ISSN: 2093-5374 / E-ISSN: 2093-5382

Federated Learning for Privacy-Aware Ubiquitous Applications

Raami Riadhusin[1*], Ahmed Hussien Ahmed[2], P. Rajan[3], Dr. Reema Mathew[4], S.S. Sivasankari[5], T. Subalaxmi[6], and Abdurakhimova Zulaykho Ikromjon Kizi[7]

[1*]Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University of Najaf, Najaf, Iraq; Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University of Najaf of Al Diwaniyah, Al Diwaniyah, Iraq. iu.tech.eng.ramy_riad@iunajaf.edu.iq, https://orcid.org/0009-0000-7956-3567

[2]College of Engineering Technique, Al-Farahidi University, Baghdad, Iraq. ahmedhussien@uoalfarahidi.edu.iq, https://orcid.org/0009-0009-4928-2882

[3]Department of Marine Engineering, AMET University, Kanathur, Tamil Nadu, India. prabhakaranrajan@ametuniv.ac.in, https://orcid.org/0009-0006-9720-123X

[4]Department of Computer Science and Engineering (Cybersecurity), Vimal Jyothi Engineering College, Chemperi, Kannur, Kerala, India. reemamathew@vjec.ac.in, https://orcid.org/0000-0003-2099-3516

[5]Senior Assistant Professor, Department of Artificial Intelligence and Machine Learning, New Horizon College of Engineering, Bengaluru, India. yes.sivasankari@gmail.com, https://orcid.org/0009-0000-8801-819X

[6]Assistant Professor, Department of Computer Science and Engineering, K.S. Rangasamy College of Technology, Tiruchengode, India. subalaxmi@ksrct.ac.in, https://orcid.org/0009-0008-3148-0453

[7]Turan International University, Namangan, Uzbekistan. zulaykhoabdurakhimova96@gmile.com, https://orcid.org/0009-0006-1885-4102

Received: June 04, 2025; Revised: July 12, 2025; Accepted: August 29, 2025; Published: September 30, 2025

Abstract

Federated Learning (FL) has emerged as a suitable option for collaborative, user-centric machine learning while protecting sensitive user data. FL differs significantly from traditional centralized frameworks that collect raw data on a central server. FL focuses on collecting model updates generated locally on edge devices. With traditional FL approaches, data must be downloaded to a central server for model training. In contrast, training occurs on the edge and only model updates are sent. This decentralized framework, unlike traditional FL approaches, is ideal for ubiquitous applications—systems woven seamlessly into everyday surroundings like smart homes, advanced mobile devices, and IoT systems—where sensitive data is constantly and automatically generated. In these systems, user privacy is paramount, and advanced methods must be implemented to ensure privacy and system efficacy. This paper discusses the integration of FL into ubiquitous environments, addressing the relevance, advantages, and disadvantages of this approach. I'd like to

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 16, number: 3 (September), pp. 319-333. DOI: *10.58346/JOWUA.2025.I3.018*

*Corresponding author: Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University of Najaf, Najaf, Iraq; Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University of Najaf of Al Diwaniyah, Al Diwaniyah, Iraq.

focus on privacy-preserving methods, but their preservation against data leakage and adversary attacks adds significant value. There are case studies to show the challenges encountered, lessons learned, and the use of FL within privacy-centric ubiquitous systems. In closing this paper, I summarize the key points and underscore the transformational potential of FL for privacy-sensitive, innovative systems. I also promote further research in this area to support its practical relevance. This paper demonstrates that among the many approaches to privacy within pervasive computing, FL is the only one that is practical and scalable.

Keywords: Federated Learning, Ubiquitous Computing, Privacy Preservation, Differential Privacy, Secure Aggregation, Edge Computing, Data Protection.

1 Introduction

Developed to answer burning questions in the application of privacy-focused systems in the current machine learning frameworks, Federated Learning delegates training of machine learning models to local edge devices. The user's data is not transferred to the user's device; instead, machine learning models are transferred. Only the parameters of the local models get shared back with the server (Kairouz et al., 2021). This approach provides users with local data models, reducing the likelihood that their data will be compromised. This enables the development of embedded systems with integrated computing and ubiquitous data collection using FL. As smart devices and embedded systems integrated into everyday activities become more widely used, and as FL disseminates privacy-respecting systems for managing large amounts of sensitive data, the study of FL's application in privacy-respecting frameworks for ubiquitous systems is timely (Salman & Alomari, 2023; Wilamowski, 2025).

Federated Learning lets us train a global machine learning model while keeping smartphones, sensors, and IoT devices at different locations, and without aggregating or sharing raw data (Duan et al., 2023). User personal data is protected because only local model updates or gradients are sent to a central server. Pervasive computing involves protecting user data as it is collected across different contexts and devices. FL assists with compliance with legal frameworks such as GDPR and HIPAA, as personal data doesn't have to leave the user's control. In addition, there is a significant improvement in the effectiveness of edge computing resources since latency and bandwidth consumption are reduced. There is a growing body of literature suggesting an increase in the use of FL in mobile networks, smart cities, and healthcare as an indicator of its applicability and the associated privacy benefits (Mathew & Asha, 2024).

