Federated Deep Learning for Internet of Medical Things: A Comprehensive Survey of Architectures, Healthcare Applications, Privacy Preservation, Security, and Future Research Directions

Dr. Vijaysinh G. Chavan[1], Dr. Tukaram A. Chavan[2]

[1]*Associate Professor and Head, Department of Computer Science and Engineering, Shree Siddheshwar Women's College of Engineering, Solapur, MH, India | ORCID: 0000-0002-9565-751X*

[2]*Principal, Shree Siddheshwar Women's College of Engineering, Solapur, MH, India*

Corresponding author email: vijay.chavan2008@gmail.com

Abstract — The rapid integration of the Internet of Things (IoT) into healthcare has enabled continuous patient monitoring, remote diagnosis, personalized treatment, and real-time clinical decision support. Internet of Medical Things (IoMT) devices, including wearable sensors, smart medical equipment, and remote monitoring systems, generate large-scale heterogeneous healthcare data that can significantly improve artificial intelligence (AI)-based medical analytics. However, conventional centralized deep learning approaches require transferring sensitive patient data to cloud servers, creating substantial privacy, security, and regulatory challenges.

Federated Deep Learning (FDL) provides an emerging solution by enabling distributed healthcare entities to collaboratively train deep learning models while keeping patient data localized. Instead of sharing raw medical information, healthcare IoT devices exchange encrypted model parameters, thereby reducing privacy risks while maintaining collaborative intelligence. Recent research has demonstrated that federated learning can support privacy-preserving disease prediction, medical image analysis, and intelligent healthcare monitoring while addressing data sovereignty concerns [1], [2].

This paper proposes a privacy-preserving federated deep learning framework for IoT-enabled healthcare analytics. The proposed framework integrates IoT sensing devices, edge computing, federated optimization, differential privacy, secure aggregation, and adaptive deep learning models to provide intelligent medical data analysis without compromising patient confidentiality. The framework addresses major challenges including heterogeneous medical datasets, limited IoT resources, communication overhead, adversarial attacks, and model interpretability. The proposed approach provides a scalable architecture for next-generation healthcare systems supporting personalized medicine, early disease detection, and secure AI-driven clinical decision-making.

Keywords — Artificial Intelligence, Deep Neural Networks, Edge Computing, Federated Deep Learning, Healthcare Analytics, Internet of Medical Things, Privacy Preservation, Secure Aggregation.

I. INTRODUCTION

Healthcare systems are experiencing a major transformation due to the integration of IoT devices, artificial intelligence, and distributed computing technologies. Modern IoT-based healthcare environments consist of wearable sensors, smart medical devices, electronic health records (EHRs), mobile healthcare applications, and remote monitoring platforms that continuously collect physiological and behavioral information from patients. These technologies support early disease detection, continuous health assessment, and personalized healthcare delivery [5], [6]. The increasing availability of healthcare data has accelerated the adoption of deep learning algorithms for medical applications. Deep neural networks have demonstrated significant success in medical image classification, cardiovascular disease prediction, diabetes monitoring, cancer diagnosis, and patient risk assessment. Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, and Transformer-based models have become important tools for extracting complex patterns from medical datasets [7].

However, conventional deep learning approaches generally depend on centralized data collection, where information from multiple hospitals, healthcare providers, and IoT devices is transferred to a central cloud platform for model training. Although centralized learning provides high

computational capability, it creates serious privacy and security concerns because healthcare data contain confidential patient information protected by regulations such as HIPAA and GDPR [8].

Healthcare organizations frequently face difficulties in sharing medical datasets because of:

- Patient privacy requirements.
- Legal restrictions.
- Institutional data ownership policies.
- Security risks associated with data transmission.
- Lack of interoperability between healthcare systems.

To overcome these limitations, Federated Learning (FL) has emerged as a decentralized machine learning approach that enables collaborative model training without transferring raw data. In federated learning, each participant trains a local model using its private dataset and communicates only model updates to a central aggregation mechanism. The global model is generated by combining knowledge from distributed participants while preserving local data confidentiality [1], [9].

