# Research on Privacy Preservation and Collaboration of Medical Big Data Based on Federated Learning and Edge Computing

**Jialin Liu**
*Computer Science and Technology College, Zhejiang Normal University, Jinhua, Zhejiang, China*

**Abstract: The multi-source and explosive growth of medical big data presents a core challenge to achieving cross-institutional collaborative modeling while ensuring privacy and security in the context of medical intelligence. Federated Learning (FL) enables collaborative training without sharing raw data, Edge Computing (EC) improves model responsiveness and energy efficiency through near-source computation, and Differential Privacy (DP) provides quantifiable privacy protection for model updates. The integration of FL, EC, and DP offers a new system framework and research direction for the secure collaboration of medical big data. This paper systematically reviews the recent research progress on the integration of FL, EC, and DP in medical scenarios, outlines typical architectures, privacy mechanisms, and optimization strategies, and compares the trade-offs among model performance, privacy assurance, and resource overhead in different schemes. This study proposes a three-dimensional evaluation framework: "Performance-Privacy-Resource," and discusses key issues such as heterogeneous data distribution, end-edge-cloud collaboration, and privacy-performance co-optimization. The research aims to provide a systematic reference and future research directions for privacy preservation and distributed intelligent collaboration in medical big data scenarios.**

**Keywords: Federated Learning; Edge Computing; Medical Big Data; Differential Privacy; Privacy Preservation**

## 1. Introduction

### 1.1 Research Background

In recent years, massive amounts of medical data have been generated from electronic health records (EHRs), medical imaging, genomic sequencing, and wearable devices, leading to high-dimensional, heterogeneous, and high-growth characteristics, reaching a massive scale. While this vast amount of data brings opportunities for precision medicine and smart healthcare services, it also imposes higher demands on data management and privacy protection. The Chinese government has listed healthcare big data as a national strategic resource and explicitly proposed to promote data development and utilization, prioritizing security and adhering to the principle of privacy protection." However, the "data silo" phenomenon is still prevalent in China's medical industry, where data from hospitals, research institutions, and community health centers is fragmented. Moreover, centralized storage and training are associated with a high risk of privacy leakage. In this context, achieving multi-institutional collaborative modeling and knowledge sharing while protecting individual privacy has become a critical issue that medical informatization urgently needs to address.

The emergence of Federated Learning (FL) and Edge Computing (EC) offers a new technical paradigm to address this problem. FL enables collaborative model training through distributed parameter aggregation without sharing raw data. EC provides computing capabilities at the edge, close to the data source, effectively reducing communication latency and bandwidth overhead. When combined with privacy-enhancing mechanisms such as Differential Privacy (DP), it can prevent data inversion and inference attacks while ensuring model utility and balancing performance. Therefore, exploring the integration path of FL, EC, and DP holds significant theoretical and practical importance for realizing privacy preservation and cross-institutional collaboration of medical big data.

### 1.2 Literature Review

1.2.1 Domestic research status

In recent years, domestic scholars have conducted extensive research on combining

 

Federated Learning (FL), Edge Computing (EC), and Differential Privacy (DP) to achieve privacy preservation for medical big data. Research focuses on protocol design, hierarchical architectures, and privacy-enhancing mechanisms. Overall, existing work mainly follows three lines: one focuses on privacy preservation protocols and lightweight implementations in edge environments (FL+EC); another focuses on combining FL and DP to achieve provable privacy guarantees (FL+DP); in addition, research has begun to explore comprehensive frameworks that systematically integrate all three (FL+EC+DP).

Research on FL + EC

In terms of privacy protocol design, some studies have proposed lightweight schemes based on secret sharing and masking to protect gradient information and enhance robustness against device dropout and collusion attacks. For example, Liu Dong et al. proposed a protocol based on shared secrets and weight masking, designed to resist device dropout and collusion attacks in an Edge Computing environment [1]. Similarly, Wang Ruijin et al. proposed the PPFLEC scheme for the Internet of Medical Things (IoMT), which also uses secret sharing technology to protect gradient information and ensures transmission integrity through digital signature algorithms. This scheme effectively improved training efficiency in the smart medical edge environment, with comparative validation showing it was 40% faster than a specific Differential Privacy scheme [2].

