REVIEW ARTICLE

A Comprehensive Review of Differential Privacy with Federated Meta-Learning for Privacy-Preserving Medical IoT

Subha Sri Telkar[1] **and Manas Kumar Yogi**[2,*]

[1] Department of Electronics and Communication Engineering, Pragati Engineering College, Surampalem 533437, India
[2] Department of Computer Science and Engineering, Pragati Engineering College, Surampalem 533437, India

Abstract

The widespread uptake of the Internet of Medical Things (IoMT) has transformed healthcare by facilitating real-time monitoring and data-driven decision-making, but maintaining data privacy and security is a vital challenge because data breaches and unauthorized access are on the rise. Differential Privacy (DP) and Federated Meta-Learning (FML) are being seen as promising candidates to tackle these issues with the model performance maintained, wherein DP adds noise to sensitive data in a controlled manner for rigorous privacy assurance, and FML allows for personalized learning across distributed IoMT devices without the need for patient data centralization. This survey delves into the combination of DP and FML for preserving privacy in medical IoT use cases by presenting noteworthy methodologies like noise mechanisms, adaptive privacy budgets, and meta-learning strategies designed for diverse healthcare data. We also review state-of-the-art techniques, assessing their performance in maintaining privacy, avoiding adversarial threats, and maximizing model utility while presenting challenges like computational overhead, communication efficiency, and the privacy-accuracy trade-offs.

Keywords: differential privacy, federated, meta-learning, internet of medical things (IoMT), privacy-preserving machine learning.

1 Introduction

1.1 Emergence of Medical IoT and Privacy Issues

The Internet of Medical Things (IoMT) has grown at a fast pace, fueled by innovation in wearable health devices, remote monitoring systems, and intelligent medical sensors. Smartwatches, continuous glucose monitors, ECG patches, and home health monitoring systems are now capable of tracking patients' health parameters in real-time [1]. These technologies are revolutionizing healthcare by providing continuous, non-invasive monitoring, early disease detection, and personalized medical interventions. With growing adoption of telemedicine and remote patient monitoring, IoMT will soon be the cornerstone of

Submitted: 18 April 2025
Accepted: 26 May 2025
Published: 25 June 2025

Vol. 1, **No.** 1, 2025.
10.62762/TWN.2025.327420

***Corresponding author:**
✉ Manas Kumar Yogi
manas.yogi@gmail.com

Citation
Telkar, S. S., & Yogi, M. K. (2025). A Comprehensive Review of Differential Privacy with Federated Meta-Learning for Privacy-Preserving Medical IoT. *ICCK Transactions on Wireless Networks*, 1(1), 16–31.

© 2025 by the Authors. Published by Institute of Central Computation and Knowledge. This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/).

healthcare.

The information from IoMT devices is extremely sensitive, including vital signs (such as heart rate, blood pressure, oxygen saturation), location data, activity, and even behavior. All of this, if analyzed well, can offer insights into disease management, predictive diagnostics, and precision medicine. But its sensitivity also makes it a target for cyber-attacks, data breaches, and unauthorized access. In contrast to conventional health records in secured hospital databases, IoMT devices function in decentralized, resource-limited environments, and hence are more vulnerable to security threats.

One of the principal concerns is the centralized storage of healthcare information, which leaves patient data open to threats including data breaches, insider attacks, and single points of failure. Classical privacy-guaranteeing measures like anonymization and encryption fall short because attackers can conduct re-identification attacks or infer sensitive information from encrypted data. Furthermore, high-frequency data transfers between IoMT devices and central servers expose them to interception attacks.

Dealing with these privacy issues necessitates sophisticated privacy-protecting methods that extend beyond traditional techniques. Federated learning (FL) and differential privacy (DP) have arisen as viable options, facilitated collaborative learning while keeping raw patient data within local devices. They reduce the level of privacy risk without preventing medical AI models from realizing the immense potential of IoMT-generated healthcare data.

1.2 Current Privacy Methods and their drawbacks

Privacy in medical IoT systems is paramount, considering the confidentiality of patient information. Some privacy-preserving methods, such as Differential Privacy (DP) and Federated Learning (FL), have been investigated to counter security threats [3]. Each method, however, has trade-offs, making a hybrid solution that best balances privacy, accuracy, and resource utilization a necessity.

1.2.1 Conventional differential privacy (DP) and its accuracy trade-offs

Differential Privacy (DP) is a mathematical framework which safeguards individual information by adding noise to query output or model parameters. This defends against attackers determining certain information on any individual within a dataset even with auxiliary knowledge. DP affords strong theory-backed privacy protections, and that is why it is a favorite for regulatory usage (e.g., GDPR, HIPAA).

Nonetheless, conventional DP methods are plagued by privacy-accuracy trade-offs. The level of noise that must be added to guarantee strong privacy tends to compromise model utility, resulting in lower accuracy and poor generalization in healthcare AI applications. Additionally, DP is generally applied in centralized environments, which makes it less appropriate for decentralized IoMT environments.

1.2.2 Federated Learning (FL) and its privacy limitations

Federated Learning (FL) improves privacy by supporting decentralized model training, such that patient data is held locally. Rather than sending raw data, only model updates (gradients or weights) are shared with a central aggregator. It minimizes data exposure risks and improves security compared to centralized machine learning [2].

However, owing to these benefits, FL continues to exhibit inherent privacy weaknesses. Gradient leakage attacks have the ability to enable attackers to recover raw training data from model updates shared between peers. FL further lacks strong privacy assurances, and rogue participants have the ability to manipulate updates for inferring confidential information or mounting adversarial attacks.

1.2.3 The need for a hybrid privacy-preserving approach

To address these challenges, a hybrid solution combining Differential Privacy (DP) and Federated Meta-Learning (FML) is required. DP can be used locally to perturb model updates, while FML provides rapid adaptation across heterogeneous medical IoT devices. This hybrid approach improves privacy, model accuracy, and computational efficiency, making it a promising solution for scalable, secure, and personalized healthcare AI.

1.3 Contribution and Paper Structure

As Internet of Medical Things (IoMT) devices become more widespread, maintaining data privacy and security is an ever-growing challenge. Existing privacy-preserving methods like Differential Privacy (DP) and Federated Learning (FL) both have their shortcomings, and a more powerful, adaptive, and scalable solution is needed. To solve these issues, we introduce Differential Privacy with Federated Meta-Learning (DP-FedMeta)—a new paradigm that unifies the privacy benefits of DP with the adaptability

and personalization of Federated Meta-Learning (FML).

