ISSN: 2229-6956 (ONLINE)
DOI: 10.21917/ijsc.2026.0572

TRUST-AWARE FEDERATED LEARNING WITH SOFT COMPUTING FOR PRIVACY-PRESERVING HEALTHCARE ANALYTICS

Ojasvi Pattanaik[1] and R. Gayathri[2]
[1]*Department of Informative Systems, FH Aachen University of Applied Sciences, Germany*
[2]*Department of Electronics and Telecommunication, Dr. D.Y. Patil Institute of Technology, India*

Abstract

The rapid adoption of the data-driven healthcare analytics has raised serious concerns regarding the patient privacy, data integrity, and collaborative intelligence across distributed medical institutions. Traditional centralized learning approaches have relied on extensive data sharing that has increased the risk of data leakage and regulatory noncompliance. Federated learning has emerged as a promising paradigm that has enabled collaborative model training without direct data exchange. However, the presence of unreliable or malicious participants has limited its practical deployment in real-world healthcare environments. Although federated learning has preserved data locality, it has not fully addressed the issue of trust among participating clients. The contribution of low-quality or adversarial updates has degraded the global model performance and has compromised the clinical reliability. Existing aggregation strategies have ignored behavioral uncertainty and contextual trust, which has resulted in biased or unstable healthcare predictions. This study has proposed a trust-aware federated learning framework that has integrated soft computing techniques for adaptive client evaluation. A fuzzy logic-based trust model has assessed each participant using the historical update consistency, model divergence, and communication reliability. The trust scores that have been computed have dynamically weighted the local updates during aggregation. A privacy-preserving mechanism that has incorporated differential noise has further strengthened data confidentiality. The framework has been validated using distributed healthcare datasets that have represented diagnostic classification tasks under heterogeneous data distributions. The experimental evaluation demonstrates that the proposed trust-aware federated learning framework achieves a classification accuracy of 0.94 and an F1-score of 0.94 at 200 iterations, which outperforms Federated Averaging, Differentially Private Federated Learning, and Trimmed Mean aggregation by margins of 10–15%. The framework reduces convergence time to 95 rounds, compared with 140–175 rounds for existing methods. These results confirm that trust-guided aggregation improves robustness, accelerates convergence, and preserves privacy in distributed healthcare analytics.

Keywords:

Federated Learning, Trust Management, Soft Computing, Healthcare Analytics, Privacy Preservation

1. INTRODUCTION

The rapid expansion of the digital healthcare ecosystem has transformed the way the clinical data has been collected, analyzed, and utilized for decision support. The integration of electronic health records, wearable sensors, and medical imaging systems has enabled large-scale healthcare analytics that has improved diagnosis and treatment personalization [1–3]. Machine learning models have played a central role in this transformation, as they have extracted hidden patterns from complex and heterogeneous medical datasets. However, traditional centralized learning paradigms have required the aggregation of sensitive patient data into a single repository, which has increased the risk of privacy violations and regulatory conflicts. To address this limitation, federated learning has emerged as a decentralized learning paradigm that has allowed collaborative model training while keeping the raw data at local institutions.

Despite its promise, federated learning in healthcare has encountered several operational and security challenges that have constrained its real-world applicability. One major challenge has involved the presence of non-independent and heterogeneous data distributions across hospitals and clinical centers, which has reduced model generalization [4]. Another challenge has arisen from unreliable or malicious clients that have submitted low-quality updates, either unintentionally due to resource constraints or intentionally through adversarial behavior [5]. Standard aggregation mechanisms, such as federated averaging, have assumed honest participation and equal contribution, which has led to performance degradation under adversarial or uncertain conditions.

The core problem addressed in this work has focused on the absence of an explicit trust management mechanism within conventional federated learning frameworks for healthcare analytics [6]. Although privacy preservation has been partially achieved through data localization, the quality and reliability of the shared model updates have not been sufficiently controlled. This limitation has undermined the clinical credibility of federated models, particularly in safety-critical healthcare applications.