Ubiquitous computing involves integrating computing resources into everyday services, devices, and systems, enabling the real-time monitoring of multiple data sources. However, the convenience and improvement in services comes with critical privacy implications. Data obtained in these systems is often sensitive, including health data, personal data, and tracking information. Failing to take the proper precautions with the data can result in privacy breach or unsolicited profiling (Abbas et al., 2024). Inadequate approaches to aggregating data centrally leave raw data exposed at the aggregation point, which is a potential entry point and can be exploited. In addition, the variety of data processing devices and the real-time data streams processed make it harder to enforce privacy (Liu et al., 2022). As a result, creating appropriate privacy management frameworks that can operate efficiently in these poorly controlled, highly variable Geodistributed ecosystems is a major challenge for the scientific and engineering communities (Abreha et al., 2022). The use of FL in ubiquitous systems alleviates privacy concerns by enabling local processing, thereby minimizing the amount of data exposed. FL systems use advanced privacy-preserving techniques, such as differential privacy, which adds noise to model updates to obscure them and prevent inference attacks, and secure aggregation techniques that keep individual

contributions to the aggregated model updates hidden (Pragadeswaran et al., 2024). In addition, the communication links between the devices and the servers are protected with encryption. These techniques strengthen the FL systems against potential data breaches or unauthorized attacks. In addition, FL supports continuous learning through the contextual adaptation of privacy-preserving models, which is ideal for ubiquitous applications. FL is useful in advanced mobile services, personalized healthcare, smart transportation, and other mobile applications. Considering how unregulated data collection and processing raise privacy issues, it is no wonder people talk about Privacy-Aware Federated Learning. As devices become increasingly inter-operable, data tracking, collection, and processing become more complex and sensitive, making functionality and privacy confounding is a greater challenge. FL's Decentralized Framework is more appropriate because it is more decentralized; working in environments with data privacy concerns is easier with less exposure of unprocessed data and local model training. These frameworks make it easier to pass regulations while keeping services private. Building privacy-preserving technology for ubiquitous computing depends on knowing how to use FL techniques in these specific use cases. This is what the paper is about. This is the domain the paper is intended to cover.

Key Contributions

- This paper examines how Federated Learning is used in ubiquitous computing, particularly focusing on privacy enhancements related to data locality and exposure reduction. The paper also examines how well-suited FL is to IoT devices that continuously stream data.
- This discusses how privacy is maintained during collaborative training by examining differential privacy, secure aggregation, and other privacy-preserving mechanisms that affect model accuracy.
- The proposed research outlines an FL architecture designed to be both resource-efficient and scalable for edge devices with constrained resources. It combines active privacy in dynamically changing networks and persistent model and fine-grained privacy control.
- Findings from the designed framework are validated through research and real-life case studies, in which privacy-preserving frameworks and policies are shown to be applicable without substantial effort, communication overhead, or trade-offs in scalability.

This paper captures views on mobility and privacy in Federated Learning (FL) by abstractions, designs, and discussions on ubiquity frameworks. This is achieved by discussing the Federated Learning overview, focusing on ubiquitous computing systems, and the privacy traps they frequently pose. The review section highlights existing Federated Learning work on privacy at the edges of IoTs and distributed systems and identifies critical gaps in prior work. The document's methodology captures the system's architecture and the explained components of federated training and differentially private secure aggregation, alongside other privacy-preserving elements. Also, the document describes the results and discussions on the experiments conducted to explain the system's multi-faceted nature in finding the balance in system performance, privacy, and model accuracy at different levels of privacy which highlight the system's multi-faceted nature. Finally, the document emphasizes and recommends techniques to engineer the technology's sensitivity for ubiquity-sensitive applications (Karimov & Sattorova, 2024).

2 Related Work

The growing interest in Federated Learning (FL) represents a new step toward addressing privacy concerns in distributed machine learning systems. FL builds on previous systems that have local units

independently train local models and share only their aggregated updates to mitigate the risk of losing useful information. Prior works attempting to reduce the communication costs also worked on improving model performance under the non-IID conditions, a given in most practical settings. These works facilitated the use of FL in privacy-preserving learning in distributed networks (Li et al., 2020).

Additional algorithms have also been created to extend the privacy-preserving potential of ubiquitous computing environments in existing frameworks that use several FL methods, cross-integrating with other embodiments of privacy-preserving computing (Yang et al., 2019). With respect to preserving clients' identities in collaborative training, much attention has been given to differential privacy, which involves adding noise to model updates, and to secure multi-party computation. Other forms of cryptography, particularly homomorphic encryption, have been suggested to secure the transfer of data from clients to central aggregators. These methods are especially important for sensitive data, for instance, healthcare and smart city use cases (Ashitha et al., 2018).

When considering Ubiquitous Computing and the Internet of Things (IoT), the difficulties posed by a wide range of devices (e.g., sensors and wearable devices), limited on-device computation capabilities, and weak communication networks should be considered (Akter et al., 2022). Researchers propose adaptive FL methods that aim to minimize privacy risk while maintaining model quality by balancing neural network training and communication between the network and devices (Geyer et al., 2021). These studies also note the importance of FL in situations that require real-time adjustment, given the continuous learning it supports in rapidly changing environments (Sharma & Iyer, 2023).

Wisdom from practical case studies relating to these systems illuminate the benefits and challenges of using FL in sensitive contexts that are built on the principles of privacy-ubiquitous systems. (Mohandas et al., 2024). Case studies reporting successful implementations of FL in healthcare monitoring systems and energy management highlight the trust participants gained from the enhanced privacy it provided (James et al., 2025). However, these case studies also highlight challenges, such as limited scalability and poor resistance to adversarial attacks, reinforcing the need to construct robust FL systems that address the challenges of practical application (Zigui et al., 2024; Cluster Head Selection and Secured Routing, 2023).

Current research focuses on addressing issues in FL for ubiquitous computing by employing adaptive learning and other complementary methods (Zhang et al., 2025). The blending of FL with reinforcement learning aims to tailor privacy controls to individual users and improve the model's accuracy (Chinnasamy, 2024). Moreover, the use of blockchain technology has been analyzed to enhance the visibility and trustworthiness in decentralized FL systems (Wu et al., 2020). This is anticipated to positively influence the adaptability, scalability, and, most importantly, the security of privacy-sensitive applications in FL (Alugubelli et al., 2022).

