Vol. 08, No. 3 (2026) 1727-1742, doi: 10.24874/PES08.03.025

Proceedings on Engineering Sciences

www.pesjournal.net

BLOCKCHAIN-ASSISTED RF-LSTM CYBER-PHYSICAL FRAMEWORK FOR SECURE DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS

M. Chitra
V. Deepa
R. Sreelakshmy
B. Venkateswarlu
K. Vidhyapriyadharshini
R. Manikandan
Firas Tayseer Ayasrah
Sudhakar Sengan[1]

Received 14.05.2026.
Revised 29.06.2026.
Accepted 05.08.2026.

Keywords:

Blockchain, Data transmission, Authentication, WSN, Security, Authorisation

A B S T R A C T

Wireless sensor networks (WSN) are used for real-time monitoring, but they are also susceptible to cyber-physical system (CPS) attacks, such as tampering and unauthorised access. Conventional privacy and security systems face scalability and resource constraints. To address these challenges, this study proposes a Blockchain-Assisted Random Forest–LSTM (BA-RF-LSTM) model for improving the security and reliability of WSNs. The BA-RF-LSTM uses blockchain (BC) for secure, distributed data transfer. Using lightweight consensus and immutable ledgers, it maintains trust, integrity, and confidentiality. Smart contracts (SC) ensure accurate data transfer and compliance with consensus protocols. BC supports decentralized authentication, data security, and logging. This study developed a simulation-based CPS to investigate secure data transmission in resource-constrained WSN environments. Under the evaluated simulation configuration, the model achieved a mean network throughput of 67.34 kbps and an end-to-end delay of 232 ms. The simulation results indicate that the proposed method can reduce network overhead and data-tampering risks while improving secure data transmission. The proposed model achieved a mean data throughput of 67.34 kbps and an end-to-end network delay of 232 ms under the evaluated configuration. The experimental results show that the proposed method optimises WSN energy consumption, minimises data tampering, and enhances data security.

© 2026 Published by Faculty of Engineerin

1. INTRODUCTION

Wireless sensor networks (WSNs) are used for data collection and transmission in Internet of Things (IoT) applications such as smart cities, environmental monitoring, and many others (Hsiao & Sung, 2021). With WSN integration, data security and privacy have become primary concerns (She et al., 2019). Conventional

[1] Corresponding author: Sudhakar Sengan
Email: sudhasengan@gmail.com; sudhakars@esec.ac.in

security measures cannot address the computational resource and real-time demands of WSNs. This has motivated the development of new models that provide data security during data transfer in these environments (Ren et al., 2018). Blockchain (BC) is considered a method to improve WSN security because it provides decentralized and secure features (Khalaf & Abdulsahib, 2021).

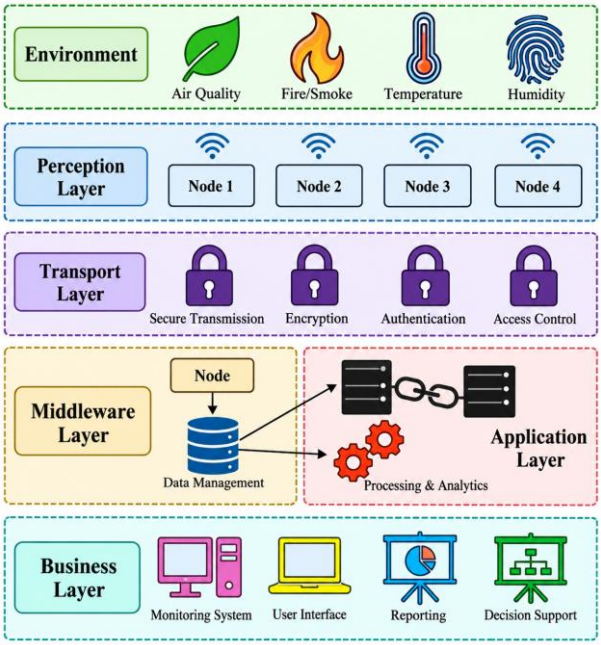


Figure 1. The Proposed BA-RF-LSTM

Integrating BC features such as decentralized trust, cryptographic hashing, and smart contracts (SCs) in WSNs can enhance data authenticity, integrity, confidentiality, and secure transaction validation. In the proposed model, BC serves as an immutable distributed ledger to record and validate sensor transactions, and SCs enable automated security-policy enforcement, access control, and transaction verification. Figure 1 shows the proposed Blockchain-Assisted Random Forest–Long Short-Term Memory (BA-RF-LSTM), which integrates BC-based security mechanisms with machine-learning (ML)-assisted anomaly detection (AD) for secure data transmission in WSNs (Rao et al., 2024).

The proposed BA-RF-LSTM for cyber-physical systems (CPS) uses BC to provide a secure, scalable method for sensor nodes (SNs) to connect to the server. The model addresses authorization, node validation, and data consistency. To address these problems, a lightweight CPS is employed that addresses the security standards and limitations of SNs (Ramasamy et al., 2021). This CPS has provided an efficient method for securing WSN data (Moinet et al., 2017). The proposed CPS integrates BC to improve data transmission integrity and reduce the risk of data manipulation and attacks. Performance analysis of BA-RF-LSTM validates its potential to enhance WSN communication security across numerous IoT applications (Sagar et al., 2024).

In this study, a CPS is used in the context of BC to improve the security of WSN data transmission. The aim is to develop and evaluate a BC-based protocol that provides authentication, data integrity, and secure communication within a WSN without relying on a single authority.

The primary objectives of this study are to:

(a) This study proposes a BA-RF-LSTM for secure data transmission in WSNs. The model combines BC-based decentralized authentication and tamper-resistant transaction logging with ML-based detection of malicious and anomalous network behavior.

(b) Detect malicious activities, including data tampering, intrusion, DoS attacks, unauthorized access, and abnormal node behavior, using ML-based AD.

(c) Ensure sensor-DI and authentication using BC's immutable distributed ledger and cryptographic hashing functions.

(d) Implement decentralized authentication and authorization to reduce dependence on a centralized security authority.

(e) Employ SC to automate transaction validation, security-policy execution, and fault-recovery actions.

(f) Evaluate the proposed BA-RF-LSTM in terms of end-to-end delay (EED), network throughput (NT), resource utilization (RU), data integrity (DI), AD accuracy, scalability, and EC.

The contribution of this study is as follows:

a) To provide decentralized, tamper-resistant, and secure data transmission without depending on a central authority. The proposed BA-RF-LSTM is designed to provide decentralized, tamper-resistant, and secure data transmission in WSNs without relying on a central authority.

b) A lightweight CPS is designed to meet the computational and resource constraints of SNs and remain secure.

c) SCs are embedded to automatically execute security policy elements, such as fault recovery, data validation, and triggering security countermeasures, in real time.

d) A decentralized authentication and authorization mechanism uses BC's immutable ledger and cryptographic hash functions, ensuring high data integrity under the evaluated conditions.

e) For the proposed BA-RF-LSTM, EED, NT, and RU are 232 *ms*, 67.34 *kbps*, and 23.2 MB, with superior results compared to the existing BC-WSN + BC-WBAN.

f) The model is scalable, enabling a network with more than 1000 nodes, achieving high security monitoring accuracy over 95% and a high fault recovery success rate (RSR) over 90%, making it an effective solution for securing real-time IoT communications across several WSN applications.

