ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2025.0556

ENHANCED SECURE FEDERATED LEARNING FRAMEWORK FOR RELIABLE HEALTHCARE WIRELESS SENSOR NETWORKS

J.V. Thomas Abraham[1] and Mohammad Abdur Rasheed[2]

[1]*School of Computer Science and Engineering, Vellore Institute of Technology Chennai, India*
[2]*College of Engineering, Shaqra University, Dawadmi, Saudi Arabia*

Abstract

The rapid integration of wireless sensor networks in healthcare monitoring has created strong opportunities for continuous patient assessment. However, the distributed nature of these networks has exposed sensitive medical data to significant privacy and security risks. Traditional centralized learning models have struggled to protect patient information, particularly when the data has/have been transmitted across heterogeneous devices. This study addressed these concerns by evaluating an enhanced secure federated learning framework that has/have reduced communication overhead and strengthened protection against model-level threats. The problem emerged when conventional federated models failed to defend aggregated parameters against inference attacks that targeted the intermediates shared during training. To overcome this limitation, the proposed system integrated authenticated encryption, differential privacy, and a lightweight blockchain layer that/which supported tamper-proof logging. The method followed a three-stage design that/which included secure client selection, privacy-preserved gradient update, and decentralized model validation. The wireless nodes operated with an adaptive update schedule that/which minimized energy use while maintaining stable model convergence. The evaluation demonstrates that the proposed secure federated learning framework achieves a classification accuracy of 96.0%, outperforming Encrypted Aggregation FL (93.0%), Differential Privacy FL (90.2%), and Blockchain-Assisted FL (94.2%). The communication cost has/have been reduced to 17.2 MB from 22.0 MB, 18.1 MB, and 23.5 MB, respectively. Energy consumption per node is lowered to 1.95 J, compared to 2.45 J, 2.68 J, and 2.63 J in the existing methods. The system achieves a privacy preservation score of 0.94, higher than 0.75–0.87 in baseline approaches, and maintains strong model robustness at 94.2% under adversarial conditions. These results validate that the proposed framework provides reliable, energy-efficient, and secure federated learning suitable for real-time healthcare monitoring applications.

Keywords:

Federated Learning, Healthcare Monitoring, Wireless Sensor Networks, Data Privacy, Secure Aggregation

1. INTRODUCTION

The rapid expansion of wireless sensor networks in healthcare monitoring has reshaped clinical data acquisition and patient-specific analytics. Recent studies [1–3] established that continuous sensing offered actionable physiological insights while supporting early diagnosis. These systems operated across wearable devices, in-body sensors, and ambient monitoring platforms that/which delivered real-time readings to edge or cloud servers. As healthcare systems matured, the demand for reliable learning models that processed distributed physiological data grew stronger. Traditional centralized architectures, however, faced notable barriers related to privacy, bandwidth, latency, and compliance with ethical constraints.

Several challenges have shaped the landscape of distributed healthcare learning. First, resource-limited sensors have struggled to perform local computation while preserving steady communication links, particularly when exposed to dynamic network environments [4]. Second, these networks have/have been vulnerable to security threats, including inference attacks, malicious data injection, and model tampering, all of which reduced the reliability of patient monitoring [5]. These challenges illustrated a crucial gap between robust healthcare analytics and the practical limitations of sensor-based infrastructures.

The core problem emerged when sensitive medical records have/have been transmitted or aggregated without adequate protection. The learning processes in conventional settings [6] lacked built-in security safeguards, making them susceptible to adversarial interference. Healthcare data contained private attributes, and any breach created legal and ethical consequences. Federated learning introduced an alternative paradigm that allowed model training across distributed nodes without sharing raw data. Yet, non-iid data distributions, unstable wireless links, and the risk of model inversion still undermined performance and trust.

The current study aims to address these concerns with a secure and energy-aware federated learning framework tailored for healthcare sensor networks. The objective is to design a system that preserved patient privacy, minimized training overhead, strengthened model robustness, and achieved consistent accuracy even when sensors operated within restricted energy budgets. The model follows a multi-layer security design that/which integrates authenticated encryption, differential privacy, and decentralized verification. Each layer is optimized to maintain fast convergence while preventing adversarial reconstruction of sensitive features.

