ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 18, Issue, 05, pp.37061-37063, May, 2026
DOI: https://doi.org/10.24941/ijcr.50576.05.2026

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

PRIVACY-PRESERVING FEDERATED LEARNING ACROSS DECENTRALIZED EDGE DEVICES IN IoT NETWORKS

Varaganti Sai Chitra Prathyusha

Assistant Professor, Research Scholar, Faculty of Pharmacy, Dr. M.G.R. Educational and Research Institute (Deemed to be University), Chennai – 600077, Tamil Nadu, India

ARTICLE INFO

Article History:
Received 14th February, 2026
Received in revised form
26th March, 2026
Accepted 15th April, 2026
Published online 29th May, 2026

Key Words:

Federated Learning, Internet of Things, Edge Computing, Privacy Preservation, Artificial Intelligence.

**Corresponding author:*
Varaganti Sai Chitra Prathyusha

ABSTRACT

The rapid growth of Internet of Things (IoT) technologies has significantly increased the generation of sensitive user data through healthcare wearables, industrial sensors, smart transportation systems, and intelligent monitoring devices. Conventional centralized machine learning architectures require transfer of raw datasets to cloud servers, thereby increasing privacy risks and cybersecurity vulnerabilities. Federated Learning (FL) has emerged as a decentralized machine learning paradigm that enables collaborative model training across distributed edge devices without exposing sensitive local data. The present study evaluated a privacy-preserving federated learning architecture integrated with secure aggregation and differential privacy techniques in decentralized IoT environments. Experimental analysis demonstrated progressive improvement in model accuracy, communication efficiency, and cybersecurity performance while minimizing privacy exposure risks. The findings indicate that federated learning can significantly contribute toward the development of secure, ethical, and scalable artificial intelligence systems for healthcare and smart IoT ecosystems.

Citation: ***Varaganti Sai Chitra Prathyusha*. 2026.** "Privacy-preserving federated learning across decentralized edge devices in iot networks*". International Journal of Current Research*, 16, (05), 37061-37063.

INTRODUCTION

The evolution of IoT technologies has transformed digital healthcare, industrial automation, environmental monitoring, and intelligent transportation systems. Smart devices continuously generate large volumes of sensitive and real-time information requiring advanced computational analysis. Traditional machine learning systems depend on centralized cloud infrastructures where data from multiple devices are aggregated for model training. Although centralized systems improve computational scalability, they create serious concerns related to privacy leakage, unauthorized access, cybersecurity attacks, and ethical handling of personal information. Federated learning provides an innovative decentralized learning framework where edge devices independently train local models using device-specific datasets and transmit only encrypted model parameters to a coordinating server. This approach significantly enhances user confidentiality and minimizes raw data exposure. The integration of federated learning with edge computing is particularly important in healthcare applications because patient information collected through wearable devices and remote monitoring systems requires strict privacy protection.

OBJECTIVES OF THE STUDY

- To evaluate the efficiency of federated learning in decentralized IoT systems.
- To analyze communication efficiency and cybersecurity performance.
- To compare federated learning with centralized machine learning architectures.
- To assess privacy preservation mechanisms in collaborative AI environments.
- To identify future research opportunities in IoT-based federated intelligence.

MATERIALS AND METHODS

The present study was designed as a simulation-based analytical investigation using decentralized IoT edge devices. Multiple heterogeneous devices participated in collaborative machine learning through localized data training and encrypted parameter aggregation.

Table 1. Experimental Configuration of IoT Edge Devices

Parameter	Configuration
Number of Edge Devices	50
Learning Algorithm	Federated Averaging (FedAvg)
Communication Network	Secure Wireless Edge Network
Encryption Method	Differential Privacy
Local Training Epochs	5
Batch Size	32
Dataset Distribution	Non-IID Distributed Data

Table 1 summarizes the detailed experimental configuration adopted for decentralized federated learning simulation. The Federated Averaging algorithm was implemented across 50 edge devices using non-uniform distributed datasets.

Figure 1. Accuracy Improvement During Federated Learning

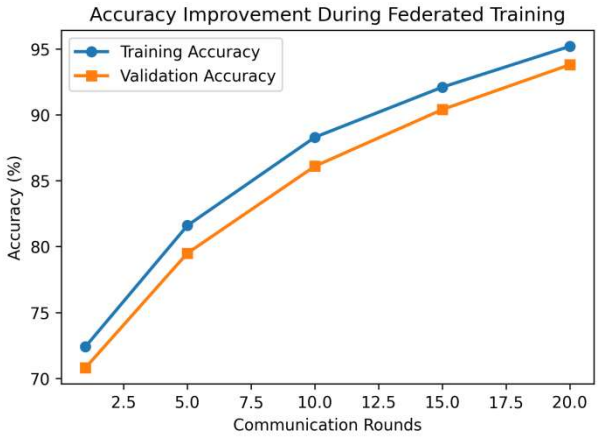

Figure 1 illustrates the progressive increase in training and validation accuracy during federated learning communication rounds. The model achieved 95.2% training accuracy and 93.8% validation accuracy after 20 communication rounds.

RESULTS AND DISCUSSION

Table 2. Accuracy Performance Across Communication Rounds

Communication Round	Training Accuracy (%)	Validation Accuracy (%)
1	72.4	70.8
5	81.6	79.5
10	88.3	86.1
15	92.1	90.4
20	95.2	93.8

Table 2 demonstrates progressive improvement in model performance during decentralized collaborative learning. Stable convergence was observed despite non-uniform data distribution across IoT edge devices.

