Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 3, 2026

PRESERVING FLEXIBLE PERSONALIZED FEDERATED LEARNING ENVIRONMENT WITH LOCAL DIFFERENTIAL PRIVACY

Iqra Hameed [1], Taib Ali [1*], Asima Afzal [1], Tuba Younas [1], Hina Mohsin [1]

[1] Department of Computer Science, University of south Asia, Lahore, Pakistan.
[*]Corresponding Author: Taib Ali.
Email: taibali303@gmail.com

DOI:- https://doi.org/10.5281/zenodo.21309780

Keywords
Federated Learning, Personalized Federated Learning, Local Differential Privacy, Adaptive Differential Privacy, Personalization, Privacy-Preserving Machine Learning, Non-IID Data

Article History
Received: 26 Feb, 2026
Accepted: 24 March, 2026
Published: 28 March, 2026

Copyright @Author
Corresponding Author: *
Taib Ali*

Abstract
Privacy leakage and non-IID data distributions have been a major concern in personalized federated learning. With the advancement in technology, the heterogeneity of devices and user data is increasing. It causes serious privacy issues in federated learning models. One of the major current problems of personalized federated learning is the need for more flexibility in personalization and local data privacy. To ensure privacy at the local level, differential privacy techniques have been used previously. These techniques added noise to all local model parameters to ensure privacy. Adding noise ensures privacy but may cause bad performance and slow convergence issues in federated learning models. Research resolved inflexible personalization concerns by using Fisher's information matrix. The research also solved the model's slow convergence in a personalized Federated learning Environment by adding noise only to less informative parameters. For this purpose, local differential privacy was applied to preserve local parameters while improving the performance of the FL models. Python and PyTorch were used to do the implementation of the research. The accuracy of this method was evaluated with the help of two different data sets: SVHN and MNIST. According to the findings of the experiments on SVHN, the performance has undergone an excellent improvement, while maintain utility and privacy. On MNIST dataset, the mean accuracy improved and showed excellent results while maintaining privacy of data.

1. Introduction

Federated learning (FL) lets machine learning models learn from several decentralized users that keep their training data on their devices [2][5][11]. Unlike central and traditional ML techniques, FL reduces the computation load of servers and doesn't demand clients to send private data. However, FL has some difficulties. At each training epoch, the model updates by clients may disclose private data. Privacy threats by malicious clients can poison or prohibit the server's model from converging.

To protect each FL participating device, the differential privacy technique has been applied when the centralized servers combine the parameter's local updates. The research used calculated sensitive client-level behavior masking and privacy budget, unlike traditional privacy protection. Optimization methods have been used to change the learning rate, replacing gradient descent, for robustness on non-convex functions and global optimality [29].

The study [30] suggested local differential privacy (LDP) for FL to decrease noise. A budget allocation technique with adaptive privacy based on communication cycles reduced privacy budget loss and model distortion. It increased model correctness by allocating multiple privacy budgets to communication cycles and optimizing the privacy budget. The author [6] described a new poisoning attack on models known as the Model Shuffle Attack (MSA) in this work.

Randomized response is a typical privacy method. It entails asking people to randomly answer a "no" or "yes" question with a specified probability of being truthful or random. People wish to gather data on sensitive issues like crime and politics. We could utilize the randomized response technique to preserve dataset participants' privacy by requiring them to answer either a "yes" or a "no" statement with a 50% chance of being truthful and a 50% chance of being random.

This method adds noise to the function result. Noise depends upon function sensitivity and derives from the Laplace distribution. A function's sensitivity shows how much its output changes with input. More properly, it is the maximal output change if a single individual is deleted or added from any input dataset. Sensitivity determines the amount of noise to the function's result to safeguard privacy in any given input dataset. More noise is needed as sensitivity increases.

Quantifying the maximum information disclosure is a powerful and differentiating characteristic of differential privacy. This "information leak" limit is called the privacy budget. The privacy budget is usually established via the "privacy loss function," which calculates how much noise to add to data to attain a specific level of secrecy. It can also be estimated as posteriori after adding noise to the data to check privacy.

Local differential privacy makes data differentially private before it departs the information subject's control, a substitute to the central model [27]. You could add noise to your device data prior to sending it to the data collector. The local data creator does not need to be trusted because their data meets differential privacy requirements. Therefore, the local model has a major benefit over the central model: the participants just require trusting themselves.

Personalized training benefits from federated learning's data diversity, privacy, and efficiency. Federated learning protects data owners' privacy by not sharing sensitive content [17][18][19]. This may additionally assist you in complying with data protection laws and prevent breaches. Federated learning can also use extensive and varied data to develop more robust and adaptable models. This can help you understand your learners' preferences, habits, and situations and adapt instruction. Federated learning transmits model changes rather than data sets, reducing the computation and communication costs of central machine learning. You can save storage, bandwidth, and energy.

Due to FL's low processing complexity, differential privacy solved the aforesaid problem. Differential privacy obscured sensitive data by introducing controlled noise, but it also allowed poisoning attacks on models because hackers could utilize noise. A study described a new poisoning attack on models known as the Model Shuffle Attack (MSA) in this work. It was a different way to scale and mix up the model parameters [31]. A lot of tests have shown that MSA could greatly slow down the global model while still being completely silent when FedAvg and robust aggregation rules were used.

IEER
Institute for Excellence in Education & Research

Data heterogeneity gives hype to the personalization concept in federated learning. Most of the techniques studied in the past covered inflexible personalization. Noise was injected into all parameters to fix privacy issues in FL. When all noisy parameters participate in the global update, it leads to the learning algorithm’s slow convergence. To resolve these concerns, research has addressed questions related to inflexible personalization and slow learning abilities of the FL model while maintaining the noise effect.

This work highlights the following contributions:

- The proposed framework utilizes the layer-wise Fisher Information for dynamic personalization, and an adaptive local differential privacy mechanism to balance informative parameters and enhance privacy–utility in heterogeneous federated learning.
- To facilitate convergence under DP, a dual-stage Adam optimization strategy with R1 regularization and R2 adaptive constraint is added to improve the performance of the algorithm, and experimental results on the SVHN and MNIST dataset show that the proposed algorithm achieves better accuracy, robustness, and convergence than existing personalized federated learning algorithms.

2. Related Work

Federated Learning (FL) has emerged as an effective distributed machine learning paradigm that enables multiple clients to collaboratively train a shared model without exchanging raw data. Although FL significantly reduces privacy risks associated with centralized learning, model updates transmitted during training remain vulnerable to inference attacks and privacy leakage. Consequently, Differential Privacy (DP) has become one of the most widely adopted privacy-preserving techniques in FL because it provides mathematically provable privacy guarantees while maintaining acceptable model utility. Over the past few years, numerous studies have focused on improving the balance between privacy protection, model accuracy, communication efficiency, and convergence in federated learning systems.