DP-FedMeta presents a privacy-conscious federated meta-learning framework in which model updates are locally trained on IoMT devices, differentially private using privacy mechanisms, and aggregated at a central server. Unlike conventional FL that does not provide strong privacy guarantees, DP-FedMeta guarantees local differential privacy (LDP) by adding controlled noise to model updates before sharing. Additionally, FML methods like Model-Agnostic Meta-Learning (MAML) enable the system to learn a prior model that is optimal and hence enables rapid adaptation to unique patient data without compromising privacy. The proposed framework balances accuracy, privacy, and computation and thus suits real-world IoT applications in the medical domain.

This paper follows the following structure:

- Section 2: We introduce the Federated Learning Framework, describing how FL is utilized in medical IoT and how updates of the local model are combined. We then introduce Local Differential Privacy mechanisms including Gaussian noise and randomized response, and treat the dynamic privacy budget adjustment.
- Section 3: We discuss Federated Meta-Learning and how meta-learning improves model generalization over heterogeneous IoMT devices. We give special mention to MAML and other meta-learning techniques that enhance personalization while ensuring privacy.
- Section 4: We introduce the proposed DP-FedMeta framework, its main components, implementation details, and privacy guarantees.
- Section 5: We compare different privacy-preserving methods in terms of privacy, accuracy, and efficiency and analyze DP-FedMeta's benefits.
- Section 6: We present important challenges and future research directions that include optimizing privacy-utility trade-offs, decreasing computational overhead, and achieving regulatory compliance in healthcare AI systems.

Through combining DP and FML, DP-Fed Meta brings forth a scalable, secure, and individualized learning solution, opening the door to next-generation AI-based healthcare solutions.

2 Related Work

2.1 Federated Learning Framework in Medical IoT

Federated Learning (FL) is a distributed machine learning paradigm. It enables model training across multiple devices or edge nodes while preserving data confidentiality. For medical IoT (Internet of Things), FL is useful as it supports healthcare organizations, wearable technology, and medical sensors to train models cooperatively without exchanging patient information directly.

2.1.1 *General Architecture of Federated Learning in Medical IoT*

A federated learning platform in medical IoT comprises the following most important components [3]:

- Edge Devices: These encompass wearable health monitors, hospital IoT devices, and mobile health apps that capture patient data like heart rate, blood pressure, ECG signals, and other physiological parameters.
- Local Model Training: A local model is trained by each IoT device or healthcare facility from its own data. Rather than sending raw patient data to a central server, model updates (e.g., gradients or weights) are sent.
- Central Aggregator (FL Server): A global coordinator (usually a cloud server or edge computing node) gathers local model updates and aggregates them to update a global model.

2.1.2 *Process of Local Model Training and Model Update Aggregation*

- Initialization: The global server initializes a global model and sends it to participating medical IoT devices.
- Local Training: The local devices train the model on their private medical dataset with local computing resources.
- Model Update Transmission: Once local training is completed, model weight updates (not raw data) are transmitted back to the global aggregator.
- Federated Averaging (FedAvg): The server sums up these updates with methods such as FedAvg, calculating the weighted average of model parameters from all nodes involved.
- Model Synchronization: The updated global model is then propagated back to the devices,

enabling continuous learning over decentralized medical IoT networks.

This framework improves data privacy, scalability, and efficiency, making it suitable for sensitive healthcare applications where confidentiality of patient data is of utmost importance.

2.2 Local Differential Privacy (LDP) Implementation

2.2.1 Device-Level Application of LDP

Local Differential Privacy (LDP) is a privacy-preserving method that keeps sensitive information secure before it exits the device. In a medical IoT federated learning (FL) system, LDP is applied at the device level to avoid unauthorized access to patient information while enabling meaningful model training. Every IoT device—like wearable health monitors or hospital sensors—uses random noise perturbation on its model updates prior to sending them to the central aggregator. This guarantees that even if an attacker intercepts the data being sent, it is still privacy-protected [4].

In the healthcare IoT environment, LDP is used to model gradients, feature values, or labels prior to aggregation. This ensures that the central server cannot reconstruct sensitive patient information while still providing useful insights to the federated model.

2.2.2 Various LDP Mechanisms

1. Gaussian Noise Mechanism: Applies Gaussian-distributed noise to numerical values (e.g., model gradients, patient vitals) prior to transmission. This is efficient when handling continuous values but needs thoughtful variance tuning to achieve privacy versus accuracy balance.
2. Randomized Response: A mechanism introduced for sensitive surveys, it randomly flips categorical or binary responses (e.g., disease status: yes/no) with a specified probability, protecting privacy while maintaining statistical accuracy.
3. Laplace Mechanism: Adds Laplace-distributed noise to impose differential privacy by rendering individual data points indistinguishable in a dataset. It works well for small-scale numerical updates.

2.2.3 Dynamic Adjustment of Noise Levels

In order to maximize privacy and model utility, levels of noise should be dynamically scaled according to [5–7]:

- Data Sensitivity: Extremely sensitive patient data (e.g., genomic data) needs more robust noise protection, while less sensitive data (e.g., steps) can cope with lower noise levels.
- Device Resources: Low-processing power and battery-limited IoT devices can use less noise to lower computational overhead, while powerful hospital servers can sustain higher noise.
- Adaptive Privacy Budgeting: Temporal privacy budget allocation keeps data utility high while maintaining long-term privacy.

By incorporating LDP into federated learning, medical IoT systems can balance data privacy, efficiency in computation, and model accuracy.

2.3 Federated Meta-Learning for Model Generalization

2.3.1 Introduction to Meta-Learning in Federated Settings

Meta-learning, or "learning to learn," is a next-generation machine learning paradigm under which models develop the capability to learn new tasks rapidly with limited training data. Under a federated learning (FL) environment, with medical IoT devices and hospitals working with heterogeneous patient datasets, typical FL models usually face data heterogeneity—variations in medical conditions, patient populations, and sensor types.

Federated Meta-Learning (FedMeta) resolves this challenge by training models to generalize more across decentralized datasets. Rather than optimizing one model for every client, FedMeta learns a flexible global model that can fine-tune easily to new data on each device, enhancing personalization and generalization.

2.3.2 Learning a Global "Prior" Model

Meta-learning facilitates the establishment of a global "prior" model—a partially trained model but useful initialization. The new medical IoT device needs just a few local updates once it is provided with the global model and achieves high accuracy on its own dataset. This is especially useful in medical applications, where patient data distributions are very different (e.g., various heart rate patterns among different age groups).

The fundamental concept is to train the model on various learning tasks (e.g., various hospital datasets) such that it learns an initialization that can generalize rapidly to novel data.

2.3.3 *Meta-Learning Algorithms for Medical IoT*

1. Model-Agnostic Meta-Learning (MAML): Among the most popular meta-learning algorithms, MAML tunes the model to be effective after a couple of gradient steps. In federated medical IoT, MAML enables IoT devices to adapt the global model to their respective patients quickly with minimal training.
2. Reptile: A more efficient variant of MAML that learns a good initialization by averaging model updates across multiple devices. It is computationally light, which makes it applicable to resource-limited IoT devices.
3. Meta-SGD: Builds upon MAML by learning adaptive learning rates, which optimizes training on heterogeneous medical datasets.