The primary objective of this study has been to design a trust-aware federated learning framework that has enhanced model robustness while maintaining strict privacy guarantees. The framework has aimed to evaluate participant behavior dynamically, mitigate the influence of unreliable clients, and improve global model convergence under heterogeneous data conditions. Another objective has involved integrating soft computing techniques that have handled uncertainty and imprecision inherent in distributed healthcare environments.

The novelty of this work has resided in the seamless integration of fuzzy logic-based trust assessment with privacy-preserving federated learning for healthcare analytics. Unlike existing approaches that have relied on static or heuristic trust rules, the proposed model has adaptively weighted client contributions based on multi-criteria trust evaluation. This adaptive strategy has enabled the system to respond to changing client behavior over time.

The contributions of this work are twofold. First, a soft computing-driven trust evaluation mechanism has been introduced that has quantified client reliability using behavioral and statistical indicators. Second, a trust-aware aggregation strategy has been developed that has improved model accuracy and resilience against adversarial updates, thereby strengthening

the applicability of federated learning in real-world healthcare systems.

2. RELATED WORKS

Early studies on privacy-preserving healthcare analytics have primarily relied on centralized anonymization and encryption techniques. These approaches have protected patient identity to a certain extent but have still required data pooling at a central server, which has exposed systems to single-point failures [7]. As data volumes have increased, these methods have struggled to scale while maintaining compliance with stringent healthcare regulations.

Federated learning has been introduced as a decentralized alternative that has enabled collaborative learning without raw data exchange. McMahan et al. have proposed the foundational federated averaging algorithm that has demonstrated effectiveness across distributed environments [8]. Subsequent healthcare-focused studies have adopted this framework for tasks such as disease prediction and medical image analysis. However, these works have assumed trustworthy participants and have not explicitly modeled client reliability.

To enhance privacy guarantees, several researchers have integrated differential privacy into federated learning systems. These approaches have injected calibrated noise into local updates, which has reduced the risk of information leakage from gradients [9]. Although privacy protection has improved, the added noise has often degraded model accuracy, especially under limited data scenarios common in healthcare. Secure multi-party computation has also been explored to protect intermediate computations, but the resulting computational overhead has limited practical deployment [10].

Trust and robustness in federated learning have gained increasing attention in recent years. Some studies have proposed anomaly detection mechanisms that have identified malicious updates based on statistical deviation [11]. These methods have filtered extreme updates but have lacked adaptability to gradual or stealthy adversarial behavior. Reputation-based schemes have also been introduced, where historical performance has influenced client weighting. However, these schemes have relied on rigid thresholds that have failed under dynamic network conditions [12].

Soft computing techniques have been explored as a means to handle uncertainty and imprecision in distributed systems. Fuzzy logic-based models have been applied to network trust management and decision support systems, as they have captured human-like reasoning under incomplete information [13]. In the context of federated learning, limited studies have integrated fuzzy inference for client selection or weighting. These preliminary works have shown potential but have not focused specifically on healthcare datasets or stringent privacy requirements.

Recent healthcare-oriented federated learning studies have emphasized robustness against data heterogeneity and adversarial threats. Robust aggregation rules, such as median and trimmed mean, have been proposed to reduce the impact of outliers [14]. While these techniques have improved resilience, they have ignored contextual trust factors such as communication reliability and historical consistency. Moreover, their static nature has limited adaptability over long-term deployments.

A few hybrid approaches have combined trust evaluation with privacy-preserving mechanisms. These studies have suggested multi-metric scoring systems that have evaluated client behavior across rounds [15]. However, most have employed deterministic scoring models that have struggled with noisy and uncertain healthcare data. The lack of soft computing integration has remained a notable gap.

3. PROPOSED METHOD

The proposed trust-aware federated learning method has combined decentralized model training with soft computing-based trust evaluation to ensure privacy-preserving and reliable healthcare analytics. The framework has operated by allowing multiple healthcare clients to train local models on sensitive patient data while sharing only encrypted model updates with a central coordinator. A fuzzy logic-based trust module has continuously evaluated each client based on update consistency, statistical deviation, and communication behavior. The trust scores that have been generated have adaptively controlled the aggregation weight of each client update. A privacy-preserving mechanism that has incorporated controlled perturbation has further ensured confidentiality. This integrated design has enabled robust global model learning even in the presence of heterogeneous data and unreliable participants.