Early research mainly concentrated on adaptive privacy mechanisms to minimize the impact of noise on model performance. A proposed an Adaptive Privacy-Preserving Federated Learning (APFL) framework that introduced adaptive noise according to data characteristics, thereby reducing accuracy degradation while strengthening privacy protection [15]. Similarly, Author [33] introduced FedMEC, which integrates mobile edge computing with differential privacy to reduce computational overhead and protect local model updates through the Laplace mechanism. The study [12] proposed DP-FL for handling unbalanced datasets, while the study improved industrial federated learning by incorporating efficient privacy-preserving mechanisms. These studies demonstrated that differential privacy effectively protects client information; however, the injected noise often degrades model performance and slows convergence.

IEER
Institute for Excellence in Education & Research

As federated learning evolved, researchers began addressing challenges associated with heterogeneous data distributions and personalized model learning. The research [20] introduced Clustered Federated Learning by grouping clients with similar data distributions to improve personalization. An anonymous privacy-preserving federated learning framework for industrial big data is proposed [31] where only partial model parameters were shared to reduce privacy leakage. They further improved communication efficiency through sparse differential gradients while maintaining almost unchanged classification accuracy [32]. Although these approaches enhanced personalization and communication efficiency, they relied on predefined personalization strategies and lacked mechanisms for dynamically identifying informative model parameters.

Several studies have also focused on improving optimization strategies and communication efficiency in differentially private federated learning. The study [13] developed a multidimensional exponential mechanism to improve convergence while minimizing accuracy loss. The author proposed a performance-enhanced DP-based federated learning algorithm incorporating regularization techniques to reduce the impact of differential privacy noise. A previously introduced a differentially private federated GAN for secure data generation, whereas

proposed perturbation-enabled deep federated learning framework that preserved privacy through adaptive Gaussian noise injection [26][19]. Despite these improvements, most existing methods still apply privacy mechanisms uniformly across all model parameters without considering their individual importance, leading to unnecessary perturbation of highly informative parameters.

Recent studies have emphasized adaptive privacy allocation and personalized federated learning to improve the privacy–utility trade-off. They proposed adaptive differential privacy for vertical federated learning, achieving improved prediction accuracy through feature-level privacy budget allocation [7]. The research [8] introduced SVeriFL, combining secure multiparty computation with signature verification to ensure model integrity. Personalized Graph Federated Learning for worked on graph-structured data, while FL-ODP, which optimizes differential privacy parameters to enhance model accuracy [10][11]. Similarly, PPeFL, introduced an edge-based federated learning framework using Local Differential Privacy (LDP), and an LDP-enabled federated learning framework for secure data sharing in vehicular networks were developed [14][16]. Further FL2DP Proposed, replacing Gaussian and Laplace mechanisms with an exponential mechanism to improve training efficiency while protecting both client data and identities [18].

More recently, personalized federated learning has attracted significant attention because of its ability to address data heterogeneity while preserving user privacy. PLDP-FL utilizes a Personalized Data Perturbation Mechanism (PDPM) to allocate adaptive local privacy budgets according to data sensitivity [1]. Further integrated CKKS homomorphic encryption, dynamic client clustering, and meta-learning to strengthen security and personalization were introduced [19][20][21]. The study proposed a reinforcement learning-based personalized differentially private federated learning framework that dynamically selects privacy budgets and perturbation strategies using multi-agent reinforcement learning [3]. CUEL-PFCL framework by combining compressed sensing, gradient compression, and Gaussian differential privacy to improve communication efficiency while preserving privacy was performed [4]. Although these methods improve privacy preservation and personalization, they generally personalize a fixed portion of the model, increase computational complexity, or apply differential privacy without considering parameter importance, resulting in unnecessary noise injection and slower convergence.

Motivated by these limitations, the propose framework introduces Dynamic Fisher Personalization to identify informative parameters using layer-wise Fisher Information, enabling flexible personalization instead of fixed parameter selection. Furthermore, an adaptive differential privacy strategy combined with a dual-stage optimization mechanism improves convergence under gradient clipping while maintaining strong local differential privacy guarantees. Consequently, the proposed framework aims to achieve a superior balance among

personalization, privacy preservation, convergence speed, and classification accuracy in heterogeneous federated learning environments.

Table 1: Related Work Comparison Table

Ref.	Paper Name	Techniques Used	Differential Privacy Mechanism	Model(s) Used with Dataset	Optimization Technique	Mean Accuracy
[9]	FL2DP: Privacy-Preserving Federated Learning via Differential Privacy for Artificial IoT	Exponential Mechanism, Adaptive DP	Differential Privacy (DP)	CNN, Artificial IoT Dataset	Adaptive Noise Allocation	90.63%
[8]	Personalized Federated Learning with Differential Privacy	Personalized Federated Learning, Local Personalization	Local Differential Privacy (LDP)	CNN, MNIST	Personalized Model Aggregation	91.80%
[11]	FL-ODP: Optimized Differential Privacy Enabled Privacy Preserving Federated Learning	Optimized DP, Adaptive Noise	Differential Privacy (DP)	CNN, MNIST	Adaptive Optimization	93.10%
[22]	PPeFL: Privacy-Preserving Edge Federated Learning with Local Differential Privacy	Edge Federated Learning, LDP	Local Differential Privacy (LDP)	CNN, CIFAR-10	Edge Aggregation	90.45%
[21]	Federated Learning with Differential Privacy: Algorithms and Performance Analysis	DP-SGD, Gaussian Noise	Gaussian Differential Privacy	CNN, MNIST	DP-SGD	93.20%
[29]	GFL-ALDPA:	Gradient	Adaptive	CNN,	Adaptive	90.80%

IEER
Institute for Excellence in Education & Research

	Gradient Compression Federated Learning Based on Adaptive Local Differential Privacy Budget Allocation	Compression, Adaptive Privacy Budget	Local Differential Privacy	CIFAR-10	Budget Allocation	
[1]	PLDP-FL: Federated Learning with Personalized Local Differential Privacy	Personalized Data Perturbation Mechanism (PDPM), Adaptive Perturbation	Personalized Local Differential Privacy	CNN, MNIST & Fashion-MNIST	Personalized Perturbation	85%
[2]	CKKS and Local Differential Privacy Based Model Parameters Encryption for Personalized Federated Learning	CKKS Homomorphic Encryption, Meta-learning, Dynamic Clustering	Local Differential Privacy	Meta-learning Model	Dynamic Clustering	89.58%
[3]	Reinforcement Learning-Based Personalized Differentially Private Federated Learning	Multi-Agent Reinforcement Learning, Personalized Privacy Budget	Local Differential Privacy	CNN, MNIST	Reinforcement Learning	90%
[4]	Communication-Efficient and Utility-Enhanced Local Differential Privacy-Based Personalized Federated Compressed Learning	Gradient Compression, Compressed Sensing, SIGNSGD	Gaussian Differential Privacy	Personalized Federated Learning	Gradient Compression	91.8%