3 Methodology

This section provides a comprehensive strategy for leveraging Federated Learning (FL) in privacy-aware pervasive applications. It begins with a detailed exposition of the phases of system design and data processing architecture then moves on to an in-depth discussion of federated model training. An account of a few classical privacy-preserving techniques is provided alongside the integrated approach. Subsequently, the system architecture and workflow are described to address the entire implementation spectrum and provide thorough insights. This approach helps ensure that privacy is embedded at every stage of the FL process lifecycle. At the same time, the model's performance within a distributed system is optimized.

3.1 System Design and Data Distribution

The methodology assumes a distributed system in which edge devices collaboratively train a machine learning model without exposing their raw data and maintain a local copy of the model trained independently. Each device reflects the heterogeneous, privacy-preserving nature of ubiquitous applications by collecting and processing data locally. The distribution of data across devices is assumed to be non-IID, i.e., the data samples differ in distribution and quantity, which creates a problem for the learning process. Local models are trained on-device and periodically synced with a central server to update the global model. This approach minimizes the amount of data that needs to be disclosed and the risk of a privacy violation, which is particularly appropriate in ubiquitous environments where data is constantly generated.

3.2 Federated Model Training and Update

Federated Learning is executed by an iterative process of local training followed by global aggregation. For each round, devices perform local model training using their private datasets and submit model update such as gradient or weight to the server. The server aggregates these uploads to update the global model without actually having raw data. Usually, aggregation is performed using a weighted averaging scheme called Federated Averaging (FedAvg). The update of the global model w_(t+1) at round t+1 is formulated as follows:

$$w_{t+1} = \sum_{k=0}^{n} \frac{n_k}{n} w_t^k \quad (1)$$

In Equation (1),

- w_{t+1} represents the updated global model weights after the $(t+1)^{th}$ training round.
- K is the total number of participating clients (devices) in the current training round.
- n_k *is the number of data samples held locally by client* k
- $n = \sum_{k=1}^{K} n_k$ is the total number of data samples across all participating clients.
- w_t^k denotes the model weights computed by client k during the t^{th}round after local training.

Equation (1) describes a primary operation of Federated Learning—integrating model updates from several distributed clients to create a new global model. It calculates a weighted average of locally trained model parameters w_t^k and assigns each client's model update a weight based on the size of the client's local dataset n_k and the total number of data samples n across all clients. Therefore, clients with more data have greater power to shape the global model. Since only model parameters are shared with the central server, collaboration remains privacy-preserving for raw data. Through the repeated application of this update rule, the global model improves with each round of training, adapting to the ubiquitously distributed, and often non-identically distributed, data.

3.3 Privacy-Preserving Techniques

Integrating privacy-preserving methods is essential in federated settings, particularly in omnipresent systems that manage sensitive personal data. Differential Privacy (DP) mechanisms apply perturbations to model updates to safeguard individual data points from exposure through the reverse-engineering of trained models. Adding noise must be conducted within a finely tuned model privacy budget to optimize the model's privacy and utility. Secure aggregation algorithms are used so that the server only receives the aggregated total of clients' updates, thereby preventing access to any individual client's contribution.

Moreover, sophisticated forms of encryption, including homomorphic encryption, enable reasoning over encrypted information, thereby protecting communication without compromising the model updates. The privacy workflow consists of several stages of encryption, noise addition, and secure aggregation, thus providing multiple forms of protection. The flow diagram below explains the privacy-preserving process of federated learning depicting the data flow starting at the clients and passing through the various privacy modules towards the aggregation server.

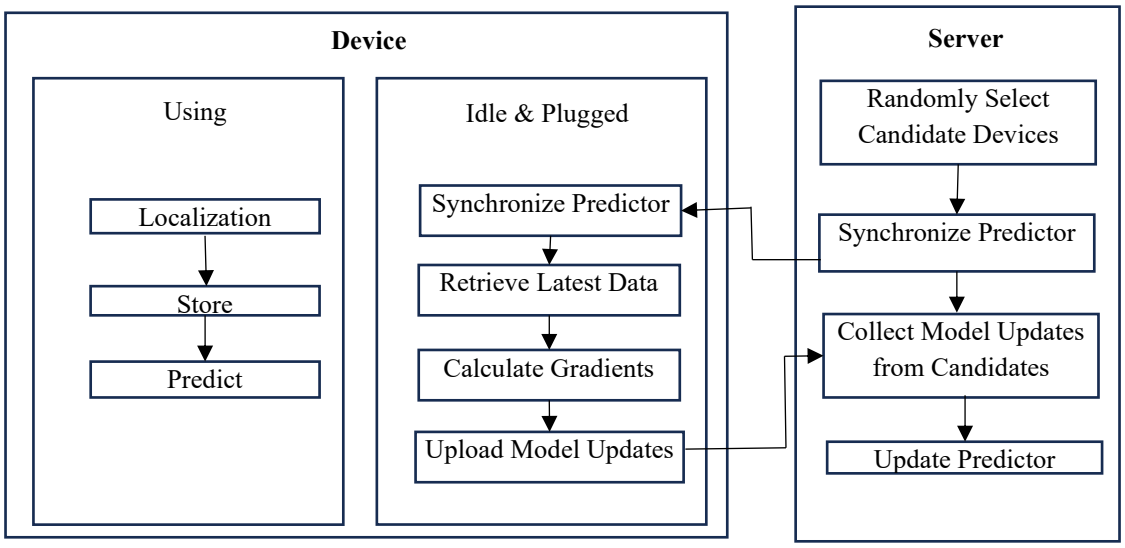

Figure 1: Federated Learning Workflow Between Device and Server

Figure 1 shows how the devices interact with the server in the process of collaborative model updating. The system on the device side has two modes: the using phase, and the idle & plugged phase. Each device during the using phase executes a localization procedure which contextually captures information and stores it locally. The device then predicts relevant information applicable to its environment based on the predictive data already stored. While in the idle & plugged phase, the device updates its local predictor with the server's global one. Then it fetches the latest data it has, and computes its local dataset gradients or model updates to upload to the server.

