiality, integrity, and authenticity on the blockchain.

- Encryption and hashing:

$$H(d) = \text{hash}(d), \quad \text{Enc}(d) = \text{encryption}(d, \text{key}) \quad (18)$$

3.8. Privacy-Preserving

3.8.1. Federated Learning

Models are trained locally at each data source and only model parameters are shared, protecting raw data privacy.

- Global model update:

$$\theta \leftarrow \frac{1}{M} \sum_{m=1}^M \theta_m \quad (19)$$

3.8.2. Homomorphic Encryption

Homomorphic Encryption enables evaluations on encrypted data unless revealing it, preserving privacy throughout processing.

- Homomorphic properties:

$$\begin{aligned} Enc(a + b) &= Enc(a) \oplus Enc(b), \quad Enc(a \times b) \\ &= Enc(a) \otimes Enc(b) \end{aligned} \quad (20)$$

3.8.3. Zero-Knowledge Proofs

Zero-Knowledge Proofs (ZKP) permit to offer up an experience of a secret w without exposing the secret itself to the examiner. This technique ensures privacy and security while establishing trust between the parties involved.

- Zero-Knowledge Proof:

$$ZKP(S, w) \rightarrow \text{Proof, Examiner}(S, \text{Proof}) = \text{True} \quad (21)$$

the statement being proved and w is the secret knowledge. The examiner learns that the report is true lack gaining any knowledge of w .

3.9. Predictive Maintenance

3.9.1. Deep Learning Models

Artificial Neural Networks (ANN) are employed to analyze historical sensor data to identify unusual patterns. This capability allows for the detection of anomalies and preemptive identification of potential failures.

- Fault probability prediction:

$$p(\text{fault at } t + \Delta t) = ANN(x(t); \theta) \quad (22)$$

3.9.2. Continuous Learning for Adaptation

Models update continuously as new data arrives, adapting to evolving conditions or equipment aging patterns.

- Parameter update rule:

$$\theta \leftarrow \theta - \eta \nabla_{\theta} L(\theta; X_{\text{new}}) \quad (23)$$

3.9.3. Integration with Automation Systems

Predicted failures can trigger automated maintenance tasks, inventory replenishment, or process adjustments, reducing downtime and increasing efficiency.

- Automated action triggered by anomaly detection:

$$\text{Action}(t) = g(\text{Anomaly}(t)) \quad (24)$$

where $\text{Action}(t)$ could be sending a maintenance order.

3.10. Security & Performance

3.10.1. Regular Security Audits & Compliance

Periodic audits ensure the system adheres to security standards and identify potential vulnerabilities for timely remediation.

- Security compliance score:

$$\mathcal{S} \geq \mathcal{S}_{\text{min_compliance}} \quad (25)$$

3.10.2. Performance Monitoring

Monitoring performance metrics (latency, throughput, resource usage) ensures the system meets Service Level Agreements (SLAs) and user expectations.

- Latency and throughput as functions of load L :

$$\lambda = f_{\text{latency}}(L), \quad \tau = f_{\text{throughput}}(L) \quad (26)$$

3.10.3. Scalability Assessments & Stress Testing

Stress tests and scalability evaluations ensure the system can handle increasing load without degraded performance.

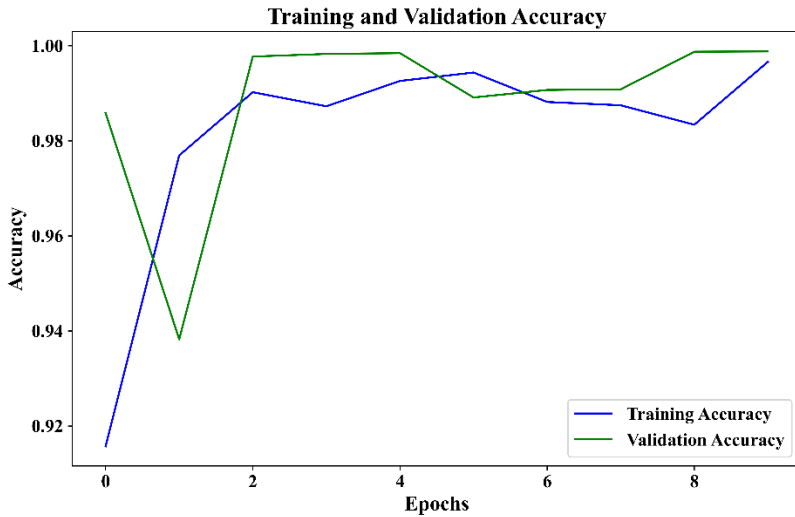
- Scalability condition:

$$\lim_{L \rightarrow \infty} \frac{\tau(L)}{L} \approx \text{constant}, \quad \lambda(L) \nrightarrow \infty \quad (27)$$