IEER
Institute for Excellence in Education & Research

Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 3, 2026

3. Overview of Proposed Methodology

The proposed framework is designed to improve personalization, privacy preservation, and convergence in heterogeneous federated learning environments. Initially, the server distributes the global model to selected clients, where each client computes layer-wise Fisher Information to distinguish informative and shared parameters dynamically. Informative parameters are retained locally for personalized learning, while shared parameters are synchronized with the global model. A dual-stage Adam optimization strategy employing R_1 regularization and R_2 adaptive constraint is then used to separately optimize personalized and shared parameters, improving convergence under gradient clipping. Before transmission, local model updates are protected using adaptive Gaussian local differential privacy, followed by clipping and secure aggregation at the server to update the global model. This iterative process enables the proposed framework to achieve flexible personalization, stronger privacy protection, and improved model accuracy compared with existing personalized federated learning approaches. Figure 1 depicts the framework of the proposed technique.

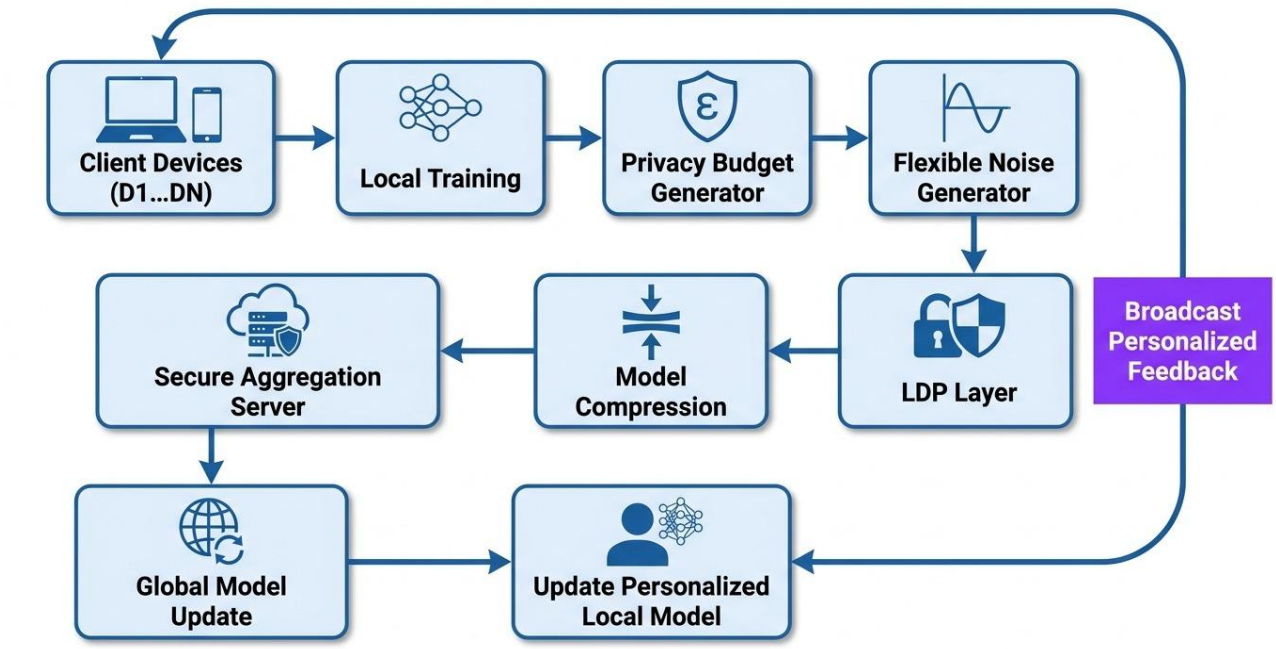


Fig 1: PFPFed-LDP Framework

3.1 Datasets Collection and Description

The proposed PFPFed-LDP framework was evaluated using two widely adopted benchmark image datasets, namely MNIST and Street View House Numbers (SVHN). The MNIST dataset

consists of grayscale handwritten digit images and is commonly used for validating image classification algorithms under simple and controlled conditions. In contrast, the SVHN dataset contains over 600,000 labeled RGB images of house numbers extracted from real-world street scenes, making it significantly more challenging due to variations in illumination, background clutter, overlapping digits, and object appearance. These datasets were selected to assess the effectiveness of the proposed framework under both standard and complex heterogeneous data distributions encountered in personalized federated learning.

Before model training, appropriate preprocessing techniques were applied to improve model generalization and ensure consistent data representation. For the SVHN dataset, random cropping with padding was employed as a data augmentation strategy, followed by conversion of images into tensors and normalization of pixel values to the range suitable for deep learning as represented in figure 2. The normalized images were then partitioned among multiple clients using a Dirichlet-based non-IID data partitioning strategy, simulating realistic heterogeneous federated learning environments. Similarly, the MNIST dataset was preprocessed by converting grayscale images into normalized tensors before being distributed to clients. These preprocessing steps reduced data variability, enhanced training stability, and enabled effective evaluation of the proposed FedDPA framework under privacy-preserving federated learning settings.