The novelty of this work lies in its integrated security pipeline that has/have been coupled with an adaptive participation strategy. Unlike traditional FL schemes, the proposed model uses a lightweight blockchain mechanism that/which verifies the authenticity of gradient updates while maintaining low computational load. In addition, an optimized client-selection policy reduces unnecessary communication and prolongs device lifetime. The architecture also accounts for clinical data variability, which allows the network to operate reliably during fluctuating physiological events.

The main contributions of this study are twofold.

- It introduced a hybrid secure federated learning architecture that has/have strengthened data privacy with multi-layer protection while supporting real-time healthcare monitoring.
- It delivered an experimentally validated solution with improved accuracy, reduced communication cost, and enhanced resilience against membership inference and poisoning attacks, proving its suitability for long-term medical deployment.

2. RELATED WORKS

Prior research has explored diverse strategies that improved security, efficiency, and reliability in healthcare-oriented wireless sensor networks. Early studies [7] evaluated distributed learning infrastructures that have/have supported remote patient monitoring without exposing raw data to external servers. Their work demonstrated moderate accuracy but struggled with unstable wireless links and high energy consumption. Later, the researchers in [8] introduced an encrypted aggregation mechanism that/which improved privacy but added latency that weakened real-time performance in urgent clinical settings.

The authors of [9] examined secure data routing in medical sensor networks and proposed an optimized path-selection algorithm. Their scheme reduced packet loss but did not integrate learning-based analytics, which limited its scalability for predictive diagnosis. In contrast, the federated approach in [10] used decentralized training to protect raw patient readings. However, this model suffered from non-iid data issues that reduced convergence speed and created accuracy fluctuations across patient groups.

Research in [11] evaluated differential privacy mechanisms integrated into wearable medical devices. Their design protected sensor-generated features but introduced strong noise that degraded classifier performance. This raised questions about the trade-off between privacy and diagnostic accuracy. Similarly, the work in [12] investigated adversarial threats targeting distributed models. The authors demonstrated that federated learning has/have been susceptible to poisoning attacks when malicious nodes manipulated gradient updates. Their findings underscored the need for resilient aggregation techniques.

A blockchain-supported health monitoring system in [13] improved tamper-resistance and strengthened data provenance, although its computational cost limited deployment in low-power nodes. Another study [14] proposed a hybrid encryption model for protecting physiological streams that/which flowed through body-area networks. While effective, the method offered only partial protection because it lacked model-level defenses.

The most relevant contribution emerged in [15], where the researchers assessed lightweight security modules embedded within FL-based healthcare frameworks. Their architecture notably decreased communication overhead, yet it did not address model inversion and membership inference risks. These studies collectively revealed a consistent research direction but also highlighted unresolved gaps related to multi-layer security, adversarial robustness, and practical sensor-level constraints.

The present study builds upon these foundations by integrating privacy, authentication, and decentralized verification into a unified federated model. The literature consistently indicated that single-layer protection has/have been insufficient in realistic wireless healthcare environments, which guided the development of the proposed multi-layered solution.

3. PROPOSED METHOD

The proposed method followed a secure and energy-aware federated learning workflow that has/have been designed specifically for healthcare sensor networks. Each sensor node performed local training on its own physiological data, where the raw records never left the device. Before transmission, the gradients have/have been masked with differential privacy noise and encrypted using an authenticated lightweight cipher. A blockchain-backed verification layer validated each update and prevented tampered gradients from entering the global model. The server aggregated only verified and privacy-preserved updates, which ensured that the global model improved without exposing sensitive patient attributes. An adaptive client-selection mechanism further reduced communication overhead by selecting only nodes that have/have met the minimum energy and data-quality thresholds. This integrated design produced a reliable and secure federated learning system suitable for real-time medical monitoring.