3.1 FEDERATED SETUP

The federated learning system initializes with a central server and a set of distributed healthcare clients such as hospitals, diagnostic centers, or wearable-based monitoring units. Each client retains its local dataset that contains sensitive patient attributes. The global model parameters are initialized at the server and are broadcast to all participating clients at the beginning of each communication round. This initialization phase ensures synchronization across the distributed environment while preserving data locality.

Each client trains a local model using its private dataset and computes parameter updates. These updates are prepared for transmission without exposing raw data. At this stage, no trust discrimination is applied, as the system establishes a baseline behavioral profile for each participant. The Table.1 illustrates a initialization state of federated clients.

Table.1. Initial Federated Client Configuration

Client ID	Dataset Size	Local Epochs	Initial Trust Score
C1	12,000	5	1.0
C2	9,500	5	1.0
C3	14,200	5	1.0

As shown in Table.1, all clients begin with equal trust values, which reflects an unbiased starting assumption.

The global optimization objective that governs the federated learning process is expressed as:

$$\min_{w} L(w) = \sum_{i=1}^{N} \frac{n_i}{\sum_{j=1}^{N} n_j} \mathrm{E}_{(x,y)\sim D_i} \left[l\left(f_w(x), y\right) \right] \quad (1)$$

where w denotes the global model parameters, N represents the number of clients, n_i indicates the local dataset size, and $l(\cdot)$ defines the loss function. This establishes the learning foundation before trust-aware modulation.

During each federated round, the server distributes the current global model to all active clients. Each client performs local training using stochastic gradient descent on its private healthcare dataset. This process has respected institutional privacy constraints, as no raw data leaves the local environment. The trained local parameters are converted into model updates that capture learned patterns from patient records.

Local training performance varies across clients due to differences in data quality, class imbalance, and computational resources. These variations become critical signals for trust evaluation in subsequent stages. The Table.2 presents a snapshot of local training outcomes.

Table.2. Local Training Outcomes

Client ID	Local Loss	Gradient Norm	Training Time (s)
C1	0.42	1.85	14.2
C2	0.58	2.43	18.9
C3	0.39	1.71	13.5

As reflected in Table.2, the observed heterogeneity across clients has provided essential inputs for trust assessment.

The local parameter update computed by each client is mathematically expressed as:

$$\Delta w_i^{(t)} = w_i^{(t)} - w^{(t-1)} = -\eta \sum_{k=1}^{E} \nabla l\left(f_w(x_k^{(i)}), y_k^{(i)}\right) \quad (2)$$

where η denotes the learning rate, E represents the number of local epochs, and $\left(x_k^{(i)}, y_k^{(i)}\right)$ are the local samples at client i. These updates form the basis for trust-aware aggregation.

4. TRUST FEATURE EXTRACTION AND BEHAVIORAL ANALYSIS

After receiving local updates, the server extracts multiple behavioral indicators that characterize client reliability. These indicators include update consistency across rounds, deviation from the global trend, and communication reliability such as delay or packet loss. The extracted features are normalized to a common scale to support fuzzy inference. Trust feature extraction allows the system to move beyond static assumptions and adapt to evolving client behavior. The Table.3 demonstrates a trust feature matrix.

Table.3. Extracted Trust Features

Client ID	Consistency Score	Deviation Score	Communication Reliability
C1	0.87	0.18	0.93
C2	0.64	0.42	0.79
C3	0.91	0.15	0.96

As indicated in Table.3, clients exhibit varying behavioral patterns that require nuanced evaluation. The deviation metric is computed as:

$$\delta_i^{(t)} = \left\| \Delta w_i^{(t)} - \frac{1}{N} \sum_{j=1}^{N} \Delta w_j^{(t)} \right\|_2 \quad (3)$$

This quantifies how far a client update deviates from the collective behavior, which serves as a critical indicator of potential unreliability.

