ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct1178

# The Edge-AI and Federated Learning Convergence Towards Strong Security and Privacy in Internet of Medical Things (IoMT) Ecosystems

Hemalatha A.

Department of IoT,
VLB Janakkiayammal College of Arts and Science
Coimbatore, India

Publication Date: 2025/11/01

**Abstract: Internet of Medical Things (IoMT) is revolutionizing the healthcare sector around the world by installing large networks of interconnected sensors and devices. However, the sheer volume, real-time nature, and sensitivity of health data put a strain on traditional centralized cloud designs, raising critical issues around latency and energy usage, as well as concerns related to privacy regulations such as HIPAA and GDPR. This review assesses the necessary architectural changes towards decentralized intelligence, with a focus on the synergy between Edge Artificial Intelligence (Edge-AI) and Federated Learning (FL). The Edge-AI minimizes latency by enabling the processing of real-time data on-device, which is crucial for life-sensitive applications. FL provides a privacy-sensitive protocol that addresses the issue of the data silo in healthcare and allows global models to be trained jointly by distributed medical institutions without sharing sensitive raw data. We thoroughly consider the architectural paradigms, the specific applications of IoMT, and the taxonomy of security risks, including physical tampering and data poisoning. We also outline the key privacy-enhancement methods (PETs), including Differential Privacy and Homomorphic Encryption, the trade-offs (e.g., accuracy versus efficiency) inherent in them, and the main research gaps, and conclude with the key future directions, including 6G connectivity.**

***Keywords:*** *Edge Computing; Federated Learning; Edge-AI;Deep Learning;Healthcare.*

**How to Cite:** Hemalatha A. (2025) The Edge-AI and Federated Learning Convergence Towards Strong Security and Privacy in Internet of Medical Things (IoMT) Ecosystems. *International Journal of Innovative Science and Research Technology*, 10(10), 2012-2016. https://doi.org/10.38124/ijisrt/25oct1178

## I. INTRODUCTION

The transformation of the Internet of Things (IoT) into the dedicated Internet of Medical Things (IoMT) has triggered unprecedented progress in healthcare, enabling uninterrupted remote patient monitoring, sophisticated diagnostics, and personalized medicine [1]. IoMT systems utilize connected sensors or implantable sensors to monitor vital health parameters, such as heart rate, blood pressure, and activity data, in real-time [2]. The ability to derive meaningful, data-driven insights using Health Analytics (HA) is the most important one [1].

### *A. Disadvantages of Centralized Systems and the Paradigm Shift.*

The use of traditional, centralized cloud-based HA models faces three inherent challenges in the application to IoMT:

The radically increasing data streams of IoMT require large bandwidth and computing power [1]. The use of centralized cloud computing results in high-latency communication and high energy usage, which is unacceptable in time-sensitive and life-critical applications [3].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct1178

Medical information is very sensitive and is subject to strict legal provisions, such as HIPAA and GDPR [4]. Traditional AI solutions require the consolidation of sensitive patient data into a central database, which poses a significant threat to massive, centralized data breaches and, by extension, violates privacy policies [4].

Medical data are often held in disconnected silos (e.g., hospitals, clinics, or research laboratories) due to concerns about privacy, competition, and regulatory compliance [5]. This fragmentation cripples the capabilities of centralized machine learning models [5]. This terrain requires a radical shift in the paradigm from centralized to distributed learning [1].

*B. Edge-AI and Federated Learning Synergy.*

The transition to distributed intelligence can be summarized with the synergistic combination of Edge-AI and FL:

- *Edge-AI:*

This decentralized computing model moves data processing closer to the source, the IoMT device or a local gateway [6]. Edge-AI can achieve a significant reduction in latency and dissipated energy by minimizing the distance data travels, which is crucial in the context of real-time decision-making to provide immediate patient safety interventions [3].