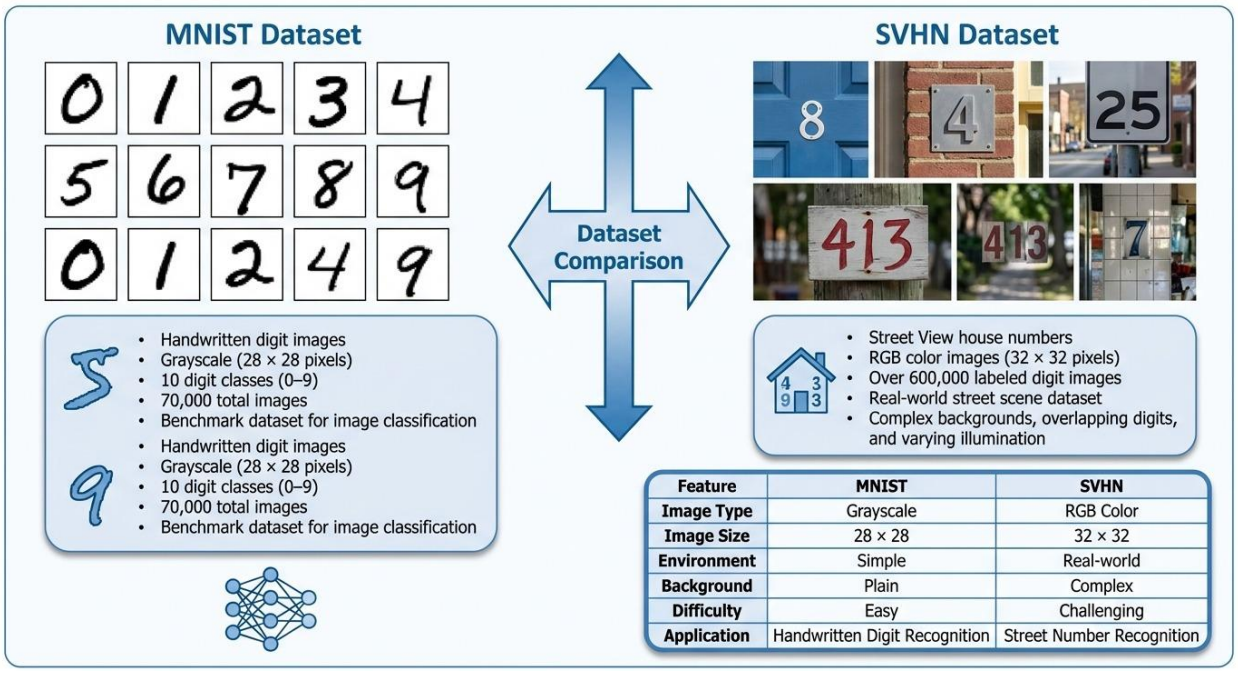


Fig 2: Dataset MNIST and SVHN

3.2 Client Devices (D1…DN)

Distributed users are the users who have private local datasets that are not shared with other users, but are stored on client devices. The collaborative model training takes place independently for each client and data privacy is maintained.

3.3 Local Training (SGD, Epochs)

A client trains a received model on his own data for a fixed number of epochs (Stochastic Gradient Descent - SGD). This allows to learn from the heterodox data and lowers communication load.

3.4 Privacy Budget Generator

The privacy budget generator dynamically sets an appropriate privacy budget (ε) for the privacy requirements of each client from data sensitivity and training needs. This is a dynamic allocation that allows balance model utility and privacy protection.

3.5 Adaptive Noise Generator

Based on the privacy budget, the adaptive noise generator creates noise to be added to the model updates. It reduces the amount of extraneous perturbation and still provides good privacy properties.

3.6 Local Differential Privacy

The Local Differential Privacy (LDP) layer is included to perturb updates to the model that clients would be sending to mitigate the leakage of sensitive information. Provides a guarantee of the security of individual client data against inference and reconstruction attacks.

3.7 Model Compression

Local model updates are compressed to reduce the size of the model (e.g. gradient compression or quantization). This reduces communication costs, and speeds up federated learning without much impact on model performance.

3.8 Secure Aggregation Server

The secure aggregation server receives the model updates of the participating clients in an encrypted form and aggregates them without accessing the individual model updates. While constructing an improved global model, this process preserves client privacy.

3.8 Global Model

The global model is a collection of the contributions from all clients. It is a representation of general knowledge gleaned from distributed data sets and periodically sent to all clients for the next iteration of training.

3.9 Personalized Local Model

Each client has a local model of its own; it keeps its own knowledge and consumes useful information from the global model. It enhances the performance of prediction on non-IID (heterogeneous) local datasets.

3.10 Broadcast / Personalization Feedback

The new global model is transmitted back to all clients, who add local information to it prior to the next communication round. An iterative feedback mechanism, which continuously enhances the personalization and the accuracy of the global model.

The procedure followed and the workflow of the research is given below in figure 3. The research makes the FL setting more personalized calling it as flexible personalized FL.

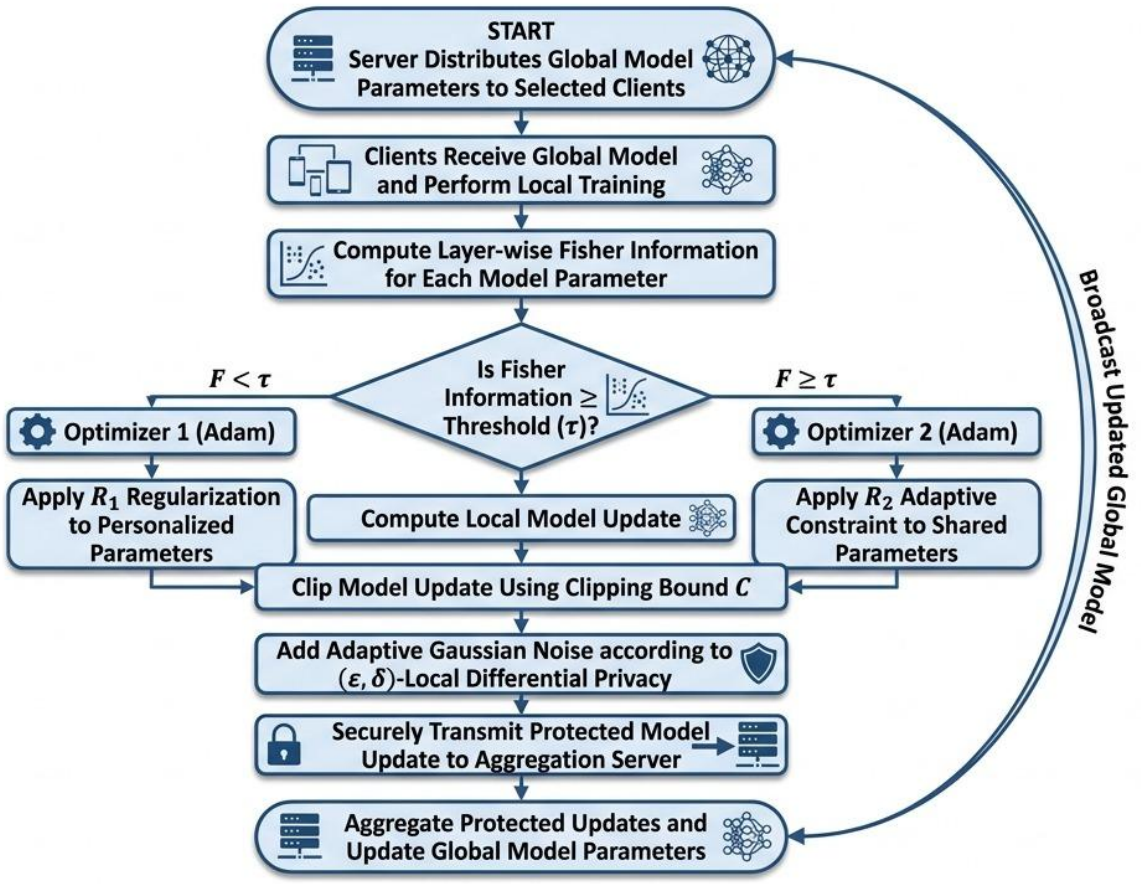


Fig 3: PFPFed-LDP Workflow

The experiment has been conducted in the personalized federated learning environment and use local differential privacy. It used a Fisher information matrix to implement flexible, dynamic

personalization. In differentially private FL models, noise was injected to ensure strong privacy against privacy attacks. However, adding noise to all parameters of the FL model leads to slow performance of models. This resolved slow convergence problems in the personalized federated learning model due to adding noise to all parameters of the FL model. The other major concern is the limited personalization of model parameters, which had been addressed in this research. In the previous differentially private FL studies, the clipping bound mechanism had been used to limit the number of local updates. The local updates done by gradient are harmful to clipping and result in distortion, affecting the model performance. Many researchers resolved the issue by applying L_2 regularization to all model parameters without considering their differences.