By incorporating meta-learning into federated learning, medical IoT systems can attain better model generalization, quicker adaptation, and enhanced personalization, ultimately leading to better patient-specific healthcare outcomes.

2.4 Personalized Model Adaptation

2.4.1 *Adapting Global Meta-Model to Patient-Specific Device Data*

While a global meta-model is trained on multiple decentralized medical IoT devices in Federated Meta-Learning (FedMeta), for efficient deployment, it has to be personalized according to each device's individual patient data. The process of adaptation includes [7]:

1. Receiving the Global Meta-Model: The medical IoT device (e.g., wearable ECG monitor or hospital sensor) receives the global meta-model from the central server.
2. Local Fine-Tuning: The device fine-tunes the meta-model on its local dataset with a few gradient steps. In contrast to traditional FL, which involves heavy local training, meta-learning allows for fast adaptation with little data and computation.
3. Optimized Predictions: After fine-tuning, the customized model is more precise for the particular patient or healthcare environment, enhancing real-time diagnostics and monitoring.

This method is especially beneficial for heterogeneous medical IoT settings, where various patients, devices, and institutions produce highly varied data distributions.

2.4.2 *Less Data and Training Requirements Because of Meta-Learning*

Meta-learning greatly minimizes the requirement for large local training since the meta-model already has a strong prior knowledge from past training on varied datasets. This leads to [8]:

- Fewer Iterations of Training: Because the model begins in a well-initialized position, local adaptation needs only a few gradient steps rather than retraining on the entire scale.
- Reduced Computational Burden: Resource-constrained IoT devices (battery-powered wearables, far-end sensors) appreciate lower energy usage and quicker processing.
- Minimal Data Requirement: With limited patient datasets, the meta-model is able to generalize rapidly, and it is ideal for privacy-critical medical applications.

2.4.3 *Applying Local Differential Privacy (LDP) During Adaptation*

Even in local fine-tuning, LDP techniques are implemented to secure sensitive medical information:

- Noise Injection (Gaussian/Laplace): The device distorts gradients or model parameters before conveying any model updates (if at all) to avoid data leakage.
- Differentially Private SGD (DP-SGD): Prevents domination of any one patient's information on model updates by clipping gradients and injecting noise, making it compliant with privacy laws such as HIPAA and GDPR.
- Privacy Budget Allocation: Because fine-tuning does not involve significant updates, a smaller privacy budget is employed, striking a privacy-model utility balance.

Through the use of personalized adaptation, meta-learning, and LDP, federated medical IoT systems obtain highly accurate, private, and efficient models, enhancing personalized healthcare performance while protecting patient data.

2.5 Secure Aggregation of Model Updates

2.5.1 Need for Secure Aggregation in Federated Learning

In Medical IoT Federated Learning, models are locally trained on devices and their updates (e.g., gradient differences or model weights) are communicated to a central aggregator. Still, these updates have the potential to reveal sensitive patient information if they are intercepted or examined. Secure aggregation provides assurance that private individual model updates are preserved, even from the central server, but with accurate computation of the global model.

Major advantages of secure aggregation are [9]:

- Maintaining Patient Privacy: Regardless of a hacker gaining access to the server, they are not able to derive private medical information from single model updates.
- Compliance with Laws: Satisfies rigorous privacy regulations such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR by making patient information never available.
- Securing Model Inversion Attacks: Does not allow attackers to restore original patient data from communicated model gradients.

2.5.2 Secure Aggregation Techniques

1. Homomorphic Encryption (HE)
   - A cryptographic method through which mathematical calculations (addition, multiplication) are performed on encrypted data without decryption.
   - In FL, every device encrypts its model updates before sending those to the server. The server aggregates the encrypted updates and only decrypts the final aggregated model.
   - Example: Paillier Encryption facilitates secure summation of encrypted values, hence appropriate for FL aggregation.
2. Secure Multi-Party Computation (SMPC)
   - A decentralized paradigm in which many parties jointly calculate a function without disclosing their local inputs.
   - Each medical IoT device divides its model updates into random shares and distributes them to a number of non-colluding servers. An individual model update can be retrieved only when the shares are collated.
   - Illustration: Shamir's Secret Sharing scheme protects against an individual entity getting a single model update.

Through the application of homomorphic encryption and SMPC, federated learning of medical IoT provides privacy-preserving model updates without compromising the security or the performance of the global model.

3 SYSTEM ARCHITECTURE

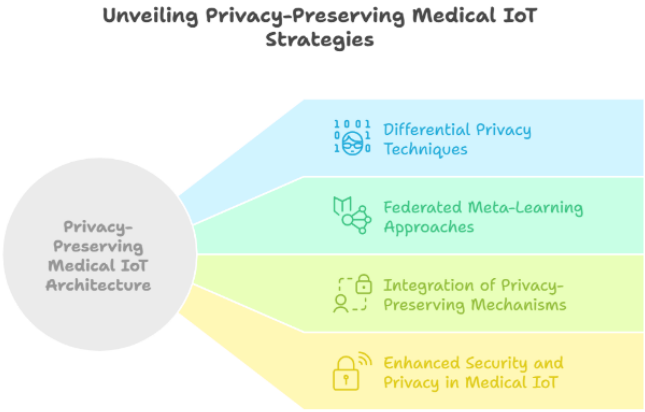

Figure 1. Architecture of DP-FedMeta.

The architecture of a privacy-preserving Medical IoT system using Differential Privacy (DP) with Federated Meta-Learning (FML) integrates secure data processing, decentralized learning, and robust privacy mechanisms, as shown in Figure 1. Edge devices, such as wearable sensors and medical monitors, collect patient data locally. Federated Learning (FL) enables model training across multiple devices without sharing raw data, while meta-learning enhances adaptability to diverse medical conditions. DP ensures privacy by adding noise to gradients before aggregation, preventing data leakage. A central server coordinates model updates securely. This architecture balances efficiency, privacy, and personalization, making it ideal for sensitive healthcare applications, as depicted in Figure 1.

3.1 Advantages of DP-FedMeta

3.1.1 Enhanced Privacy Protection in DP-FedMeta

DP-FedMeta leverages Local Differential Privacy (LDP) and secure aggregation to provide robust privacy guarantees. This ensures that sensitive user data remains protected even in adversarial settings.

Local Differential Privacy (LDP) LDP ensures that individual client updates are randomized before they

are shared with the central server, preventing direct exposure of raw data. Unlike traditional Differential Privacy (DP), which applies noise at the server level, LDP adds noise at the client side, ensuring privacy even if the server is compromised. This means that each client's update is indistinguishable from others within a certain statistical range, preventing adversaries from inferring sensitive information about any single participant [10].