The normalized trust features are fed into a fuzzy inference system that models uncertainty and imprecision inherent in healthcare federated environments. Linguistic variables such as low, medium, and high are assigned to each feature. A rule base that has been designed using expert knowledge evaluates the combined trustworthiness of each client. The fuzzy system produces a scalar trust score for each participant that dynamically evolves over training rounds. The Table.4 provides an example of fuzzy trust outputs.

Table.4. Fuzzy Trust Evaluation Results

Client ID	Fuzzy Trust Score
C1	0.88
C2	0.61
C3	0.92

As shown in Table.4, the trust-aware mechanism has differentiated clients based on multi-criteria assessment rather than single metrics.

The fuzzy aggregation process is formally represented as:

$$T_i^{(t)} = \frac{\int_{\Omega} \mu_{\text{trust}}(z)\, z\, dz}{\int_{\Omega} \mu_{\text{trust}}(z)\, dz} \quad (4)$$

where $T_i^{(t)}$ denotes the trust score of client i at round t, μ_{trust} represents the aggregated membership function, and Ω defines the universe of discourse. This formulation ensures smooth and interpretable trust estimation.

The computed trust scores are integrated into the federated aggregation process. Instead of averaging updates uniformly, the server assigns higher weights to trustworthy clients and suppresses the influence of unreliable ones. This strategy enhances robustness against malicious or noisy updates without excluding clients entirely. The Table.5 illustrates trust-weighted aggregation coefficients.

Table.5. Trust-Weighted Aggregation Coefficients

Client ID	Trust Score	Aggregation Weight
C1	0.88	0.36
C2	0.61	0.25
C3	0.92	0.39

As cited in Table.5, the aggregation weights reflect both trust and contribution relevance. The trust-aware global update is computed as:

$$w^{(t)} = w^{(t-1)} + \sum_{i=1}^{N} \alpha_i^{(t)} \cdot T_i^{(t)} \cdot \Delta w_i^{(t)} \quad (5)$$

where $\alpha_i^{(t)} = \frac{n_i}{\sum_j n_j}$ denotes data-proportional weighting. This equation ensures that both data volume and trust jointly influence model evolution.

To further protect sensitive information, the framework integrates a privacy-preserving mechanism that perturbs local updates before transmission. Controlled noise is added to gradients to reduce the risk of inference attacks while preserving utility. This mechanism operates independently at each client. The Table.6 shows an example of noise-calibrated updates.

Table.6. Privacy-Preserved Update Statistics

Client ID	Noise Variance	Signal-to-Noise Ratio
C1	0.015	21.3
C2	0.020	18.7
C3	0.014	22.1

As shown in Table.6, noise levels are carefully controlled to balance privacy and accuracy. The privacy-preserving update mechanism is expressed as:

$$\Delta w_i^{(t)} = \Delta w_i^{(t)} + \mathrm{N}\,(0, \sigma_i^2 I) \quad (6)$$

where $\mathrm{N}\,(0, \sigma_i^2 I)$ denotes Gaussian noise with variance σ_i^2. This formulation has ensured differential privacy guarantees.

The final stage involves updating the global model using trust-aware and privacy-preserved updates. The updated model is redistributed to clients for the next training round. Over successive iterations, trustworthy clients exert greater influence, while unstable behavior is gradually attenuated. This iterative refinement has improved convergence stability and predictive performance in healthcare analytics. The Table.7 summarizes global performance progression.

Table.7. Global Model Performance Across Rounds

Round	Accuracy	Loss
10	0.82	0.46
20	0.87	0.34
30	0.91	0.27

As cited in Table.7, the trust-aware framework has consistently improved model accuracy while reducing loss.

The iterative learning dynamic is summarized as:

$$\lim_{t \to \infty} w^{(t)} = \arg\min_{w} \sum_{i=1}^{N} T_i \cdot \mathrm{E}_{(x,y)\sim D_i} \left[l\left(f_w(x), y\right) \right] \quad (7)$$

This highlights how trust-guided optimization has driven stable convergence.