- *Federated Learning:*

This distributed machine learning system enables a single global model to be trained in collaboration with multiple clients (such as equipment or organizations) without exchanging raw local data [5]. Clients send and receive updates or gradients of the model, thus maintaining the confidentiality of Electronic Health Records (EHRs) and addressing the data silo issue [1].

This review explains how this convergence ensures both real-time performance (Edge-AI) and data privacy and collaboration (FL) in the IoMT system.

## II.THEORETICAL FOUNDATIONS

*A. Layered Edge-IoMT Architecture.*

A typical IoMT system has a multi-layered architecture [7]. The Perception Layer comprises IoMT devices, sensors, and actuators that collect and digitalize raw patient data (e.g., heart rate, motion activity) [2].

- *Network Layer (Edge/Fog):*

This middle layer receives and performs initial processing of data and then sends it to the cloud [7].

- *Application Layer (Cloud):*

This layer manages long-term storage, EHR integration, and executes advanced machine-learning algorithms for deep analytics and personalized recommendations [2].

*B. Edge Computing vs. Fog Computing.*

The terms are often used interchangeably, but they refer to different scopes of localized intelligence [8]: Edge Computing is processing implemented on the source, the device itself, or a gateway in immediate proximity [9]. It allows processing of data in real-time and has minimal computational overhead [8].

Fog Computing serves as a decentralized middle layer between the edge and the cloud [10]. Fog servers collect information from numerous edge devices, filter out unwanted measurements, and optimize traffic before sending the results to the cloud [9].

The significance of edge nodes in IoMT lies in their ability to perform initial data processing, which includes filtering noise, aggregation, real-time anomaly detection, and encryption [2]. Only condensed and time-constrained alerts or salient features are typically forwarded to in-depth analytics [2]. This is a significant part of offloading computation, thereby reducing communication overhead and extending the operational lifetime of resource-constrained sensors by transferring the computational load to more powerful edge gateways [6]. It has been shown that offloading should be addressed as a multi-objective optimization problem, balancing latency, energy usage, and the reliability of edge computing nodes, explicitly to prevent the exposure of user information [11].

*C. Federated Learning Topologies.*

Two main topologies are used in the implementation of FL that are relevant to healthcare [12]:

- *Cross-Device FL:*

It involves multiple devices, including patient wearables and home sensors, which are characterized by intermittent connectivity and non-IID (non-independent and Identically Distributed) data [12].

- *Cross-Silo FL:*

Includes a small number of hospitals, medical centers, or pharmaceutical firms [13]. Every organization has its own secure, isolated silos of proprietary, high-quality data. Cross-silo FL is essential to facilitate medical research and the training of diagnostic models across networked healthcare organizations, as each organization disseminates updates of models after local training on its secure data [13].

*D. Architectural Paradigms: Federated Learning vs. Decentralized Federated Learning.*

The choice of a Federated Learning architecture determines how the aggregation should be conducted, as well as the system's resilience. Centralized Federated Learning (CFL) relies on a single global server, typically located in the cloud, to select models, coordinate, and consolidate local model weights. Conversely, Decentralized Federated Learning (DFL) eliminates the point of failure by implementing peer nodes that use a consensus protocol to complete the model [1]. These structural differences have far-reaching effects on security and efficiency of operations.

\

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct1178

Table 1: Comparison Between Centralized and Decentralized Federated Learning Architectures [1].

| Parameter | Centralized Federated Learning (CFL) | Decentralized Federated Learning (DFL) |
|---|---|---|
| Model Selection | A global server (cloud) picks the model and defines some initial hyperparameters. | Peer-nodes form a consensus protocol to finalize the model. |
| Communication Round | Synchronous and timestamping | timestamping Asynchronous and chunk-based processing. |
| Mechanism of Communication | Client-Server (local nodes send the gradients to the central server) | Distributed with cross-verification and followed by a block propagation phase. |
| Key Algorithms | FedAvg, FedCS, FedProx, q-FedAvg. | Gossip-based FL, BlockFL, ChainFL, BAFFLE. |
| Attacks | Data Poisoning, Label Flipping, and Convergence-based Attacks. | Sybil attacks, distributed denial-of-service attacks, and Knowledge-based attacks. |
| Security Mechanism | Homomorphic encryption, Secure multi-party communication. | Zero-knowledge proof, Blockchain-based miner verification, Turbo coding. |