Through LDP, DP-FedMeta prevents membership inference attacks, in which a malicious user tries to decide whether any target user was used during the training procedure. Although an attacker can access model updates shared between parties, the added noise significantly obscures meaningful individual contributions.

Secure Aggregation Secure aggregation is another significant part of the privacy-preserving framework of DP-FedMeta. It offers encryption for an aggregate of model updates by the individual participants or aggregation such that the central server cannot access individual contributions but instead receives an aggregated result.

This approach protects against gradient inversion attacks, where an adversary attempts to reconstruct private training data from model updates. Since the server never has access to individual updates in plaintext, such attacks become infeasible.

Resilience to Privacy Attacks By combining LDP and secure aggregation, DP-FedMeta is highly resilient to a wide range of privacy threats, including:

- Eavesdropping attacks, where attackers intercept communication between clients and servers.
- Model inversion attacks, where adversaries attempt to reverse-engineer training data from model parameters.
- Collusion attacks, where multiple malicious participants attempt to extract sensitive information from aggregated updates.

This strong privacy foundation makes DP-FedMeta a reliable and secure approach for federated meta-learning, balancing privacy with effective model training.

3.1.2 Improved Model Accuracy

One of the primary flaws of federated learning with DP is accuracy degradation due to added noise for privacy. The proposed DP-FedMeta mitigates the detrimental impacts of this added noise by incorporating meta-learning to boost model generalization and compensate against the adverse impacts of Differential Privacy mechanisms.

Overcoming Loss in Accuracy Through Meta-Learning Meta-learning, or "learning to learn," allows models to learn to adapt to new tasks rapidly with little training data. Rather than learning from scratch, the model learns an optimal initialization that enables fast fine-tuning. For DP-FedMeta, this reduces the effect of DP-introduced noise in the following manners [11]:

- Faster Convergence: Meta-learning causes the model to achieve optimal performance in a smaller number of training iterations, minimizing the total effect of noisy updates.
- Improved Generalization: The initialization learned in meta-learning is robust by nature and enables the model to be highly accurate even with privacy-preserving noise during training.
- Effective Knowledge Transfer: As meta-learning derives common patterns from heterogeneous clients, the model can generalize among various tasks even in the case of noisy individual client updates.

Improvements in Medical IoT Applications Accuracy In Medical IoT (Internet of Things) use cases, where patient data is extremely sensitive, DP-FedMeta guarantees both privacy and superior model accuracy. A few dominant examples are:

Personalized Disease Prediction: A federated meta-learning model based on noisy patient data across various hospitals can still have high accuracy for predicting ailments such as diabetes or cardiovascular disease by exploiting meta-learning's flexibility.

- Wearable Health Monitoring: Patient-specific data is gathered by smartwatches and IoT-based health devices. DP-FedMeta supports effective anomaly detection in case of abnormal heartbeats or blood glucose readings, even when privacy restrictions introduce noise in the training set.
- Medical Image Analysis: DP-FedMeta provides robust classification of X-rays or MRI images by federated models with high accuracy despite privacy-protecting perturbations, facilitating enhanced early detection of diseases.
- By combining meta-learning with DP methods,

DP-FedMeta strikes a good balance between accuracy and privacy, making it very appropriate for privacy-concerning applications such as medical IoT.

3.1.3 Reduced Resource Consumption

Decreased Resource Usage in DP-FedMeta Efficient use of resources is an important issue for IoT devices, which tend to have limited computer processing power, storage, and battery life. DP-FedMeta is particularly tailored to minimize the resource load without compromising privacy and model quality.

Resource Efficiency for Low-Resource IoT Devices Conventional federated learning involves heavy local training and communication, which can be computationally intensive for IoT devices. DP-FedMeta tackles these issues by [11]:

- Reducing Local Computation: Meta-learning allows the model to learn an optimal initialization so that IoT devices can fine-tune their local models with fewer updates. This decreases the number of training epochs needed, reducing CPU and memory usage.
- Minimizing Model Complexity: Because DP-FedMeta takes advantage of shared knowledge among devices, each IoT node has less training data and fewer computational resources needed in order to exhibit good performance.
- Maximizing Energy Efficiency: By limiting the requirement of extensive local training, DP-FedMeta enables IoT devices to save battery power, which is essential in wearables, medical sensors, and smart home gadgets.

Reduction of Local Training and Communication Overhead

- Frequent model updates and central server communication in regular federated learning generate high bandwidth and latency, which is detrimental for IoT networks. DP-FedMeta addresses this by:
- Less Communication Rounds: As meta-learning achieves faster convergence, the IoT devices need to communicate less with the central server, resulting in less network congestion.
- Compressed Model Updates: Local Differential Privacy (LDP) and secure aggregation together guarantee that only required information is exchanged, minimizing transmitted data size.

Adaptive Participation: DP-FedMeta provides selective participation for devices that have low power or unreliable connections, avoiding waste of resources.

Real-World Impact For Medical IoT, like implantable devices and smart health monitors, DP-FedMeta guarantees that key models are efficiently updated without burdening low-power devices. In the same way, in industrial IoT and smart homes, it facilitates smooth federated learning while maintaining both device longevity and privacy.

By reducing local computation and communication, DP-FedMeta makes privacy-preserving federated learning feasible for actual IoT applications without sacrificing efficiency or security, or accuracy.

Facilitation of Personalized Healthcare through DP-FedMeta DP-FedMeta is an important enabler in personalized healthcare through the facilitation of patient-customized medical models with stringent privacy assurances. Through the integration of federated meta-learning and differential privacy, DP-FedMeta provides a means for healthcare organizations and Internet-of-Things-based medical devices to train models over sensitive patient information without revealing individual records.

3.1.4 Enablement of Personalized Healthcare

Development of Personalized Medical Models Classic machine learning algorithms in healthcare tend to use centralized data aggregation, which compromises privacy and restricts individualization. DP-FedMeta is able to bridge this gap by:

- Training from Scattered Patient Data: Clinics, hospitals, and wearable sensors can jointly train models without exchanging raw information, maintaining confidentiality of the patients.
- Meta-learning component allows the model to adapt quickly to the specific patient data with minimal fine-tuning so that the predictions and recommendations are highly personalized.
- Differential privacy mechanisms ensure that even though personalized models learn from multiple patients, no individual data is exposed, thereby suiting it for HIPAA-compliant applications.