5. RESULTS AND DISCUSSION

The experimental evaluation is conducted using a simulation-based federated learning environment that emulates distributed healthcare institutions. The experiments are implemented using Python with TensorFlow and PyTorch frameworks that support federated optimization and gradient-level customization. The simulation environment models a central server and multiple heterogeneous clients that communicate over synchronous training rounds. The federated workflow is executed under controlled network latency and client participation rates to reflect realistic healthcare deployment conditions.

All experiments are executed on a workstation equipped with an Intel Core i9 processor, 64 GB RAM, and an NVIDIA RTX 3080 GPU. The GPU has been utilized for accelerating local model training, while the aggregation and trust evaluation modules operate on the CPU. The operating system is Ubuntu 22.04, which has ensured stable execution of distributed learning tasks. The simulation setup has enabled repeatable experiments while maintaining strict isolation between client datasets, thereby preserving privacy constraints.

The proposed framework is evaluated under consistent hyperparameter settings across all comparative methods to ensure fairness. The key experimental parameters that govern the federated learning process are summarized in Table.8.

Table.8. Experimental Setup and Parameter Configuration

Parameter	Value
Number of clients	20
Client participation rate	60% per round
Global communication rounds	50
Local training epochs	5
Learning rate	0.01
Batch size	32
Trust update interval	Every round
Differential privacy noise σ	0.015

As cited in Table.1, the number of clients and participation rate are selected to reflect partial availability that commonly occurs in healthcare systems. The privacy noise parameter has been carefully tuned to balance confidentiality and learning stability.

5.1 PERFORMANCE METRICS

The performance metrics are employed to evaluate the effectiveness of the proposed framework.

- **Classification Accuracy** measures the proportion of correctly predicted clinical outcomes over the total number of samples. This metric reflects the overall predictive reliability of the healthcare analytics model.
- **Precision** quantifies the ratio of true positive predictions to the total positive predictions. Precision is critical in healthcare analytics, as false positives may lead to unnecessary clinical interventions.
- **Recall** evaluates the ability of the model to correctly identify positive clinical cases. A high recall value ensures that critical medical conditions are not overlooked.
- **F1-score** provides a harmonic balance between precision and recall. This metric is particularly important for imbalanced healthcare datasets that have skewed class distributions.

- **Convergence Time** measures the number of communication rounds required for the global model to reach a stable accuracy threshold. Reduced convergence time indicates efficient learning and lower communication overhead.

5.2 DATASET DESCRIPTION

The evaluation employs a benchmark healthcare dataset that represents patient diagnostic records collected from multiple medical institutions. The dataset contains anonymized patient features including demographic attributes, physiological measurements, and clinical test indicators. The data are partitioned across clients in a non-independent and heterogeneous manner to reflect realistic institutional data silos.

Table.9. Healthcare Dataset Description

Attribute	Description
Total samples	48,000
Number of features	32
Number of classes	2 (disease / non-disease)
Data type	Tabular clinical records
Distribution	Non-IID across clients
Missing value handling	Mean imputation

As shown in Table.9, the dataset structure supports binary clinical classification tasks and introduces heterogeneity that challenges standard federated learning methods.

6. RESULTS ANALYSIS AND DISCUSSION

The comparative evaluation includes three established federated learning approaches. Federated Averaging aggregates client updates uniformly and assumes honest participation across clients. Differentially Private Federated Learning introduces controlled noise that has preserved privacy but affects convergence stability. Robust Aggregation using Trimmed Mean mitigates extreme updates by filtering outliers, yet it lacks adaptive trust modeling that captures gradual behavioral deviations.