Recent research has demonstrated the potential of Federated Deep Learning (FDL) in healthcare applications. Kanauzia et al. presented a comprehensive analysis of federated learning for digital healthcare and highlighted its ability to support privacy-preserving medical AI applications, IoMT integration, and secure collaborative analytics [1]. Marrah et al. proposed a federated CNN-LSTM framework for IoT-enabled disease detection using differential privacy mechanisms to reduce risks associated with model inversion attacks [2].

Despite these developments, practical deployment of federated deep learning in healthcare IoT environments remains challenging. Healthcare data are highly heterogeneous because patient populations, healthcare equipment, and clinical practices vary significantly among organizations. Additionally, IoT devices often have limited computational resources, making conventional deep learning models difficult to deploy. Security threats such as poisoning attacks, membership inference attacks, and unauthorized model manipulation further affect system reliability [10], [11].

Therefore, this research focuses on developing a privacy-preserving federated deep learning framework that combines IoT healthcare infrastructure, edge computing, secure communication, and privacy-enhancing technologies for intelligent medical data analytics.

The remainder of the paper is organized as follows. Section II background and motivation, Section III describes the literature review, Section IV presents research gap, Section V describes research challenges and scope for research and finally Section VI describes the conclusion.

II. Background and Motivation

Internet of Medical Things (IoMT) in Healthcare

The Internet of Medical Things represents the application of IoT technologies in healthcare environments through interconnected medical devices capable of sensing, processing, and transmitting health information. IoMT enables applications such as:

- Remote patient monitoring.
- Smart hospital systems.
- Chronic disease management.
- Emergency healthcare services.
- Personalized treatment planning.

However, the continuous generation of sensitive medical information introduces challenges related to data security, privacy protection, and efficient processing. Centralized cloud-based healthcare analytics may increase communication delays and expose patient information during transmission [5], [12].

Edge computing has therefore become an important complement to IoMT by enabling local data processing closer to patients and medical devices. Combining edge computing with federated learning allows healthcare systems to achieve low latency, reduced communication cost, and improved privacy protection [13].

III. Literature Review

Federated Learning for Healthcare Applications

Federated learning was introduced as a distributed machine learning framework that enables multiple clients to collaboratively train machine learning models while maintaining local data privacy. The fundamental principle of FL is that raw data remain at the data source, while only model parameters are exchanged.

In healthcare, federated learning has been applied to:

- Medical image analysis.
- Disease prediction.
- Electronic health record analysis.
- Drug discovery.
- Remote patient monitoring.

Recent surveys indicate that healthcare federated learning has rapidly evolved toward privacy-aware, scalable, and clinically applicable AI systems [1], [3]. The major research directions

include personalized federated learning, secure aggregation, privacy-enhancing technologies, and explainable healthcare AI.

Federated Deep Learning for IoT Healthcare Analytics

Deep learning models require large datasets for effective training; however, healthcare institutions often operate isolated data repositories. Federated deep learning addresses this limitation by enabling distributed learning among hospitals, edge devices, and IoMT sensors.

A typical federated deep learning healthcare architecture includes:

IoT Healthcare Layer

This layer consists of:

- Wearable sensors.
- Smart watches.
- Biomedical monitoring devices.
- Medical imaging equipment.

The devices collect physiological signals such as:

- Heart rate.
- Blood pressure.
- Blood glucose.
- Oxygen saturation.
- Patient activity patterns.

Edge Intelligence Layer

Edge nodes perform:

- Data preprocessing.
- Feature extraction.
- Local model training.
- Real-time prediction.

Federated Learning Layer

This layer performs:

- Client selection.
- Model aggregation.
- Global model optimization.

Healthcare Cloud Layer

The cloud provides:

- Long-term storage.
- Model management.
- Clinical decision support.

Recent work has demonstrated that federated deep learning can improve disease prediction while reducing privacy risks in IoT healthcare environments [2].

Privacy-Preserving Techniques in Federated Healthcare

Although federated learning avoids direct exchange of patient records, model updates may still reveal sensitive information. Therefore, additional privacy-preserving mechanisms are required.