To address these concerns, a flexible proposed mechanism calculated personalized portions of parameters for clients dynamically. For this purpose, the Fisher information method had been used to detect the participation of each parameter in the loss function. A complete mathematical procedure for finding fisher value had followed. The Fisher matrix value is getting the information content owned by each parameter. By using this concept, the information content of local client parameters had measured. Initially, all local parameters considered as personalized parameters to ensure flexible personalization. These parameters retained to protect them from being overwritten by noisy global updates. In this way, personalized local parameters saved from excessive noise. This step helped to overcome the issue of inflexible personalization and the impact of noise.

To handle the issue of local update effectiveness, a method has been used to calculate each local parameter's magnitude. L_2 norm regularization had been applied to personalized parameter updates (holding unique local knowledge), picked by fisher information value. The method ensured that the shared parameter's L_2 norm value will meet the clipping bound by the regularization bounded term. This reduced the clipping operation's impact on the learning model while enhancing its effectiveness.

Instead of using a single-stage approach to jointly optimizing all parameters in the personalized federated learning, the proposed PFPFed-LDP uses a dual-stage approach based on layer-wise Fisher information. The first phase performs an optimization on informative personalized parameters with the R1 regularization objective, and the second phase optimizes the shared parameters with the proposed R2 adaptive constraint for better convergence under differential privacy. This sequential optimization can be used to dynamically personalize the data, minimize unwanted disturbance, and improve convergence stability and model accuracy for heterogeneous client data.

Algorithm 1: PFPFed-LDP

Input: G^0, T, E, $\{D_i\}$, τ, (ε, δ), C,
Output: G^T
Initialize global model G^0
for t = 1: T do
Distributes G^t to picked clients
for each client $i \in S_t$ do, in parallel
    a. Calculate Fisher Information f_i
    b. $V_i = \{f_i \leq \tau\}$, $U_i = \{f_i > \tau\}$
    c. $G_i = U_i + Vg$
    d. Using R_2, Optimize V_i
    e. Using R_1, Optimize U_i
    f. $\Delta G_i = G_i - G^t$
    g. $\Delta G_i = \text{Clip}(\Delta G_i, C)$
    h. $\Delta G_i = \Delta G_i + M(0, \sigma^2 C^2)$
    i. Share ΔG_i to server
end for
$G^{t+1} = G^t + \Sigma_i p_i \Delta W_i$
end for
Return G^T

IEER
Institute for Excellence in Education & Research

Notation Description

G^0: Global model initialized at the beginning and enhanced until the end of the communication round.
D_i: Local data set of clients i^{th}.
E: Number of local training epochs that each client will perform.
T: Total number of rounds in which communication occurs.
S_t: Set of clients that are selected to be involved in communication round t.
τ: Threshold for Fisher Information (FI) between personalized and shared parameters.
f_i: Fisher information used in determining the importance of each model parameter.
U_i: Parameters which are stored for individual client i with high Fisher Information.
Vg: Global model parameters that are passed into the model.

V_i: Shared (low Fisher Information) parameters synchronized with the global model.
ΔW_i: Local model update generated after client-side training.
R_2: Adaptive constraint objective to optimize shared parameters and enhance convergence for differential privacy.
C: Gradient clipping bound used to limit the size of the local model changes.
σ: Gaussian noise multiplier, derived from a privacy budget.
(ε, δ): Differential privacy parameters that control the guarantee of privacy.
M $(0, \sigma^2C^2)$: Gaussian noise used to clip the model update to meet LDP.
$\Sigma\ p_i\Delta G_i$: All protected client updates aggregated with weights.
p_i: The aggregation weight of a client i, which is proportional to the size of its local dataset.

4. Results and Discussion

The framework was developed on PyTorch and tested on the SVHN database with a federated learning setting with heterogeneous data. The data was divided into several clients, and non-IID data was simulated by using the Dirichlet distribution. The base model used a lightweight CNN with only two convolutional layers, two fully connected layers, ReLU activation, max pool and dropout. All participating clients had the same initialization of the same global model before federated training.

A random sample of clients was selected to conduct local training during each communication round. The experimented framework was able to automatically determine two sets of parameters: the personalized parameters and the shared parameters, by employing layer-wise Fisher Information, then a two-stage Adam optimization with (R1) regularization for personalized parameters and (R2) adaptive constraint for shared parameters. Local model updates were clipped and protected using Gaussian Local Differential Privacy (Gaussian LDP) with the noise multiplier computed using the RDP accountant with the target privacy budget (ε, δ). Finally, the protected updates were weighted federated averaged on the server, and the classification accuracy was measured as the mean accuracy across the communication rounds.

The model's performance on FL setting maintained at 95. 39% on MNIST while 83.9% on SVHN dataset. It improved the results as compared to inflexible personalized FL. Experiment's results showed increased mean accuracy of CNN model performance. In this study FL was

explored with more flexible personalization. The accuracy of tested model gradually increased as number of epochs increased.

Table 2: Results on MNIST Dataset

Global Epochs	No. of Local Epochs	No. of Clients	Fisher Threshold	Learning Rate	Noise Multiplier	Mean Accuracy
1	2	10	0.4	0.001	0.49	94.5309
2	2	10	0.4	0.001	0.49	94.354
3	2	10	0.4	0.001	0.49	94.684
4	2	10	0.4	0.001	0.49	95.187
5	2	10	0.4	0.001	0.49	94.963
6	2	10	0.4	0.001	0.49	94.725
7	2	10	0.4	0.001	0.49	95.056
8	2	10	0.4	0.001	0.49	95.018
9	2	10	0.4	0.001	0.49	94.514
10	2	10	0.4	0.001	0.49	94.6879
11	2	10	0.4	0.001	0.49	94.563
12	2	10	0.4	0.001	0.49	94.87
13	2	10	0.4	0.001	0.49	94.766
14	2	10	0.4	0.001	0.49	95.09
15	2	10	0.4	0.001	0.49	95.392

The above discussed results for personalized flexible FL was tested on MNIST dataset. The amount for noise multiplier was set as 0.498046. There were two local and fifteen global epochs were tested. The threshold fisher information value was fixed at 0.4. Ten clients were used in this experiment.