The remainder of the article is organized as follows: the overview of BC-based WSN is specified in Section 1, the complete analysis of the BC-WSN with research gaps is specified in Section 2, the proposed BA-RF-LSTM for WSN is presented in Section 3; the article is concluded in Section 4.

2. RELATED WORKS

Traditional WSNs had limitations in detecting malicious nodes due to centralized decision-making. The proposed CSP, which combines BC-WSNs, has shown improvements in NT and transparency. Malicious-node detection and data aggregation also improved (Awan et al., 2022), but this method presents integration problems and performance overhead (Krishna et al., 2024; Jyothi et al., 2025; Natraj et al., 2025).

The centralized network model and the potential for node attacks make wireless body area networks (WBANs) vulnerable to security risks, as prior work has shown (Ismail et al., 2023). A BC that integrates authentication and blind signatures enhances data security and reliability. Although this solution improves data-transfer Security, it is not scalable and cannot be applied to larger networks. When securing WSNs against malicious node attacks, other research shows that conventional BCs' Merkle hash trees perform poorly (Xiao et al., 2020; Mann et al., 2025).

Data storage security has been improved, and the recommended unbounded cryptographic accumulator has solved problems with non-member proofs. However, this approach is more advanced and may face scalability and performance challenges (Baptist et al., 2026; Chaudhari et al., 2025; Baptist et al., 2025; Cheekati et al., 2025;

Finally, integrating BC with software-defined networking (SDN) has proven effective for enhancing the privacy and Security of healthcare IoT. This model enhances Security, efficiency, and access control; however, scalability and integration remain challenges (Wang et al., 2020).

Several studies have verified the use of BC to ensure data integrity and secure transmission in WSNs. BC provides an unalterable record that bad actors can barely manipulate after data is captured. Authors stress the importance of BC in ensuring safe data communication, maintaining only authorized nodes (equipment) during data communication, and preventing unauthorized access or alteration (Hasan et al., 2022).

BC transparency can occasionally conflict with the privacy of sensitive data, particularly in the medical field. To address this, privacy-preserving solutions such as homomorphic encryption and zero-knowledge proofs (ZKPs) are proposed. Anonymity and confidentiality in healthcare CPS are extremely imperative, and several studies investigate privacy-sensitive BC protocols for IoT networks (Ghanimi et al., 2024).

A critical weakness of several studies is that BC is not scalable to WSNs. Although BC can provide a high level of Security, its efficiency may decline as the number of connected devices increases, particularly in busy networks such as healthcare systems with many medical sensors.

Related research has investigated BC-enabled cyber-physical models for distributed IoT applications. Wang et al. (2025) suggest a BC-empowered human-cyber-physical system (H-CPS) for smart agriculture that integrates blockchain, IoT, AI, edge computing, and remote-sensing technologies. The model supports decentralized and tamper-resistant data management, traceability, secure information sharing, and data-driven decision-making. Although this work validates the feasibility of BC integration in distributed CPS environments, scalability and resource overhead remain important considerations when adapting such models.

In some works, Sharding, Layer 2 solutions, and hybrid BC have been suggested to address these scalability problems. Decentralization of BC is itself fault-tolerant. Nevertheless, network resilience cannot be guaranteed in the face of device failures or attacks. Authors suggest using redundancy and backups in BC to improve fault tolerance in industrial CPS and environmental monitoring networks. Nevertheless, critical application fault resilience, such as that in healthcare, remains a field in need of further research (Alarood et al., 2025).

CPS that enable real-time decision-making are required for numerous healthcare applications. Although BC has been proven secure for data transmission, it suffers from latency and a time-consuming consensus process, which is undesirable in networks that require rapid responses. Authors emphasize that a more rapid consensus mechanism (CM) and the integration of edge computing are required to enable low-latency decision-making (Khan et al., 2025).

Resource constraints, distributed deployment, malicious-node attacks, and the limitations of centralized security mechanisms are serious security challenges to traditional WSNs. Authors have explored BCs to improve decentralized trust, authentication, traceability, and secure data management in WSN environments (Awan et al., 2022; Ramasamy et al., 2021; She et al., 2019).

Moreover, WBANs are susceptible to illegal access, data tampering, and privacy attacks because they transmit highly sensitive sensor data over resource-limited WSNs. Such networks can use BC-based data-sharing architectures to improve data integrity, access control, and transaction traceability (Xiao et al., 2020; Hasan et al., 2022). However, using BC introduces extra computational, communication, storage, and scalability

overheads that must be considered when deploying BC-based security mechanisms in resource-constrained WSNs.

Moldovyan et al. (2017) investigated randomized pseudo-probabilistic encryption algorithms designed to strengthen cryptographic security by randomized encryption mechanisms. Although this work provides a relevant cryptographic perspective on secure data protection, it does not specifically address BC-based WSNs, Merkle-tree limitations, malicious-node detection, or cryptographic accumulators. Therefore, its relevance to the present study is limited to the underlying data confidentiality and cryptographic security features.

This section reviews the literature on BC integration in WSN, highlighting improvements in Security and performance across WSN and healthcare IoT, while noting the challenges of scalability and complexity (Table 1).

Table 1. Complete analysis of BC-WSN

Reference	Inference	Outcome	Technique Used	Significance
Hewa et al. (2022)	Conventional WSNs face challenges in detecting malicious nodes due to their centralized decision-making.	The BC-based method provides enhanced traceability, fairness, and Security for WSNs.	BC-WSN	Improved malicious node detection, online information aggregation, and overall WSN security management.
Mustafa et al. (2016).	WBANs are vulnerable to security attacks due to their centralized CSP and the potential for node tampering.	BC-WBAN improves Security and stability with enhanced data security	Authentication and blind signature protocols, BC	Provides a more secure and reliable data transmission system in WBANs.
Moldovyan et al. (2017)	Investigated randomized pseudo-probabilistic encryption approaches for strengthening cryptographic data protection	Randomization in the encryption process enhances cryptographic protection and increases resistance to cryptanalytic attacks.	Randomized pseudo-probabilistic encryption	Provides a relevant cryptographic perspective on data confidentiality and secure data protection; however, the study does not specifically address blockchain-based Networks, Merkle trees, malicious-node detection, or cryptographic accumulators.
Wu (2018)	Combining BC with SDN can address security and privacy problems in healthcare IoT	The network improves secure data sharing and management in SDWBANs, with low latency and high NT.	BC, SDN, SC	Enhances data confidentiality, access control, and overall system efficiency in healthcare IoT applications.

3. PROPOSED BA-RF-LSTM FOR WSN

Let the WSN consist of $'N'$ SNs denoted as $S = \{s_1, s_2, \dots, s_N\}$. Each SN generates a data packet D_i at time $'t'$, where the transaction was generated by the node s_i is embodied in Equation (1).

$$T_i = (D_i, S_i, H_i) \quad (1)$$

where D_i is sensed data, S_i is node identity, and H_i is the cryptographic hash value computed as in Equation (2).

$$H_i = H(D_i \parallel S_i) \quad (2)$$

The BC based CM validates each transaction before including it in the distributed ledger.
For a valid transaction, Equation (3)

$$C(T_i) = \begin{cases} 1, & H(T_i) < \text{Target} \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

To secure data transmission, lightweight encryption transforms the plaintext message $'M'$into ciphertext $'C'$, Equation (4).

$$C = E_L(M, k) \quad (4)$$

where $'k'$ is the encryption key; decryption retrieves the original message Equation (5).

$$M = D_L(C, k) \quad (5)$$

Feature vectors are extracted from network traffic and sensor behavior Equation (6)

$$X_i = [x_1, x_2, x_3, \dots, x_m] \quad (6)$$

where features include NT, EED, node energy, packet size, authentication failures, and traffic rate.