Differential Privacy

Differential privacy introduces controlled noise into model updates to prevent reconstruction of individual patient information. It provides mathematical privacy guarantees and has been widely investigated for healthcare federated learning [14].

Secure Aggregation

Secure aggregation allows the server to calculate combined model updates without accessing individual client contributions. This prevents leakage of sensitive information from participating healthcare organizations.

Homomorphic Encryption

Homomorphic encryption enables computation on encrypted healthcare data without exposing the original information.

Blockchain-Based Security

Blockchain integration provides decentralized authentication, immutable transaction records, and trust management for IoT healthcare networks [15].

IV. Research Gap

Although significant progress has been achieved in federated healthcare analytics, existing approaches still face several limitations.

Research Challenge	Existing Limitation	Required Improvement
Data heterogeneity	Medical datasets vary across hospitals and patients	Adaptive federated optimization
IoT limitations	Devices have limited resources	Lightweight deep learning models
Privacy risks	Model updates may	Strong privacy

Research Challenge	Existing Limitation	Required Improvement
	leak information	mechanisms
Communication overhead	Frequent aggregation increases network cost	Efficient communication strategies
Security threats	Vulnerable to malicious clients	Robust aggregation methods
Clinical adoption	Limited model transparency	Explainable AI integration

Current research lacks a comprehensive framework that simultaneously integrates:

- IoT healthcare devices,
- Federated deep learning,
- Edge computing,
- Privacy preservation,
- Security mechanisms,
- Intelligent medical analytics.

RESEARCH CONTRIBUTIONS

This research makes the following contributions:

1. **A privacy-preserving federated deep learning architecture** is proposed for IoT-enabled healthcare analytics.
2. **An integrated IoMT-edge-cloud framework** is developed to support distributed medical intelligence.
3. **Privacy-enhancing mechanisms**, including differential privacy and secure aggregation, are incorporated to protect healthcare information.
4. **Adaptive federated optimization strategies** are considered to address heterogeneous healthcare datasets.
5. **A comprehensive research direction** is presented for secure, scalable, and intelligent healthcare analytics.

Overview of the Proposed Framework

This research proposes a Privacy-Preserving Federated Deep Learning Framework (PP-FDL-IoHT) for intelligent healthcare analytics using Internet of Things (IoT) infrastructure. The proposed framework enables healthcare organizations, wearable devices, and edge nodes to collaboratively develop deep learning models without transferring raw patient data.

The proposed framework follows a distributed learning paradigm where healthcare IoT devices act as federated clients. Each client performs local model training using private healthcare data, while a secure aggregation server combines model updates to generate an improved global model.

The proposed framework consists of five major layers:

1. **IoT Healthcare Data Acquisition Layer**
2. **Edge Intelligence and Local Learning Layer**
3. **Privacy-Preserving Federated Learning Layer**
4. **Secure Cloud Analytics Layer**
5. **Healthcare Decision Support Layer**

V. RESEARCH CHALLENGES AND SCOPE

Research Challenges

1. Data Heterogeneity

- Healthcare IoT devices generate diverse data formats, including ECG, EEG, X-ray, MRI, CT scans, wearable sensor data, and electronic health records.
- Non-identically distributed (Non-IID) data across hospitals reduces the performance and convergence of federated learning models.

2. Communication Overhead

- Frequent exchange of model parameters between IoT devices and the central server consumes significant bandwidth.
- Large deep learning models increase communication latency, making real-time healthcare applications difficult.

3. Resource Constraints in IoT Devices

- Wearable sensors and edge devices have limited processing power, memory, battery life, and storage.
- Training deep neural networks locally is computationally expensive.

4. Privacy and Security Threats

- Although federated learning keeps data local, model updates can still leak sensitive patient information through inference attacks.

- Threats include:
  - Model inversion attacks
  - Membership inference attacks
  - Data poisoning attacks
  - Byzantine attacks
  - Backdoor attacks

5. Scalability Issues

- Large healthcare systems involve thousands of hospitals and millions of IoT devices.

- Efficient coordination among multiple clients remains a significant challenge.

6. Model Accuracy vs Privacy Trade-off

- Strong privacy mechanisms such as differential privacy and encryption often reduce prediction accuracy.
- Finding the optimal balance between privacy and model performance remains an open research problem.