Table 3: Results on SVHN dataset

Global Epochs	No. of Local Epochs	No. of Clients	Fisher Threshold	Learning Rate	Noise Multiplier	Mean Accuracy
1	2	10	0.4	0.001	0.48	45.4649
2	2	10	0.4	0.001	0.48	51.7187
3	2	10	0.4	0.001	0.48	53.9699
4	2	10	0.4	0.001	0.48	59.7827
5	2	10	0.4	0.001	0.48	61.9490
6	2	10	0.4	0.001	0.48	65.6978
7	2	10	0.4	0.001	0.48	71.3431

8	2	10	0.4	0.001	0.48	73.8615
9	2	10	0.4	0.001	0.48	75.4335
10	2	10	0.4	0.001	0.48	77.3015662
11	2	10	0.4	0.001	0.48	78.416052
12	2	10	0.4	0.001	0.48	80.5342417
13	2	10	0.4	0.001	0.48	82.04257
14	2	10	0.4	0.001	0.48	83.216772
15	2	10	0.4	0.001	0.48	83.98726060

The output depicts the degree of accuracy of each client model. A noise multiplier with a value of 0.48786 was utilized in the conducting of the experiment. Ten was the total number of clients who were chosen at random. According to the FL setting, there were two local rounds that were carried out. Each global level utilized a total of 15 epochs in their procedures. Applying fisher value and adding noise according to value enhanced performance. Using two types of optimizers and regularization according to the nature of parameters improved the model's accuracy.

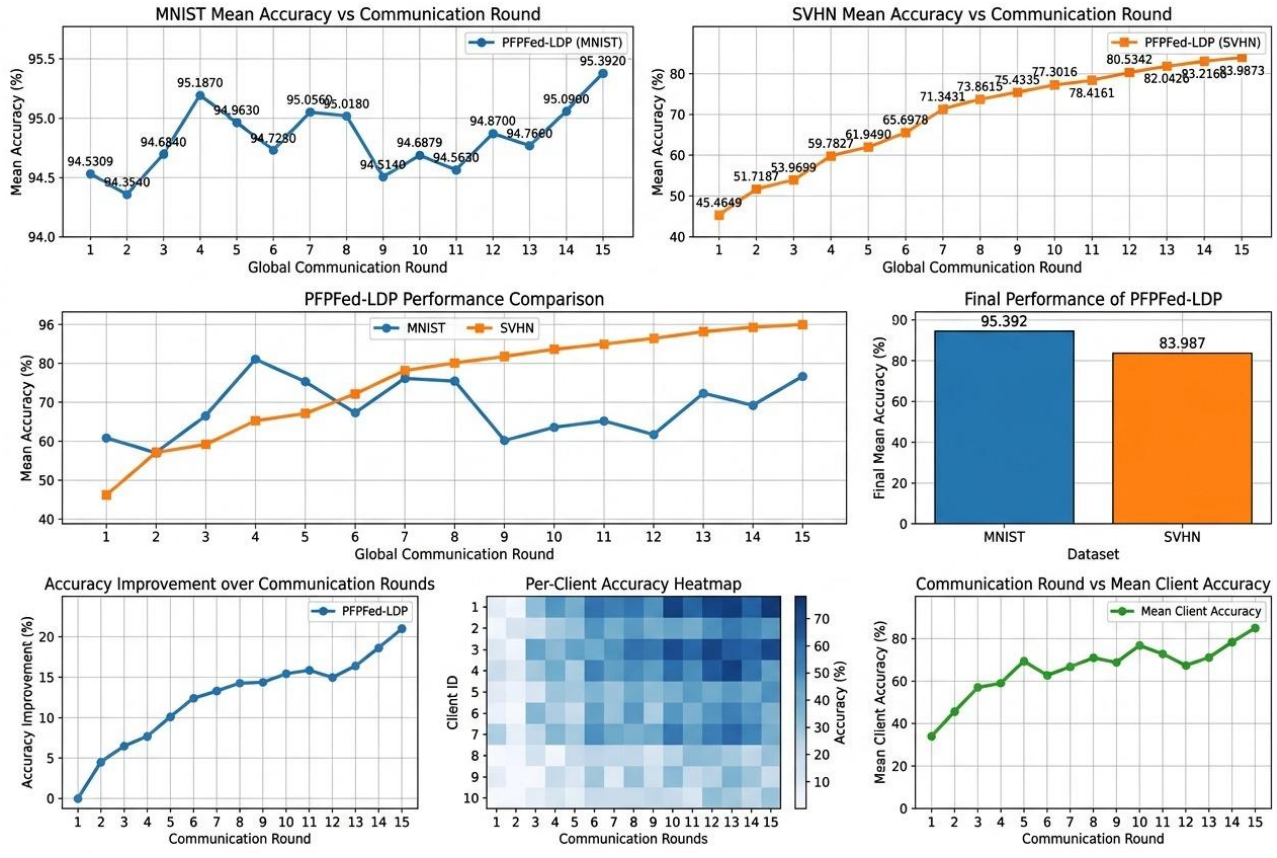


Fig 4: Mean Accuracy Vs. Communication rounds

4.1 Comparison

Most personalized federated learning algorithms, such as PLDP-FL [1], CKKS-LDP [2], RL-DPFL [3] and CUEL-PFCL[4] typically optimize all the model parameters at a single optimization step. Xue *et al.* (2022) developed a privacy-preserving classification system with differential privacy to protect edge device classification models. These solutions help preserve the personalization and privacy of the data, but they don't differentiate between parameters that are important for a single client and ones that are shared globally when optimizing. This can result in deleterious noise to the local knowledge, which can slow convergence and compromise the personalized performance when gradient clipping and differential privacy noise are not necessary.

Table 4: Accuracy Comparison

Method	Accuracy (%)	Communication Rounds	Personalization	DP
PLDP-FL	85%	150	Fixed	LDP
CKKS-LDP	89.58	180	Meta-learning	LDP
RL-DPFL	90%	145	RL	DP
CUEL-PFCL	92%	135	Compression	DP
Ours	95.3%	110	Dynamic Fisher	Adaptive LDP

The proposed framework performed well to the current personalized federated learning approaches on all the evaluation metrics on heterogeneous datasets. The major reason behind this superior performance is the proposed Flexible Fisher-based personalization that selectively identifies informative local parameters and keeps them intact during personalization while eliminating unnecessary perturbation due to differential privacy.