Research on FL + DP

In the direction of introducing Differential Privacy into Federated Learning, Wang Shengsheng et al. proposed a privacy-preserving federated learning algorithm for multi-lesion detection in CT medical images. They introduced a Differential Privacy mechanism into the FL framework, specifically for the task of multi-lesion detection in CT medical images, by injecting DP noise into local model parameters and improving the RetinaNet detector structure. This approach achieved an mAP of approximately 75% while protecting the privacy of the original images, effectively balancing privacy protection, communication efficiency, and model performance [3].

Research on the Integration of FL + Edge + DP

Domestic scholars have recently begun exploring comprehensive frameworks that systematically integrate FL, EC, and DP. Zhang Xuejun et al. proposed a Differential Privacy Federated Learning model for RSS fingerprint indoor localization in an edge computing environment. This scheme achieved 84.63% accuracy on the CIFAR-10 dataset and 94.86% on the Mall dataset, reducing computational and communication burdens through a lightweight CNN model and a periodic update strategy. Although primarily applied to RSS fingerprint localization, its approach to edge deployment and privacy enhancement is relevant to medical scenarios (such as ward localization and health monitoring) [4]. Dong Shaohua et al. proposed the ECDPFL framework for Differential Privacy protection in Federated Learning for hierarchical edge computing, which introduces Local Differential Privacy at both the client and edge server levels and optimizes the timing of end-to-edge and edge-to-cloud aggregation. This scheme demonstrated good classification performance and convergence speed on datasets like CIFAR-10 and MNIST (reaching 80.12% on CIFAR-10 and 92.82% on MNIST), highlighting the potential of hierarchical differential privacy strategies in balancing privacy and performance [5]. The research by Liu Jingyuan et al. is more targeted, proposing an incentive mechanism for energy efficiency and privacy preservation in a Mobile Edge Computing (MEC)-assisted medical federated learning system. The scheme reported a clear improvement in accuracy (+2.89%) on a real medical dataset and provided loss convergence curves for qualitative analysis. Regarding privacy, it employed a differential privacy mechanism with a quantifiable privacy budget ε, supporting personalized privacy settings. In terms of resource optimization, it treated Energy Efficiency (EE) as a core optimization objective and managed communication energy consumption through game-theoretic optimization of transmission power. This study demonstrates the practical feasibility of the FL+EC+DP integrated scheme in healthcare systems [6]. Overall, domestic research has proposed various practical solutions at the protocol design, hierarchical aggregation, and system level. Initially focusing on the combination of FL+EC or FL+DP technologies, the research has gradually evolved toward systematic integration of all three. However, challenges remain prevalent, including insufficient empirical validation, incomplete reporting of multi-dimensional quantitative indicators, lack of privacy attack testing, and

 

inadequate quantification of resource efficiency.

1.2.2 International research status

International research on medical big data privacy preservation started earlier and has accumulated rich experience in algorithms, systems, and application validation. The focus of international research includes: edge federated learning frameworks for resource-constrained devices, adaptive mechanisms for differential privacy, and the application of cryptographic methods such as homomorphic encryption or secure multi-party computation in federated scenarios. Overall, international research has followed three main lines: one focusing on federated learning optimization in edge environments (FL+EC); another focusing on combining FL and DP to achieve provable privacy guarantees (FL+DP); and recently, the comprehensive framework systematically integrating all three (FL+EC+DP) has become a research hotspot.

Research on FL + EC

In terms of edge-based federated learning, Aminifar et al. proposed an edge federated learning framework for resource-constrained mobile health systems, considering the computational and bandwidth limitations of IoT devices. They validated it using data from wearable devices for epilepsy monitoring, demonstrating the feasibility of edge collaborative training while preserving privacy. The scheme reduces communication frequency with the cloud through local aggregation at the edge server. However, its privacy protection mainly relies on data localization and lacks quantifiable privacy guarantees [7].