## III. EDGE-AI AND FEDERATED LEARNING IOMT APPLICATIONS.

### *A. Predictive Diagnostics and Collaborative Research.*

Federated Learning facilitates the creation of high-quality predictive models by combining statistically distinct datasets across multiple medical institutions [14]. It is an essential feature in the timely identification of problems, such as sepsis or specific cancer risks, where extensive data coverage helps improve the accuracy of models [15].

- *Clinical Translation:*

A systematic review of Federated Learning in healthcare suggests that, despite the strengths of FL across a wide range of data types, especially medical imaging and neural networks, most studies are proof-of-concept studies with only five articles demonstrating a practical application of FL in a clinical setting [14]. The most common specialties that utilize FL are radiology and internal medicine [14].

- *Multi-Institutional Genomics:*

Federated Learning can be utilized in competitive fields like genomics and drug discovery to enable pharmaceutical and research laboratories to collaboratively train their models without disclosing proprietary data, using privacy-preserving mechanisms such as Differential Privacy [16].

### *B. Real-Time Remote Monitoring and Intervention.*

Edge AI is essential for time-sensitive remote monitoring. Edge devices perform real-time anomaly detection, such as abnormal ECG rhythms or patient falls, locally [2]. On-device decentralization in decision-making provides a quick response without relying on cloud resources [6]. With the increasing number of IoMT devices, the use of robust, deep-learning-based anomaly detection systems should be complemented by a robust intrusion detection system (IDS) deployed at the device level to mitigate the growing cyber threats [17].

### *C. Smart Hospital Operations*

Edge-AI also enhances operational efficiency by leveraging local sensors and computer vision to navigate complex environments [18]. Applications include:

- *Asset Tracking:*

The location and use of medical equipment are tracked in real-time with the help of computer vision AI and IoT sensors [18]. Computer vision can track and locate the movement of assets without the need for manual scanning or physical tags, thereby reducing asset losses and ensuring the instant availability of essential surgical tools [18].

- *Resource Optimization:*

Predictive analytics and automated inventory counts ensure both minimized operational costs and optimized resource use [18].

## IV. SECURITY MECHANISMS, THREATS, AND COUNTERMEASURES.

The security of the Edge-AI/Federated Learning paradigm needs to be addressed on two different threat surfaces: the vulnerable physical edge infrastructure and the collaborative model training process.

### *A. Edge Specific Security Threats.*

The localized, resource-constrained nature of IoMT devices makes them particularly vulnerable to physical and network-level attacks [19].

- *Physical Tampering:*

IoMT devices can be attacked by exploiting vulnerabilities in firmware to install malware, manipulate, or disable sensor functionality [20]. Poor encryption, poor authentication, and the inability to update firmware regularly are the main risk factors [19].

- *Network and Denial-of-Service (DoS) attacks:*

DoS attacks flood devices with requests, thereby affecting operational availability, which is vital in life-support systems [20]. Man-in-the-Middle (MitM) attacks also enable the attacker to intercept, modify, or replay sensitive patient information exchanged between sensors and gateways [20].

### *B. FL-Specific Model Integrity and Model Privacy Attacks.*

Federated Learning also changes the security considerations of raw data to the model updates, or gradients and weights, shared among the clients.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct1178

- *Data and Model Poisoning:*

Poisoning is an attack that is executed by malicious clients who upload distorted data or model updates to pollute the global model [21]. This can occur through:

- *Label Flipping:*

Direct modification of local training data class label [21].

- *Gradient-Based Poisoning*

Poisoning of model updates to optimize the impact of poisoning the learning objective, frequently to add backdoors [21].