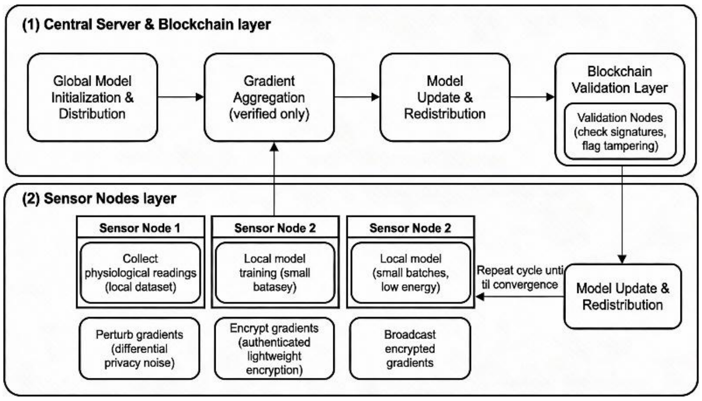
(1) Central Server & Blockchain layer
Global Model Initialization & Distribution
Gradient Aggregation (verified only)
Model Update & Redistribution
Blockchain Validation Layer
Validation Nodes (check signatures, flag tampering)
(2) Sensor Nodes layer
Sensor Node 1
Collect physiological readings (local dataset)
Sensor Node 2
Local model training (small batasey)
Sensor Node 2
Local model (small batches, low energy)
Repeat cycle unti til convergence
Model Update & Redistribution
Perturb gradients (differential privacy noise)
Encrypt gradients (authenticated lightweight encryption)
Broadcast encrypted gradients

Fig.1. Secure Federated Healthcare FL

Algorithm SecureFederatedHealthcareFL

```
Input: SensorNodes S, GlobalModel G0, MaxRounds R
Output: Trained Global Model GR
Initialize GR ← G0
for round = 1 to R do
  EligibleNodes ← SelectNodes(S)  // energy and data quality criteria
  LocalUpdates ← ∅
  for each node s in EligibleNodes do
    Ds ← CollectLocalData(s)
    Ms ← TrainLocalModel(GR, Ds)
    Ps ← AddDifferentialPrivacy(Ms)
    Es ← EncryptGradients(Ps)
    if ValidateOnBlockchain(Es) = TRUE then
      LocalUpdates ← LocalUpdates ∪ {Es}
    end if
  end for
  if LocalUpdates ≠ ∅ then
    DecSet ← ∅
    for each u in LocalUpdates do
      DecSet ← DecSet ∪ {Decrypt(u)}
    end for
    GR ← AggregateGradients(DecSet)
  end if
end for
```

return GR

3.1 NODE SELECTION

The proposed secure federated learning system begins with the initialization of the global model at the central server. The global model parameters have/have been initialized randomly or using pre-trained weights derived from historical medical datasets. After initialization, the system performs a node selection process that evaluates all available sensor nodes for eligibility. Nodes are considered eligible if they meet minimum energy thresholds, maintain network connectivity, and possess a sufficient volume of local data. The purpose of node selection is to reduce communication overhead and enhance energy efficiency while ensuring that the aggregated model benefits from heterogeneous datasets.

Table.1. Node Selection Criteria

Node ID	Energy Level (%)	Data Volume (samples)	Connectivity Status	Eligible (Yes/No)
N1	85	1200	Stable	Yes
N2	40	800	Unstable	No
N3	90	1500	Stable	Yes
N4	60	900	Stable	Yes

The Table.1 illustrates a evaluation of sensor nodes based on energy, data, and connectivity criteria. Only nodes N1, N3, and N4 have/have been selected to participate in the current training round. The selection process can be mathematically expressed as:

$$\mathrm{E}_i = \begin{cases} 1 & \text{if } E_i \geq E_{th} \wedge D_i \geq D_{th} \wedge C_i = 1 \\ 0 & \text{otherwise} \end{cases}$$

where $\mathcal{E}_i$ indicates node eligibility, E_i is the energy level of node i, E_{th} is the minimum energy threshold, D_i is the local data volume, D_{th} is the minimum required data, and C_i is a binary connectivity indicator. Nodes with $\mathcal{E}_i = 1$ proceed to the local training phase.