Advantages in Patient-Specific Treatment and Monitoring DP-FedMeta improves live patient

monitoring and accurate treatment through various means:

- Personalized Disease Forecasting: A diabetic patient's glucose wearable can calibrate a model to forecast blood sugar levels according to individual eating and activity patterns, facilitating better control.
- Customized Medication Advice: Personalized models can recommend ideal dosages for a drug based on one's genetic makeup, lifestyle, and medical history, enhancing treatment efficacy.
- Early Health Anomalies Detection: IoT devices like ECG monitors or smartwatches can pick up unusual heartbeats or early signs of stroke, learning a person's baseline measurements while maintaining privacy.

By facilitating privacy-preserving personalization, DP-FedMeta changes the face of digital healthcare forever, so that patients are provided with personalized treatments while their sensitive medical information is protected. This innovation opens up avenues for safer, smarter, and more potent healthcare solutions in the age of medicine by AI.

3.1.5 System Robustness

System robustness is the capacity of a system to provide stable performance in spite of hardware failure and data format variation. A robust system guarantees minimum downtime, effective error recovery, and fault-free data integration, which is vital to preserve performance and accuracy in dynamic conditions.

Handling Device Failures Hardware and software failures, e.g., server crashes, network outages, or hardware faults, significantly affect system performance. To avoid these risks, fault-tolerant systems use redundancy techniques such as backup servers, failover policies, and distributed computation models. Cloud solutions provide a greater fault tolerance in that workloads are dynamically redistributed on a pool of servers, eliminating single points of failure.

Besides redundancy, predictive maintenance and real-time monitoring methods aid in the identification of possible failures before they happen. Error-handling methods, including rollback and recovery procedures, ensure that systems are able to rapidly recover previous stable states, preserving limited data loss and service interruptions.

Handling Data Heterogeneity New systems have to handle heterogeneous data formats from multiple sources, such as structured, semi-structured, and unstructured data. Data encoding, schema, and quality differences create integration and consistency issues. To solve this, resilient systems use scalable data processing architectures, middleware technology, and interoperability standards that normalize communication between disparate components.

Sophisticated data fusion and machine learning methods improve system resilience by detecting inconsistencies, normalizing formats, and validating data accuracy. Adaptive processing algorithms may adapt dynamically to new data types, allowing for efficient processing of changing datasets.

By efficiently managing device failures as well as data heterogeneity, a system increases its resilience, guaranteeing continuous operation, high data integrity, and consistent performance under varying conditions.

4 Implementation Considerations

4.1 Noise Calibration and Management of Privacy Budget

4.1.1 Challenges in Calibrating Noise for LDP

Local Differential Privacy (LDP) preserves privacy by introducing noise to individual data points prior to transmission. But calibrating this noise to the right level is a key challenge. If the noise is too high, accuracy in aggregated results is lost, and unreliable insights are generated. If the noise is too low, privacy protection is lost, and there is a higher risk of sensitive information being inferred.

A Hamiltonian noise correction challenge is balancing utility and privacy. The level of noise varies with the privacy parameter (ϵ) so that smaller values assure greater privacy while compromising on data quality. Various types of data noise (categorical, numerical, or high-dimensional data) call for customized noise mechanisms, including Laplace, Gaussian, or randomized response methods, all with differing trade-offs.

Another problem is maintaining fairness and consistency across heterogeneous datasets. Certain data distributions are more vulnerable to noise distortion than others. Dynamic noise adaptation methods, which adapt noise levels according to data sensitivity and distribution, reduce the problem but introduce complexity in implementation [12].

4.1.2 *Significance of Controlling the Privacy Budget*

The privacy budget (ϵ) determines the amount of information that can be disclosed while ensuring differential privacy. Every query or data collection draws on a share of this budget, and too many queries can drain it, resulting in privacy violations.

Good management of the privacy budget is important to ensure long-term data privacy. This can be achieved through the implementation of privacy-preserving mechanisms such as privacy composition rules and budget allocation techniques. These mechanisms prevent aggregated exposure of sensitive information through successive interactions with the data.

An effectively managed privacy budget allows organizations to balance usability and privacy, keeping data valuable for analysis while protecting confidentiality of individuals. Proper budget allocation prolongs the duration of data usability without causing privacy degradation over time.

4.2 Meta-Learning Algorithm Selection and Optimization

4.2.1 *Considerations to Account for When Selecting a Meta-Learning Algorithm*

Meta-learning, or "learning to learn," strives to enhance the capacity of a model to learn new tasks swiftly. The choice of appropriate meta-learning algorithm is based on a variety of important considerations [11]:

- Task Distribution – The variability and structure of tasks determine algorithm selection. When tasks have similar structures, gradient-based algorithms such as Model-Agnostic Meta-Learning (MAML) work well. When tasks differ greatly, memory-based methods such as Recurrent Neural Networks (RNNs) or transformer-based meta-learners might be more appropriate.
- Data Availability – Certain meta-learning algorithms need big labeled datasets, while others can learn from small samples. For low-data cases, metric-based algorithms such as Prototypical Networks or Siamese Networks should be used.
- Computational Complexity – Second-order gradients are needed for gradient-based meta-learning (e.g., MAML), which adds computation expense. Black-box models like memory-augmented networks might be more efficient but lose interpretability.
- Adaptability vs. Generalization – Some algorithms learn quickly to adapt to new tasks (e.g., MAML), while others are geared towards generalizing over tasks (e.g., Bayesian Optimization-based methods). It is a function of whether the focus is on quick learning or strong generalization.

4.2.2 *Optimization of Meta-Learning Parameters*

Tuning of meta-learning algorithms means that hyperparameters need to be optimized at both the base and meta-level:

Meta-Learning Rate – Controls how fast the meta-learner adapts task-specific models. There is a need to balance so as not to overfit or have slow convergence. Adaptive learning rate algorithms, like Adam or Lookahead, can enhance performance.

- Number of Inner-Loop Updates – In models like MAML, the number of gradient steps per task influences adaptation quality. Very few steps delay learning, whereas many result in overfitting to individual tasks.
- Regularization and Loss Function Choice – L1/L2 regularization, dropout, or task-specific loss functions enhance generalization on a wide variety of tasks.

Through proper selection and tuning of a meta-learning algorithm, models can perform enhanced task adaptation, efficient learning, and better performance on different data distributions.

4.3 Secure Aggregation Efficiency and Scalability

4.3.1 *Computational and Communication Costs of Secure Aggregation*

Secure aggregation ensures that individual data contributions remain private while enabling collaborative model training. However, it introduces computational and communication overhead, impacting system efficiency [12].

- Computational Costs – Secure aggregation methods, e.g., homomorphic encryption, secret sharing, and secure multi-party computation (MPC), involve intricate cryptographic computations. Homomorphic encryption provides high security but is computationally costly because of extensive modular exponentiation. Secret sharing methods, e.g., Shamir's Secret Sharing, are less computationally costly but require extra steps

for data reconstruction. Lightweight masking methods, e.g., additively homomorphic noise, strike a balance between security and efficiency.