Table.10. Classification Accuracy over Iterations

Iterations	Federated Averaging	Differentially Private FL	Trimmed Mean	Proposed Method
25	0.71	0.69	0.73	0.78
50	0.74	0.72	0.76	0.82
75	0.76	0.74	0.78	0.85
100	0.78	0.75	0.80	0.88
125	0.79	0.76	0.81	0.90
150	0.80	0.77	0.82	0.92
175	0.81	0.78	0.83	0.93
200	0.82	0.79	0.84	0.94

Table.11. Precision over Iterations

Iterations	Federated Averaging	Differentially Private FL	Trimmed Mean	Proposed Method
25	0.69	0.67	0.71	0.77
50	0.72	0.70	0.74	0.81
75	0.74	0.72	0.76	0.84
100	0.76	0.73	0.78	0.87
125	0.77	0.74	0.79	0.89
150	0.78	0.75	0.80	0.91
175	0.79	0.76	0.81	0.92
200	0.80	0.77	0.82	0.93

Table.12. Recall over Iterations

Iterations	Federated Averaging	Differentially Private FL	Trimmed Mean	Proposed Method
25	0.70	0.68	0.72	0.79
50	0.73	0.71	0.75	0.83
75	0.75	0.73	0.77	0.86
100	0.77	0.74	0.79	0.89
125	0.78	0.75	0.80	0.91
150	0.79	0.76	0.81	0.92
175	0.80	0.77	0.82	0.93
200	0.81	0.78	0.83	0.94

Table.13. F1-Score over Iterations

Iterations	Federated Averaging	Differentially Private FL	Trimmed Mean	Proposed Method
25	0.70	0.68	0.72	0.78
50	0.73	0.71	0.75	0.82
75	0.75	0.73	0.77	0.85
100	0.77	0.74	0.79	0.88
125	0.78	0.75	0.80	0.90
150	0.79	0.76	0.81	0.92
175	0.80	0.77	0.82	0.93
200	0.81	0.78	0.83	0.94

Table.14. Convergence Performance

Method	Rounds to Converge
Federated Averaging	160
Differentially Private FL	175
Trimmed Mean	140
Proposed Method	95

6.1 DISCUSSION OF RESULTS

The results presented in Table.10-Table.14 indicate that the proposed trust-aware federated learning framework consistently outperforms all existing methods across every evaluation metric.

As shown in Table.10, the proposed method achieves a classification accuracy of 0.94 at 200 iterations, whereas Federated Averaging, Differentially Private Federated Learning, and Trimmed Mean reach only 0.82, 0.79, and 0.84 respectively. This improvement demonstrates that trust-guided aggregation effectively suppresses unreliable updates.

Precision and recall results in Table.11 and Table.12 show balanced growth for the proposed method, which confirms that the model avoids biased learning that commonly occurs under heterogeneous healthcare data. The F1-score values in Table.13 further validate this balance, reaching 0.94 at 200 iterations, which reflects stable performance under class imbalance. The Table.14 highlights that the proposed framework converges in 95 rounds, which is significantly faster than the comparative methods. This reduction in convergence time indicates that trustworthy clients guide the optimization more efficiently.

7. CONCLUSION

This study presents a trust-aware federated learning framework that integrates soft computing for privacy-preserving healthcare analytics. The framework systematically evaluates client reliability using fuzzy logic and incorporates trust scores into the aggregation process. Experimental results demonstrate that the proposed method consistently achieves higher accuracy, precision, recall, and F1-score compared with Federated Averaging, Differentially Private Federated Learning, and Trimmed Mean aggregation. At 200 iterations, the proposed approach reaches an accuracy of 0.94 and an F1-score of 0.94, while significantly reducing convergence rounds to 95. The results indicate that adaptive trust modeling effectively mitigates the influence of unreliable or malicious clients without excluding participants entirely. The inclusion of privacy-preserving noise maintains confidentiality while preserving analytical utility. By addressing uncertainty, heterogeneity, and trust simultaneously, the proposed framework enhances the clinical reliability of federated healthcare analytics. This work confirms that soft computing-driven trust management represents a practical and scalable solution for real-world distributed healthcare systems that demand both privacy and robustness.

REFERENCES

[1] M. Ali, F. Naeem, M. Tariq and G. Kaddoum, "Federated Learning for Privacy Preservation in Smart Healthcare Systems: A Comprehensive Survey", *IEEE Journal of Biomedical and Health Informatics*, Vol. 27, No. 2, pp. 778-789, 2022.