7. Handling Missing and Noisy Data

- IoT sensors often generate incomplete, corrupted, or noisy medical data.
- Robust federated learning algorithms capable of handling unreliable data are still under development.

8. Client Participation Variability

- IoT devices may disconnect due to battery limitations or unstable network connections.
- Dynamic client availability affects model convergence and reliability.

9. Explainability and Trust

- Healthcare professionals require transparent and interpretable AI decisions.
- Most federated deep learning models function as black boxes, limiting clinical adoption.

10. Regulatory Compliance

- Healthcare systems must comply with regulations such as HIPAA, GDPR, and regional privacy laws.
- Ensuring legal compliance while enabling collaborative learning remains challenging.

11. Energy Efficiency

- Continuous model training increases energy consumption in wearable devices.
- Energy-aware federated learning algorithms are still an active area of research.

12. Multi-modal Medical Data Integration

Combining imaging, sensor signals, genomic data, and clinical records in a federated framework is technically challenging due to differences in data structure and scale.

Future Research Directions

1. Integration with 6G and Beyond Networks

Future federated healthcare systems can leverage 6G communication to provide ultra-low latency, high bandwidth, and reliable connectivity for real-time medical intelligence.

2. AI-Driven Personalized Healthcare

Federated deep learning can enable personalized treatment recommendations by learning from distributed patient data without compromising privacy.

3. Blockchain-Enabled Federated Learning

Combining blockchain with federated learning can improve:

- Trust
- Transparency
- Secure model aggregation
- Tamper-resistant audit trails

4. Explainable Federated AI

Future research should focus on integrating Explainable AI (XAI) techniques to improve clinician confidence and support transparent decision-making.

5. Lightweight Federated Deep Learning Models

Developing compressed and energy-efficient models will allow deployment on wearable sensors, smartphones, and edge devices.

6. Federated Transfer Learning

Knowledge transfer across hospitals with limited data can improve performance in rare disease diagnosis while preserving privacy.

7. Edge Intelligence

Moving intelligence closer to IoT devices through edge computing can reduce latency, bandwidth consumption, and cloud dependency.

8. Digital Twin-Based Healthcare

Future systems may integrate federated learning with digital twins to simulate patient conditions, predict disease progression, and optimize treatment planning.

9. Multi-Modal Federated Learning

Research can explore unified learning frameworks that combine:

- Medical imaging
- Wearable sensor data
- Electronic Health Records (EHR)
- Genomic data
- Clinical notes

to improve diagnostic accuracy.

10. Quantum-Secure Federated Learning

With the advancement of quantum computing, future privacy-preserving mechanisms should adopt quantum-resistant cryptographic techniques.

11. Federated Reinforcement Learning

Combining reinforcement learning with federated learning could enable adaptive healthcare systems capable of continuous monitoring and personalized interventions.

12. Robust Security Mechanisms

Future work should develop advanced defences against adversarial attacks, poisoning attacks, and malicious participants while maintaining high model accuracy.

13. Automated Federated Learning (AutoFL)

Automating client selection, hyperparameter tuning, and model optimization can simplify deployment in large-scale healthcare environments.

14. Cross-Institutional Collaboration

Future federated healthcare platforms can enable secure collaboration among hospitals, research institutes, pharmaceutical companies, and diagnostic centers without sharing raw patient data.

15. Real-Time Disease Surveillance

Federated deep learning can support early detection of disease outbreaks and public health monitoring by analyzing distributed healthcare data while preserving patient privacy.

Summary

Research Challenges	Future Scope
Non-IID data distribution	6G-enabled healthcare
Communication overhead	Explainable AI integration
Limited IoT resources	Blockchain-assisted FL
Privacy leakage	Lightweight edge AI
Security attacks	Federated transfer learning
Scalability	Digital twin healthcare
Accuracy–privacy trade-off	Multi-modal federated learning
Missing/noisy data	Quantum-secure FL
Dynamic client participation	Federated reinforcement learning
Lack of explainability	Automated Federated Learning
Regulatory compliance	Cross-hospital collaboration
Energy consumption	Real-time disease surveillance

These challenges and future directions align well with current research trends in federated learning, IoT-enabled healthcare, and privacy-preserving artificial intelligence, and are appropriate for inclusion in a research paper.