- Communication Costs – Multiple rounds of interaction between the participants and the central server are needed in secure aggregation protocols. Pairwise encryption, key exchanges, and masked summation result in high bandwidth overhead, especially in bandwidth-limited environments. Compressed updates, quantization, and differential privacy-based noise reduction are some techniques that reduce high communication costs without sacrificing security.

4.3.2 Scalability in Large-Scale IoT Deployments

Scaling secure aggregation in IoT networks means managing thousands or even millions of devices with different connectivity and computational power.

- Hierarchical Aggregation – Intermediate nodes or edge devices carry out partial aggregation instead of a central server, thus lowering communication overhead. Hierarchical models enhance efficiency without compromising privacy guarantees.
- Selective Participation and Adaptive Sampling – Not all devices need to participate in every aggregation round. The adaptive sampling method selects the most representative devices and reduces the amount of congestion within the network, preserving model accuracy.
- Fault Tolerance and Dropout Resilience – Devices of IoT usually encounter connectivity problems. Secure aggregation needs to cope with device dropouts using redundancy mechanisms, threshold cryptography, or delayed aggregation strategies.

In optimization of computation, reduction of the communication cost and scalable architectures can make secure aggregation support large IoT networks efficiently in terms of both privacy and efficiency.

4.4 Managing Heterogeneity in Devices and Data Variability

4.4.1 Managing Device Variations in Computing Resources and Data Features

Distributed learning scenarios have varying levels of devices regarding processing capability, memory, battery life, and network connection. These differences influence the speed and dependability of model training.

- Federated Learning with Adaptive Aggregation – FedAvg-type algorithms can be extended with weighted aggregation, where updates from high-resource devices are assigned more weight so that balanced learning is preserved while contributions from low-resource devices are included.
- Model Compression and Quantization – Minimizing model size through methods such as pruning, knowledge distillation, and quantization enables low-power devices to contribute without inordinate computational expense.
- Asynchronous Updates – Rather than forcing all devices to send updates at once, asynchronous federated learning allows devices to contribute at any time they are available, enhancing training continuity in spite of hardware differences.
- Edge Computing and Hierarchical Training – Partitioning some computation to edge servers or intermediate nodes minimizes the load on low-power devices and minimizes communication cost.

4.4.2 Solving the Issue of Non-IID Data

- Non-Independent and Identically Distributed (non-IID) data is problematic for federated and distributed learning, as various devices gather data from distinct environments that result in local models with a biased nature.
- Personalized Federated Learning – Methods such as model fine-tuning or meta-learning allow local models to better fit into their respective data distributions without diminishing generalization.
- Sharing Data with Privacy-Protecting Methods – Some degree of shared data representation, like the sharing model embeddings rather than raw data, can assist in aligning varying distributions without loss of privacy.
- Clustered Federated Learning – Clustering devices with comparable data distributions enables more effective training and prevents dominant distributions from distorting overall model performance.

Through these methods, systems can easily address device heterogeneity and non-IID data in order to provide reliable and equitable learning in varying settings.

4.5 Regulatory Compliance and Ethics

4.5.1 Privacy Compliance

Appropriate compliance with privacy regulations is essential in data-intensive systems, especially in sectors like healthcare, finance, and social networking. Some of the vital regulations are:

- General Data Protection Regulation (GDPR) – GDPR requires strict data protection practices such as informed consent, right to erasure of data, and data transparency when processing. Organizations need to adopt data minimization, encryption, and anonymization practices to ensure GDPR compliance.
- Health Insurance Portability and Accountability Act (HIPAA) – In medical uses, HIPAA demands safe treatment of Protected Health Information (PHI). Compliance involves applying de-identification methods, imposing rigorous access controls, and providing secure data transmission to avoid unauthorized access [13].
- California Consumer Privacy Act (CCPA) – As with GDPR, CCPA gives consumers ownership of their personal data, obliging businesses to make data collection practices transparent and provide users with an opt-out on sharing data [13].

Organizations will need to adopt privacy-by-design guidelines, undertake periodic audits, and provide safe storage and processing of data to meet these regulatory needs.

4.5.2 Ethical Considerations in Data Collection and Use

In addition to compliance with the law, there are ethical concerns regarding the collection, storage, and utilization of data.

- User Consent and Transparency – Ethical data acquisition involves the requirement of informed consent and explicit notification of how data shall be utilized. Dark patterns or deceptive consent processes betray user trust and ethical norms.
- Bias and Fairness – Machine learning algorithms trained from biased data have the potential to perpetuate discrimination. Having diverse and representative data collection and applying fairness-aware algorithms reduces bias.
- Data Ownership and Control – The users must have control over their data, and they should be able to alter or erase it. Decentralized methods, like federated learning, maintain user privacy through data storage on local devices.

By combining regulatory compliance with ethical best practices, organizations can create trusted, privacy-respecting systems that honor user rights and ensure fairness.

5 Future Directions and Open Challenges

5.1 Advanced Differential Privacy Techniques

As privacy issues in medical IoT applications keep on rising, stronger differential privacy (DP) methods are being investigated to attain data protection and model utility. Conventional DP methods, including the Laplace and Gaussian mechanisms, offer strong privacy assurances at the cost of adding substantial noise, which compromises model performance. To overcome these drawbacks, focused differential privacy (CDP) and other advanced DP architectures offer improved privacy-accuracy trade-offs [14].

CDP, an extension of standard DP, offers a stronger privacy analysis by capping the total privacy loss across multiple queries. This is especially helpful in federated meta-learning applications, where frequent model updates can cause excessive privacy budget usage. With the use of Rényi differential privacy (RDP) or zero-concentrated differential privacy (zCDP), medical IoT systems can obtain stronger privacy guarantees without compromising data utility.

Another promising approach is privacy amplification by subsampling, which employs a random subset of data in each training iteration, hence minimizing the overall privacy loss. This approach is especially relevant in federated learning since it limits the exposure of each data point across training rounds. Another approach is adaptive DP mechanisms that dynamically change noise sizes based on the sensitivity of different model parameters, hence facilitating better privacy-utility trade-offs.

Despite all these advances, it is difficult to implement these techniques in real medical IoT settings. One needs to balance computational overhead, privacy budgeting, and regulatory compliance so that security and usability are not sacrificed. Future research needs to tackle the integration of advanced DP techniques with cryptography techniques like secure multiparty computation (SMPC) and homomorphic encryption to further strengthen privacy protection in federated meta-learning. With these innovative DP approaches, privacy-ensuring medical IoT systems are able to achieve enhanced security while not degrading the

performance of AI-driven healthcare solutions.