On the other hand, the server-side selects a random subset of candidate devices that will be active during the update cycle. The server synchronizes its predictor with these selected devices, retrieves their model updates, and uses the aggregated updates to refine the global predictive model. The distributed learning and model improvement across devices make this loop continuously efficient.

3.4 System Architecture

The architecture also incorporates the boundaries of privacy, scalability, and efficiency in widespread applications. Trust boundaries are delineated on the diagram which distinguishes the three core components of the system: edge devices or clients, a central aggregation server, and integrated privacy modules. Clients are responsible for data capture, model training, and communicating model updates. They are resource-constrained, like any generic IoT device, in terms of processing capability, power consumption, and battery life, thus enabling lightweight full training and communication. The central server supervises the FL process by collecting local model updates from different users and sending the global model back to them. Throughout the system, privacy modules implement differential privacy, secure aggregation, and encryption on both the client and server sides. The system's modular structure makes it fault-tolerant and scalable, allowing new devices to be added or removed without negatively

affecting overall performance. The architecture diagram below provides an overview of the components, the roles each plays, the secure communication channels around each interface for data confidentiality, and the security levels applied in the system.

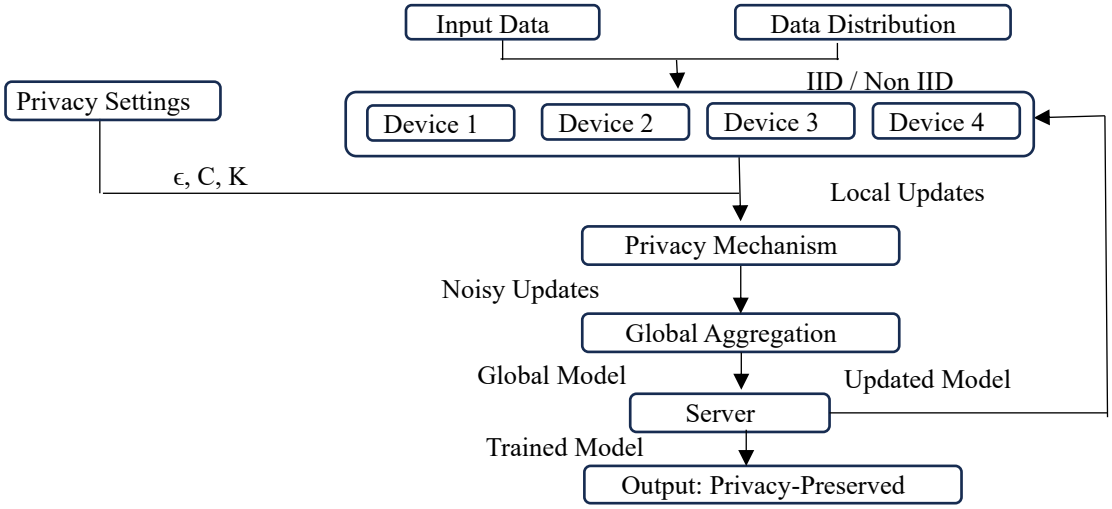

Figure 2: Federated Learning System Architecture with Integrated Privacy Mechanism for Ubiquitous Applications

Figure 2 illustrates the structure of a Federated Learning (FL) system which is tailored for privacy-preserving, ubiquitous applications. The process starts with the input data being partitioned across several clients these may operate under IID or non-IID conditions. Each client, comprising mobile phones, IoT sensors, or edge devices, trains a model with its proprietary data without sending the raw data to a central server. Following this, the local model updates undergo processing with a privacy mechanism, which may include the application of differential privacy or noise addition to alter sensitive data attributes.

As participants define the privacy budget, CCC clipping norm, and KKK number of partnering clients, privacy settings are assigned. The global model is created in the global aggregation step, where the noisy local updates are aggregated. Usually, a central server performs the aggregation, which does not have individual data but has access to sanitized model updates. During this iterative process, after several rounds, the output is a global model that preserves privacy and can be used on all devices from participants. This model and its specifications allow privacy preserving collaborative learning in the rapidly evolving decentralized systems characteristic of ubiquitous computing.

The trade-offs between Accuracy, Privacy Budget, and Latency in Federated Learning can be illustrated using a multi-variable function that describes the interrelationships among these three components: privacy, latency, and model accuracy.

The function A (ϵ, L) describes model accuracy; in the given scenario, the model accuracy depends on the privacy budget (ϵ) and latency (L). The privacy budget ϵ quantifies the degree of distortion or noise added to the data to safeguard privacy, while L (latency) specifies the communication delay or the total time required to complete training. During model training, as the privacy threshold is strengthened (i.e., ϵ becomes lower), model accuracy A is compromised because excessive noise is introduced to the data to maintain privacy. Likewise, latency L can be a model-accuracy detractor due to the longer time required to aggregate updates from various devices in a federated learning system.

This dependence and increment of model accuracy as a function of privacy and latency is described as:

$$A(\epsilon, L) = \alpha \cdot \frac{1}{1 + \beta \cdot \epsilon} \cdot \frac{1}{1 + \gamma \cdot L}$$

Here, α is a scaling constant, and β and γ are parameters that control the rates at which privacy and latency impact accuracy, respectively. The function $\frac{1}{1+\beta \cdot \epsilon}$ shows that as ϵ decreases (higher privacy), the accuracy $A(\epsilon, L)$ decreases, with a sharper decline for larger β. Similarly, the term $\frac{1}{1+\gamma \cdot L}$ captures how increased latency diminishes model accuracy, with a more pronounced effect as γ increases.