The ML classifier learns the mapping in Equation (7).

$$f: X \to Y \quad (7)$$

where $Y = \{0,1\}$, with $'0'$ is normal behavior and 1 as malicious activity.

For random forest (RF) classification, the final prediction is obtained using ensemble averaging, as in Equation (8).

$$RF(x) = \frac{1}{N_T}\sum_{i=1}^{N_T} T_i\,(x) \quad (8)$$

where $T_i(x)$ is the output of the i^{th}decision tree and $N_T$is the number of trees.

For temporal AD analysis, long short-term memory (LSTM) computes gated sequential updates.

The forget gate is defined as Equation (9)

$$f_t = \sigma(W_f[h_{t-1}, x_t] + b_f) \quad (9)$$

The input gate is given by Equation (10)

$$i_t = \sigma(W_i[h_{t-1}, x_t] + b_i) \quad (20)$$

The candidate cell state is defined as in Equation (11)

$$\tilde{c}_t = \tanh(W_c[h_{t-1}, x_t] + b_c) \quad (31)$$

The updated cell state is given by Equation (12)

$$c_t = f_t \odot c_{t-1} + i_t \odot \tilde{c}_t \quad (42)$$

The output gate is computed as in Equation (13)

$$o_t = \sigma(W_o[h_{t-1}, x_t] + b_o) \quad (53)$$

The hidden state is given in Equation (14)

$$h_t = o_t \odot \tanh(c_t) \quad (64)$$

The AD score is calculated from the deviation between experimental and predicted values in Equation (15)

$$A_t = \mid T_t^{obs} - T_t^{pred} \mid \quad (75)$$

An attack or AD is detected when Equation (16)

$$y_t = \begin{cases} 1, & A_t > \theta \\ 0, & A_t \le \theta \end{cases} \quad (86)$$

where θ is the anomaly threshold.

The AD accuracy is computed as in Equations (17)-(20).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (97)$$

Precision is:

$$Precision = \frac{TP}{TP+FP} \quad (108)$$

Recall is:

$$Recall = \frac{TP}{TP+FN} \quad (119)$$

The F1-score is:

$$F1 = \frac{2\times Precision\times Recall}{Precision+Recall} \quad (20)$$

The NT is computed as in Equation (21)

$$NT = \frac{N_{tx}}{T_{obs}} \quad (212)$$

where N_{tx} is the number of successfully transmitted packets and T_{obs} is observation time.

EED is defined as Equation (22)

$$EED = T_{receive} - T_{send} \quad (22)$$

The DI score is measured as in Equation (23)

$$DI = \frac{N_{valid}}{N_{total}} \times 100 \quad (23)$$

The total EC of the CPS-enabled BA-RF-LSTM is given by Equation (24)

$$EC = \sum_{i=1}^{N} E_i \quad (24)$$

The overall optimization objective of the proposed BC-assisted ML is formulated as Equation (25)

$$\min J = \alpha(EED) + \beta(EC) - \gamma(NT) - \delta(Accuracy) \quad (25)$$

where:

- $\alpha, \beta, \gamma, \delta$ are weighting coefficients,
- EED is transmission delay,
- EC is energy consumption,
- NT is throughput,
- $Accuracy$ is AD accuracy.

The proposed ML ensures secure and reliable data transmission in WSNs embedded with BC-based CPSs. Here, each SN continuously collects environmental or network data and sends it via a decentralized BC. The model aims to provide secure communication, detect malicious activity, maintain DI, and improve transmission efficiency in a resource-limited WSN.

Initially, the SN generates real-time data, such as temperature, humidity, pressure, and communication data. Each data packet sent is converted to a BC transaction, with the node identity and a cryptographic hash value added. This process ensures that unauthorized users cannot modify the data being sent. Every transaction is permanently and publicly recorded on the BC, enhancing transparency, traceability, and fault tolerance across the network.

The encryption mechanism improves confidentiality and reduces the risk of eavesdropping and unauthorized data access. Protection against replay attacks also requires suitable freshness mechanisms, such as timestamps,

sequence numbers, or nonces, combined with authentication and integrity verification.

Before transmission, the sensor encrypts the data using a predefined secret key. This encryption also protects against replay attacks and unauthorized data access. On the receiving side, the same secret key decrypts the data, recovering the original sensor data without compromising it. WSNs are resource-constrained networks; hence, lightweight cryptographic algorithms that minimize computation time and EC are preferred.

The ML component of the model is mainly responsible for AD. Network traffic data and sensor communication patterns are used as input features. These features include packet delivery ratio (PDR), node energy level, authentication failures, NT, EED, and abnormal communication frequency. The extracted features are then fed into an ML-based classifier to distinguish normal from malicious network behavior.

The proposed BA-RF-LSTM model effectively applies RF + LSTM to detect attacks. RF is an ensemble-learning classifier that combines multiple decision trees to improve classification robustness and reduce the risk of overfitting. It is particularly well-suited to detecting malicious nodes and abnormal traffic patterns in WSNs. Sequential sensor traffic patterns are also analysed using LSTM. As WSNs continuously generate time-series communication data, LSTM can effectively capture long-term dependencies and AD communication behavior associated with cyberattacks.

The AD mechanism compares the sensors' behavior with the expected behavior of a normal sensor. Node activity is classified as anomalous when its deviation from the expected behavior exceeds a predefined threshold. The mechanism can detect the following attacks: denial-of-service (DoS), data tampering, unauthorized access, malicious packet injection, and node failure. The BC is integrated with SCs, which automatically approve transactions and respond to security irregularities as soon as they are identified.

The performance of the proposed BA-RF-LSTM is evaluated using EED, NT, RU, AD accuracy, DI, and EC. The experimental results show that the proposed BA-RF-LSTM-based secure data transmission model effectively reduces EED, increases PDR, ensures DI, and reduces resource usage compared with conventional WSN security mechanisms.

The proposed ML-assisted BC provides a scalable, decentralized, and secure network for WSNs operating in CPS environments. These features of BC security, lightweight cryptography, SC, and intelligent AD mechanisms enhance the reliability, robustness, and real-time Security of IoT applications, making them more secure and resistant to attacks.

To develop the BA-RF-LSTM for WSN, start with BC, in which each node of the WSN acts as an individual member. The basic method generates transactions that encapsulate data and metadata.

A. Transactions: Each transaction t_i is a tuple defined as (D_i ,S_i ,H_i), where D_i is the data to be transmitted, S_i is the sender's detection or node identifier. H_i is the transaction's cryptographic hash function (HF), calculated as Hi=H(Di‖Si). H is a cryptographic HF that maps concatenated data and the sender's identity to a fixed-length hash.

B. CM: A transaction 't_i' to be incorporated into the BC is subjected to a CM as 'C', making it computationally difficult for any transaction to be incorporated into the BC without the user's consent. For example, in the Proof-of-Work system, the CM is calculated using Equation (26).

$$C(t_i)=\text{True if } H(t_i)<\text{Target} \quad (26)$$

where "Target" is a difficulty threshold that adjusts based on the network's overall computational power.

