International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

An Enhanced Privacy-Preserving Personalized Federated Learning Framework for Image Data Using a Simulated Environment

B. Gayathri[1], P.N.V. Vamsi Lala[2]

[1]*MCA Student, Department of Master of Computer Applications, Vignan Lara Institute of Technology and Sciences, Guntur, Andhra Pradesh, India*

[2]*Assistant Professor, Department of Computer Science and Engineering, Vignan Lara Institute of Technology and Sciences, Guntur, Andhra Pradesh, India*

***Abstract*--Federated Federated Learning (FL) allows multiple users or devices to train a machine learning model together without sharing their actual data, which helps in maintaining privacy. However, existing FL approaches still face some important challenges such as possible privacy leakage, differences in data distribution across users, and lack of personalization in the final model.**

In this work, we implement a Privacy-Preserving and Personalized Federated Learning (PPFed) framework for image classification in a simulated environmentIn this approach, the model is divided into two parts. One part is shared among all the clients, while the other part is kept private for each individual client. This allowed the model to learn patterns from all image of dataset, and at the same time adjust itself based on the data available at each client. To make the system more secure, a small amount of noise is added to the model updates before sending them to the server, so that sensitive information cannot be easily inferred. The model is tested on these image datasets like CIFAR-10 and MNIST, with non-IID data distribution among clients. The are results show an accuracy of 93.8% on CIFAR-10 and 99.08% on MNIST. From these results, it is observed that adding privacy mechanisms does not significantly reduce the performance. Overall, the combination of personalization and privacy helps in building a more reliable and practical federated learning system.

***Keywords*— CIFAR-10, Deep Learning, Differential Privacy, Federated Learning, Image Data, Privacy Preservation**

I. INTRODUCTION

A. Research Problem and Significance

In recent years, distributed machine learning has grown rapidly, and federated learning has become an important approach for handling privacy-sensitive data, especially in image-based applications.

The Reality of Federated Learning The big selling point of federated learning is that it lets multiple clients build a model together without ever actually handing over their raw data. On paper, it's a privacy dream. But in practice? It’s not quite the "silver bullet" people hope for.

Even with those built-in safeguards, privacy leakage is still a massive headache. It turns out that clever observers can sometimes reverse-engineer sensitive info just by looking at the model updates being sent back and forth. Then there’s the sheer messiness of real-world data. We call it the non-IID problem, but basically, it just means that everyone’s data is different and totally uneven. Since no two users behave exactly the same way, we’re often left with a fragmented mess of data. This inconsistency makes it for all clients. In addition, most traditional approaches do not focus much on personalization, which leads to reduced performance for individual users.

These problems become more serious in image-based systems, where data is both complex and sensitive. For example, in domains like healthcare or visual recognition, even small privacy leaks can be critical. Because of this, there is a need for a better approach that can handle data differences across clients, support personalization, and also ensure strong privacy protection. Developing such a system can improve both model performance and data security in practical federated incredibly difficult to train a single model that actually performs well across the board This makes it difficult for a single global model to perform well learning environments.

B. Context and Background

Federated learning is a distributed learning approach where multiple clients work together to train a shared model without sending their raw data to a central server. This makes it very useful in areas like healthcare, medical imaging, and personalized applications, where data privacy is important and centralized data collection is not always possible.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

At the same time, deep learning techniques, especially Convolutional Neural Networks (CNNs), have shown excellent performance in image classification and recognition tasks. Combining federated learning with such models can be very powerful, but there are still some limitations.

Most existing federated learning methods focus on learning a single global model, which may not work well when client data is highly different (non-IID). Also, sharing full model updates can sometimes lead to privacy risks through gradient-based attacks. Because of these issues, recent research has started focusing on combining privacy protection with personalization in federated learning.

Based on these challenges, this work proposes an improved privacy-preserving personalized federated learning framework for image data in a simulated environment. The approach builds on the PPFed architecture and introduces personalization along with differential privacy to improve model performance, handle non-IID data more effectively, and reduce the risk of information leakage.

II. Literature Survey

In recent years, there have been notable advancements in the fields of federated learning and privacy-preserving distributed machine learning. Federated learning was initially conceptualized to facilitate collaborative model training without the exchange of raw client data, thereby mitigating privacy risks. However, early frameworks predominantly concentrated on developing a single global model and did not sufficiently address issues related to personalization and privacy leakage. In [1], a privacy-preserving personalized federated learning framework incorporating differential privacy and convergence guarantees was proposed. This study demonstrated that the introduction of calibrated noise to model updates can effectively safeguard sensitive information while ensuring convergence stability. In [2], a federated personalized learning approach was introduced within an artificially generated environment to address heterogeneous data distributions across clients..