- *Model Inversion/Gradient Reconstruction Attacks*

These privacy attacks aim to infer the original sensitive training data, such as patient features, by reverse-engineering shared model parameters or gradients [22]. Recent literature has recorded the efficacy of gradient inversion attacks [22], but a severe trade-off exists: model updates need to be informative (utility) without revealing raw data (privacy).

*C. Privacy Enhancement Techniques (PETs).*

To ensure the security of the Federated Learning training cycle, it is necessary to employ privacy-enhancing methods:

- *Differential Privacy (DP):*

DP provides robust, provable privacy guarantees by adding controlled noise/perturbation to model updates (gradients) before sending them to the central server [23]. By limiting the influence of any one record, DP inhibits the inference of any particular patient information, but this can create a trade-off with model utility and accuracy [16].

- *Homomorphic Encryption (HE):*

HE enables the central server to execute computational tasks, such as the aggregation (summation) of model updates (gradients), on encrypted model updates (ciphertexts) [23]. This ensures that the server does not have access to plaintext gradients, thereby offering a high level of protection against model inversion attacks [23].

- *Blockchain Integration:*

Decentralized Federated Learning systems often utilize blockchain technology to create a verifiable ledger that is tamper-proof, enabling the recording and verification of gradient transactions [1]. The adoption of consensus protocols ensures the aggregation mechanism is protected against Sybil attacks and provides transparency, particularly in cross-cluster (Cross-Silo) collaborations [1].

## V. DIFFICULTIES, OPPOSING OPINIONS, AND GAPS IN RESEARCH.

Although the technology holds potential, several fundamental problems and trade-offs hinder the popularization of Edge-AI and Federated Learning (FL) in the Internet of Medical Things (IoMT).

*A. Resource Constraints and Trade-offs of Efficiency.*

The computational difference between advanced models of Artificial Intelligence (AI), including Deep Neural Networks, and low-power IoMT edge devices is significant [24].

- *Model Compression vs. Accuracy*

Model pruning and quantization methods minimize the memory footprint required to deploy models. However, both have the negative impact of inherently degrading model accuracy, a critical issue in medical diagnostics [24].

- *Energy Efficiency*

It requires further development of cross-layer co-design of custom hardware and algorithms to optimize the energy consumption of battery-constrained IoMT devices, which does not adversely affect model performance [24].

*B. Data Heterogeneity and Communication Cost.*

Non-IID Data: IoMT data are observed across a wide range of devices, patient groups, and geographic areas, resulting in statistically heterogeneous (non-IID) datasets [1]. It has been known that this heterogeneity violates the stability and accuracy of the global FL model [25]. The next generation of aggregation needs to implement equity-sensitive weighting, depending on the quality of data and resource availability, to reduce client drift [25].

- *Communication Overhead:*

The rapid convergence of the model necessitates a high communication frequency, but this can overload the limited IoMT networks [25]. It is suggested that adaptive synchronization strategies can be used to dynamically adjust the frequency and size of model updates depending on network conditions, thereby attempting to achieve an optimal trade-off between the rate of convergence and communication cost [25].

*C. Interpretability and Standardization Gaps.*

The absence of trust in black-box AI models is a key obstacle to clinical acceptance, especially when more complex algorithms, such as pruning, hide the underlying decision-making mechanism [24]. Explainable AI (XAI), based on rule-based systems or Local Interpretable Model-agnostic Explanations (LIME), is necessary to make predictions understandable to physicians and patients, which is required to meet ethical and regulatory audit demands [1].

The lack of standardization of IoMT data formats and FL implementation protocols across device vendors further contributes to the clinical translation gap, which is already low (5⁻) due to the low real-world application rate (5□% in [4]) [14].