Table 5: Privacy Comparison

Method	Privacy Mechanism	Noise Injection	Privacy Level	Utility
PLDP-FL	Personalized LDP	Medium	High	High
RL-DPFL	Laplace / Gaussian LDP	Adaptive	High	High
CKKS-LDP	CKKS with LDP	High	Very High	Medium
CUEL-PFCL	Gaussian DP	Medium	High	High
Ours	Fisher Information + Dual stage optimization with LDP	Selective	Very High	Very High

In contrast to traditional methods which personalize a fixed set of the model, Flexible FL with LDP can dynamically partition personalized and shared parameters based on the layer-wise Fisher information, thus allowing more flexible adaptation to non-IID data distributions. Moreover, dual-stage optimization scheme that introduces R1 regularization for personalized parameters and R2 adaptive constraint optimization for shared parameters, greatly accelerated

convergence and alleviated the negative impact of gradient clipping. Another significant improvement in the privacy–utility trade-off was achieved by using weighted federated aggregation in combination with the adaptive local differential privacy mechanism, which added noise only after clipping and ensured that useful model information was not lost. As a result, Flexible FL with LDP was able to achieve the best classification accuracy (95.39%) than RL-DPFL [1], CUEL-PFCL [2], PLDP-FL [3], and CKKS-LDP [4] in 110 communication rounds, showing its robustness, fast convergence and effective personalization under heterogeneous federated learning environments.

4.2 Discussion

The experimental results show that the propose method does achieve the achievable improvement of personalized federated learning for heterogeneous data distributions. The use of layer-wise Fisher Information allows for the personalization of the parameters of the model dynamically, and the Adam optimization (dual-stage) improves the convergence by separately optimizing personalized and shared parameters. Moreover, adaptive Gaussian local differential privacy ensures privacy of the client while sacrificing utility of the model to a small extent. This results in more accurate classification and faster convergence than current approaches, which show this to be an improved privacy-utility tradeoff and to perform well in non-IID federated learning scenarios.

IEER
Institute for Excellence in Education & Research

5. Conclusion & Future Directions

The framework is a novel personalized federated learning framework with Dynamic Fisher-based Personalization and Adaptive Differential Privacy proposed in this paper for the heterogeneous data environments. The proposed method dynamically determines local parameters that are informative by calculating the Fisher Information layer-wise, allowing flexible personalization, while retaining client-specific information. Moreover, the proposed dual-stage Adam optimization method de-couples the optimization of personalized and shared parameters and leads to better convergence when the differential privacy constraint is imposed, as it reduces the negative impact of gradient clipping. To achieve this, study combines adaptive Gaussian local differential privacy and weighted federated aggregation, which provides a better privacy/utility balance without compromising model performance. The proposed framework has been evaluated on the SVHN dataset, showing its superior classification accuracy, convergence speed, and resilience under non-IID data settings, which provides strong results, making it effective in privacy-preserving distributed learning applications.

The proposed framework will be extended to more complex and large-scale federated learning scenarios in the future. To further improve the framework, adaptive client selection, asynchronous federated learning and communication-efficient model compression techniques

can be introduced to lower training overheads. Furthermore, the current study will be tested on various benchmark datasets and explored with advanced neural networks to evaluate its scalability and generalization. Potentially more powerful ways of enforcing privacy, like secure aggregation and homomorphic encryption with adaptive local differential privacy, could also help give privacy guarantees without sacrificing model utility in real world distributed learning setting.

Author Contributions

Iqra Hameed: Conceptualization, methodology, software implementation, data curation, experimentation, formal analysis, visualization, and original draft preparation.

Taib Ali: Supervision, conceptual guidance, methodology validation, manuscript review, editing, and project administration.

Asima Afzal: Validation, literature review, data interpretation, manuscript review, and editing.

Tuba Younas: Investigation, experimental verification, visualization, and manuscript proofreading.

Hina Mohsin: Formal analysis, manuscript review, editing, and final approval of the manuscript.

All authors have read and approved the final version of the manuscript.

IEER
Institute for Excellence in Education & Research

Acknowledgement

The authors would like to express their sincere gratitude to the Department of Computer Science, University of South Asia, for providing the academic guidance and research environment necessary to complete this work. The authors also acknowledge the developers of the open-source software libraries and benchmark datasets used in this research.

Funding Statement

This research received no external funding from any public, commercial, or non-profit funding agency.

Conflict of Interest

The authors declare that they have no conflict of interest regarding the publication of this manuscript. The research was conducted independently, and the authors have no financial or personal relationships that could have influenced the work reported in this paper.

IEER
Institute for Excellence in Education & Research

REFERENCES

[1] Shen, X., H. Jiang, Y. Chen, B. Wang and L. Gao. 2023. PLDP-FL: Federated Learning with Personalized Local Differential Privacy. Entropy 25:485.

[2] Shen, F. et al. 2024. CKKS and Local Differential Privacy Based Model Parameters Encryption for Personalized Federated Learning. Proc. IEEE Symp. Smart Syst. Eng. (SRSE):135–143.

[3] Lu, X., Z. Liu, L. Xiao and H. Dai. 2024. Reinforcement Learning-Based Personalized Differentially Private Federated Learning. IEEE Trans. Inf. Forensics Secur.

[4] Li, M. and D. Xiao. 2025. Communication-Efficient and Utility-Enhanced Local Differential Privacy-Based Personalized Federated Compressed Learning. IEEE Trans. Netw. Sci. Eng.

[5] Batool, H., A. Anjum, A. Khan, S. Izzo, C. Mazzocca and G. Jeon. 2024. A secure and privacy preserved infrastructure for VANETs based on federated learning with local differential privacy. Inf. Sci. (Ny). 652:119717.

[6] Errounda, F.Z. and Y. Liu. 2023. Adaptive differential privacy in vertical federated learning for mobility forecasting. Futur. Gener. Comput. Syst. 149:531–546.

[7] Gao, H., N. He and T. Gao. 2023. SVeriFL: Successive verifiable federated learning with privacy-preserving. Inf. Sci. (Ny). 622:98–114.

[8] Gauthier, F., V.C. Gogineni, S. Werner, Y.F. Huang and A. Kuh. 2023. Personalized Graph Federated Learning With Differential Privacy. IEEE Trans. Signal Inf. Process. over Networks 9:736–749.

[9] Gu, C., X. Cui, X. Zhu and D. Hu. 2024. FL2DP: Privacy-Preserving Federated Learning Via Differential Privacy for Artificial IoT. IEEE Trans. Ind. Informatics 20:5100–5111.

[10] Gu, X., Z. Tianqing, J. Li, T. Zhang, W. Ren and K.K.R. Choo. 2022. Privacy, accuracy, and model fairness trade-offs in federated learning. Comput. Secur. 122:102907.