5.2 Edge Computing Integration

The integration of federated meta-learning and edge computing is a promising approach to enhancing the privacy and efficiency of medical IoT systems. The traditional cloud-based learning paradigms are at a disadvantage due to high latency, bandwidth limitations, and security risks because of centralized processing. With edge computing, computations can be performed close to IoT devices, reducing the utilization of centralized servers and promoting real-time decision-making in healthcare.

One of the key advantages of edge computing in federated meta-learning is that it reduces communication overhead. In standard federated learning, frequent model updates have to be communicated from edge devices to a centralized server, consuming power and generating network traffic. Edge computing solves this problem by enabling intermediate edge nodes, such as hospital lobbies or wearable device hubs, to perform local aggregations and then communicate optimized updates to the global model. This hierarchical approach significantly enhances scalability and efficiency.

Secondly, edge computing also enhances the privacy protection through the reduction of exposure to data. With private healthcare data saved in local edge nodes instead of passing to cloud servers, data breaches are reduced. With differential privacy techniques, alongside edge-based federated meta-learning, privacy protection is strong while the accuracy of the model is preserved. Edge devices even use techniques like secure enclaves and trusted execution environments (TEE) in a bid to safeguard patient data even more. While these advantages, there are some issues that need to be resolved in order to achieve the complete potential of edge computing in medical IoT [15]. The constrained processing and storage capabilities of edge devices would restrict sophisticated meta-learning computations. Resource management techniques like model compression, quantization, and adaptive learning strategies need to be employed to achieve optimized performance. In addition, interoperability of multiple IoT devices and common privacy policies over distributed nodes needs to be ensured, which is still a topic of research.

Future studies will concentrate on developing effective yet light-weight edge-based federated meta-learning frameworks that optimize the trade-offs between computational efficiency, privacy, and model effectiveness. By integrating edge computing and sophisticated privacy-preserving methods, medical IoT systems will be able to provide real-time, secure, and scalable AI-based healthcare services.

5.3 Handling Complicated Medical Information

Applying differential privacy-enabled federated meta-learning (DP-FedMeta) to high-dimensional, long-tailed, and complex medical data, like time-series signals, medical images, and multi-modal data, is a demanding process. Compared with structured tabular data, these data have a tendency towards high dimensionality, temporal dependence, and complex spatial relationships, making it difficult to strike a balance between privacy protection and model usefulness.

One of the primary difficulties in handling time-series clinical data such as electrocardiograms (ECGs), electroencephalograms (EEGs), and continuous glucose monitoring (CGM) data is preserving temporal dependencies and differential privacy. Standard DP mechanisms such as additive noise injection can disrupt the sequential patterns required for effective predictions. Techniques such as recurrent neural networks (RNNs) and transformers require special DP techniques, e.g., noise suppression through adaptive privacy budgets or structured noise injection, to maintain temporal coherence in clinical predictions [15].

Similarly, medical imaging data like MRI and CT scans must be treated with certain DP techniques sensitive to spatial relations. Generic DP mechanisms applied universally over pixels can destroy image quality and disrupt diagnostic functionality. Sophisticated methods like differentially private generative adversarial networks (DP-GANs) or local noise injection to background pixels can maintain diagnostic features without compromising privacy.

Multi-modal clinical data, with text, signals, and images, is even more challenging due to the heterogeneity of the data. DP across multiple data types while maintaining inter-modal relationships requires new solutions, such as modality-specific privacy budgets and hierarchical DP mechanisms.

Additionally, combining DP with federated meta-learning across medical data of intricate structures calls for effective privacy budget control in order to avoid unnecessary noise aggregation.

Methods such as per-layer DP calibration for deep networks and privacy amplification via subsampling can help alleviate privacy-utility trade-offs.

Optimization of DP techniques for multi-modal data, imaging, and medical time-series is the future. Hybrid techniques combining DP with cryptographic techniques such as homomorphic encryption and SMPC could further offer improved privacy with the integrity of medical AI models.

5.4 Blockchain Integration to Enable Auditability

The integration of blockchain with differential privacy-federated meta-learning (DP-FedMeta) is an efficient way of realizing auditability, data integrity, and secure provenance for medical IoT [16]. Since federated meta-learning involves numerous decentralized devices and organizations exchanging model updates, it must offer an open and tamper-evident record of interactions for regulatory conformance and trust.

Blockchain offers an immutable, decentralized ledger that can be used to securely record all model updates, privacy budgets, and data access requests. Through the use of smart contracts, blockchain enforces policy automatically, whereby only the requested parties can access certain data while ensuring strict privacy controls. This is especially useful in privacy-preserving health applications, where regulatory compliance like HIPAA and GDPR need to be ensured.

One of the key advantages of blockchain in DP-FedMeta is that it can generate secure audit trails. All transactions, including model updates, privacy budget allocations, and access permissions, are recorded as cryptographically signed blocks. This prevents unauthorized modifications and allows regulators and healthcare providers to verify compliance without gaining access to sensitive patient data. Blockchain-based timestamping also makes all interactions traceable, improving accountability in federated learning pipelines.

Blockchain also aids data provenance by tracing source and changes to clinical data. This aids model reliability by allowing clinicians and researchers to confirm whether training data has been tampered with, altered, or used in accordance with mutually agreed privacy protocols. Zero-knowledge proofs (ZKPs) are also one of the methods that can aid privacy by allowing verification without exposing underlying sensitive information [15].

Although it has its benefits, integrating blockchain with medical IoT is challenging, such as scalability, energy efficiency, and latency. Light blockchain structures, such as permissioned blockchains and layer-2 scaling solutions, will be the future direction of research in order to support efficient and privacy-preserving federated meta-learning in medical applications. Blockchain integration with advanced DP algorithms will facilitate strong privacy protection and clear auditability in AI-driven healthcare systems.

5.5 Real-World Deployment and Evaluation

Real-world deployment in healthcare IoT systems is necessary to study its usability, security, and efficacy. While theoretical models and simulation provide a sense of privacy-utility trade-offs, real-world evaluation needs to be performed to study system performance under real-world limitations, e.g., network variability, device heterogeneity, and integration with clinical workflow.

One of the greatest challenges of using DP-FedMeta in a clinical setting is following healthcare regulations such as HIPAA, GDPR, and local privacy laws. Care must be taken to make sure differential privacy mechanisms can effectively protect patient data while being compliant with evolving regulatory ecosystems through appropriate privacy budgeting and transparent privacy-preserving computations. Interpretability of federated meta-learning models is also crucial to clinical setting adoption since medical practitioners must be sure of AI-derived insights in order to inform well-informed medical decisions. Another major challenge is heterogeneity of hospital infrastructures and medical IoT devices. Many medical devices are used in different medical environments with heterogeneous data formats, heterogeneous communication protocols, and different computational capabilities to process data. This makes the federated learning process difficult to standardize and seamless interoperability. Edge devices can be resource-constrained and lack sufficient capabilities to execute sophisticated meta-learning computations to provide differential privacy, and this implies some techniques such as model compression and adaptive learning are needed for lightweight optimizations.