Research on FL + DP

International research has accumulated considerable empirical experience in medical imaging and diagnostic tasks by integrating Differential Privacy with Federated Learning. Shukla et al. reported in Scientific Reports on a Federated Learning + Differential Privacy model for breast cancer diagnosis, using the Wisconsin Breast Cancer Diagnostic dataset and injecting DP noise into the FL framework. At a privacy budget of ε=1.9, the combined FL+DP model achieved an accuracy of 96.1%, nearly comparable to the model without privacy constraints, while effectively resisting inference attacks on patient data. This demonstrated the feasibility of FL+DP in multi-institutional medical collaborative modeling [8]. The framework proposed by AlSalman et al. further combines techniques such as homomorphic encryption to achieve high-accuracy diagnosis in cross-institutional collaboration, significantly improving accuracy and meeting clinical real-time requirements while ensuring privacy [9].

Research on the Integration of FL + Edge + DP

Systematic integration has become a research hotspot internationally. Rauniyar et al., in their review, systematically summarized the latest progress of FL in medical applications, pointing out that FL can achieve high accuracy (e.g., Dice coefficient 0.85+ for cancer diagnosis) and improve generalization through multi-institutional collaboration, while EC reduces latency and improves response time. Regarding privacy preservation, they detailed how DP provides quantifiable privacy protection (ε budget) and combines it with cryptography (secret sharing) to enhance security, resist collusion, and use data localization to avoid sharing raw data. This review provides comprehensive theoretical guidance for the application of the FL+EC+DP integrated technology in the medical field [10].

Overall, international research provides more methodological support for algorithm optimization and system implementation. These studies have been validated on real medical datasets and provided quantifiable performance, privacy, and resource metrics, offering important theoretical and practical foundations for medical big data privacy preservation. However, they still face the challenge of achieving an acceptable compromise between ensuring privacy, controlling resource overhead, and maintaining model performance in heterogeneous medical environments, with no unified solution yet. Integrated schemes also generally lack sufficient empirical testing against privacy attacks [11].

### 1.3 Specific Research Objectives

This paper aims to systematically explore the integrated application of FL, EC, and DP in medical big data privacy preservation. By constructing a "Performance-Privacy-Resource" three-dimensional evaluation framework, we compare and assess the advantages and disadvantages of different technical schemes. We summarize the core challenges of existing research and propose feasible optimization paths for medical scenarios, providing theoretical guidance and practical recommendations for the

 

construction of secure, efficient, and scalable distributed medical intelligence systems [12].

## 2. Research Methodology

This chapter systematically elaborates on the overall design and methodological framework of this research, including the research content, approach, technical route, literature retrieval, and quality control methods. To ensure the scientific rigor, objectivity, and verifiability of the research results, the methodology follows the principles of "Systematicity-Objectivity-Reproducibility," combining systematic review and comparative analysis methods [13].

### 2.1 Research Content

This study employs a Systematic Review method, combined with Inductive Analysis and Comparative Analysis. The specific approach is as follows:

2.1.1 Systematic Literature Retrieval and Screening

Keyword Determination: Core Chinese and English keywords and their synonyms are selected, such as "Federated Learning," "Edge Computing," "Differential Privacy," and "Medical Big Data".

Database Selection: Including CNKI, Wanfang, IEEE Xplore, ScienceDirect, SpringerLink, PubMed, etc.

Retrieval Strategy: Boolean logic is used to combine keywords, limiting the time range (2017-2025),and supplementing relevant literature through "citation tracking".

2.1.2 Technical Path and Scheme Extraction

Core technical elements (FL type, edge deployment method, privacy mechanism, etc.) are extracted from each document to construct a classification system (FL+Edge / FL+DP / FL+Edge+DP), identifying architectural commonalities and differences.

2.1.3 Evaluation Metrics and Comparative Dimensions

Performance Metrics: Model Accuracy, Recall, F1-score, Convergence Epochs.

Privacy Metrics: Differential Privacy budget ε, Noise magnitude δ, Privacy leakage probability, Anti-attack performance.