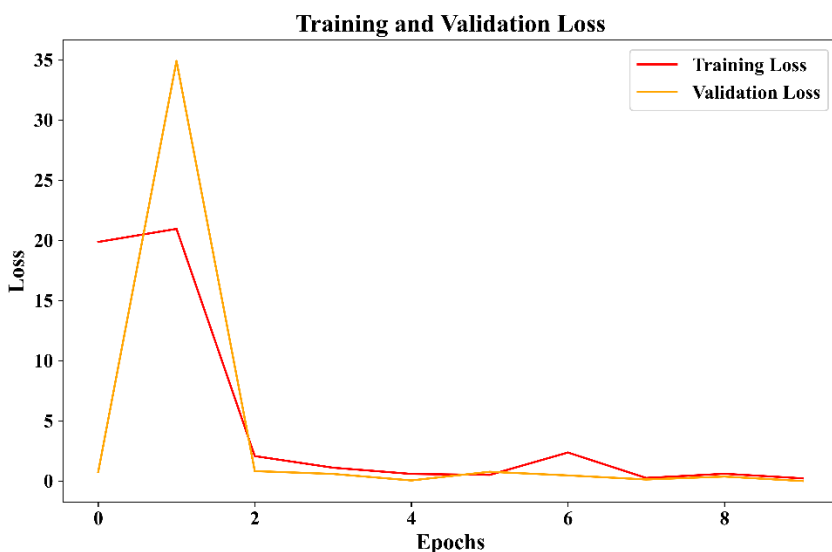
4. Result and Discussion

4.1. Model Evaluation

The accuracy plot shows the training and validation accuracy over epochs in the model training process. First, equally the training and validation accuracies start at different levels. The training accuracy is lower than that of the validation. With the progression of training, both the accuracies rise considerably and sharply by the second epoch. After the initial increase, accuracy during training levels off and remains consistently high, either at or above 98%, indicating a strong fit to the training data. The variability in validation accuracy reflects the efficiency of the model when used to current, unseen data. Even though it peaks at third epoch, further oscillation can be considered as due to overfitting to indicate that the model seems over-trained on the particular data and hence would possibly not generalize well to unknown data.



(a) Accuracy Plot



(b) Loss Plot

Figure 2: Training and Validation Plot

The loss Plot illustrates the training and validation loss across epochs. In the early stages, both losses decrease, which is typical as the model learns from training data. However, the training loss shows a more consistent and gradual decline, indicating effective learning. On the other hand, at the beginning the validation loss decreases but then shows a significant spike at the second epoch, suggesting that the model maybe learning the data patterns to the training data that do not generalize the validation set. Following this spike, the validation loss trends downward again, albeit with minor fluctuations, possibly due to adjustments in the model's parameters to reduce overfitting and improve its generalization on the validation data. This Plot hints at the challenges in achieving a model that balances well between fitting the training data and applying to new data.