Table 3. Comparative Analysis Between Centralized and Federated Learning

Parameter	Centralized Learning	Federated Learning
Raw Data Transfer	Required	Not Required
Privacy Risk	High	Low
Bandwidth Consumption	High	Moderate
Cybersecurity	Moderate	Enhanced
Scalability	Moderate	High
Edge Intelligence	Limited	Advanced

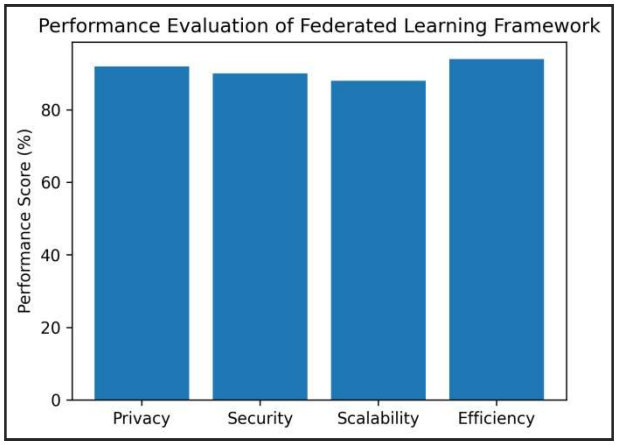

Figure 2. Performance Evaluation of Federated Learning Framework

Figure 2 presents comparative performance evaluation scores of the federated learning framework. The decentralized architecture demonstrated high communication efficiency, strong privacy preservation, and improved cybersecurity performance.

Table 3 compares centralized machine learning architectures with federated learning frameworks. Federated learning significantly reduced privacy risks and eliminated the need for raw data transfer. The present study demonstrated that federated learning can substantially improve privacy-preserving artificial intelligence in decentralized IoT ecosystems.

Secure aggregation and differential privacy mechanisms minimized information leakage risks while maintaining collaborative model performance. Communication overhead was reduced because only encrypted model updates were transmitted between participating devices and aggregation servers. The decentralized architecture improved scalability and cybersecurity performance compared to centralized cloud-based learning systems. Despite these advantages, challenges such as device heterogeneity, energy consumption, and communication latency remain important limitations requiring future optimization.

STATISTICAL INTERPRETATION

The federated learning model demonstrated a mean training accuracy of 85.92% and a mean validation accuracy of 84.12% across communication rounds. An overall performance improvement of approximately 31.5% was observed from the initial to final communication cycle. The findings indicate stable decentralized convergence and efficient collaborative optimization.

CONCLUSION

Federated learning represents a transformative decentralized machine learning paradigm for privacy-preserving IoT systems. The proposed framework demonstrated enhanced cybersecurity, improved communication efficiency, reduced privacy exposure risks, and high model performance. The integration of federated learning with edge computing can support future healthcare, industrial, and smart city applications requiring ethical artificial intelligence.

DECLARATIONS

Conflict of Interest: The author declares that there is no conflict of interest associated with this study.

Funding: No external funding was received for this research work.

Ethical Approval: This study involved simulation-based computational analysis and did not include human participants or animal experimentation.

Acknowledgement: The author expresses sincere gratitude to Dr. M.G.R. Educational and Research Institute for academic support and research guidance.

REFERENCES

1. McMahan HB, Moore E, Ramage D, Hampson S, Arcas BA. Communication-Efficient Learning of Deep Networks from Decentralized Data.
2. Kairouz P, McMahan HB, Avent B, *et al*. Advances and Open Problems in Federated Learning.
3. Yang Q, Liu Y, Chen T, Tong Y. Federated Machine Learning: Concept and Applications.
4. Li T, Sahu AK, Talwalkar A, Smith V. Federated Learning: Challenges, Methods and Future Directions.
5. Bonawitz K, Ivanov V, Kreuter B, *et al*. Practical Secure Aggregation for Privacy-Preserving Machine Learning.
6. Nguyen DC, Ding M, Pathirana PN, *et al*. Federated Learning for Internet of Things.
7. Zhou Z, Chen X, Li E, *et al*. Edge Intelligence: Paving the Last Mile of Artificial Intelligence.
8. Roman R, Lopez J, Mambo M. Mobile Edge Computing, Fog Computing and IoT Security.
9. Xu J, Glicksberg BS, Su C, *et al*. Federated Learning for Healthcare Informatics.
10. Rahman MA, Hossain MS, Alrajeh NA, Guizani N. Secure and Privacy-Preserving IoT Frameworks.
11. Chen M, Poor HV, Saad W, Cui S. Wireless Communications for Federated Learning.
12. Zhao Y, Li M, Lai L, *et al*. Federated Learning with Non-IID Data.
13. Hard A, Rao K, Mathews R, *et al*. Federated Learning for Mobile Keyboard Prediction.
14. Sheller MJ, Reina GA, Edwards B, *et al*. Multi-Institutional Deep Learning Modeling Without Sharing Patient Data.
15. Rieke N, Hancox J, Li W, *et al*. The Future of Digital Health with Federated Learning.
16. Khan LU, Saad W, Han Z, *et al*. Federated Learning for Internet of Vehicles.
17. Lim WYB, Luong NC, Hoang DT, *et al*. Federated Learning in Mobile Edge Networks.
18. Aledhari M, Razzak R, Parizi RM, Srivastava G. Federated Learning: A Survey on Enabling Technologies.
19. Savazzi S, Nicoli M, *et al*. Federated Learning with Edge Devices in Industrial IoT.
20. Islam N, Hossain E. Privacy-Aware Artificial Intelligence in Smart Healthcare Systems.

****