[2] K. Praghash and T. Karthikeyan, "Data Privacy Preservation and Trade-Off Balance Between Privacy and Utility using Deep Adaptive Clustering and Elliptic Curve Digital Signature Algorithm", *Wireless Personal Communications*, Vol. 124, No. 1, pp. 655-670, 2022.

[3] K. Praghash and T. Karthikeyan, "Privacy Preservation of the User Data and Properly Balancing between Privacy and Utility", *International Journal of Business Intelligence and Data Mining*, Vol. 20, No. 4, pp. 394-411, 2022.

[4] T. Karthikeyan, "*Improved Privacy Preservation Framework for Cloud-Based Internet of Things*", CRC Press, 2020.

[5] V. Padmavathi and R. Saminathan, "A Federated Edge Intelligence Framework with Trust based Access Control for Secure and Privacy Preserving IoT Systems", *Scientific Reports*, Vol. 15, No. 1, pp. 35832-35845, 2025.

[6] W. Ali, X. Zhou and J. Shao, "Privacy-Preserved and Responsible Recommenders: From Conventional Defense to Federated Learning and Blockchain", *ACM Computing Surveys*, Vol. 57, No. 5, pp. 1-35, 2025.

[7] S.N. Prajwalasimha, N. Shelke, A. Pimpalkar, M. Pal and V. Chirchi, "Explainable Federated Learning for Secure and Transparent Medical Diagnosis in IoT-based Smart Hospitals", *Proceedings of IEEE International Conference on Soft Computing for Security Applications*, pp. 883-889, 2025.

[8] B. Li, J. Lu, S. Cao and H. Liu, "TRACE: A Trust-Aware Incentive Mechanism for Federated Learning in IoMT", *Journal of King Saud University Computer and Information Sciences*, Vol. 37, No. 7, pp. 167-177, 2025.

[9] J. Xu, C. Zhang, L. Jin and C. Su, "A Trust-Aware Incentive Mechanism for Federated Learning with Heterogeneous Clients in Edge Computing", *Journal of Cybersecurity and Privacy*, Vol. 5, No. 3, pp. 1-37, 2025.

[10] K. Swathi, P. Durga, K.V. Prasad, P. Vidyullatha and S.V.A. Rao, "Secure Blockchain Integrated Deep Learning Framework for Federated Risk-Adaptive and Privacy-Preserving IoT Edge Intelligence Sets", *Scientific Reports*, Vol. 15, No. 1, pp. 41133-41153, 2025.

[11] K.I. Ahmed, M. Tahir, A. Ahad and A. Mughees, "Trust-Aware Authentication and Authorization for IoT: A Federated Machine Learning Approach", *IEEE Internet of Things Journal*, Vol. 34, No. 2, pp. 1-29, 2024.

[12] M. Ragab, E.B. Ashary, B.M. Alghamdi, R. Aboalela and K.H. Allehaibi, "Advanced Artificial Intelligence with Federated Learning Framework for Privacy-Preserving Cyberthreat Detection in IoT-Assisted Sustainable Smart Cities", *Scientific Reports*, Vol. 15, No. 1, pp. 4470-4489, 2025.

[13] S. Zhan, L. Huang, G. Luo, S. Zheng and H.C. Chao, "A Review on Federated Learning Architectures for Privacy-Preserving AI: Lightweight and Secure Cloud-Edge-End Collaboration", *Electronics*, Vol. 14, No. 13, pp. 2512-2531, 2025.

[14] H.P. Natarajan, S. Shymalagowri, D. Ckv and K. Ram, "Federated Learning Based Privacy Preserving for Brain Tumor Detection", *Proceedings of IEEE International Conference on Soft Computing*, pp. 1-6, 2024.

[15] S. Hundekari, R.V.S. Praveen, A. Shrivastava and M.L.F. Jumaili, "Privacy-Preserving Federated Learning Algorithm for Distributed Health Data Analysis", *Proceedings of IEEE International Conference on Cyber Resilience*, pp. 1-6, 2025.