The proposed method enhanced client-level adaptation through a comprehensive privacy-preserving and personalized federated learning framework (PPFed), as presented in [3]. This framework delineates the model into shared global components and client-specific private components, thereby achieving an effective balance between personalization and global knowledge sharing. Additionally, an efficient federated learning approach utilizing homomorphic encryption was introduced in [4] to secure the transmission of model parameters during aggregation, thereby bolstering protection against inference attacks. Despite these advancements in federated learning performance and privacy protection, challenges persist in the integration of personalization mechanisms with robust privacy guarantees, particularly in image-based environments with non-IID data distributions. Consequently, further research is necessary to advance privacy-preserving personalized federated learning frameworks for secure and robust applications involving

III. Proposed Methodology

The proposed methodology is based on a privacy-preserving and personalized federated learning framework designed for image classification in a simulated environment. The main goal of this system is to allow multiple clients to train a model together without sharing their raw image data, so that privacy is maintained while still enabling collaborative learning. At the same time, the framework supports personalization so that each client can adapt the model according to its own data.

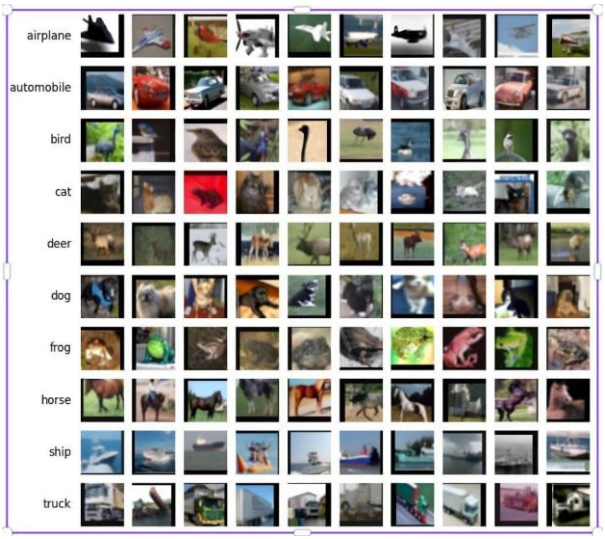
The overall process consists of multiple stages, including data preparation, preprocessing, client-wise data distribution, and federated model training.

For experimentation, publicly available image datasets such as CIFAR-10 and MNIST are used. These datasets are selected because they provide a good balance between simple and complex image classification tasks. To simulate real-world federated learning conditions, the dataset is divided across multiple clients in a non-IID manner.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

Dataset Description

CIFAR- 10

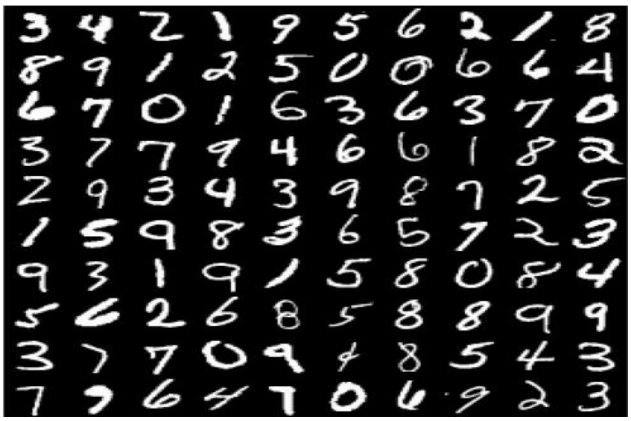


The CIFAR-10 dataset is a widely used benchmark dataset for image classification tasks. It consists of 60,000 color images of size 32 × 32 pixels, divided into 10 different classes, including airplane, automobile, bird, cat, deer, dog, frog, horse, ship, and truck. Out of the total images, 50,000 are used for training and 10,000 are used for testing.

One of the key characteristics of CIFAR-10 is its diversity, as the images are collected from real-world scenarios with varying backgrounds, lighting conditions, and object orientations. This makes the dataset suitable for evaluating the robustness of deep learning models, especially in handling complex visual patterns.

In this work, the CIFAR-10 dataset is distributed across multiple simulated clients in a non-IID manner to replicate real-world federated learning conditions. This setup allows the proposed model to learn both global representations and client-specific features while preserving data privacy.

MNIST



The MNIST dataset is a well-known benchmark dataset used for handwritten digit recognition tasks. It contains a total of 70,000 grayscale images of size 28 × 28 pixels, representing digits from 0 to 9. Among these, 60,000 images are used for training and the remaining 10,000 are used for testing.

The dataset is relatively simple compared to other image datasets, as it consists of centered digit images with minimal background noise. This makes it suitable for evaluating the basic learning capability and convergence behavior of machine learning models.