C. Cryptographic scheme: The CPS is essential for data security and privacy in the BC network. It uses HF and encryption algorithms to protect data from unauthorised access and modification.

D. Hash function (HF): The cryptographic HF 'H ', as a function mapping input data to a fixed-size output hash, is assumed in Equation (27).

$$H:\{0,1\}*\rightarrow\{0,1\}^n \quad (137)$$

The Security of 'H' is measured in terms of collisions and preimage attacks. In particular, the probability that two different inputs have the same hash value (a collision) is defined in Equation (28).

$$\Pr[H(x) = H(y)] < \epsilon \quad (28)$$

where 'ϵ' is the collision probability, ideally close to '0'.

E. Encryption and decryption: Implement lightweight encryption to secure data D_i, transmitted between nodes. The encryption function E_L Transforms PT into CT as 'C' using a key 'k' in Equation (29).

$$C = E_L(M,k) \quad (29)$$

where 'M' is the plaintext (PT) message and 'k' is the encryption key. Conversely, decryption D_L retrieves the original PT from the ciphertext (CT) specified in Equation (30).

$$M = D_L(C,k) \quad (30)$$

4. RESULT AND DISCUSSION

4.1. Experimental/Simulation Setting

The proposed BA-RF-LSTM was evaluated in a simulation-based environment developed using Network Simulator-3 (NS-3). The WSN topology, sensor-node communication, network traffic, faults, cyberattacks, transmission delays, throughput, and resource-utilization characteristics were simulated computationally. Hardware platforms such as Arduino Uno, Raspberry Pi, ESP32/ESP8266, Wi-Fi/LoRa communication modules, gateway nodes, and server-class blockchain nodes were considered as reference configurations for modeling the computational and communication characteristics of a prospective physical deployment; these devices were not assembled into a complete physical WSN testbed in the present study. Similarly, this work signified Ethereum/Hyperledger Fabric, SC functionality, and lightweight consensus mechanisms at the architectural and simulation/configuration level to evaluate BC-assisted transaction validation and security behavior. Therefore, interpret all quantitative results in this study as simulation-based results under the specified configuration rather than measurements from a physically deployed WSN/BC system.

The proposed BA-RF-LSTM is compared with the BC-WSN and BC-WBAN baseline methods on three main network performance metrics: EED, NT, and RU. Figure 2 shows the EED of the evaluated methods. Figure 2 also shows the proposed model's EED performance. Figure 3 shows the corresponding NT comparison, verifying BA-RF-LSTM's data transmission performance over the baseline methods. Figure 4 compares RU and discusses the computational resource requirements of the three methods. Table 4 provides the numerical data for Figures 2–4, enabling a uniform quantitative analysis.

For the BA-RF-LSTM test results, this study used an SN with microcontrollers and Wi-Fi modules. These nodes are connected to a server that handles block computations and data storage in the BC. This study used software components such as Ethereum and Hyperledger Fabric to manage the SC and consensus algorithms. In this study, we developed a simulation environment using Network Simulator-3 to visualize networks. Using this configuration, we measured the model's security features, response time, and NT.

Three criteria were used to measure BA-RF-LSTM's performance. EED measures the time for data to reach the central server from the SN and the time for BC transactions to complete. NT focuses on the volume of data sent and analyzed. The network's ability to manage data and perform BC operations relates to NT, and it uses the memory and computational resources of SN and BC applications.

This key metric helps measure the model's impact on CSP performance and prevents it from imposing excessive demand on system components. Together, these steps allow the user to see how well the model protects and secures data during transmission and how well the network's sensors are working. Table 4 provides a detailed analysis of performance metrics across different methods.

The proposed BA-RF-LSTM achieved an EED of 232 *ms*, NT of 67.34 *kbps*, and RU of 23.2 MB. In comparison, BC-WSN recorded an EED of 545 *ms*, NT of 34.45 *kbps*, and RU of 87.6 MB, whereas BC-WBAN recorded an EED of 645 *ms*, NT of 45.23 *kbps*, and RU of 64.3 MB. Under the evaluated experimental conditions, the proposed BA-RF-LSTM therefore achieved lower EED and RU and higher NT than the two baseline methods.

a) Data Collection and Transmission

Step 1: Each SN generates sensor data and sends it to the BC via edge nodes.

Step 2: The BC registers each transmission as a new block, with the SC activated to verify the data and ensure its accuracy and Security.

b) Fault Simulation

Step 1: Simulate faults (such as sensor failures, network failures, or cyberattacks) to test the network**'s** ability to manage them effectively.

Step 2: AD and security-monitoring tools evaluate the network's ability to detect these faults.

Step 3: Make recovery decisions based on the BC records or SC principles (*e.g.,* switching to backup sensors or re-establishing broken communication paths).
c) Analysis of Results and Evaluation.

Step 1: Verify the network's Security by measuring the AD rates for malicious activity and DI.
Step 2: Measure EED, NT, and RU.

Step 3: Verify the *network's* scalability by adding more sensors and devices.

4.2. Simulation Parameter

Table 2 summarizes the key parameters used to simulate secure data transmission and BA-RF-LSTM within a CPS. This is crucial in determining the parameters used to evaluate the performance, Security, and scalability of the BC-enabled network**.**

Table 2. Simulation Setup

Parameter	Description	Units	Expected Values	Notes
Number of Sensors	The number of SNs in the network that generate data and transmit it to the BC.	Sensors	10-500+	The scale varies based on simulation complexity.
Data Generation Rate	The rate at which SNs generate and transmit data.	Data points/sec	10-100+	Simulated sensor data rate (*e.g.*, temperature, ECG readings).
BC - CM	The consensus protocol used to verify transactions (sensor data) in the BC.	-	Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT)	Affects transaction verification speed and energy efficiency.
Blockchain Block-Confirmation/Consensus Latency	Time taken for a block containing sensor data to be confirmed by the network.	Milliseconds (*ms*)	500-1000 *ms*	Lower confirmation time is better for real-time applications.
SC Execution Time	Time taken by the BC to execute an SC based on predefined rules (*e.g.*, fault recovery)	*ms*	< 500 *ms*	Essential for automated recovery actions in CPS.
Network Latency	The delay in data transmission from sensor nodes to the BC network or the edge nodes.	*ms*	< 100 *ms*	Low EED is crucial for making real-time decisions.
Encryption Overhead	Encrypting data before transmission introduces computational overhead to ensure Security.	% of total resources	5-15%	Ensures data confidentiality but may impact performance.
Fault Detection Accuracy	The accuracy of the model in detecting faults or anomalies in sensor data (*e.g.*, sensor failures, data tampering).	%	90-100%	Higher accuracy ensures timely detection and intervention.
Intrusion Detection Rate (IDR)	The rate at which security breaches or attacks are detected by the Intrusion Detection System (IDS).	%	DI and Security achieve 100% immutability.	Higher values indicate stronger security defenses.
AD Accuracy	The network's ability to detect AD behaviour in sensor data or communication patterns.	%	DI and Security achieve 100% immutability.	Detects attacks such as eavesdropping and MITM attacks.
Maximum Blockchain Transaction Processing Capacity (TPS)	The number of data transmission transactions the BC processes per second.	TPS	50-1000 TPS	Measures the network's transaction processing capacity
DI	The percentage of transmitted data that remains untampered with in the BC.	%	99-100%	Ensures the authenticity of sensor data in the network.
Scalability	The network's ability to handle increasing numbers of SNs without significant performance degradation.	-	10-1000+ sensors	Measures the network's ability to scale in large networks.
EC	The amount of EC consumed by the SN, edge devices, and BC network.	Joules	50-200 Joules per day	Important for battery-operated sensors in IoT environments.
RSR	The percentage of successful recovery actions triggered after a fault is detected.	%	90-100%	Measures how reliable the network's fault recovery is.
Latency for Fault Recovery	The time the network takes to recover from a detected fault, including SC execution and automated actions.	*ms*	< 500 *ms*	Ensures quick recovery for real-time applications.
NT (BC)	The throughput of the BC network, *i.e.*, the number of transactions (sensor data logs) it can process per second.	*Transactions/sec*	50-5000	Measures the processing speed of BC transactions.
Intrusion Detection Rate (IDR)	Rate at which the IDS correctly detects security intrusions or attacks	%	Not evaluated	A separate quantitative IDR metric was not evaluated in the present study.
AD Accuracy	Classification accuracy of the AD in distinguishing normal and malicious/anomalous network behaviour	%	97.48%	Proposed BA-RF-LSTM result; detailed classification metrics are reported in Table 7