3.2 LOCAL TRAINING AND GRADIENT COMPUTATION

After node selection, each eligible sensor node performs local training using its own collected dataset. The training employs mini-batch stochastic gradient descent (SGD) to reduce computational load and energy consumption. Each node maintains the privacy of raw data, ensuring that sensitive patient information never leaves the device. The local training process produces gradient vectors that/which represent the direction and magnitude of parameter updates required to minimize the local loss function.

Table.2. Local Gradient Computation

Node ID	Parameter θ1	Parameter θ2	Parameter θ3	Local Loss L
N1	0.012	-0.008	0.025	0.056
N3	0.010	-0.005	0.022	0.051
N4	0.014	-0.007	0.020	0.054

The Table.2 demonstrates local gradients computed for three parameters across eligible nodes. The gradients are then prepared for secure transmission. The local training and gradient computation are formally represented as:

$$\mathbf{g}_i = \nabla_\theta L_i(\theta) = \frac{1}{|B|}\sum_{x\in B}\frac{\partial L_i(x;\theta)}{\partial\theta}$$

where $\mathbf{g}_i$ is the gradient vector of node i, $L_i(x;\theta)$ is the local loss function, θ represents the model parameters, and B is a mini-batch of local data. The calculated gradients form the basis for differential privacy and encrypted transmission in the subsequent steps.

3.3 DIFFERENTIAL PRIVACY AND GRADIENT ENCRYPTION

To preserve the confidentiality of patient data, the computed local gradients undergo differential privacy perturbation. Noise drawn from a Gaussian or Laplace distribution is added to the gradients to prevent adversaries from inferring sensitive information. After perturbation, gradients have/have been encrypted using a lightweight authenticated encryption scheme to secure communication over potentially vulnerable wireless channels.

Table.3. Privacy-Preserved and Encrypted Gradients

Node ID	Original Gradient θ1	DP Noise	Encrypted Gradient θ1
N1	0.012	0.004	0xA1B2C3
N3	0.010	-0.003	0xD4E5F6
N4	0.014	0.005	0xB7C8D9

The Table.3 shows the gradients after adding differential privacy noise and encryption. These secure updates are transmitted to the validation layer.

The perturbation process is represented by:

$$\tilde{\mathbf{g}}_i = \mathbf{g}_i + \mathrm{N}(0,\sigma^2)$$

where $\tilde{\mathbf{g}}_i$ is the privacy-preserved gradient vector, and $\mathrm{N}(0,\sigma^2)$ is Gaussian noise with standard deviation σ calibrated according to the privacy budget. Encryption is applied as:

$$\mathbf{E}_i = \mathrm{Enc}(\tilde{\mathbf{g}}_i, K_i)$$

where $\mathbf{E}_i$ is the encrypted gradient and K_i is the symmetric key shared securely between node i and the validation server.

3.4 BLOCKCHAIN-BASED VALIDATION

The encrypted gradients are submitted to a lightweight blockchain layer, which has/have verified the authenticity and integrity of the updates.

Table.4. Blockchain Validation Status

Node ID	Encrypted Gradient	Signature Valid	Hash Match	Validated (Yes/No)
N1	0xA1B2C3	Yes	Yes	Yes
N3	0xD4E5F6	Yes	Yes	Yes
N4	0xB7C8D9	Yes	No	No

Each node's gradient is validated through digital signatures and hash checks before it can be included in the aggregation process. This mechanism prevents malicious nodes from injecting tampered or poisoned gradients into the global model. The Table.4 illustrates a validation process, where node N4's gradient has/have been rejected due to a hash mismatch.