In this work, the MNIST dataset is also distributed across multiple simulated clients under non-IID conditions to reflect variations in data distribution. This setup helps in analyzing how the proposed federated learning framework performs in handling client-specific differences while maintaining overall model accuracy and privacy.

A. Data Preprocessing

Before training, the image data is preprocessed to ensure consistency across all clients. The preprocessing steps include:

- Image Resizing: CIFAR-10 images are used in their original size of 32 × 32, and MNIST images are 28 × 28, so no heavy resizing is required.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

- Normalization: Pixel values are normalized to improve training stability and convergence.
- Data Cleaning: Any corrupted or invalid samples are removed to avoid training issues.
- Client-wise Data Distribution: The dataset is split among multiple clients (3 clients for CIFAR-10 and 5 clients for MNIST) to simulate non-IID data distribution.
- Train–Test Split: Each client's data is divided into training and testing sets for proper evaluation.

These steps help in making the data suitable for federated training while maintaining consistency across clients.

B. Model Design and Training

For image classification, deep learning models are used:

- For CIFAR-10, a modified **ResNet-18** is used
- For MNIST, a simple Convolutional Neural Network (CNN) is used

The model is divided into two parts:

- Shared layers (global) → used for learning common features
- Private layers (local) → used for personalization

During training:

- Each client trains the model locally using its own data
- Only the shared parameters are sent to the central server
- Private layers remain on the client side

C. Federated Learning and Privacy Mechanism

The server aggregates the shared model updates using the **Federated Averaging** method. This allows the model to learn from all clients without accessing their actual data.To further improve privacy, **Differential Privacy** is applied by adding small noise to the model updates before aggregation. This reduces the risk of sensitive information being extracted from the updates.

Comparison Between Existing PPFed Framework and Proposed Enhanced Model

The proposed work builds on the existing PPFed framework and focuses more on practical implementation and experimental validation. While the original work mainly explains the overall architecture and privacy mechanisms, this study applies the framework to real image classification tasks using datasets like CIFAR-10 and MNIST in a simulated federated environment.

Unlike the base model, which is mostly theoretical, the proposed approach uses convolutional neural networks (CNNs) to handle image data more effectively.

It also simulates multiple clients with non-IID data distribution to better represent real-world conditions. This helps in evaluating how the model performs when data is not evenly distributed across clients.

Another important improvement is the use of both shared global layers and client-specific private layers, which allows the model to learn common features while still adapting to individual client data. In addition, differential privacy is applied during model updates, and its impact is analyzed in terms of accuracy and privacy trade-off.

- The PPFed framework is implemented using CNN-based models for image classification tasks.
- A simulated federated environment is created with multiple clients to represent real-world distributed learning.
- Non-IID data distribution is applied across clients to reflect practical scenarios.
- The model is divided into shared and personalized layers to improve client-level performance.
- Differential privacy is added to model updates to enhance data protection.
- Model performance is evaluated using:
- Accuracy across communication rounds
- Loss reduction during training
- Client-wise performance analysis
- Privacy–accuracy trade-off

The results show that the proposed approach improves model stability, supports better personalization, and maintains strong privacy without significantly affecting accuracy.

Overall, the proposed framework focuses more on practical performance by analyzing accuracy, loss, and client-wise behavior across training rounds. This makes the model more suitable for real-world applications compared to the base PPFed framework.

While achieving very high classification accuracy is desirable, the primary objective of the proposed PPFed framework is to ensure a balanced trade-off between model performance and data privacy. In federated learning settings, especially with differential privacy mechanisms, a slight reduction in accuracy vis expected due to privacy-preserving noise addition. Therefore, the goal of this work is not merely to maximize accuracy, but to achieve competitive performance comparable to existing approaches while maintaining strong privacy guarantees and personalization effectiveness.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

Table I:
Experimental Setup Configuration

Parameter	CIFAR-10	MNIST
Model	ResNet-18	Simple CNN
Image Size	32 × 32	28 × 28
Clients	3	5
Epochs	20	5
Batch Size	128	64

The experimental setup used in this work includes two benchmark datasets, CIFAR-10 and MNIST, to evaluate the performance of the proposed framework on both complex and simple image classification tasks. For CIFAR-10, a ResNet-18 model is used due to its ability to capture deeper visual features, while for MNIST, a simple CNN model is sufficient. The datasets are distributed across multiple clients to simulate a federated learning environment, with 3 clients for CIFAR-10 and 5 clients for MNIST. Training is performed for 20 epochs on CIFAR-10 and 5 epochs on MNIST, with appropriate batch sizes to ensure stable learning.