IDR was not independently quantified in the present evaluation and is therefore reported as "Not evaluated." In this work, we evaluated AD performance separately using classification accuracy, precision, recall, F1, FPR, and detection time. The proposed BA-RF-LSTM achieved an AD accuracy of 97.48% (Table 7).

The simulation hardware setup (Table 3) for the proposed BA-RF-LSTM for secure data transmission in WSNs is shown. The components listed in this table represent reference hardware/software configurations used to parameterize and describe the simulated BA-RF-LSTM. A complete physical implementation using these devices and blockchain platforms was not constructed or experimentally validated in this study.

Table 3. Reference Hardware and Software Configuration Represented in the Simulation Environment

Component	Hardware/Software	Description	Role in Simulation
Sensor Nodes (SN)	Microcontroller/Development Boards	Arduino Uno - Raspberry Pi - ESP32/ESP8266	Responsible for collecting data (*e.g.*, temperature, humidity, pressure); WSN with a gateway node
Sensors	Temperature Sensors: DHT11, DHT22 Pressure Sensors Humidity Sensors	Multiple sensors for environmental monitoring	Sensor data collection and transmission
Power Supply	Battery or Solar Panels	Power source for SN and gateway nodes	Ensures continuous operation of SN in remote areas
Gateway Nodes	Raspberry Pi, BeagleBone Black	Aggregates data from SN - Communicates with BC network (Wi-Fi or LoRa)	Serves as an intermediary between SN and the central server; Prepares data for BC validation
BC Node	Desktop PC/Server	Intel i5+ - 8GB RAM+ - SSD 100GB+ - Ethernet/Wi-Fi	Hosts the BC network; Stores data on the BC ledger; Runs consensus algorithms
BC	Hyperledger Fabric, Ethereum Geth (Go-Ethereum)	Software for running the BC network	Maintains the BC ledger and ensures DI - Executes SC for automated data validation
CM	Proof of Authority (PoA), Practical Byzantine Fault Tolerance (PBFT)	Lightweight consensus algorithm for validating data	Ensures only authentic data from SN is accepted and validated before storing on the BC
SC	Solidity (for Ethereum) Chaincode (for Hyperledger)	Used to automate verification, access control, and data sharing	Ensures that data is correctly verified and access to data is controlled based on predefined conditions
Networking Equipment	Wi-Fi Router/Access Points, LoRa Gateway (Optional)	Provides network connectivity between sensor nodes, gateway nodes, and the central server	Helps WSN across devices in the network; For long-range communication (LoRa) in large or remote networks
Server for Data Processing	Central Server	Desktop or server-class computer with necessary hardware specifications	Central data processing, analysis, and BC interaction Stores final validated data

4.3. Performance Metrics

The BC-enabled CPS ensures DI and security by implementing a BC that resists manipulation or eavesdropping once data is stored in the ledger. This cryptographically hashed property is also distributed and agreed upon via a CM, ensuring that only valid, authentic transactions are recorded.

This is measured by the percentage of valid transactions to the number of transactions recorded that have not been tampered with, Equation (31)

$$DISE = \frac{N_{valid}}{N_{total}} \times 100 \quad (31)$$

Latency, or fault recovery time, is the time between fault detection and the initiation of effective recovery activity after verification. In healthcare CPS, a quick response in emergent situations, such as ensuring patient safety, is imperative because delays can result in patient harm, requiring low latency,

$$L_{frt} = T_{recover} - T_{fault} \quad (32)$$

The NT of BC transactions measures the number of sensor data logs or control transactions the network can handle in one second (Equation (32)). Large-scale CPS requires high NT because many devices transmit data continuously. Effective NT ensures that the network can maintain active tasks without bottlenecks (Equation (33).

$$T_{bps} = \frac{N_{tx}}{T_{obs}} \quad (33)$$

Network scalability specifies how a BA-RF-LSTM can serve more connected nodes without compromising performance. A scalable network can avoid degradation in EED, NT, or Security, enabling reliable operation of an extensive healthcare network or a smart city deployment (Equation (34).

$$S = \frac{P(N)}{N} \quad (34)$$

Security monitoring measures network use and detects and responds to cyberattacks or unauthorized access attempts. An increase in the rate of detection implies that the IDS is sound in detecting the presence of threats like tampering, DoS attacks, or data interception Equation (35)

$$SME = \frac{TP}{TP+FN} \times 100 \quad (35)$$

The overall EC of BC nodes, sensors, and edge devices during continuous operation is determined by their EC. Maximizing this measure makes CPS sustainable, particularly for battery-powered or remote healthcare monitoring equipment, Equation (36).

$$EC = \sum_{i=1}^{n} E_i \quad (36)$$

4.4. Performance Illustration

The performance of the proposed BA-RF-LSTM is evaluated using RU, EED for data transmission, NT, and BC overhead. The results are compared with traditional WSNs without BC.

Table 4 and Figure 2 show that the network data-transmission EED of BA-RF-LSTM is 232 ms, compared with 545 ms for BC-WSN and 645 ms for BC-WBAN. This metric represents communication delay within the simulated WSN path and is distinct from blockchain block-confirmation/consensus latency. The latter is evaluated separately and falls within the 500–1,000 ms range under the proposed configuration.

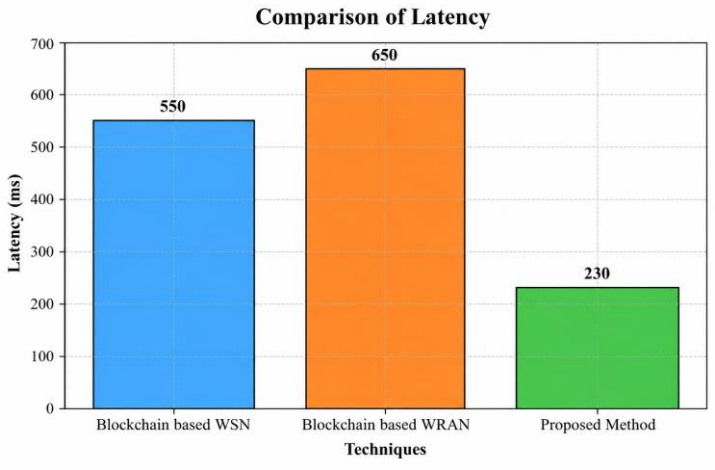


Figure 2. Comparison of EED

Table 4. Comparison of EED, NT, and RU

Technique	Network Data-Transmission EED **(ms)**	**Data Throughput (kbps)**	**RU (MB)**
BC-WSN	545	34.45	87.6
BC-WBAN	645	45.23	64.3
Proposed BA-RF-LSTM	**232**	**67.34**	**23.2**