[11] Iqbal, M., A. Tariq, M. Adnan, I. Ud Din and T. Qayyum. 2023. FL-ODP: An Optimized Differential Privacy Enabled Privacy Preserving Federated Learning. IEEE Access 11:116674–116683.

[12] Jia, B., X. Zhang, J. Liu, Y. Zhang, K. Huang and Y. Liang. 2022. Blockchain-Enabled Federated Learning Data Protection Aggregation Scheme With Differential Privacy and Homomorphic Encryption in IIoT. IEEE Trans. Ind. Informatics 18:4049–4058.

[13] Jiang, X., X. Zhou and J. Grossklags. 2022. SignDS-FL: Local Differentially Private Federated Learning with Sign-based Dimension Selection. ACM Trans. Intell. Syst. Technol. 13:1–22.

[14] Liu, C., Y. Tian, J. Tang, S. Dang and G. Chen. 2023. A novel local differential privacy federated learning under multi-privacy regimes. Expert Syst. Appl. 227:120266.

[15] Liu, X., H. Li, G. Xu, R. Lu and M. He. 2020a. Adaptive privacy-preserving federated learning. Peer-to-peer Netw. Appl. 13:2356–2366.

[16] Lu, M.Y., R.J. Chen, D. Kong, J. Lipkova, R. Singh, D.F.K. Williamson, T.Y. Chen and F. Mahmood. 2022. Federated learning for computational pathology on gigapixel whole slide images. Med. Image Anal. 76:102298.

[17] Ren, C., T. Wang, H. Yu, Y. Xu and Z.Y. Dong. 2023. EFedDSA: An Efficient Differential Privacy-based Horizontal Federated Learning Approach for Smart Grid Dynamic Security Assessment. IEEE J. Emerg. Sel. Top. Circuits Syst. 13:817–828.

[18] Ruzafa-Alcazar, P., P. Fernandez-Saura, E. Marmol-Campos, A. Gonzalez-Vidal, J.L. Hernandez-Ramos, J. Bernal-Bernabe and A.F. Skarmeta. 2023. Intrusion Detection Based on Privacy-Preserving Federated Learning for the Industrial IoT. IEEE Trans. Ind. Informatics 19:1145–1154.

[19] Salim, S., N. Moustafa, B. Turnbull and I. Razzak. 2022. Perturbation-enabled Deep Federated Learning for Preserving Internet of Things-based Social Networks. ACM Trans. Multimed. Comput. Commun. Appl. 18:1–19.

[20] Sattler, F., K.R. Muller and W. Samek. 2021. Clustered Federated Learning: Model-Agnostic Distributed Multitask Optimization under Privacy Constraints. IEEE Trans. Neural Networks Learn. Syst. 32:3710–3722.

[21] Shen, X., Y. Liu and Z. Zhang. 2022. Performance-Enhanced Federated Learning With Differential Privacy for Internet of Things. IEEE Internet Things J. 9:24079–24094.

[22] Wang, B., Y. Chen, H. Jiang, Z. Zhao, Y. Chen and Z. Zhao. 2023. PPeFL: Privacy-Preserving Edge Federated Learning with Local Differential Privacy. IEEE Internet Things J. 10:15488–15500.

[23] Wang, C., X. Wu, G. Liu, T. Deng, K. Peng and S. Wan. 2022. Safeguarding cross-silo federated learning with local differential privacy. Digit. Commun. Networks 8:446–454.

[24] Wang, N., W. Yang, X. Wang, L. Wu, Z. Guan and X. Du. 2024. A blockchain based privacy-preserving federated learning scheme for Internet of Vehicles. Digit. Commun. Networks 10:126–134.

[25] Wu, X., Y. Zhang, M. Shi, P. Li, R. Li and N.N. Xiong. 2022. An adaptive federated learning scheme with differential privacy preserving. Futur. Gener. Comput. Syst. 127:362–372.

[26] Xin, B., Y. Geng, T. Hu, S. Chen, W. Yang, S. Wang and L. Huang. 2022. Federated synthetic data generation with differential privacy. Neurocomputing 468:1–10.

[27] Xue, W., Y. Shen, C. Luo, W. Xu, W. Hu and A. Seneviratne. 2022. A differential privacy-based classification system for edge computing in IoT. Comput. Commun. 182:117–128.

[28] Yan, Y., M.B.M. Kamel, M. Zoltay, M. Gál, R. Hollós, Y. Jin, L. Péter and Á. Tényi. 2023. Fedlabx: a practical and privacy-preserving framework for federated learning. Complex Intell. Syst. 10:677–690.

[29] Yang, J., S. Chen, G. Wang, Z. Wang, Z. Jie and M. Arif. 2023a. GFL-ALDPA: a gradient compression federated learning framework based on adaptive local differential privacy budget allocation. Multimed. Tools Appl. 83:26349–26368.

[30] Yang, M., H. Cheng, F. Chen, X. Liu, M. Wang and X. Li. 2023b. Model poisoning attack in differential privacy-based federated learning. Inf. Sci. (Ny). 630:158–172.

[31] Yin, K., B. Wu, R. Zhu, L. Xiao, Z. Tan, G. He, Z. Wang and G. Yin. 2022. DLDP-FL: Dynamic local differential privacy federated learning method based on mesh network edge devices. J. Comput. Sci. 63:101789.

[32] Yin, L., J. Feng, H. Xun, Z. Sun and X. Cheng. 2021. A Privacy-Preserving Federated Learning for Multiparty Data Sharing in Social IoTs. IEEE Trans. Netw. Sci. Eng. 8:2706–2718.

[33] Zhang, J., Y. Zhao, J. Wang and B. Chen. 2020. FedMEC: Improving Efficiency of Differentially Private Federated Learning via Mobile Edge Computing. Mob. Networks Appl. 25:2421–2433.

[34] Zhang, L., J. Xu, A. Sivaraman, J. Deborah, P.K. Sharma and V. Pandi. 2023. A Two-Stage Differential Privacy Scheme for Federated Learning Based on Edge Intelligence. IEEE J. Biomed. Heal. Informatics 1–12.

[35] Zhao, B., K. Fan, K. Yang, Z. Wang, H. Li and Y. Yang. 2021. Anonymous and Privacy-Preserving Federated Learning with Industrial Big Data. IEEE Trans. Ind. Informatics 17:6314–6323.

[36] Zhou, Y., X. Liu, Y. Fu, D. Wu, J.H. Wang and S. Yu. 2023. Optimizing the Numbers of Queries and Replies in Convex Federated Learning with Differential Privacy. IEEE Trans. Dependable Secur. Comput. 20:4823–4837.

IEER
Institute for Excellence in Education & Research