This function shows how privacy, latency, and accuracy interact, focusing on lower privacy (less than ϵ) and higher latency (extended communication time) and how they affect the decline of the model. For the system to function, these elements must be optimized to work alongside privacy and latency requirements.

Under the given realistic limitations, the system most frequently aims to maximize the model's accuracy (A (ϵ, L)) given that privacy and latency levels are restricted to certain bounds. The optimization problem, therefore, is formulated as:

$$\max_{\epsilon, L} \; A(\epsilon, L) = \max_{\epsilon, L} \left(\alpha \cdot \frac{1}{(1 + \beta \cdot \epsilon)} \cdot \frac{1}{(1 + \gamma \cdot L)}\right)$$

The system keeps trying to figure out the most the most accurate level the best privacy level ϵ and the least latency Lso the model accuracy is the best possible while staying within optimal system ϵ and system latency criteria. To sum up, the system cares about the most accurate privacy preservation, lowest possible latency, and the greatest accuracy in federated learning systems.

Step 1: Data Collection

1. Input

- Let $D_i(t)$represent the data collected by client $i$at time t. This data can include sensor readings, user inputs, or other relevant data.
- Each client $i$has a data set $D_i(t)$consisting of $N_i$data points: $D_i(t) = \{d_1, d_2, \ldots, d_{N_i}\}$.

Step 2: Data Preprocessing

2. Preprocessing

- Clean and preprocess the data $D_i(t)$to remove noise and normalize features:

$$D_i^{\text{clean}}(t) = f(D_i(t))$$

where $f()$is the preprocessing function that includes noise reduction, normalization, and other steps required to prepare the data for training.

Step 3: Privacy Preservation (Differential Privacy)

3. Privacy Function

- Add noise to the data to preserve privacy. For differential privacy, noise is added based on the privacy budget ϵ:

$$D_i^{\text{private}}(t) = D_i^{\text{clean}}(t) + \mathcal{N}(0, \sigma^2)$$

where $\mathcal{N}(0, \sigma^2)$represents the noise added to each data point, and $\sigma$is the noise scale determined by the privacy budget ϵ.

4. Privacy Function for Accuracy

- The model accuracy as a function of privacy budget $\epsilon$is given by:

$$A(\epsilon) = \alpha \cdot \frac{1}{1 + \beta \cdot \epsilon}$$

where $\alpha$and $\beta$are constants that control how privacy affects model accuracy.

Step 4: Local Model Training

5. Local Training

- Each client $i$uses their private data $D_i^{\text{private}}(t)$to train a local model $\theta_i(t)$:

$$\theta_i(t) = \arg\min_{\theta} \mathcal{L}(\theta, D_i^{\text{private}}(t))$$

where $\mathcal{L}(\theta, D_i^{\text{private}}(t))$represents the loss function (e.g., cross-entropy loss or mean squared error) for client i's model.

6. Update Rule

- The local model $\theta_i(t)$is updated based on the local dataset:

$$\theta_i(t+1) = \theta_i(t) - \eta \cdot \nabla \mathcal{L}(\theta_i(t), D_i^{\text{private}}(t))$$

where $\eta$is the learning rate.

Step 5: Federated Aggregation

7. Federated Aggregation

- After local training, the clients send their model updates $\theta_i(t+1)$to the central server. The server aggregates the local updates using a weighted average, with weights based on the amount of data $N_i$available at each client:

$$\theta_{\text{server}}(t+1) = \frac{1}{\sum_{i=1}^{N} N_i} \sum_{i=1}^{N} N_i \cdot \theta_i(t+1)$$

where $N$is the number of clients.

8. Model Update

- The central server updates the global model $\theta_{\text{global}}(t+1)$as follows:

$$\theta_{\text{global}}(t+1) = \theta_{\text{server}}(t+1)$$

Step 6: Privacy and Communication Optimization

9. Communication Efficiency

- The communication efficiency between the clients and the server can be optimized by reducing the frequency of updates (fewer rounds of communication). Let Rrepresent the number of communication rounds:

$$R_{\text{opt}} = \arg\min_{R} (\text{Communication Overhead})$$

where the overhead depends on factors like privacy budget, model size, and training time.

10. Latency Adjustment

- Latency in communication is also impacted by the privacy level ϵ. Higher privacy requires more noise and thus more communication rounds, leading to higher latency:

$$L(\epsilon) = \gamma \cdot \epsilon + \delta$$

where $\gamma$and $\delta$are constants that define how privacy affects latency.

Step 7: Global Model Update and Evaluation

11. Global Model Evaluation

- Once the global model is updated, evaluate its performance on a validation dataset D_{val}(held by a subset of clients or the server):

$$A_{\text{global}} = \frac{1}{|D_{\text{val}}|} \sum_{i=1}^{|D_{\text{val}}|} \mathbb{I}(\hat{y}_i = y_i)$$

where $\mathbb{I}$is the indicator function, $\hat{y}_i$is the predicted label, and $y_i$is the true label.

12. Feedback and Iteration

- Based on the global model's evaluation, feedback is given to the clients to further refine their local models. This process repeats for multiple iterations until convergence or a stopping criterion is met (e.g., maximum number of rounds, satisfactory accuracy, or resource constraints).

4 Results and Discussion

Assessing the performance of the constructed Federated Learning framework confirms that equilibrium is sustained between the performance of the model and the constraints of privacy within the various contexts of ubiquitous computing. The framework was assessed across various edge devices within the confines of simulated IoT environments experiencing non-IID data distributions. The model's accuracy, latency of communication, and privacy budget expenditure (ε) were calculated and assessed to determine

the tradeoff value within the FL privacy-preserving methods framework. The results indicate that the use of differential privacy and secure aggregation techniques does not significantly detract from the model's accuracy and, to a great extent, heightened the safeguarding of sensitive information. The framework demonstrated effective control of resource which further confirms the system's flexibility and resourcefulness given variable participation of devices and shifting network conditions.