Resource Metrics: Communication rounds, Computational latency, Energy consumption, Bandwidth utilization.

## 3. Research Results

Based on the systematic retrieval and screening of relevant high-quality papers (2017–2025), this chapter first conducts an overall literature statistics and trend analysis. Then, based on the "Performance-Privacy-Resource" three-dimensional evaluation framework, an in-depth comparative analysis of the three mainstream technology combinations (FL+EC, FL+DP, FL+EC+DP) is performed, and core comprehensive evaluations and findings are extracted.

### 3.1 Literature Statistics

Statistical analysis of the final included papers shows that the integration of all three (FL+EC+DP) accounts for the highest proportion (22.6%), indicating that this direction has become a current research hotspot. Research on FL+DP (15.1%) and FL+EC (11.3%) also accounts for a considerable proportion, with the remainder being extended combinations including blockchain, homomorphic encryption, and other technologies.

Regarding the completeness of data reporting, the analysis found that:

A majority of the papers (66.0%) reported parseable performance metrics (e.g., accuracy, mAP);

Over half of the papers (52.8%) provided privacy parameters (e.g., Differential Privacy budget ε);

A smaller portion of papers (28.3%) reported resource metrics such as latency, communication overhead, or energy consumption;

Only a limited number of papers (15.1%) simultaneously provided complete quantitative data for all three categories: performance, privacy, and resources.

### 3.2 Comparative Analysis Based on the Three-Dimensional Framework

3.2.1 FL + EC analysis

The core of this type of scheme is to empower Federated Learning with Edge Computing to achieve near-data processing.

Performance Dimension:

The advantage is that Edge Computing can significantly reduce communication latency and improve system response speed, performing well in real-time medical applications (such as remote monitoring). The disadvantage is that the computational limitations of edge devices restrict model complexity, and the problem of data heterogeneity (Non-IID) is prominent, often

 

leading to slower model convergence or accuracy fluctuations. However, most papers do not quantitatively report the convergence speed.

Privacy Dimension

The advantage is that "data non-expatriation" provides basic privacy protection, reducing the risk of centralized data leakage. The disadvantage is the lack of quantifiable privacy assurance; model gradients still face leakage risks during transmission, and most schemes have not been validated to resist advanced inference attacks.

Resource Dimension

The advantage is that by finely tuning the privacy budget ε, most schemes can maintain high model accuracy (e.g., >96%) even after introducing noise. The disadvantage is that Differential Privacy inevitably leads to a loss of utility, and model accuracy and convergence can significantly decrease, especially when the ε value is set too small or the data dimension is high.

3.2.2 FL + DP analysis

The core of this type of scheme is to provide provable privacy assurance for Federated Learning through Differential Privacy.

Performance Dimensions

The advantage is that by finely tuning the privacy budget ε, most schemes can maintain high model accuracy (e.g., >96%) even after introducing noise. The disadvantage is that Differential Privacy inevitably leads to a loss of utility, and model accuracy and convergence can significantly decrease, especially when the ε value is set too small or the data dimension is high.

Privacy Dimension

The advantage is that it provides quantifiable and provable privacy protection (ε-DP), which can effectively resist attacks such as membership inference and gradient leakage, making it one of the current gold standards for privacy preservation. The disadvantage is that pure DP cannot defend against collusion attacks, and most studies lack empirical testing in actual attack scenarios.

Resource Dimensions

The advantage is that the computational overhead of the Differential Privacy mechanism itself is relatively small, making it easy to deploy on resource-constrained devices. The disadvantage is that the addition of noise may slow down model convergence, indirectly increasing the total communication rounds and resource consumption.

3.2.3 FL+EC+DP scheme analysis

This type of scheme is a system-level integration of the former two, aiming to coordinate their respective advantages to achieve global optimization of privacy, performance, and resources.