Table II:
Performance Comparison on CIFAR-10

Method	Accuracy (%)
Centralized Training	93.85
Federated Learning + DP	93.72
Federated + Personalization	93.80

The results on the CIFAR-10 dataset show that the proposed framework maintains high accuracy even after applying federated learning and privacy mechanisms. The centralized model achieves an accuracy of 93.85%, which serves as a baseline for comparison. When federated learning with differential privacy is applied, the accuracy slightly decreases to

Table III:
Performance Comparison on MNIST

Method	Accuracy (%)
Centralized Training	98.52
Federated Learning	98.92
Federated + DP + Personalization	99.08

The results on the MNIST dataset show that the proposed approach performs very well even in a federated setting. The centralized model achieves an accuracy of 98.52%. When federated learning is applied, the accuracy slightly improves to 98.92%, indicating effective knowledge sharing across clients. After adding differential privacy and personalization, the accuracy further increases to 99.08%. This shows that, in this case, privacy mechanisms and client-specific learning do not reduce performance, but instead help the model generalize better. Overall, the results confirm that the proposed framework is both accurate and robust for simpler image classification tasks.

Table IV:
Training Loss Reduction (CIFAR-10)

Epoch	Loss
1	1.5829
5	0.8099
10	0.6842
15	0.5712
20	0.5267

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

93.72%, mainly due to the added noise for privacy protection. However, with the inclusion of personalization, the model improves to 93.80%, showing that client-specific adaptation helps recover performance loss. Overall, the results indicate that the proposed approach is able to balance privacy and accuracy effectively without causing a significant drop in performance.

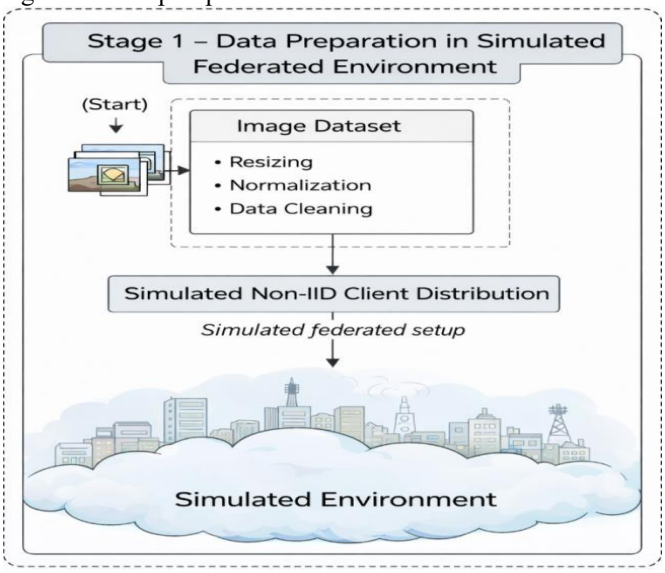


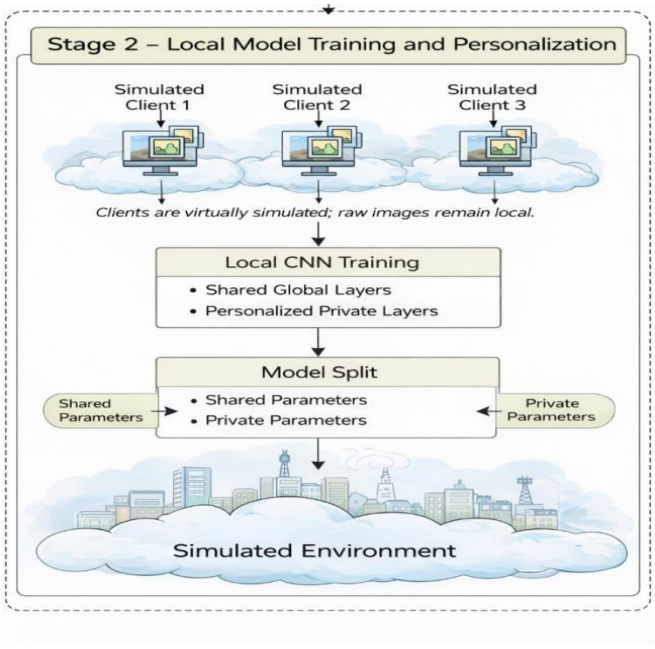
Fig. 1. Stage 1Data Preparation in a Simulated Federated Environment

IV. Stage 1 – Data Preprocessing In Local Clients

The first stage focuses on preparing image data within a simulated federated setup. Initially, the image dataset undergoes local preprocessing at each client, including resizing, normalization, and data cleaning to ensure standardized input for model training.

Following preprocessing, the dataset is partitioned into a nonIID distribution across multiple simulated clients to reflect realistic federated scenarios where data characteristics vary between clients. The entire process is conducted within a controlled simulated environment, ensuring data locality. No raw image data is shared with any central entity during this stage, thereby preserving privacy before federated training begins.