Table 1: Performance Metrics of Federated Learning Under Varying Privacy Budgets

Privacy Budget (ε)	Model Accuracy (%)	Communication Overhead (MB)	Privacy Risk Level	Training Time (min)
0.1 (High Privacy)	82.3	120	Low	45
0.5	87.7	115	Medium	40
1.0 (Low Privacy)	90.5	110	High	38

Table 1 illustrates how the FL system's performance is influenced by variations in the privacy budget (ε). Higher ε values imply weaker privacy protections which also translate to less noise being added to model updates. Concerning model accuracy, the relative accuracy decline is from 90.5% at ε=1.0 to 82.3% at ε=0.1. However, the communication overhead remains stable which indicates promising aggregation protocols. Relative to the disclosed privacy, modal training time increases because more noise and encryption for computation must also be processed. Increased model training time to ensure strong privacy dissclosure is a positive characteristic because it indicates strong privacy disclosure is possible with only moderate trade-offs in predictability and scalability.

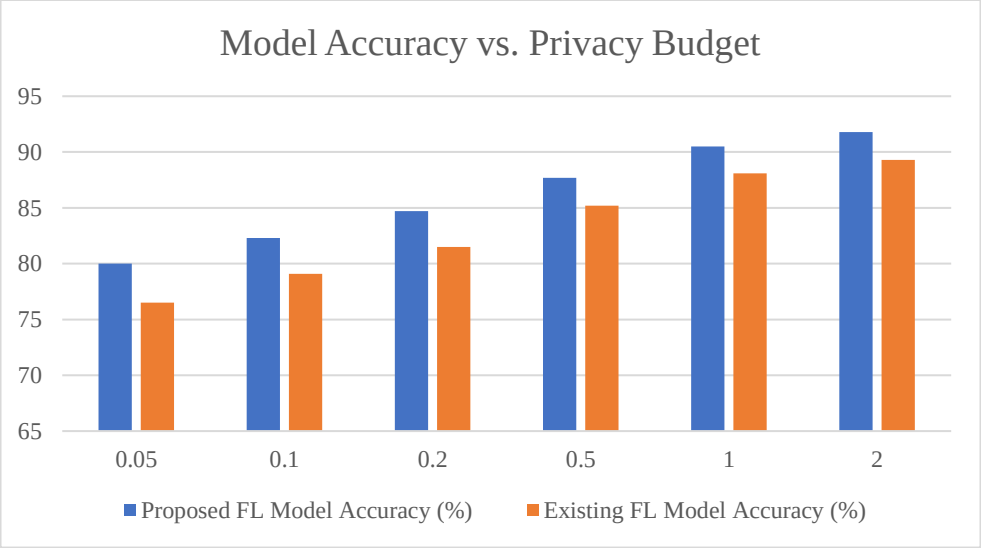

Figure 3: Model Accuracy vs. Privacy Budget

The results of the proposed Federated Learning (FL) figure 3 method's accuracy against a competing existing FL method are shown in Figure 3, and is discussed at different intervals of the privacy budget, ε. Each budget determines data privacy and the accuracy of the model; lower ε values yield tighter privacy. The score indicates that for both models, privacy budget accuracy improves as the budget span increases, showing a 0.05 to 2.0 budget span, suggesting privacy and utility balance. The proposed FL model, however, did prevail at all gaps, showing improved accuracy under privacy boundaries. Learning and privacy restrain addition are significant on enduring scenarios. Most notable delta efficacy being at lower budget accounts, showing high privacy accuracy without the model collapsing under privacy controls.

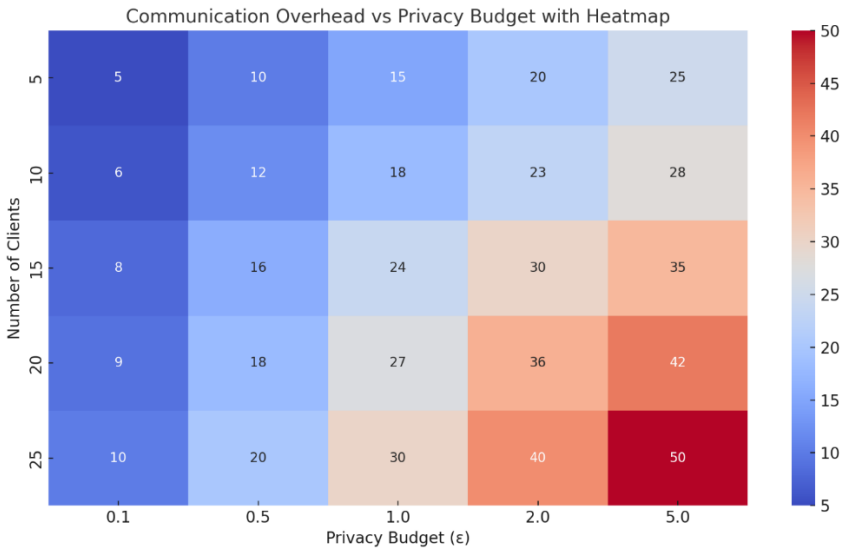

Figure 4: Communication Overhead Vs Privacy Budget with Heatmap

Figure 4 illustrates how communication overhead changes with privacy budget (ε) and the number of clients. The color intensity indicates the level of overhead, making it easier to see the relationship between these variables. The trade-offs among model accuracy, privacy budget (ε), and latency in a federated learning system are illustrated. The relationship is explained where accuracy is a function of changes in privacy budget (ε) and latency. In general, models with lower privacy budgets (stronger privacy, lower ε) and more noise to protect user data learn less. Higher ε and less noise means exposed more reliable data, therefore, accuracy improves. Latency is also a vital contributor. More latency, especially during federated training under stricter privacy (lower ε), induces a slight drop in accuracy due to extended communication breaks between the clients and the server. This suggests extended communication breaks during privacy tight rounds lead to slower learning of the model. This scenario explains the degradation of performance. Stronger privacy leads to a loss in accuracy, and latency makes this impact more severe, as demonstrated in the 3D surface plot. This illustrates the need to strike a balance between the performance and privacy protection in federated learning systems.