## VI. CONCLUSION AND FUTURE DIRECTIONS.

The combination of Edge-AI and Federated Learning provides a robust and necessary framework for secure, efficient, and privacy-compliant healthcare provision in the age of the IoMT. With localization, Edge-AI addresses the key issue of latency that centralized cloud systems face. Through decentralization of training, FL helps reduce the risks of centralized data breaches and enables collaboration across institutions.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct1178

The future research should focus on translating theoretical FL models into practical clinical applications to cover the significant gaps in clinical implementation and standardization.

- *6G Networks*

6G networks will provide the ubiquitous edge services and the massive scale needed by future IoMT systems to support ultra-low latency and high bandwidth needed to connect and integrate DT and large-scale and efficient deployment of FL.

- *Secure and Explainable AI (XAI)*

It is essential to build intrinsically secure and explainable models (e.g. based on rule-based and fuzzy mechanisms) to achieve clinical trust, regulatory accountability, and reliability of life-critical decisions.

## REFERENCES


[1]. V. K. Prasad, P. Bhattacharya, D. Maru, S. Tanwar, A. Verma, A. Singh, A. K. Tiwari, R. Sharma, A. Alkhayyat, F.-E. Turcanu, and M. S. Raboaca, "Federated Learning for the Internet-of-Medical-Things: A Survey," Mathematics, vol. 11, no. 1, p. 151, Dec. 2022.

[2]. U. Islam, M. N. Alatawi, A. Alqazzaz, Sulaiman Alamro, B. Shah, and F. Moreira, "A hybrid fog-edge computing architecture for real-time health monitoring in IoMT systems with optimized latency and threat resilience," Scientific Reports, vol. 15, no. 1, Jul. 2025.

[3]. P. Bhattacharya, A. Mukherjee, B. Bhushan, S. K. Gupta, Thippa Reddy Gadekallu, and Z. Zhu, "A secured remote patient monitoring framework for IoMT ecosystems," Scientific Reports, vol. 15, no. 1, Jul. 2025.

[4]. R. M. Rajab, M. Abuhmida, I. D. Wilson, and R. P. Ward, "A Review of IoMT Security and Privacy Related Frameworks.," in Proceedings of the 23rd European Conference on Cyber Warfare and Security, 2024.

[5]. N. T. Madathil, F. K. Dankar, M. Gergely, Abdelkader Nasreddine Belkacem, and Saed Alrabaee, "Revolutionizing Healthcare Data Analytics with Federated Learning: A Comprehensive Survey of Applications, Systems, and Future Directions," Computational and Structural Biotechnology Journal, vol. 28, pp. 217–238, Jan. 2025.

[6]. W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A Survey on the Edge Computing for the Internet of Things," IEEE Access, vol. 6, pp. 6900–6919, 2018.

[7]. S. Hamdan, M. Ayyash, and S. Almajali, "Edge-Computing Architectures for Internet of Things Applications: A Survey," Sensors, vol. 20, no. 22, p. 6441, Nov. 2020.

[8]. D. C. Klonoff, "Fog Computing and Edge Computing Architectures for Processing Data From Diabetes Devices Connected to the Medical Internet of Things," Journal of Diabetes Science and Technology, vol. 11, no. 4, pp. 647–652, Jul. 2017.

[9]. P. M. Gupta, "Integration Of Edge And Fog Computing In Iot-Based Healthcare Applications - A Review," Journal of Positive School Psychology , pp. 1940–1957, 2022.

[10]. Y.-A. Daraghmi, E. Y. Daraghmi, R. Daraghma, H. Fouchal, and M. Ayaida, "Edge–Fog–Cloud Computing Hierarchy for Improving Performance and Security of NB-IoT-Based Health Monitoring Systems," Sensors, vol. 22, no. 22, p. 8646, Nov. 2022.

[11]. Y. Li and W. Zhang, "Task-Offloading Strategy of Mobile Edge Computing for WBANs," Electronics, vol. 13, no. 8, pp. 1422–1422, Apr. 2024.

[12]. T. Xia, J. Han, A. Ghosh, and C. Mascolo, "Cross-device Federated Learning for Mobile Health Diagnostics: A First Study on COVID-19 Detection," arXiv.org, 2023. [Online]. Available: https://arxiv.org/abs/2303.07067.