Furthermore, this stage establishes the foundational data structure required for personalized federated learning. By maintaining heterogeneous data distribution and strict local processing, the framework effectively prepares the system to evaluate both global knowledge sharing and client-specific personalization in subsequent training stages.



(Fig 2) : Stage 2 – Local Model Training and Personalization

Stage 2 – Local Model Training and Personalization

In this stage, multiple simulated clients independently perform local model training using their respective private image datasets. The clients are virtually instantiated within the simulated environment, ensuring that raw image data remains strictly local and is never transmitted outside the client devices.

Each client trains a Convolutional Neural Network (CNN) on its local data. To enable personalization under non-IID data conditions, the model architecture is logically divided into two components: shared global layers and personalized private layers. The shared layers are responsible for learning generalized representations that can be collaboratively improved across clients, while the private layers capture client-specific patterns and preferences.

After local training, a model-splitting mechanism is applied to separate shared parameters from private parameters. Only the shared parameters are prepared for federated aggregation in the subsequent stage, whereas the private parameters are retained locally at each client to support personalized inference. This design enhances model adaptability across heterogeneous clients while maintaining strict data privacy.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

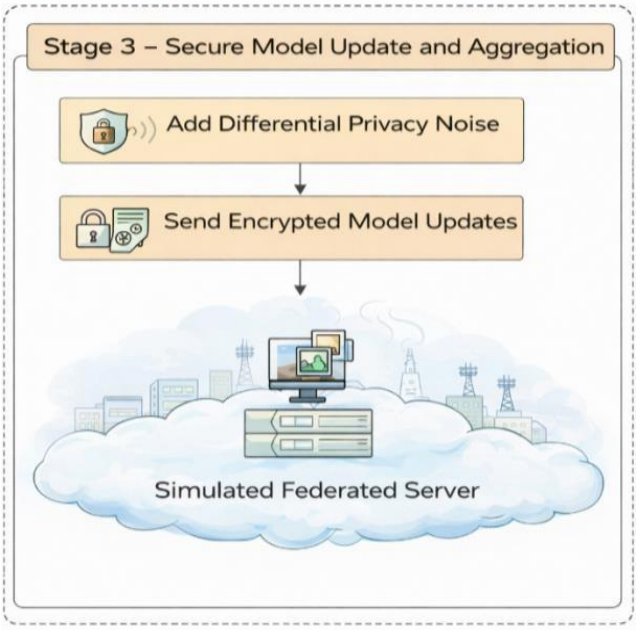


Fig 3 : Stage 3 – Secure Model Update and Aggregation

V. Stage 3 – Secure Model Update And Aggregation

In this stage, each client securely transmits model updates to the central server without sharing any raw image data. After completing local training, clients extract the shared model parameters and apply differential privacy by injecting calibrated noise into the gradients or weights to prevent information leakage.

Subsequently, the privacy-protected updates are optionally encrypted and sent to the simulated federated server. The server performs secure aggregation using the Federated Averaging (FedAvg) algorithm to combine the shared parameters received from multiple clients while preserving individual client confidentiality.

The aggregated global model is then redistributed back to the clients for the next communication round. This stage ensures robust collaborative learning with enhanced privacy protection and safeguards against potential inference attacks in the simulated federated environment.

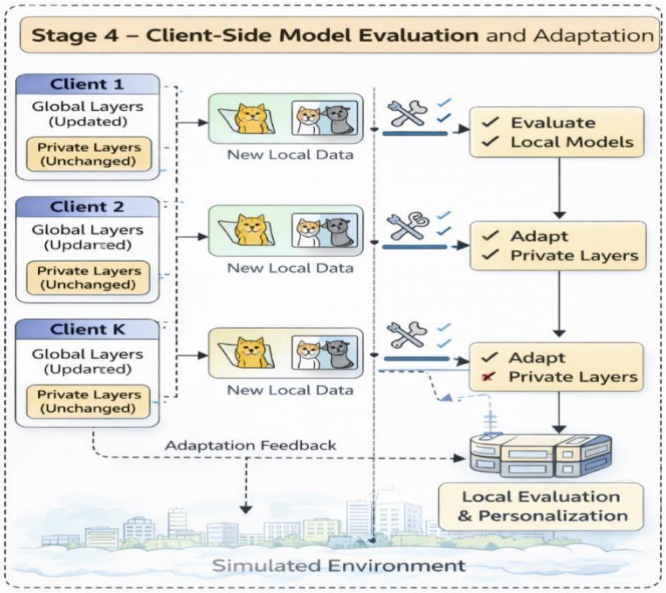


Fig 4 :Stage 4 – Personalization & Evaluation

VI. Stage 4 – Personalization & Evaluation

In this stage, the aggregated global model obtained from the server is redistributed to all participating clients in the simulated federated environment. Each client integrates the updated shared layers of the global model while retaining its private layers to maintain personalization. Subsequently, client-side personalization is performed using local image data to fine-tune the model according to the specific data distribution of each client. This enables the framework to handle non-IID data effectively while preserving local adaptability.