5 Conclusion

Federated Learning (FL) is a groundbreaking accomplishment in the privacy-preserving usage of ubiquitous applications since there is no need to exchange raw data to train models. This work demonstrated that the privacy-preserving, decentralized arrangement of FL, with the added mediation of differential privacy, secure aggregations, and encryption, resolves the core privacy challenges of pervasive computing environments. Empirical proof on model privacy frameworks validated strong privacy guarantees concerning model accuracy, communication overhead, and the privacy of underlying data. The design of the system focused on versatility and scalability to accommodate the range of edge devices used in IoT ecosystems. Besides, the practical value and benefits of FL in real-world scenarios, particularly in sensitive domains like healthcare and smart environments, is indisputable. While the challenges of non-IID data and a range of devices still need to be resolved, advancements in adaptive algorithms and technologies to mitigate privacy risks are promising. FL provides a privacy-sensitive, adaptable architecture in the upward trend of intelligent ubiquitous systems. It continuously invites endeavors to enhance its robustness and simplify its deployment.

References

[1] Abbas, S. R., Abbas, Z., Zahir, A., & Lee, S. W. (2024, December). Federated learning in smart healthcare: a comprehensive review on privacy, security, and predictive analytics with IoT integration. In *Healthcare*, *12*(24), 2587. MDPI. https://doi.org/10.3390/healthcare12242587

[2] Abreha, H. G., Hayajneh, M., & Serhani, M. A. (2022). Federated learning in edge computing: a systematic survey. *Sensors*, *22*(2), 450. https://doi.org/10.3390/s22020450

[3] Akter, M., Moustafa, N., Lynar, T., & Razzak, I. (2022). Edge intelligence: Federated learning-based privacy protection framework for smart healthcare systems. *IEEE Journal of Biomedical and Health Informatics*, *26*(12), 5805-5816. https://doi.org/10.1109/JBHI.2022.3192648

[4] Alugubelli, N., Abuissa, H., & Roka, A. (2022). Wearable devices for remote monitoring of heart rate and heart rate variability—what we know and what is coming. *Sensors*, *22*(22), 8903. https://doi.org/10.3390/s22228903

[5] Ashitha, M. A., Sivachandran, K., & Rathika, S. B. (2018). Healthcare data mining from multi source data. *International Journal of Advances in Engineering and Emerging Technology*, *9*(2), 54-58.

[6] Chinnasamy. (2024). A Blockchain and Machine Learning Integrated Hybrid System for Drug Supply Chain Management for the Smart Pharmaceutical Industry. *Clinical Journal for Medicine, Health and Pharmacy*, *2*(2), 29-40.

[7] Duan, Q., Huang, J., Hu, S., Deng, R., Lu, Z., & Yu, S. (2023). Combining federated learning and edge computing toward ubiquitous intelligence in 6G network: Challenges, recent advances, and future directions. *IEEE Communications Surveys & Tutorials*, *25*(4), 2892-2950. https://doi.org/10.1109/COMST.2023.3316615

[8] Geyer, R. C., Klein, T., & Nabi, M. (2017). Differentially private federated learning: A client level perspective. https://doi.org/10.48550/arXiv.1712.07557

[9] James, A., Elizabeth, C., Henry, W., & Rose, I. (2025). Energy-efficient communication protocols for long-range IoT sensor networks. *Journal of Wireless Sensor Networks and IoT*, *2*(1), 62-68.

[10] Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... & Zhao, S. (2021). Advances and open problems in federated learning. *Foundations and trends® in machine learning*, *14*(1–2), 1-210. https://doi.org/10.1561/2200000083

[11] Karimov, N., & Sattorova, Z. (2024). A systematic review and bibliometric analysis of emerging technologies for sustainable healthcare management policies. *Global Perspectives in Management*, *2*(2), 31-40.

[12] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. *IEEE signal processing magazine*, *37*(3), 50-60. https://doi.org/10.1109/MSP.2020.2975749

[13] Liu, X., Li, H., Xu, G., Lu, R., & He, M. (2020). Adaptive privacy-preserving federated learning. *Peer-to-peer networking and applications*, *13*(6), 2356-2366. https://doi.org/10.1007/s12083-019-00869-2

[14] Liu, Z., Guo, J., Yang, W., Fan, J., Lam, K. Y., & Zhao, J. (2022). Privacy-preserving aggregation in federated learning: A survey. *IEEE Transactions on Big Data*. https://doi.org/10.1109/TBDATA.2022.3190835

[15] Mathew, C., & Asha, P. (2024). FedProx: FedSplit algorithm based federated learning for statistical and system heterogeneity in medical data communication. *Journal of Internet Services and Information Security*, *14*(3), 353-370. https://doi.org/10.58346/JISIS.2024.I3.021

[16] Mohandas, R., Veena, S., Kirubasri, G., Mary, I. T. B., & Udayakumar, D. R. (2024). Federated learning with homomorphic encryption for ensuring privacy in medical data. *Indian Journal of Information Sources and Services*, *14*(2), 17-23. https://doi.org/10.51983/ijiss-2024.14.2.03.