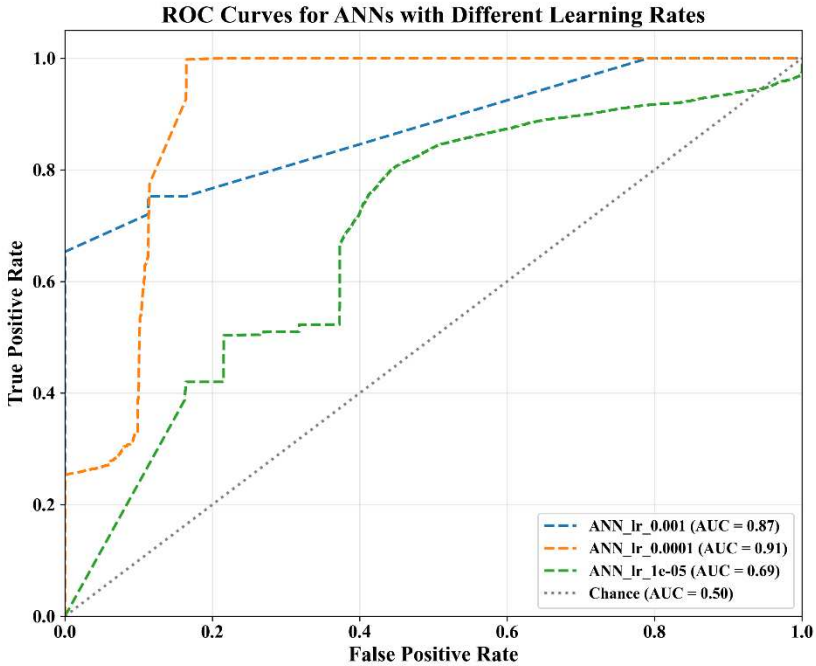


Figure 3: Receiver Operating Characteristic (ROC)

Fig.3 is comparing performance of ANNs that are trained with various learning rates (0.001, 0.0001, and 1e-05) by plotting TPR vs FPR at several threshold levels. The dashed curves show ROC for each learning rate and AUC measures the overall performance. The best performance is attained by the model with the learning rate of 0.0001, with an AUC of 0.91, indicating high discrimination ability. The model with the learning rate of 0.001 follows (AUC = 0.87), and the model with 1e-05 performs badly (AUC = 0.69), which is slightly better than random chance (AUC = 0.50, the diagonal line).

4.2. Confusion Matrix

Fig. 4 shows confusion matrix for a binary categorization issue where the class are labeled as Normal and Attack. The confusion matrix reveals that the model accurately predicted 4,842 instances as "Attack" and 25,562 instances as "Normal." However, there were 29 false positives where "Normal" was misclassified as "Attack," and 7 false negatives where "Attack" was misclassified as "Normal." The color intensity of the cells reflects the frequency of predictions, with higher values represented by darker shades. Overall, the model demonstrates high accuracy with minimal misclassifications.

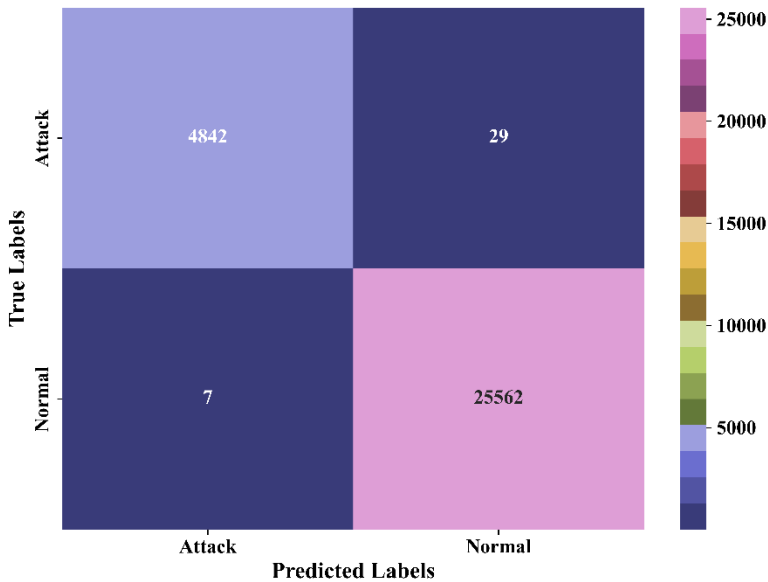


Figure 4: Confusion Matrix

4.3. Performance Analysis of Proposed Work

The provided metrics indicate an exceptionally high-performing model. The Accuracy of 99.88% signifies that nearly all predictions were correct. Similarly, Precision of 99.89% reflects a low rate of FP, while the Recall of 99.97% indicates the model is outstanding at determining all appropriate cases with minimal FN. The F1 Score of 99.93% balances precision and recall, ensures powerful overall performance. The Jaccard Index of 99.86% highlights strong similarity between predicted and actual sets, while Kappa is 99.56% suggests a high agreement beyond chance. The FPV and FNR are extremely down at 0.006% and 0.00027%, respectively, further underscoring the model's reliability and precision in predictions.