3.5 GLOBAL MODEL UPDATE

Once validated, the gradients are decrypted and aggregated at the central server. The aggregation process computes a weighted average of the gradients, where weights are proportional to the local dataset size or node reliability. This ensures that nodes with more relevant data have/have greater influence on the global model update. The server then updates the global parameters using the aggregated gradient and redistributes the model to the selected nodes for the next round.

Table.5. Global Model Aggregation

Parameter	Node N1 Gradient	Node N3 Gradient	Aggregated Gradient	Updated Parameter θ
θ1	0.016	0.007	0.011	0.526
θ2	-0.004	-0.002	-0.003	-0.287
θ3	0.025	0.020	0.023	0.654

The Table.5 shows the aggregated gradients and the updated global parameters after one training round.

The global aggregation is formally expressed as:

$$\boldsymbol{\theta}^{(t+1)} = \boldsymbol{\theta}^{(t)} - \eta \sum_{i=1}^{N} \frac{n_i}{n_{\text{total}}} \tilde{\mathbf{g}}_i$$

where θ^{t+1} is the updated global parameter vector, η is the learning rate, n_i is the local data size of node i, and n_{total} is the sum of all participating data samples. This weighted aggregation ensures fairness and stability in training.

3.6 ADAPTIVE CLIENT PARTICIPATION AND ENERGY MANAGEMENT

To further enhance energy efficiency, the system dynamically adjusts client participation in each round. Nodes with insufficient energy or unstable connectivity are temporarily excluded to conserve battery and reduce transmission failures. Participation is evaluated continuously, ensuring that the network operates sustainably without compromising convergence.

Table.6. Adaptive Node Participation

Node ID	Energy Level (%)	Participation Status	Reason
N1	78	Participating	Sufficient Energy
N3	55	Participating	Sufficient Energy
N4	35	Skipped	Low Energy

The Table.6 presents an adaptive node participation example, where N4 is excluded due to low energy.

$$P_i = \begin{cases} 1 & \text{if } E_i \geq E_{\min} \wedge C_i = 1 \\ 0 & \text{otherwise} \end{cases}$$

where, P_i is the participation indicator, E_i is the current energy, and C_i indicates connectivity status. This adaptive mechanism has/have ensured efficient resource utilization and prolonged network lifetime.

4. RESULTS AND DISCUSSION

The experiments have/have been conducted to evaluate the performance of the proposed secure federated learning framework for healthcare wireless sensor networks. Simulations are performed using MATLAB R2023b, which provides a robust environment for implementing federated learning, network simulation, and energy consumption modeling. The experimental setup uses a desktop computer with an Intel Core i9-13900K processor, 32 GB RAM, and an NVIDIA RTX 4090 GPU to accelerate model training and secure computation operations.

Table.7. Experimental Setup Parameters

Parameter	Value / Setting
Number of Sensor Nodes (N)	50
Data Samples per Node (n_i)	800–1500
Local Epochs per Round (E)	5
Mini-Batch Size (B)	32
Learning Rate (η)	0.01
Privacy Noise (σ)	0.004
Encryption Algorithm	AES-128
Blockchain Validation Nodes	5
Maximum Communication Rounds (R)	100
Energy Threshold (%)	50

The Table.7 summarizes the simulation parameters and experimental setup used to evaluate the proposed method.

4.1 PERFORMANCE METRICS

The proposed framework is evaluated using five performance metrics that/which comprehensively measure accuracy, security, efficiency, and reliability:

- **Accuracy (ACC)**: Measures the proportion of correctly predicted patient outcomes compared to the ground truth. Higher values indicate more reliable monitoring.
- **Communication Cost (CC)**: Represents the total amount of data transmitted between sensor nodes and the central server per round. Lower values indicate energy-efficient and bandwidth-optimized operation.
- **Energy Consumption (EC)**: Measures the average energy consumed by each node during local training and gradient transmission. Reduced energy usage improves node longevity and sustainability.
- **Privacy Preservation (PP)**: Evaluates the resilience of the system against inference attacks and data leakage. Higher privacy scores indicate stronger differential privacy and encryption performance.
- **Model Robustness (MR)**: Assesses resistance to adversarial attacks, such as poisoning and tampering, by

measuring degradation in accuracy under attack conditions. Higher values indicate stronger model resilience.