[17] Pragadeswaran, S., Subha, N., Varunika, S., Moulishwar, P., Sanjay, R., Karthikeyan, P., ... & Vaasavathathaii, E. (2024). Energy Efficient Routing Protocol for Security Analysis Scheme

Using Homomorphic Encryption. *Archives for Technical Sciences*, *31*(2), 148-158. https://doi.org/10.70102/afts.2024.1631.148

[18] Prakash, M., & Prakash, A. (2023). Cluster Head Selection and Secured Routing Using Glowworm Swarm Algorithm and Hybrid Security Algorithm for Over IoT-WSNs. *International Academic Journal of Innovative Research*, *10*(2), 01-09. https://doi.org/10.71086/IAJIR/V10I2/IAJIR1004

[19] Salman, R. H., & Alomari, E. S. (2023). Survey: Homomorphic Encryption-based Deep Learning that Preserves Privacy. *International Academic Journal of Science and Engineering*, *10*(2), 153-163. https://doi.org/10.9756/IAJSE/V10I2/IAJSE1019

[20] Sharma, A., & Iyer, R. (2023). AI-powered Medical Coding: Improving Accuracy and Efficiency in Health Data Classification. *Global Journal of Medical Terminology Research and Informatics*, *1*(1), 1-4.

[21] Wilamowski, G. J. (2025). Embedded system architectures optimization for high-performance edge computing. *SCCTS Journal of Embedded Systems Design and Applications*, *2*(2), 47-55.

[22] Wu, T., Wu, F., Qiu, C., Redouté, J. M., & Yuce, M. R. (2020). A rigid-flex wearable health monitoring sensor patch for IoT-connected healthcare applications. *IEEE Internet of Things Journal*, *7*(8), 6932-6945.https://doi.org/10.1109/JIOT.2020.2977164

[23] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST)*, *10*(2), 1-19. https://doi.org/10.1145/3298981

[24] Zigui, L., Caluyo, F., Hernandez, R., Sarmiento, J., & Rosales, C. A. (2024). Improving Communication Networks to Transfer Data in Real Time for Environmental Monitoring and Data Collection. *Natural and Engineering Sciences*, *9*(2), 198-212. https://doi.org/10.28978/nesciences.1569561.

Authors Biography

Raami Riadhusin is affiliated with the Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University of Najaf, Najaf, Iraq. His academic and research interests focus on computer engineering, information technology, and applied computing systems. He contributes to advancing innovative approaches in computational methods, systems analysis, and emerging technologies within engineering education and practice.

Ahmed Hussien Ahmed is affiliated with the College of Engineering Technique, Al-Farahidi University, Baghdad, Iraq. His research interests include engineering technology, computer systems, and applied sciences, with a focus on innovative methodologies that enhance engineering education and technical problem-solving. He is actively engaged in academic research and contributes to advancing the field of engineering techniques in higher education.

P. Rajan is a Teaching assistant in the Department of Marine Engineering, bringing a remarkable blend of academic and industry expertise to the classroom. With over 31 years of sailing experience, with 2 years' workshop experience including 15 years as a 3rd Engineer, and nearly 14 years of teaching experience, he offers deep insights into marine operations and engineering. He holds a B.E. in Mechanical Engineering and a MOT Class 4 old Certificate, specializing in Marine Engineering. His teaching portfolio includes key subjects such as Marine Internal Combustion Engines and Marine Auxiliary Machinery and marine workshop including ship in campus. A member of the Institute of Marine Engineers (India).

Dr. Reema Mathew is an accomplished academic currently serving as Professor in the Computer Science and Engineering Department at Vimal Jyothi Engineering College, Chemperi, Kerala. She holds a Ph.D. in Computer Science from Kannur University, with research focused on deep learning techniques for brain tumor classification. Her academic journey includes an M.E. in Applied Electronics and a B. Tech in Electronics and Communication Engineering. With over 18 years of teaching experience, she has held multiple leadership roles and published several research papers in biomedical image processing and signal processing. She is senior IEEE member. Her interested areas for research include Image processing, AI&ML, Deep learning, IOT& Cybersecurity, Digital Forensics, and AI & Cyber security.

S.S. Sivasankari is a passionate educator and researcher, currently pursuing her Ph.D. She holds an MTech from Sathyabama University and a B.E. from Anna University, with over 10 years of teaching experience in the field of engineering education. She is presently working as a Senior Assistant Professor at New Horizon College of Engineering. Her research interests include Deep Learning and Machine Learning, where she focuses on developing intelligent and data-driven systems. She has made meaningful contributions to the academic community, with a citation count of 120 and an h-index of 4, underscoring the impact of her scholarly work.

T. Subalaxmi working as Assistant Professor in the Department of Computer Science and Engineering at K. S. Rangasamy College of Technology, Tiruchengode, India. I have graduated in B.E., Computer Science and Engineering at Amrita Institute of Technology, Coimbatore, Tamilnadu, India and secured Master of Engineering in Computer Science and Engineering at Kumaragure College of Technology, Coimbatore, Tamilnadu, India. I am Pursuing Ph.D., in Computer Science and Engineering at K. S. Rangasamy College of Technology, Tiruchengode, Tamilnadu, India. I am in teaching profession for more than 13 years. I have presented 02 papers in National and International Conferences. Her main area of interest includes Computer Networks and Network Security, Cloud Computing and Machine Learning.

Abdurakhimova Zulaykho Ikromjon Kizi is affiliated with Turan International University, Namangan, Uzbekistan. Her academic interests include education, social sciences, and sustainable development studies. She is dedicated to exploring innovative approaches in higher education, youth development, and social inclusion within the context of Uzbekistan's evolving academic landscape. Her research contributes to strengthening educational quality and promoting cross-cultural academic collaboration.