Table 1: Performance Metrics Table of Proposed ANN

Metric	Value
Accuracy	99.88173
Precision	99.88668
Recall	99.97262
F1_score	99.92963
Jaccard	99.85936
Kappa	99.55926
FPV	0.005954
FNR	0.000274

Fig. 5, the bar chart illustrates the performance metrics of a model, showing exceptionally high values across all parameters: Accuracy (99.88%), Precision (99.88%), Recall (99.97%), F1-score (99.92%), Jaccard (99.85%), and Kappa (99.55%). The metrics show the model has great accuracy, precision, recall, and F1 score. It ensures that the mode has a very low amount of false classifications. In Fig. 6, the error metrics, shown as FPV and FNR, are shown to be extremely low, at

0.005954% and 0.000274%, respectively. This shows that the model will give the wrong classification quite rarely. The figure displays the overall performance of the models using the performance metrics, powerful error handling, and good classification performance.

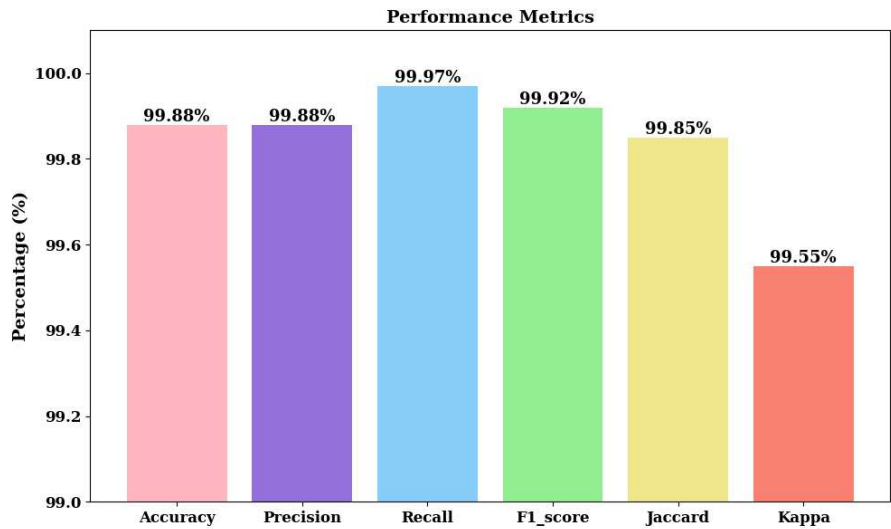


Figure 5: Performance Metrics of Proposed ANN

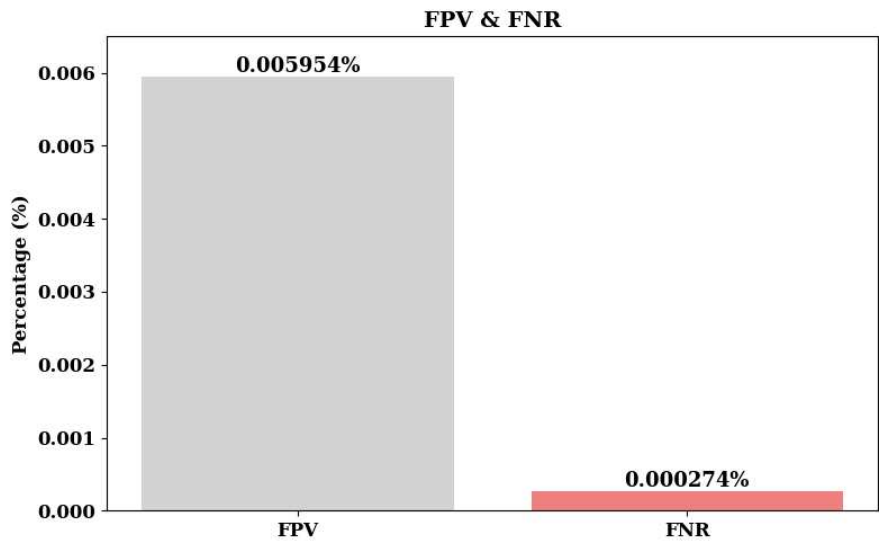


Figure 6: Performance Metrics (FPV & FNR) of Proposed ANN

4.4. Comparative Analysis of the Proposed Work

Table 2 correlates the performance metrics of various techniques including the suggested method ANN and methods used in other research work in terms of accuracy, precision, recall and F1-score. The proposed method using ANN achieves the highest performance in accuracy 99.88% and recall 99.97% indicating its ability to correctly identify relevant cases with minimal errors. In comparison Nouman et al. (2023) employing the HIDT method achieves inexpensive metrics with slightly higher precision 99.92% and F1-score 99.89% showing balanced performance across all parameters. Kumar et al. (2023) using BiLSTM attains lower recall 96.76% and F1-

score 97.1% signifying room for development in capturing true positives. Mishra (2023) using HGB delivers consistent metrics across accuracy precision and recall 99% with an F1-score of 99.5% highlighting robust but little lower performance when compared to other methods. Overall, the proposed ANN method establishes superior general performance metrics it the most effective approach among the compared techniques.