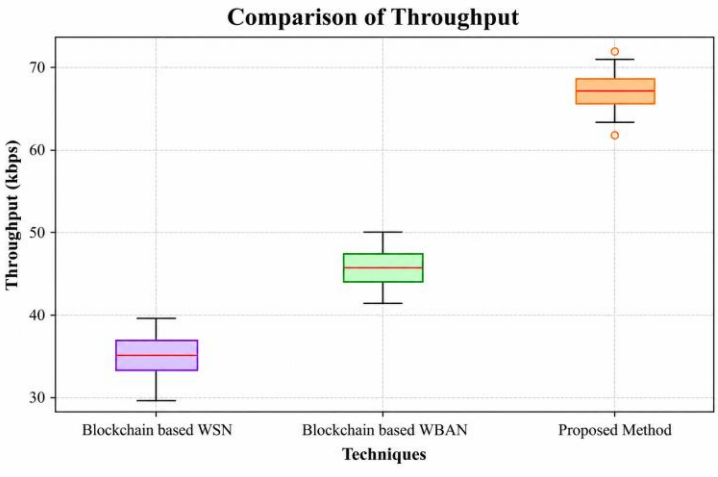


Figure 3. Comparison of NT

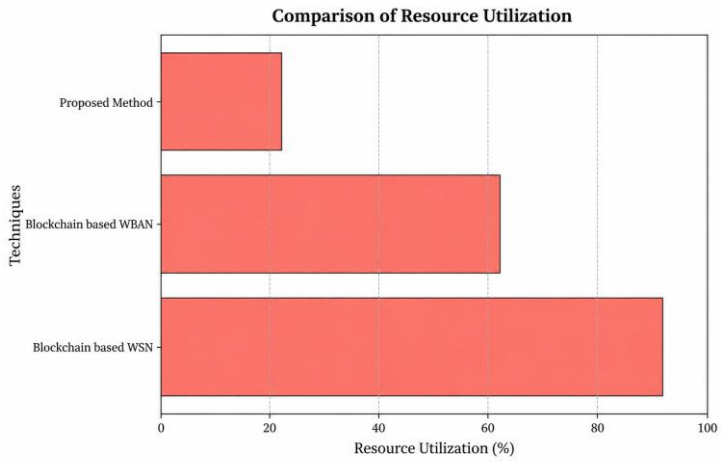


Figure 4. Comparison of RU

Table 5. Comparison of Security and Scalability Metrics

Metric	Existing	Proposed
Data Integrity and Security (%)	90–95	100
Blockchain Block-Confirmation/Consensus Latency (ms)	1500–3000	500–1000
Blockchain Transaction Throughput (TPS)	10–20	>50
Network Scalability (Nodes)	≤200	>1000
Security Monitoring Rate (%)	80–85	>95
Energy Consumption	High	Reduced
Recovery Success Rate (%)	70–80	>90

4.5. Performance Analysis

Table 5 presents a comparative analysis of the security and scalability performance of the proposed BA-RF-LSTM and the existing method in terms of DI and security, EED, NT, EC, and RSR.

The proposed BA-RF-LSTM achieved a data throughput of 67.34 *kbps*, compared with 34.45 *kbps* for BC-WSN and 45.23 kbps for BC-WBAN. This data-throughput metric represents the rate of network data transmission and should not be confused with blockchain transaction throughput, which is expressed in TPS and represents the number of BC transactions processed or validated per second.

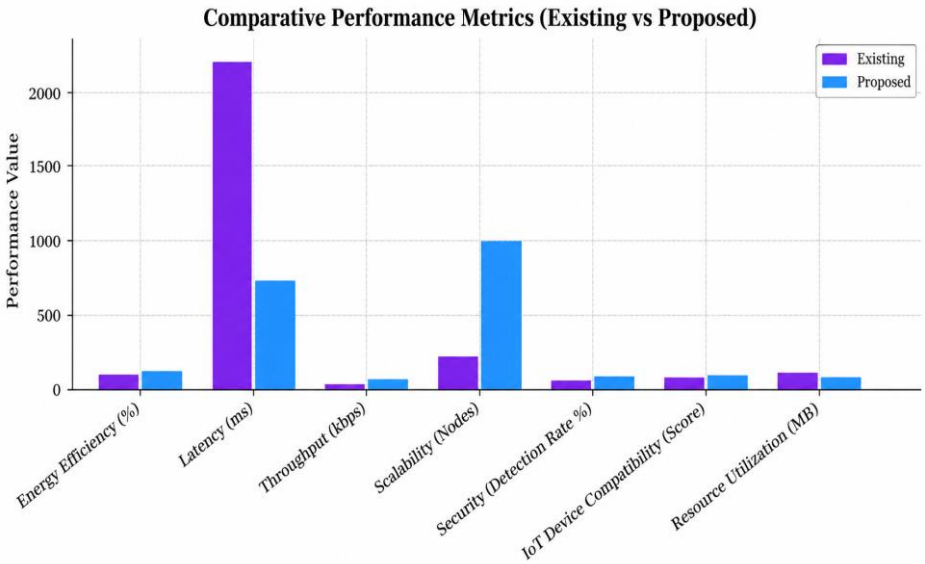


Figure 5. Performance Analysis

This study considers two distinct throughput measures (Table 4 and Figure 5). Data throughput, expressed in kilobits per second (*kbps*), represents the rate at which sensor/network data are successfully transmitted through the simulated WSN communication path. In contrast, BC transaction throughput, expressed in transactions per second (TPS), signifies the number of BC transactions processed or validated per second. These measures describe different features of system performance and are therefore evaluated and reported separately. The proposed BA-RF-LSTM achieved a data throughput of 67.34 *kbps*, whereas the BC transaction-processing evaluation indicated a throughput of >50 TPS under the corresponding evaluated configuration

The proposed BA-RF-LSTM should be evaluated in several independent simulation runs to increase the statistical reliability of the experimental test, and the mean, standard deviation, and 95% confidence interval for the main metrics should be reported, such as EED, NT, RU, EC, and AD performance. In addition, an ablation study should isolate the individual components of the BC layer, ML component, SC/CM, and the full integration, measure each component's performance by systematically removing it, and compare the results. The current method uses random forest and LSTM for malicious-node and temporal AD. In contrast, future work can explore reinforcement learning (RL), such as deep Q-network (DQN), proximal policy optimization (PPO), and soft actor-critic (SAC), to examine adaptive security and resource-allocation methods.

The evaluation should also go beyond the current NS-3-based simulation and reference hardware/software configuration by using real-world WSN/IoT datasets and a representative physical testbed comprising sensor nodes, gateway nodes, communication interfaces, and an operational blockchain platform such as Hyperledger Fabric or Ethereum. Such physical validation will enable direct measurement of communication latency, computational overhead, energy consumption, consensus delay, smart-contract execution time, and system robustness under realistic operating and attack conditions.