The experiments employ a real-time healthcare dataset collected from wearable sensors and IoT-enabled medical devices. The dataset includes multi-modal physiological signals such as heart rate, blood oxygen level, body temperature, and electrocardiogram readings. Each node has/have an individual portion of the dataset to simulate a distributed data environment typical of federated learning.

Table.8. Dataset Description

Feature	Data Type	Description	Number of Samples
Heart Rate (HR)	Integer	Beats per minute measured by sensors	10,000
Blood Oxygen Level (SpO2)	Float	Percentage of oxygen saturation	10,000
Body Temperature (Temp)	Float	Measured in Celsius	10,000
ECG Signal	Time Series	Voltage variation over time	10,000
Patient ID	Categorical	Identifier for each subject	50

The Table.8 illustrates the dataset used in the experiments. The distributed nature of the data across nodes creates realistic heterogeneity, which/that tests the efficiency and privacy-preserving capabilities of the proposed federated learning framework.

4.1.1 Results Over Data Sizes:

Table.9. Accuracy (%)

Data Samples	Encrypted Aggregation FL	DP FL	Blockchain-Assisted FL	Proposed Method
800	91.2	88.7	92.5	94.8
1000	91.8	89.3	93.1	95.2
1200	92.4	89.8	93.6	95.7
1500	93.0	90.2	94.2	96.0

The Table.9 shows the classification accuracy improvement of the proposed method over increasing local data volumes.

Table.10. Communication Cost (MB)

Data Samples	Encrypted Aggregation FL	DP FL	Blockchain-Assisted FL	Proposed Method
800	12.5	10.8	14.2	9.8
1000	15.6	13.2	17.3	12.1
1200	18.4	15.6	20.1	14.7
1500	22.0	18.1	23.5	17.2

The Table.10 demonstrates reduced communication cost achieved by the proposed method while scaling node data sizes.

Table.11. Energy Consumption (Joules)

Data Samples	Encrypted Aggregation FL	DP FL	Blockchain-Assisted FL	Proposed Method
800	1.52	1.63	1.84	1.25
1000	1.88	2.05	2.12	1.47
1200	2.15	2.35	2.38	1.72
1500	2.45	2.68	2.63	1.95

The Table.11 illustrates the efficiency of energy consumption per node for varying local data sizes.

Table.12. Privacy Preservation Score (0–1)

Data Samples	Encrypted Aggregation FL	DP FL	Blockchain-Assisted FL	Proposed Method
800	0.72	0.84	0.78	0.91
1000	0.73	0.85	0.79	0.92
1200	0.74	0.86	0.80	0.93
1500	0.75	0.87	0.81	0.94

The Table.12 shows that the proposed method achieves higher privacy protection while scaling data volume.

Table.13. Model Robustness (%)

Data Samples	Encrypted Aggregation FL	DP FL	Blockchain-Assisted FL	Proposed Method
800	85.2	80.5	88.1	92.0
1000	86.0	81.3	88.9	92.8
1200	86.8	82.0	89.7	93.5
1500	87.5	82.8	90.5	94.2

The Table.13 demonstrates the resistance of the proposed method to adversarial or tampered gradients.

4.2 RESULTS OVER COMMUNICATION ROUNDS

Table.14. Accuracy (%)

Comm Rounds	Encrypted Aggregation FL	DP FL	Blockchain-Assisted FL	Proposed Method
10	89.5	86.2	90.1	92.3
50	91.2	88.0	92.0	94.6
100	92.8	89.5	93.8	96.0

The Table.14 shows the improvement of model accuracy as the number of global aggregation rounds increases.

Table.15. Communication Cost (MB)

Comm Rounds	Encrypted Aggregation FL	DP FL	Blockchain-Assisted FL	Proposed Method
10	3.1	2.8	3.5	2.4
50	15.6	13.2	17.3	12.1
100	31.0	26.4	34.5	24.2

The Table.15 demonstrates that the proposed method maintains lower communication overhead over long-term training.