[13]. J. Ogier Du Terrail, S.-S. Ayed, E. Cyffers, F. Grimberg, C. He, R. Loeb, P. Mangold, T. Marchand, O. Marfoq, E. Mushtaq, B. Muzellec, C. Philippenko, S. Silva, M. Teleńczuk, S. Albarqouni, S. Avestimehr, A. Bellet, A. Dieuleveut, M. Jaggi, and S. Karimireddy, "FLamby: Datasets and Benchmarks for Cross-Silo Federated Learning in Realistic Healthcare Settings."

[14]. Z. L. Teo, L. Jin, S. Li, D. Miao, X. Zhang, W. Y. Ng, T. F. Tan, D. M. Lee, K. J. Chua, J. Heng, Y. Liu, R. S. M. Goh, and D. S. W. Ting, "Federated machine learning in healthcare: A systematic review on clinical applications and technical architecture," Cell Reports Medicine, vol. 5, no. 2, p. 101419, Feb. 2024.

[15]. S. R. Abbas, Z. 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. 2587–2587, Dec. 2024.

[16]. M. E. Yahiaoui, M. Derdour, R. Abdulghafor, S. Turaev, M. Gasmi, A. Bennour, A. Aborujilah, and M. A. Sarem, "Federated Learning with Privacy Preserving for Multi-Institutional Three-Dimensional Brain Tumor Segmentation," Diagnostics, vol. 14, no. 24, p. 2891, Dec. 2024.

[17]. A. Khan, M. Rizwan, O. Bagdasar, A. Alabdulatif, S. Alamro, and A. Alnajim, "Deep Learning-Driven Anomaly Detection for IoMT-Based Smart Healthcare Systems," Computer Modeling in Engineering & Sciences, vol. 141, no. 3, pp. 2121–2141, 2024.

[18]. V. K. Rathi, N. K. Rajput, S. Mishra, B. A. Grover, P. Tiwari, A. K. Jaiswal, and M. S. Hossain, "An edge AI-enabled IoT healthcare monitoring system for smart cities," Computers & Electrical Engineering, vol. 96, p. 107524, Dec. 2021.

[19]. L. Dzamesi and N. Elsayed, "A Review on the Security Vulnerabilities of the IoMT against Malware Attacks and DDoS," arXiv.org, 2025. [Online]. Available: https://arxiv.org/abs/2501.07703.

[20]. C. M. Mejía-Granda, J. L. Fernández-Alemán, J. M. Carrillo, and J. A. García-Berná, "Security vulnerabilities in healthcare: an analysis of medical devices and software," Medical & Biological Engineering & Computing, vol. 62, no. 1, Oct. 2023.

[21]. J. Wu, J. Jin, and C. Wu, "Challenges and Countermeasures of Federated Learning Data Poisoning Attack Situation Prediction," Mathematics, vol. 12, no. 6, pp. 901–901, Mar. 2024.

[22]. H. S. Sikandar, H. Waheed, S. Tahir, S. U. R. Malik, and W. Rafique, "A Detailed Survey on Federated Learning Attacks and Defenses," Electronics, vol. 12, no. 2, p. 260, Jan. 2023.

[23]. X. Gu, F. Sabrina, Z. Fan, 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, p. 6539, Jan. 2023.

[24]. T. Wang, J. Guo, B. Zhang, G. Yang, and D. Li, "Deploying AI on Edge: Advancement and Challenges in Edge Intelligence," Mathematics, vol. 13, no. 11, pp. 1878–1878, Jun. 2025.

[25]. A. Daulay, K. Ramli, R. Harwahyu, T. Hidayat, and B. Pranggono, "Novel Federated Graph Contrastive Learning for IoMT Security: Protecting Data Poisoning and Inference Attacks," Mathematics, vol. 13, no. 15, p. 2471, Jul. 2025.