Performance Dimensions

The advantage is that Edge Computing ensures response speed, and hierarchical/adaptive DP techniques reduce the impact of noise on overall model performance, showing performance levels close to non-privacy-preserving schemes in many studies (e.g., >92% on CIFAR-10). The disadvantage is the high system complexity, requiring fine-grained coordination and optimization across multiple layers.

Privacy Dimension

The advantage is that it builds a defense-in-depth system, possessing both the quantifiable guarantee of DP and the ability to deploy hybrid mechanisms (e.g., DP + Secret Sharing) by leveraging the distributed nature of the edge, resulting in the highest level of security. The disadvantage is the high implementation complexity and the continued lack of sufficient empirical attack testing.

Resource Dimensions

The advantage is that Edge Computing effectively reduces the communication overhead of the core network, and the computational lightness of DP makes it easy to integrate into end devices. The disadvantage is that complex privacy mechanisms (such as those combined with cryptographic methods) may introduce additional computational and communication burdens at the edge layer, requiring delicate design for balance.

### 3.3 Comprehensive Comparison under the Three-Dimensional Framework

Based on the above analysis, this study qualitatively assesses the comprehensive performance of the three technical schemes—FL+EC, FL+DP, and FL+EC+DP—across the three dimensions of performance, privacy, and resources. The results are summarized in Table 1. This table clearly shows the comprehensive evaluation and core trade-offs of different schemes.

### 3.4 Core Research Findings are as follows

Significant Performance-Privacy Trade-off Exists: As shown in Table 1, the FL+DP scheme

sacrifices some performance for a high level of privacy protection. The Differential Privacy budget ε is a key regulatory metric and needs to be dynamically adjusted based on the sensitivity of the clinical scenario.

Complex Privacy-Resource Trade-off: Strong privacy mechanisms alone (such as homomorphic encryption) can provide a high level of security but come with huge computational and communication overheads. Therefore, hybrid privacy mechanisms, as represented by the FL+EC+DP scheme, become the preferred future direction.

Performance-Resource Trade-off can be mitigated by architectural optimization: As shown in Table 1, the FL+EC scheme effectively supports medium-level performance requirements with its "High" resource efficiency. Further combination with strategies such as model compression and selective parameter updates can further alleviate the performance bottleneck caused by resource constraints on edge devices.

Assessment Blind Spot: However, most current literature suffers from insufficient quantification of the resource dimension and lacks empirical testing against privacy attacks. This leads to uncertainty regarding the actual protection capabilities and true resource consumption of many schemes, posing challenges for scheme selection and final deployment, as illustrated in Table 1.

**Table 1. Comprehensive Comparison of Different Technical Schemes under the Three-Dimensional Evaluation Framework**

| Technical Scheme | Performance | Privacy | Resource | Applicable Scenario |
|---|---|---|---|---|
| FL+EC | Medium | Low | High | Medium applications with low privacy requirements and focus on real-time response (e.g., remote monitoring) |
| FL+DP | Medium | High | Medium | Medical applications with high privacy requirements and acceptable performance loss (e.g., multi-institutional collaborative diagnosis) |
| FL+EC+DP | High | High | Medium | Medical applications with high requirements for privacy, performance, and resources (e.g., smart hospitals, cross-institutional collaboration) |

## 4. Discussion

Based on the systematic review of 53 related papers and the comparative analysis under the "Performance-Privacy-Resource"
three-dimensional framework, this section further discusses the key challenges, technical bottlenecks, and future research directions for the integrated FL, Edge, and DP schemes in the medical big data scenario.

### 4.1 Key Challenges and Future Countermeasures

4.1.1 Heterogeneous data distribution and model convergence

Medical data exhibits significant heterogeneity; data distribution, quality, and volume may vary greatly among different medical institutions. This heterogeneity can lead to decreased model convergence speed, reduced accuracy, and even model divergence in Federated Learning. Although existing research has proposed some countermeasures (such as improved algorithms like FedProx and FedMA), their effectiveness in real medical scenarios requires further validation.

Future Directions:

Develop more robust aggregation algorithms that can adaptively adjust the weights of different participants to mitigate the negative impact of heterogeneous data on model convergence.