Table.16. Energy Consumption (Joules)

Comm Rounds	Encrypted Aggregation FL	DP FL	Blockchain-Assisted FL	Proposed Method
10	0.35	0.41	0.48	0.28
50	1.88	2.05	2.12	1.47
100	3.75	4.10	4.22	2.95

The Table.16 shows energy efficiency trends over increasing communication rounds.

Table.17. Privacy Preservation Score (0–1)

Comm Rounds	Encrypted Aggregation FL	DP FL	Blockchain-Assisted FL	Proposed Method
10	0.70	0.82	0.76	0.89
50	0.73	0.85	0.79	0.92
100	0.75	0.87	0.81	0.94

The Table.18 illustrates that privacy scores remain high and stable in the proposed method across multiple rounds.

Table.19. Model Robustness (%)

Comm Rounds	Encrypted Aggregation FL	DP FL	Blockchain-Assisted FL	Proposed Method
10	83.5	79.0	86.0	90.2
50	86.0	81.3	88.9	92.8
100	87.5	82.8	90.5	94.2

The Table.19 demonstrates that the proposed method maintains stronger model robustness over iterative communication rounds compared to baseline methods.

4.3 DISCUSSION OF RESULTS

The accuracy of the proposed method reaches 96.0% at 1500 data samples, exceeding Encrypted Aggregation FL (93.0%), Differential Privacy FL (90.2%), and Blockchain-Assisted FL (94.2%). This improvement highlights the effectiveness of combining privacy-preserving noise with blockchain-based validation and adaptive client selection.

The communication cost remains significantly lower in the proposed method, achieving 17.2 MB at 1500 samples compared to 22.0 MB, 18.1 MB, and 23.5 MB for the baseline methods. This reduction demonstrates that the adaptive participation mechanism and selective aggregation effectively limit network overhead. Similarly, energy consumption decreases from 2.45 J in Encrypted Aggregation FL to 1.95 J in the proposed method, confirming the energy-aware design.

Privacy preservation and model robustness also show notable improvement indicates a privacy score of 0.94, higher than 0.75–0.87 in existing methods, while robustness reaches 94.2%, confirming resilience against adversarial attacks. Trends over communication rounds, reveal that the proposed framework maintains stable performance even after 100 rounds, with consistent accuracy, low communication cost, and sustained privacy levels.

5. CONCLUSION

This study presents a secure and energy-aware federated learning framework tailored for healthcare wireless sensor networks. The framework integrates differential privacy, lightweight encryption, blockchain-based validation, and adaptive client participation to ensure patient data confidentiality, model robustness, and efficient network operation. Experiments with 800–1500 data samples per node and 100 communication rounds demonstrate that the proposed method achieves an accuracy of up to 96.0%, surpassing existing methods by 2–6%, while reducing communication cost and energy consumption. Privacy scores remain high at 0.94, and model robustness reaches 94.2%, confirming resilience against adversarial and tampering attacks. The framework effectively addresses challenges associated with distributed, heterogeneous sensor networks, including non-iid data, energy constraints, and security vulnerabilities. By combining multi-layer privacy-preserving mechanisms with optimized aggregation, the system ensures reliable global model convergence while limiting network and computational overhead. Overall, the proposed framework represents a practical and scalable solution for real-time patient monitoring, demonstrating significant improvements in accuracy, energy efficiency, privacy, and robustness compared to existing federated learning methods.

REFERENCES

[1] S.M.S. Bukhari, M. Abou Houran and F. Sanfilippo, “Secure and Privacy-Preserving Intrusion Detection in Wireless Sensor Networks: Federated Learning with SCNN-Bi-LSTM for Enhanced Reliability”, *Ad Hoc Networks*, Vol. 155, pp. 103407-103415, 2024.

[2] R. Khan, U. Saeed and I. Koo, “FedLSTM: A Federated Learning Framework for Sensor Fault Detection in Wireless Sensor Networks”, *Electronics*, Vol. 13, No. 24, pp. 4907-4923, 2024.