Table 2: Performance Metrics Comparison with Existing Techniques

Authors	Techniques Used	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
Proposed Method	ANN	99.88	99.88	99.97	99.92
Kumar et al (2023)	BiLSTM	99.03	99.01	96.76	97.1
Mishra (2023)	HIDT	99.86	99.92	99.94	99.89
Nouman et al (2023)	HGB	99	99	99	99.5

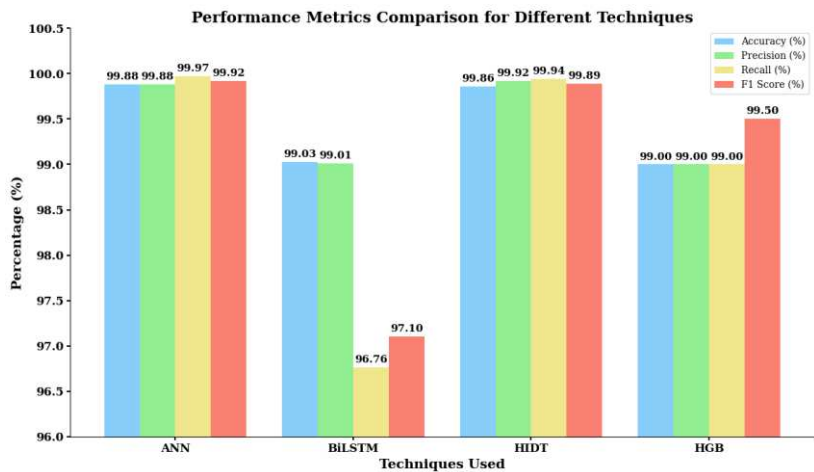


Figure 7: Performance Metrics

Fig. 7 shows the performance metrics of different techniques such as ANN, BiLSTM, HIDT, and HGB, as applied in different studies. The performance of the ANN technique as presented in our work is outstanding with an accuracy 99.88%, precision 99.88%, recall 99.97% and an F1 Score 99.92%. The performance of the BiLSTM technique is rather convincing with an accuracy 99.03%, precision 99.01%, a somewhat lower recall 96.76%, and an F1 Score of 97.10%. The HIDT technique shows outstanding performance, with an accuracy 99.86%, precision 99.92%, recall 99.94%, and an F1 Score 99.89%. Eventually, the HGB method shows outstanding performance, with an accuracy, precision, recall, and F1 Score 99.00%. Even if all other methods have good metrics, none of them can beat the proposed method, ANN, with the highest value among all of them. This shows the outstanding performance in the proposed method.

5. Conclusion

The proposed method leverages blockchain, privacy-preserving techniques, and predictive maintenance models to ensure the IoT environment is secure, scalable, and reliable. It has an accuracy 99.88%, precision 99.89%, recall 99.97%, and F1 score

99.93%, which shows the robust security and dynamic efficiency. The error rate is also very low, with FPR 0.005954% and FNR 0.000274%, ensuring accurate prediction and security operations. By integrating blockchain, federated learning, and lightweight cryptographic methods, the method establishes a reliable, scalable, and secure solution for modern IoT infrastructures. The future enhancements can include optimizing computational efficiency, scalability using advanced methods like proof-of-authority and blockchain scalability such as sharding, and other privacy-preserving methods such as zero-knowledge proofs, integrating edge AI and FL models in IoT applications.