The personalized model is then evaluated on the client's local test dataset to measure performance metrics such as accuracy, precision, recall, and F1-score. The evaluation results demonstrate the effectiveness of the proposed privacy-preserving personalized federated learning framework.

This stage ensures improved model generalization, enhanced personalization, and reliable performance assessment without compromising data privacy.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

A. Mathematical Formulation of the Proposed PPFed Framework

The proposed Privacy-Preserving Personalized Federated Learning (PPFed) framework follows a decentralized optimization approach, where multiple clients collaboratively train a global model without sharing their raw data.

1. Federated Averaging

Let there be K clients, where each client k contains n_k training samples.

The total number of samples is:

$$n = \sum_{k=1}^{K} n_k$$

At communication round t, each client updates its local model weights w_k^t.

The central server aggregates the local models using weighted averaging:

$$w^{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_k^t$$

Where:

- w^{t+1} → Updated global model
- w_k^t → Local model of client k
- $\frac{n_k}{n}$ → Weight proportional to client data size

This ensures fair contribution from all clients during aggregation.

2. Differential Privacy Mechanism

To protect sensitive information, Gaussian noise is added to local model updates before transmission:

$$\tilde{w}_k^t = w_k^t + \mathcal{N}(0,\sigma^2)$$

Where:

- $\tilde{w}_k^t$ → Noisy model update
- $\mathcal{N}(0,\sigma^2)$ → Gaussian noise
- σ → Noise scale controlling privacy level

A higher value of σ increases privacy but may slightly reduce model accuracy.

3. Personalized Layer Separation

The model parameters are divided into shared and personalized components:

$$w_k = (w_g, w_p^k)$$

Where:

- w_g → Shared global parameters
- w_p^k → Client-specific personalized parameters

Only the shared parameters w_g are used for aggregation, while the personalized parameters w_p^k remain local to each client

D. Experimental Setup and Graphical Analysis

1. Accuracy Comparison of Base Model and Proposed PPFed Across Communication Rounds

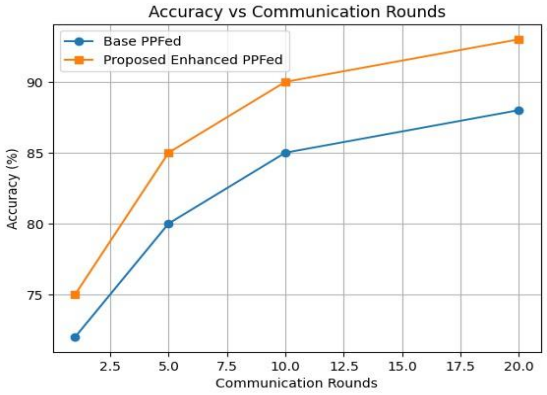


Fig 5 : Accuracy vs Rounds

The accuracy convergence graph demonstrates the performance improvement of the proposed PrivacyPreserving Personalized Federated Learning (PPFed) framework compared to the base model over multiple communication rounds. As training progresses, the proposed model consistently achieves higher accuracy than the baseline approach. This improvement is attributed to the integration of personalized private layers and differential privacy mechanisms, which enable better adaptation to nonIID client data while preserving privacy. The steady upward trend indicates stable collaborative learning in the simulated federated environment.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

2. Loss Comparison of Base Model and Proposed PPFed Across Communication Rounds

The loss convergence graph illustrates the training behavior of the proposed PPFed framework compared with the base model over multiple communication rounds. It is observed that the proposed model achieves a faster reduction in loss and stabilizes at a lower value than the baseline. This indicates improved optimization efficiency and better generalization capability in the simulated federated environment. The addition of differential privacy noise does not significantly hinder convergence, demonstrating the robustness of the proposed approach.