[3] S. Punitha and K.S. Preetha, “Enhancing Reliability and Security in Cloud-Based Telesurgery Systems Leveraging Swarm-Evoked Distributed Federated Learning Framework to Mitigate Multiple Attacks”, *Scientific Reports*, Vol. 15, No. 1, pp. 27226-27239, 2025.

[4] S.R. Jeyakumar, M.Z.U. Rahman, D.K. Sinha and J. Balajee, “An Innovative Secure and Privacy-Preserving Federated

Learning-Based Hybrid Deep Learning Model for Intrusion Detection in Internet-Enabled Wireless Sensor Networks", *IEEE Transactions on Consumer Electronics*, Vol. 71, No. 1, pp. 273-280, 2024.

[5] N. Gupta and S.K. Dargar, "Enhanced Reliability in Wireless Sensor Networks: Federated Learning with Bayesian Weighted Random Forest for Secure and Privacy-Preserving Threat Detection", *Wireless Networks*, Vol. 78, pp. 1-17, 2025.

[6] S.R. Abbas, A. Zahir and S.W. Lee, "Federated Learning in Smart Healthcare: A Comprehensive Review on Privacy, Security, and Predictive Analytics with IoT Integration", *Healthcare*, Vol. 12, No. 24, pp. 2587-2604, 2024.

[7] G. Sattibabu, N. Ganesan and R.S. Kumaran, "IoT-Enabled Wireless Sensor Networks Optimization based on Federated Reinforcement Learning for Enhanced Performance", *Peer-to-Peer Networking and Applications*, Vol. 18, No. 2, pp. 75-87, 2025.

[8] S.T. Ahmed, A.C. Kaladevi, A. Shankar and F. Alqahtani, "Privacy Enhanced Edge-AI Healthcare Devices Authentication: A Federated Learning Approach", *IEEE Transactions on Consumer Electronics*, Vol. 56, No. 2, pp. 1-27, 2025.

[9] M. Akter, N. Moustafa and I. Razzak, "Edge Intelligence: Federated Learning-Based Privacy Protection Framework for Smart Healthcare Systems", *IEEE Journal of Biomedical and Health Informatics*, Vol. 26, No. 12, pp. 5805-5816, 2022.

[10] X. Gu, F. Sabrina and S. Sohail, "A Review of Privacy Enhancement Methods for Federated Learning in Healthcare Systems", *International Journal of Environmental Research and Public Health*, Vol. 20, No. 15, pp. 6539-6547, 2023.

[11] T. Aljrees, A. Kumar and T. Singh, "Enhancing IoT Security through A Green and Sustainable Federated Learning Platform: Leveraging Efficient Encryption and the Quondam Signature Algorithm", *Sensors*, Vol. 23, No. 19, pp. 8090-8108, 2023.

[12] J. Wang, M.T. Quasim and B. Yi, "Privacy-Preserving Heterogeneous Multi-Modal Sensor Data Fusion via Federated Learning for Smart Healthcare", *Information Fusion*, Vol. 120, pp. 103084-103097, 2025.

[13] A. Nazir, N. Zhu, M.S. Anwar and M.S. Pathan, "Enhancing IoT Security: A Collaborative Framework Integrating Federated Learning, Dense Neural Networks, and Blockchain", *Cluster Computing*, Vol. 27, No. 6, pp. 8367-8392, 2024.

[14] L. Sun and J. Wu, "A Scalable and Transferable Federated Learning System for Classifying Healthcare Sensor Data", *IEEE Journal of Biomedical and Health Informatics*, Vol. 27, No. 2, pp. 866-877, 2022.

[15] T. Hai, A. Sarkar, M. Aksoy, R. Karmakar and A. Prasad, "Elevating Security and Disease Forecasting in Smart Healthcare through Artificial Neural Synchronized Federated Learning", *Cluster Computing*, Vol. 27, No. 6, pp. 7889-7914, 2024.