Declaration

Data Availability

Not applicable

Conflicts of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have influenced the work reported in this paper.

Funding Statement

The authors present their appreciation to King Saud University for funding this research through the Ongoing Research Funding program, (ORF-2025-1006), King Saud University, Riyadh, Saudi Arabia.

Author Contributions

Haitham A. Mahmoud: Conceptualization, methodology, supervision, writing review & editing.

Ahmed T. Soliman: System design, blockchain framework development, validation.

Mohammed El-Meligy: Predictive maintenance model design, performance evaluation, data analysis.

Azhar Imran: Privacy-preserving algorithms, federated learning integration, software implementation.

Abdelaty Edrees Abdelgawad: Manuscript writing—original draft, literature review, result interpretation.

All authors read and approved the final manuscript.

Ethical Approval

This study does not involve human participants, patient data, or animal experiments. Ethical approval was therefore not required.

Consent to Participate

Not applicable, as no human subjects were involved in this study.

Consent for Publication

All authors consent to the publication of this manuscript.

Competing Interests

The authors declare no competing interests.

Acknowledgment

The authors present their appreciation to King Saud University for funding this research through the Ongoing Research Funding program, (ORF-2025-1006), King Saud University, Riyadh, Saudi Arabia.

Reference

1. Edge-IIoTset Cyber Security Dataset of IoT & IIoT. 2022. Kaggle. Available from: <https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iiot-iiot>.

2. Alabadi, M., Habbal, A., and Guizani, M. 2024. An Innovative Decentralized and Distributed Deep Learning Framework for Predictive Maintenance in the Industrial Internet of Things. *IEEE Internet of Things Journal*.
3. Amjad, S., Craß, S., Taudes, A., and Svetinovic, D. 2024. Privacy and Security Requirements Challenges in Blockchain-Based Decentralized Federated Learning. In *Proceedings of the 2024 IEEE 32nd International Requirements Engineering Conference Workshops (REW)*. IEEE, 348–352.
4. Liu, J., Sun, C. A., Wu, T., and Aiello, M. 2024. Blockchain-based Privacy-preserving Data Service Provisioning for Internet of Things. In *Proceedings of the 2024 IEEE International Conference on Web Services (ICWS)*. IEEE, 524–534.
5. Kashif, M., and Kalkan, K. 2024. EPIoT: Enhanced privacy preservation-based blockchain mechanism for Internet-of-Things. *Computer Networks* 238, 110107.
6. Singh, S., Rathore, S., Alfarraj, O., Tolba, A., and Yoon, B. 2022. A framework for privacy-preservation of IoT healthcare data using federated learning and blockchain technology. *Future Generation Computer Systems* 129, 380–388.
7. Zhou, Q., Lai, C., Guo, Q., Ma, H., and Zheng, D. 2022. A novel privacy protection scheme for Internet of Things based on blockchain and privacy set intersection technique. *Journal of Cloud Computing* 11(1), 93.
8. Alabadi, M., and Habbal, A. 2023. Next-generation predictive maintenance: leveraging blockchain and dynamic deep learning in a domain-independent system. *PeerJ Computer Science* 9, e1712.
9. Chen, J., Li, K., and Philip, S. Y. 2021. Privacy-preserving deep learning model for decentralized VANETs using fully homomorphic encryption and blockchain. *IEEE Transactions on Intelligent Transportation Systems* 23(8), 11633–11642.
10. Kumar, P., Kumar, R., Gupta, G. P., Tripathi, R., Jolfaei, A., and Islam, A. N. 2023. A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare systems. *Journal of Parallel and Distributed Computing* 172, 69–83.
11. Nouman, M., Qasim, U., Nasir, H., Almasoud, A., Imran, M., and Javaid, N. 2023. Malicious node detection using machine learning and distributed data storage using blockchain in WSNs. *IEEE Access* 11, 6106–6121.
12. Mishra, S. 2023. Blockchain and machine learning-based hybrid IDS to protect smart networks and preserve privacy. *Electronics* 12(16), 3524.