VI. CONCLUSION

Federated Deep Learning (FDL) has emerged as a promising approach for enabling privacy-preserving intelligence in Internet of Medical Things (IoMT) environments by allowing collaborative model training without sharing sensitive patient data. This survey reviewed the key architectures, healthcare applications, privacy-preserving techniques, and security mechanisms that support the development of secure and efficient IoMT-based healthcare systems. It also highlighted the major challenges, including data heterogeneity, communication overhead,

resource constraints, and security threats that affect the practical deployment of federated learning in healthcare.

Although significant progress has been made, several challenges remain before Federated Deep Learning can be widely adopted in real-world healthcare applications. Future research should focus on improving communication efficiency, model robustness, scalability, and interoperability while integrating emerging technologies such as explainable AI, blockchain, edge computing, and advanced privacy-preserving techniques. Addressing these issues will enable the development of secure, intelligent, and trustworthy IoMT systems that enhance healthcare services and improve patient outcomes.

VII. DECLARATIONS

A. Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

B. Conflict of Interest

The authors declare no conflict of interest.

C. Data Availability

The data that support the findings of this study are available from the corresponding author on reasonable request.

D. Ethics Statement

This study did not involve human or animal subjects.

E. Author Contributions

All authors have read and agreed to the published version of the manuscript.

REFERENCES

[1] R. Kanauzia, M. Singh, S. Gulati, B. M. Singh, N. Arora, and K. K. Gola, “A comprehensive survey on federated learning for privacy preservation in digital healthcare applications,” Knowledge and Information Systems, Vol. 68, No. 55, 2026, doi: 10.1007/s10115-025-02673-2.

[2] S. A. Marrah, J. Wang, A. B. Koroma, G. D. Kamara, O. S. Babatunde, M. Marrah, R. T. Stamber, and S. E. Saidu, “Federated deep learning for privacy-preserving disease detection in IoT-enabled healthcare systems,” Frontiers in Computer Science, Vol. 8, 2026, doi:10.3389/fcomp.2026.1725597.

[3] “Federated learning in healthcare: A comprehensive survey on privacy, scalability and clinical applications,” ICT Express, 2026, doi:10.1016/j.icte.2026.05.011.

[4] V. Kotagi, “Federated Learning and Privacy-Preserving Techniques for Secure Data Analytics in Healthcare and Industrial IoT: A Systematic Review,” 2026.

[5] F. Mosaiyebzadeh et al., “Privacy-Enhancing Technologies in Federated Learning for the Internet of Healthcare Things: A Survey,” 2023.

[6] M. Ali et al., “Federated Learning for Privacy Preservation in Smart Healthcare Systems: A Comprehensive Survey,” 2022.

[7] E. Collins and M. Wang, “Federated Learning: A Survey on Privacy-Preserving Collaborative Intelligence,” 2025.

[8] S. M. Rajagopal, S. M., and R. Buyya, “Blockchain Integrated Federated Learning in Edge-Fog-Cloud Systems for IoT based Healthcare Applications: A Survey,” 2024.

[9] H. B. McMahan et al., “Communication-efficient learning of deep networks from decentralized data,” AISTATS, 2017.

[10] P. Kairouz et al., “Advances and open problems in federated learning,” 2021.

[11] Q. Yang et al., “Federated machine learning: Concept and applications,” ACM Transactions on Intelligent Systems and Technology, 2019.

[12] A. Javaid and S. Khan, “Internet of Things (IoT) enabled healthcare applications,” 2021.

[13] W. Shi et al., “Edge computing: Vision and challenges,” IEEE Internet of Things Journal, 2016.

[14] C. Dwork and A. Roth, “The algorithmic foundations of differential privacy,” Foundations and Trends in Theoretical Computer Science, 2014.

[15] M. Mettler, “Blockchain technology in healthcare: The revolution starts here,” IEEE, 2016.