Introduce Personalized Federated Learning (PFL) schemes, allowing different medical institutions to fine-tune more suitable local models based on their own data characteristics, while sharing global knowledge.

Explore the combination of Meta-Learning and Federated Learning to rapidly adapt to new medical tasks with different data distributions using cross-domain knowledge.

4.1.2 End-Edge-Cloud collaboration and resource optimization in the FL+Edge+DP

In the FL+Edge+DP scheme, how to reasonably allocate computing tasks, optimize communication overhead, and manage energy consumption across the end-edge-cloud three-tier architecture is a complex systems engineering problem. Existing research often focuses on optimization at a single layer, lacking a global perspective and dynamic scheduling for the entire system.

Future Directions:

 

Develop a co-optimization framework for end-edge-cloud that comprehensively considers the allocation of computation, communication, and storage resources, using methods like reinforcement learning or game theory to achieve dynamic optimization of task assignment.

Explore the differentiated division of labor between edge intelligence and cloud intelligence, with the edge layer performing lightweight inference, data preprocessing, and preliminary aggregation, and the cloud layer being responsible for complex model training, global optimization, and long-term knowledge storage.

Deeply research the application of techniques such as model compression and knowledge distillation in edge federated learning to adapt to resource-constrained devices.

4.1.3 Privacy-performance co-optimization

The core challenge faced by the FL+Edge+DP scheme is how to minimize the impact on model performance while ensuring the strength of privacy protection. A fixed privacy budget ε is difficult to adapt to dynamic training processes and changing medical scenarios.:

Develop adaptive Differential Privacy mechanisms that dynamically adjust the noise level based on data sensitivity, model training stage (e.g., initial versus convergence), and real-time privacy requirements.

Explore hybrid privacy mechanisms, employing different strengths of privacy protection at different layers (end devices using LDP, edge using secure aggregation) to achieve a fine-grained balance between privacy and efficiency.

Design adaptive privacy budget allocation strategies that dynamically allocate the privacy budget based on the contribution of each training round to model convergence, avoiding waste or premature exhaustion of the privacy budget.

4.1.4 Privacy attacks and defense

Although existing mechanisms provide strong theoretical privacy guarantees, they may still face various privacy attacks in practical applications. As discussed in Section 3.3, current research generally lacks empirical testing against privacy attacks, resulting in an assessment blind spot regarding the actual protection capabilities of the schemes.

Future Directions:

Strengthen empirical research on privacy attacks, systematically testing the success rate of attacks such as membership inference and gradient leakage on real or simulated medical datasets, and establishing standardized benchmark testing environments.

Develop more robust hybrid defense mechanisms, for example, combining Differential Privacy (to provide provable protection) and Secure Multi-Party Computation (to resist collusion attacks), or introducing Trusted Execution Environments (TEE) to protect critical computation processes.

Explore active detection and response mechanisms for privacy attacks, using anomaly behavior analysis to detect potential attacks in real-time and take mitigation measures.

## 5. Conclusion and Outlook

This paper systematically reviews the integrated application of Federated Learning (FL), Edge Computing (EC), and Differential Privacy (DP) in medical big data privacy preservation and collaboration. By constructing the "Performance-Privacy-Resource" three-dimensional evaluation framework and reviewing and comparing 53 core papers, this study clarifies the characteristics, advantages, and limitations of the three technical schemes: FL+EC, FL+DP, and FL+EC+DP. The main conclusions are as follows.

Technological Integration is an Inevitable Trend: Standalone FL technology struggles to meet the complex demands for privacy, efficiency, and performance in medical scenarios. Deep integration with EC and DP has become the critical technical path for building the next generation of medical collaborative intelligence systems.

Trade-off is the Core Issue: As revealed in Chapter 3, a profound trade-off exists among performance, privacy, and resources. Future technical optimization requires a focus on the synergy and compromise among these three, rather than isolated breakthroughs.

Evaluation System Needs Improvement: Current research suffers from notable deficiencies in the quantitative evaluation of resource overhead and empirical testing of privacy defense. Establishing a more comprehensive and standardized evaluation system is a prerequisite for the technology's practical implementation.