Network end-to-end delay (EED) measures the simulated data-transmission delay from the sensor node through the WSN communication path to the receiving gateway/server endpoint. It does not include BC block-confirmation or consensus-processing time. BC-related latency is evaluated separately using the block-confirmation/consensus latency, which signifies the time required to validate a transaction, execute the applicable consensus procedure, and confirm the corresponding BC record. Under the evaluated configuration, the proposed BA-RF-LSTM achieved a network EED of 232 *ms*, whereas the BC in block-confirmation latency was configured/evaluated within the 500–1,000 *ms* range.

However, these results must be aligned with the computational and communication overhead caused by cryptographic processing, transaction validation, consensus rounds, and SC execution. This analysis provides a more precise description of the computational complexity, scalability boundaries, and practical limitations of the proposed CPS based on the BC.

Optimized consensus and off-chain mechanisms reduce EC. The RSR reached 90%, compared with 70–80% in baseline methods. Table 6 highlights the metrics addressed in this work.

Table 6. Highlights the performance metrics of the proposed model

Metric	Without BC	With BC (Proposed CPS)	Remarks
EC per Node	Baseline (100%)	~109%	Slight increase due to encryption & batch commit
Blockchain-Inclusive Transaction Latency	~550 *ms*	~750–950 *ms*	Consensus overhead included
NT (packets/sec)	~1550 packets/sec	~1350–1400 packets/sec	Slight reduction due to on-chain verification
BC Overhead	None	~18–28%	On-chain hash storage & consensus rounds
DI	Low	High	Merkle root verification & immutable ledger
RU	Moderate	High (up to ~1100 nodes)	Off-chain storage ensures minimal performance drop
Security Features	Basic (encryption)	Advanced	Confidentiality, integrity, provenance, auditability

Accuracy, precision, recall, F1-score, false-positive rate (FPR), and detection time are used to evaluate the AD performance of the proposed BA-RF-LSTM. The proposed BA-RF-LSTM achieved the best classification accuracy of 97.48% with a precision of 97.71%, recall of 97.16%, and F1 of 97.43%. In comparison, RF, LSTM, and RF-LSTM achieved accuracies of 91.84%, 93.27%, and 95.62%. The proposed model also reduced FPR to 2.31%, compared with 8.42% for RF, 6.91% for LSTM, and 4.37% for RF-LSTM. BA-RF-LSTM also achieved an average detection time of 34.8 *ms*, indicating the feasibility of near-real-time AD in resource-constrained WSN environments. These results prove that the combination of RF-based ensemble classification, LSTM-based temporal feature learning, and BC-assisted security mechanisms may improve the robustness and reliability of detecting malicious activities (Table 7).

Table 7. Comparative AD performance

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-(%)	FPR (%)	Detection Time (ms)
RF	91.84	92.10	90.76	91.43	8.42	38.6
LSTM	93.27	93.65	92.48	93.06	6.91	46.3
RF-LSTM	95.62	95.91	95.18	95.54	4.37	41.7
Proposed BA-RF-LSTM	97.48	97.71	97.16	97.43	2.31	34.8

4.6. Limitations of the Study

This study has several limitations to consider when interpreting the reported results. First, we did not perform statistical validation based on multiple independent experimental runs; therefore, measures such as standard deviation, confidence intervals, and statistical significance tests are not available. Second, we did not conduct a formal ablation study to quantify the individual contributions of the blockchain layer, RF, LSTM, SC, and CM. Third, we did not implement or experimentally compare RL methods such as PPO and SAC with the proposed BA-RF-LSTM, and we present them only as directions for future investigation. Finally, we did not validate the model using a real-world or representative physical WSN/IoT testbed under diverse operational and attack conditions. Consequently, interpret the reported findings as evidence from the evaluated configuration rather than proof of general superiority, deployment readiness, or performance across heterogeneous real-world WSN environments.

5. CONCLUSION AND FUTURE WORK

The proposed BA-RF-LSTM obtained an EED of 232 *ms*, a data throughput (*kbps*) of 67.34, and an RU of 23.2 MB under the evaluated conditions and exhibited favorable performance against selected BC-WSN + BC-WBAN baselines. These results show a possible combination of BC-assisted security with RF-LSTM-based AD for secure data transmission in WSNs. However, the findings are limited to the experimental configuration considered in this study. The authors did not perform statistical validation across independent runs, ablation analysis, comparisons with PPO and SAC, or validation on a real-world or representative physical testbed. Therefore, the authors cannot yet make more general statements about robustness, generalizability, real-world deployment, or outperforming other methods.

Future work should address these limitations with statistically rigorous experiments, component-level ablation studies, broader algorithmic comparisons, and validation on representative real-world WSN/IoT testbeds.

References:

Alarood, A., Ibrahim, A., Abubakar, A., & Alsulami, A. (2025). Examining the factor's influencing IoT-blockchain based secure transmission services. *Scientific Reports*, *15*(1), 33426. https://doi.org/10.1038/s41598-025-18885-z

Awan, S., Javaid, N., Ullah, S., Khan, A. U., Qamar, A. M., & Choi, J. G. (2022). Blockchain-based secure routing and trust management in wireless sensor networks. *Sensors*, *22*(2), 411. https://doi.org/10.3390/s22020411

Baptist, L. J., Selvam, J., & Chakkaravarthy, D. M. (2025). A model for detecting cybersecurity intrusions using machine learning techniques. *International Journal of Electronic Security and Digital Forensics*, *17*(5), 582–592. https://doi.org/10.1504/IJESDF.2025.148217

Baptist, L. J., Selvam, J., & Chakkaravarthy, D. M. (2026). Machine learning-based cyber-attack recognition model. *International Journal of Electronic Security and Digital Forensics*, *18*(1), 56–68. https://doi.org/10.1504/IJESDF.2026.150185

Chaudhari, A., Deshpande, V., & Midhunchakkaravarthy, D. (2025). A comprehensive review of reinforcement learning-based routing algorithms for wireless sensor networks. *International Journal of Computer Networks and Applications*, *12*(3), 449–474. https://doi.org/10.22247/ijcna/2025/28

Cheekati, S., Borra, C. R., Pareek, P. K., Rayala, R. V., Sri Nandhini Kowsalya, S., & Selvam, J. (2025). Cybersecurity threat detection using OpCyNet and DBRA: A deep learning approach for DDoS attack mitigation on CICDDoS2019. *In the 13th IEEE International Conference on Smart Grid*, pp. 782–788. https://doi.org/10.1109/ICSMARTGRID66138.2025.11071797

Ghanimi, H. M. A., et al. (2024). Merkle-Damgård hash functions and blockchains: Securing electronic health records. *Journal of Discrete Mathematical Sciences and Cryptography*, *27*(2-A), 237–248. https://doi.org/10.47974/JDMSC-1878

Hasan, K., Chowdhury, M. J. M., Biswas, K., Ahmed, K., Islam, M. S., & Usman, M. (2022). A blockchain-based secure data-sharing framework for Software Defined Wireless Body Area Networks. *Computer Networks*, *211*, No. 109004. https://doi.org/10.1016/j.comnet.2022.109004

Hewa, T., Braeken, A., Liyanage, M., & Ylianttila, M. (2022). Fog computing and blockchain-based security service architecture for 5G industrial IoT-enabled cloud manufacturing. *IEEE Transactions on Industrial Informatics*, *18*(10), 7174–7185. https://doi.org/10.1109/TII.2022.3140792

Hsiao, S. J., & Sung, W. T. (2021). Employing blockchain technology to strengthen Security of wireless sensor networks. *IEEE Access*, *9*, 72326–72341. https://doi.org/10.1109/ACCESS.2021.3079708