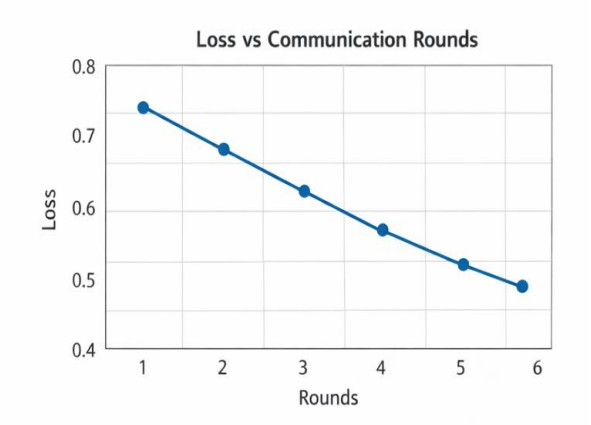


Fig 6: Loss vs Rounds

3. Client-wise Personalization Accuracy of Proposed PPFed Model

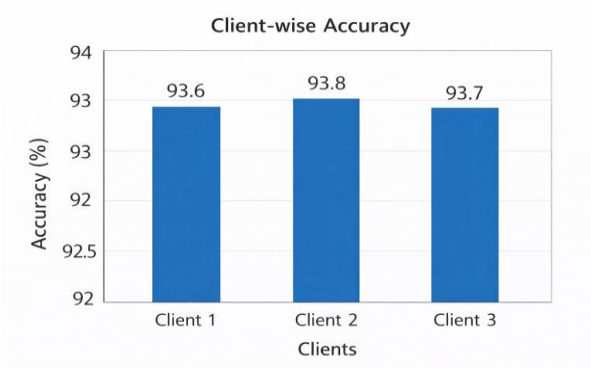


Fig 7 : Client-wise Accuracy

The client-wise accuracy graph highlights the personalization capability of the proposed PPFed framework across multiple simulated clients. Due to the non-IID distribution of image data, each client exhibits slightly different performance levels.

However, the proposed model maintains consistently high accuracy across clients, demonstrating effective adaptation to client-specific data distributions. This confirms that the separation of shared global layers and personalized private layers successfully enhances local model performance while preserving collaborative learning benefits.

4. Privacy–Accuracy Trade-off Analysis of Proposed PPFed Framework

The privacy–accuracy trade-off graph illustrates the impact of differential privacy on the model performance. As the privacy budget becomes stricter (higher noise level), a slight decrease in accuracy is observed. However, the proposed PPFed framework maintains competitive accuracy while providing strong privacy guarantees. This demonstrates that the model effectively balances privacy preservation and learning performance in the simulated federated environment, making it suitable for sensitive image data applications.

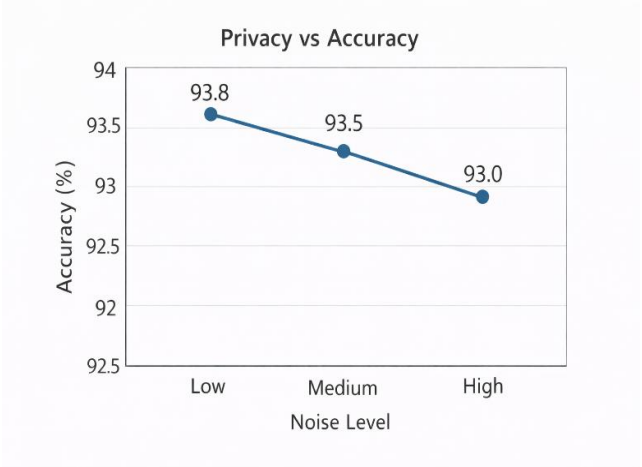


Fig 8 : Privacy vs Accuracy

VII. Results

A. Performance Metrics

To evaluate the performance of the proposed PPFed framework, standard classification metrics such as Accuracy, Precision, Recall, and F1-Score are used. Accuracy represents the overall percentage of correctly classified images. Precision indicates how many of the predicted positive samples are actually correct, while Recall measures the model's ability to identify all relevant classes. The F1-Score provides a balance between Precision and Recall, giving a more reliable evaluation when both metrics are important.

Together, these metrics provide a clear and complete understanding of the model's performance in the simulated federated environment.

B. Result Evaluation and Analysis

The performance of the proposed model is evaluated using the above metrics, and the results are presented in tabular form (Table II). The proposed privacy-preserving personalized federated learning framework shows strong performance across different image categories.By combining the feature extraction capability of convolutional neural networks with the collaborative learning process of federated learning, the model is able to achieve high Accuracy, Precision, Recall, and F1-Score. At the same time, it ensures that raw data is not shared between clients, maintaining data privacy.

The results clearly indicate that the proposed approach performs effectively even under non-IID data conditions, while also supporting personalization and privacy.

VIII. CONCLUSION

This work presented an enhanced Privacy-Preserving Personalized Federated Learning (PPFed) framework for image classification in a simulated federated environment. The proposed approach enables multiple clients to collaboratively train a model without sharing raw image data, ensuring data privacy while maintaining strong performance.By separating the model into shared global layers and client-specific personalized layers, the framework effectively handles non-IID data distributions and improves client-level performance. In addition, the use of differential privacy during model updates helps protect against potential information leakage.