This research suggests that the field will continue to deepen in the following directions: on the theoretical level, adaptive and personalized algorithms will become research hotspots; on the engineering level, automated

 

management and scheduling for end-edge-cloud collaboration are key; on the practical level, large-scale deployment and compliance validation in real medical workflows will be the ultimate test of value. We hope that the three-dimensional framework and systematic analysis proposed in this paper can provide a clear roadmap for subsequent researchers and practitioners, jointly advancing medical intelligence under privacy protection towards maturity.

**References**

[1] LIU Dong, PEI Xikai, LAI Jinshan, WANG Ruijin, ZHANG Fengli. Privacy Protection Scheme Combining Edge Intelligent Computing and Federated Learning[J]. Journal of University of Electronic Science and Technology of China, 2023, 52(1): 95-101.

[2] R. Wang, J. Lai, Z. Zhang, X. Li, P. Vijayakumar and M. Karuppiah, "Privacy-Preserving Federated Learning for Internet of Medical Things Under Edge Computing," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 854-865, Feb. 2023.

[3] Wang Shengsheng, Lu Shuzhen, Cao Bin. Medical Image Object Detection Algorithm for Privacy-Preserving Federated Learning[J]. Journal of Computer-Aided Design & Computer Graphics, 2021, 33(10): 1553-1562.

[4] Zhang Xuejun, He Fucun, Gai Jiyang, et al. A Differentially Private Federated Learning Model for Indoor Fingerprint Localization in Edge Computing [J]. Computer Research and Development, 2022,59(12):2667-2688.

[5] DONG Shao-hua,MA Xin-chun,FAN Xiao-chao.Differential Privacy Protection Using Federated Learning in Layered Edge Computing[J].Computer Science and Development,2025,35(04):53-58.

[6] J. Liu, Z. Chang, K. Wang, Z. Zhao and T. Hämäläinen, "Energy-Efficient and Privacy-Preserved Incentive Mechanism for Mobile Edge Computing-Assisted Federated Learning in Healthcare System," in IEEE Transactions on Network and Service Management, vol. 21, no. 4, pp. 4801-4815, Aug. 2024.

[7] Aminifar, Amin, Matin Shokri, and Amir Aminifar. “Privacy-Preserving Edge Federated Learning for Intelligent Mobile-Health Systems.” Future Generation Computer Systems 161 (December 1, 2024): 625–37.

[8] Shukla, S., Rajkumar, S., Sinha, A. Shukla, S., Rajkumar, S., Sinha, A. et al. Federated learning with differential privacy for breast cancer diagnosis enabling secure data sharing and model integrity. Sci Rep 15, 13061 (2025).

[9] H. AlSalman, M. S. Al-Rakhami, T. Alfakih and M. M. Hassan, "Federated Learning Approach for Breast Cancer Detection Based on DCNN," in IEEE Access, vol. 12, pp. 40114-40138, 2024.

[10] A. Rauniyar et al., "Federated Learning for Medical Applications: A Taxonomy, Current Trends, Challenges, and Future Research Directions," in IEEE Internet of Things Journal, vol. 11, no. 5, pp. 7374-7398, 1 March1, 2024.

[11] A. Maurya et al., "Federated Learning for Privacy-Preserving Severity Classification in Healthcare: A Secure Edge-Aggregated Approach," in IEEE Access, vol. 13, pp. 102339-102358, 2025.

[12] K. Thumula, H. Holla, C. Gutti, A. A. Sasikumar and H. Gogineni, "PrivFED: Protecting User Privacy in Federated Learning Systems Through Differential Privacy," 2025 8th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech), Kolkata, India, 2025, pp. 1-6.

[13] B. Wang, Y. Chen, H. Jiang and Z. Zhao, "PPeFL: Privacy-Preserving Edge Federated Learning With Local Differential Privacy," in IEEE Internet of Things Journal, vol. 10, no. 17, pp. 15488-15500, 1 Sept.1, 2023.

 