Ismail, S., Dawoud, D. W., & Reza, H. (2023). Securing wireless sensor networks using machine learning and blockchain: A review. *Future Internet*, *15*(6), Article 200. https://doi.org/10.3390/fi15060200

Jyothi, V. E., Rajashree, R., Phani, S., Hugar, L., Shaik, R., & Poddar, S. (2025). Artificial intelligence-powered protocols for enhancing Security in next-generation communication networks. *In Proceedings of the 3rd International Conference on Intelligent Cyber Physical Systems and Internet of Things*, pp. 1107–1112. https://doi.org/10.1109/ICoICI65217.2025.11252990

Khalaf, O. I., & Abdulsahib, G. M. (2021). Optimized dynamic storage of data (ODSD) in IoT based on blockchain for wireless sensor networks. *Peer-to-Peer Networking and Applications*, *14*(5), 2858–2873. https://doi.org/10.1007/s12083-021-01115-4

Khan, A. A., Yang, J., Laghari, A. A., Baqasah, A. M., Alroobaea, R., Ku, C. S., Alizadehsani, R., Acharya, U. R., & Por, L. Y. (2025). BAIoT-EMS: Consortium network for small-medium enterprises management system with blockchain and augmented intelligence of things. *Engineering Applications of Artificial Intelligence*, *141*, 109838. https://doi.org/10.1016/j.engappai.2024.109838

Krishna, R. J., et al. (2024). Security and privacy concerns in social networks: A mathematically modified metaheuristic-based approach. *Journal of Discrete Mathematical Sciences and Cryptography*, *27*(2-A), 371–382. https://doi.org/10.47974/JDMSC-1892

Mann, M., Badoni, R. P., Narooka, P., Janarthanan, M., Mahajan, R. A., Samriya, J. K., & Panwar, D. (2025). Spatiotemporal trust evaluation using a neutrosophic model under sensor uncertainty. *Discover Computing*, *28*(1). https://doi.org/10.1007/s10791-025-09750-8

Moinet, A., Darties, B., & Baril, J. L. (2017). Blockchain-based trust and authentication for decentralized sensor networks. arXiv. https://arxiv.org/abs/1706.01730

Moldovyan, A. A., Moldovyan, N. A., Berezin, A. N., & Shapovalov, P. I. (2017). Randomized pseudo-probabilistic encryption algorithms. *XX IEEE International Conference on Soft Computing and Measurement*. https://doi.org/10.1109/SCM.2017.7970481

Mustafa, A., & Hendrawan. (2016). Calculation of encryption algorithm combination for video encryption using two layers of AHP. *In Proceedings of the 10th International Conference on Telecommunication Systems Services and Applications*, pp. 1–7. https://doi.org/10.1109/TSSA.2016.7871099

Natraj, N., Midhunchakkaravarthy, J., & Mishra, B. K. (2025). A quantitative framework for the selection of hybrid consensus mechanisms in blockchain-IoT systems. *EAI Endorsed Transactions on Internet of Things*, *11*, https://doi.org/10.4108/eetiot.10249

Ramasamy, L. K., KP, F. K., Imoize, A. L., Ogbebor, J. O., Kadry, S., & Rho, S. (2021). Blockchain-based wireless sensor networks for malicious node detection: A survey. *IEEE Access*, *9*, 128765–128785. https://doi.org/10.1109/ACCESS.2021.3111923

Rao, G. R. K., et al. (2024). Enhanced Security in federated learning by integrating homomorphic encryption for privacy-protected collaborative model training. *Journal of Discrete Mathematical Sciences and Cryptography*, *27*(2-A), 361–370. https://doi.org/10.47974/JDMSC-1891

Ren, Y., Liu, Y., Ji, S., Sangaiah, A. K., & Wang, J. (2018). Incentive mechanism of data storage based on blockchain for wireless sensor networks. *Mobile Information Systems*, *2018*, Article 6874158. https://doi.org/10.1155/2018/6874158

Sagar, P. V., et al. (2024). Secure multi-party computation in deep learning: Enhancing privacy in distributed neural networks. *Journal of Discrete Mathematical Sciences and Cryptography*, *27*(2-A), 249–259. https://doi.org/10.47974/JDMSC-1879

She, W., Liu, Q., Tian, Z., Chen, J. S., Wang, B., & Liu, W. (2019). Blockchain trust model for malicious node detection in wireless sensor networks. *IEEE Access*, *7*, 38947–38956. https://doi.org/10.1109/ACCESS.2019.2902811

Wang, J., Chen, W., Wang, L., Sherratt, R. S., Alfarraj, O., & Tolba, A. (2020). Data secure storage mechanism of sensor networks based on blockchain. *Computers, Materials & Continua*, *65*(3), 2365–2384. https://doi.org/10.32604/cmc.2020.011567

Wang, X., Wu, Q., Zeng, H., Yang, X., Cui, H., Yi, X., Piran, M. J., Luo, M., & Que, Y. (2025). Blockchain-Empowered H-CPS Architecture for Smart Agriculture. *Advanced Science*, *12*(27), 2503102. https://doi.org/10.1002/advs.202503102

Wu, F. S. (2018). Research of cloud platform data encryption technology based on ECC algorithm. *IEEE International Conference on Virtual Reality and Intelligent Systems,* pp. 125–129. https://doi.org/10.1109/ICVRIS.2018.00038

Xiao, L., Han, D., Meng, X., Liang, W., & Li, K. C. (2020). A secure framework for data sharing in private blockchain-based WBANs. *IEEE Access*, *8*, 153956–153968. https://doi.org/10.1109/ACCESS.2020.3018119

M. Chitra
Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, 600089,
Chennai, Tamil Nadu, India.
chitramurugaiyan1988@gmail.com
ORCID 0000-0001-5926-4121

V. Deepa
Department of Information Technology,
Sri Ramakrishna College of Arts & Science,
Coimbatore, 641006,
Tamil Nadu, India.
vdeepa@srcas.ac.in
ORCID 0009-0001-4939-0519

R. Sreelakshmy
Department of Electronics and Communication Engineering,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
Chennai, 600062,
Tamil Nadu, India.
drsreelakshmyr@gmail.com
ORCID 0000-0002-1198-8347

B. Venkateswarlu
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram 522502,
Andhra Pradesh, India
bvenki289@gmail.com
ORCID 0000-0003-1597-9269

K. Vidhyapriyadharshini
Department of BBA, Malla Reddy Technical Campus (A Constituent Unit of Malla Reddy Vishwavidyapeeth,
Deemed to be University, 500100,
Hyderabad, India
vidhya1341986@gmail.com
ORCID 0009-0009-6518-9418

R. Manikandan
Department of Electronics and Communication Engineering
Panimalar Engineering College,
Chennai, 600123,
Tamil Nadu, India
eiemanikandan.r@gmail.com
ORCID 0000-0002-2055-6634

Firas Tayseer Ayasrah
College of Education, Humanities and Science, Al Ain University,
Al Ain, P.O. Box: 64141,

UAE
firas.ayasrah@aau.ac.ae
ORCID 0000-0002-6477-000X

Sudhakar Sengan
Department of Computer Science and Engineering, Erode Sengunthar Engineering College, Erode, 638057,
Tamil Nadu, India
sudhasengan@gmail.com;
sudhakars@esec.ac.in
ORCID 0000-0003-4901-1432