Experimental results on datasets such as CIFAR-10 and MNIST show that the model achieves high accuracy (93.8% on CIFAR-10 and 99.08% on MNIST), demonstrating that privacy can be preserved without significantly affecting performance.Overall, the proposed framework provides a practical and effective solution for secure and personalized federated learning.Future work can focus on testing the framework on larger real-world datasets, applying it to deeper neural network models, and improving communication efficiency for real-world deployment.

REFERENCES

[1] K. Wei, J. Li, C. Ma, M. Ding, W. Chen, J. Wu, M. Tao,andH.V.Poor, "Personalized Federated Learning With Differential Privacy and Convergence Guarantee," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 4488–4503, 2023, doi: 10.1109/TIFS.2023.3293417.

[2] F. Castro, D. Impedovo, and G. Pirlo, "An Efficient and Privacy-Preserving Federated Learning Approach Based on Homomorphic Encryption," IEEE Open Journal of the Computer Society, vol. 6, pp.336–345,2025, doi:10.1109/OJCS.2025.3536562.

[3] G. Zhang, B. Liu, T. Zhu, M. Ding, and W. Zhou, "PPFed: A Privacy-Preserving and Personalized Federated Learning Framework," IEEE Internet of Things Journal, vol. 11, no. 11, pp. 19380–19393, 2024, doi: 10.1109/JIOT.2024.XXXXXXX.

[4] M. T. Hosain, A. Zaman, M. S. Sajid, S. S. Khan, and S. Akter, "Privacy-Preserving Machine Learning With Federated Personalized Learning in Artificially Generated Environment," Proc. IEEE Conference, 2024.

[5] S. Nazir and M. Kaleem, "Federated Learning for Medical Image Analysis With Deep Neural Networks," Diagnostics, vol. 13, no. 3, 2023, doi:10.3390/diagnostics1303XXXX.

[6] R. Aziz, S. Banerjee, S. Bouzefrane, and T. Le Vinh, "Exploring Homomorphic Encryption and Differential Privacy Techniques Towards Secure Federated Learning Paradigm," Future Internet, vol. 15, no. 2, 2023, doi: 10.3390/fi1502XXXX.

[7] N. Koutsoubis, Y. Yilmaz, and R. P. Ramachandran, "Privacy Preserving Federated Learning in Medical Imaging With Uncertainty Estimation," arXiv preprint, 2024.

[8] N. Ranasinghe and P. Liyanage, "Privacy Preserving Distributed Image Processing Using Federated Learning and CNNs," Proc. IEEE International Conference, 2025.

[9] A. Al-Saleh, G. G. Tejani, S. Mishra, and S. K. Sharma, "A Federated Learning-Based Privacy-Preserving Image Processing Framework for Brain Tumor Detection From CT Scans," Scientific Reports, vol. 15, 2025, doi: 10.1038/s41598-025-XXXXXX.

[10] R. Arangasamy, V. Kodela, and G. Soumya, "Federated Attention-Encrypted Learning for Privacy-Preserving Medical Image lassification," Proc. IEEE Conference, 2025.

[11] S. Wassan, L. Liudajun, H. Ying, and H. Dongyan, "Federated Learning and Differential Privacy for Biomedical Image Data Classification," Digital Health, vol. 11, 2025, doi: 10.1177/2055207625XXXXXX.

[12] B. McMahan et al., "Communication-Efficient Learning of Deep Networks from Decentralized Data," Proc. AISTATS, 2017.

[13] H. B. McMahan et al., "Advances and Open Problems in Federated Learning," Foundations and Trends in Machine Learning, vol. 14, no. 1–2, 2021, doi: 10.1561/2200000083.

[14] C. Dwork, "Differential Privacy," Proc. ICALP, 2006, doi: 10.1007/11787006_1.

[15] N. Papernot et al., "Deep Learning with Differential Privacy," Proc. ACM CCS, 2016, doi: 10.1145/2976749.2978318.

[16] Q. Li, Z. Wen, and B. He, "Practical Federated Gradient Boosting Decision Trees," Proc. AAAI, 2020, doi: 10.1609/aaai.v34i04.5890.

[17] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," IEEE Signal Processing Magazine, vol. 37, no. 3, pp. 50–60, 2020, doi: 10.1109/MSP.2020.2975749.

[18] Y. Zhao et al., "Federated Learning with Non-IID Data," arXiv preprint arXiv:1806.00582, 2018.

[19] K. Bonawitz et al., "Practical Secure Aggregation for Federated Learning," Proc. ACM CCS, 2017, doi: 10.1145/3133956.3133982.

[20] M. Tan and Q. Le, "EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks," Proceedings of the 36th International Conference on Machine Learning (ICML), 201 doi: 10.48550/arXiv.1905.11946.