6 Conclusion

Differential privacy-enabled federated meta-learning (DP-FedMeta) is a pioneering framework for privacy-protecting medical IoT applications, which achieves both data utility and robust privacy assurance.

Through the integration of differential privacy (DP) with federated meta-learning, DP-FedMeta enables collaborative machine learning model training from decentralized medical IoT devices while keeping sensitive patient information safe and confidential. This solution helps evade data risks in centralized storage and transmission, which makes it an attractive choice for AI-based healthcare applications. One of the major contributions of DP-FedMeta is that it can improve both model flexibility and privacy safeguarding in dynamic medical settings. Federated meta-learning supports effective knowledge transfer among scattered medical institutions, enabling quick model updates with lower communication expenses. At the same time, differential privacy mechanisms guarantee that individual patient information cannot be derived, which helps to resolve serious privacy issues in healthcare. The combination of edge computing and blockchain further enhances security, scalability, and auditability, opening the door to secure and transparent medical AI systems. Despite its advantages, the successful deployment of DP-FedMeta in real-world clinical settings requires overcoming several challenges. Regulatory compliance, interoperability between heterogeneous medical IoT devices, and computational constraints on edge devices must be addressed to ensure seamless adoption. Additionally, privacy-preserving techniques must be optimized to maintain model performance while preventing adversarial attacks and privacy breaches. Future research should focus on refining DP mechanisms, improving edge-based federated learning efficiency, and integrating blockchain for secure audit trails.

In summary, DP-FedMeta can transform privacy-preserving AI in healthcare by facilitating secure, decentralized, and smart medical IoT applications. Overcoming implementation challenges and further research in this area will be important to unlock the full potential of DP-FedMeta in actual healthcare settings, ultimately resulting in better patient outcomes and enhanced data privacy protection.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Thilakarathne, N. N., Muneeswari, G., Parthasarathy, V., Alassery, F., Hamam, H., Mahendran, R. K., & Shafiq, M. (2022). Federated learning for privacy-preserved medical internet of things. *Intell. Autom. Soft Comput*, *33*(1), 157-172.

[2] Adnan, M., Kalra, S., Cresswell, J. C., Taylor, G. W., & Tizhoosh, H. R. (2022). Federated learning and differential privacy for medical image analysis. *Scientific reports*, *12*(1), 1953. [CrossRef]

[3] Aouedi, O., Sacco, A., Piamrat, K., & Marchetto, G. (2022). Handling privacy-sensitive medical data with federated learning: challenges and future directions. *IEEE journal of biomedical and health informatics*, *27*(2), 790-803. [CrossRef]

[4] Pfitzner, B., Steckhan, N., & Arnrich, B. (2021). Federated learning in a medical context: a systematic literature review. *ACM Transactions on Internet Technology (TOIT)*, *21*(2), 1-31. [CrossRef]

[5] Chronis, C., Varlamis, I., Himeur, Y., Sayed, A. N., Al-Hasan, T. M., Nhlabatsi, A., ... & Dimitrakopoulos, G. (2024). A survey on the use of federated learning in privacy-preserving recommender systems. *IEEE Open Journal of the Computer Society*. [CrossRef]

[6] Chaddad, A., Wu, Y., & Desrosiers, C. (2023). Federated learning for healthcare applications. *IEEE internet of things journal*, *11*(5), 7339-7358. [CrossRef]

[7] Afzal, M. U., Abdellatif, A. A., Zubair, M., Mehmood, M. Q., & Massoud, Y. (2023). Privacy and security in distributed learning: A review of challenges, solutions, and open research issues. *IEEE Access*, *11*, 114562-114581. [CrossRef]

[8] Wang, Q., Yin, H., Chen, T., Yu, J., Zhou, A., & Zhang, X. (2022). Fast-adapting and privacy-preserving federated recommender system. *The VLDB Journal*, *31*(5), 877-896. [CrossRef]

[9] Annappa, B., Hegde, S., Abhijit, C. S., & Ambesange, S. (2024). Fedcure: A heterogeneity-aware personalized federated learning framework for intelligent healthcare applications in iomt environments. *IEEE Access*, *12*, 15867-15883. [CrossRef]

[10] Li, H., Ge, L., & Tian, L. (2024). Survey: federated learning data security and privacy-preserving in edge-Internet of Things. *Artificial Intelligence Review*, *57*(5), 130. [CrossRef]

[11] Amiri, Z., Heidari, A., Navimipour, N. J., Esmaeilpour, M., & Yazdani, Y. (2024). The deep learning applications in IoT-based bio-and medical informatics:

a systematic literature review. *Neural Computing and Applications*, *36*(11), 5757-5797. [CrossRef]

[12] Saha, S., Hota, A., Chattopadhyay, A. K., Nag, A., & Nandi, S. (2024). A multifaceted survey on privacy preservation of federated learning: progress, challenges, and opportunities. *Artificial Intelligence Review*, *57*(7), 184. [CrossRef]

[13] Abbas, Z., Ahmad, S. F., Syed, M. H., Anjum, A., & Rehman, S. (2023). Exploring Deep Federated Learning for the Internet of Things: A GDPR-Compliant Architecture. *IEEE Access*, *12*, 10548-10574. [CrossRef]

[14] Wei, K., Li, J., Ding, M., Ma, C., Yang, H. H., Farokhi, F., ...& Poor, H. V. (2020). Federated learning with differential privacy: Algorithms and performance analysis. *IEEE transactions on information forensics and security*, *15*, 3454-3469. [CrossRef]

[15] Qi, P., Chiaro, D., Guzzo, A., Ianni, M., Fortino, G., & Piccialli, F. (2024). Model aggregation techniques in federated learning: A comprehensive survey. *Future Generation Computer Systems*, *150*, 272-293. [CrossRef]

[16] Tan, A. Z., Yu, H., Cui, L., & Yang, Q. (2022). Towards personalized federated learning. *IEEE transactions on neural networks and learning systems*, *34*(12), 9587-9603. [CrossRef]



Subhasri Telkar received B.Tech degree in electronics and communication engineering, M.Tech in VLSI. She is pursuing Ph.D in the area of VLSI. Her areas of interest are VLSI, ES, IOT, Cybersecurity, and signal processing. (Email: subhasri.t@pragati.ac.in)



Manas Kumar Yogi currently working as Assistant Professor in CSE Department of Pragati Engineering College (A), Surampalem has a teaching experience of more than 14 Years. With a paper publication record of over 285 papers from past 13 years, he has also published 15 book chapters and 6 patents and 4 books. His research area includes IoT, cyber-security, cyber-physical systems and soft computing. (Email: manas.yogi@gmail.com)