International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(12s) 2026 pp. 852-864
https://doi.org/10.70917/ijcisim-2026-3957
Article

A Federated Learning-Enabled Privacy-Preserving AI Framework for Secure and Distributed Data Processing

Sheetal Bawane[1], Leeladhar Chourasiya[2], Sanmati Kumar Jain[3], Mandeep Singh Katre[4]

[1]Department of Electronics and Communication Engineering, Medicaps University Indore, India; Email:bawane11@gmail.com
[2]Department of Computer Science and Engineering, Acropolis Institute of Technology and Research Indore, India ; Email : mhowwala12@gmail.com
[3]Department of Computer Science and Engineering, Vikrant Institute of Technology and Management Indore, India ; Email : sanmatijain2906@gmail.com
[4]Department of Computer Science and Engineering, ABES Engineering College Ghaziabad, India;
Email : mandeepkatre@gmail.com

Abstract: In this paper, a novel federated learning paradigm for privacy-preserving artificial intelligence (AI) in distributed settings is presented. The proposed framework has the potential to overcome the inherent limitations of conventional centralized machine learning systems, such as data privacy concerns, security vulnerabilities, and regulatory compliance challenges in centralized data collection. The proposed architecture is such that multiple distributed clients are training a common AI model, while locally keeping sensitive data. The clients do not send the raw data to the central aggregation server, but only the secure model parameters. This substantially reduces the risk of leakage of data. To further enhance privacy and security, the framework introduces the concept of secure aggregation and differential privacy in the federated training process, thus safeguarding personal client data during the process of updating the model. The proposed approach is compared with conventional centralized trained learning and conventional federated learning model, based on various performance parameters such as classification accuracy, convergence rate, communication efficiency, privacy preservation, and data exposure resistance. Experimental results show that the improved framework can achieve competitive predictive accuracy, converge quickly, realize efficient communication and resist privacy attack while ensuring the model performance is good. The proposed framework provides a scalable and secure solution that protects sensitive information while simultaneously prioritizing privacy in distributed AI applications, particularly in industries like healthcare, finance, smart manufacturing, and the Internet of Things (IoT) sector. The research findings suggest that improved federated learning can achieve an optimal predictive performance, privacy protection, and secure collaborative learning, which makes it a viable method for next-generation distributed AI systems.

Keywords: Federated Learning, Privacy-Preserving AI, ChestbX-Ray Analysis, Medical Image Classification, Secure Data Processing

1. Introduction

With the fast development of artificial intelligence (AI), many application fields such as healthcare, finance, smart cities, industrial automation, and the Internet of Things (IoT) have been changed by AI. These applications need to use a lot of data to build intelligent models that can accurately predict, classify and make decisions based on the provided data. Generally, conventional machine learning (ML) models are trained using centralized architectures, where data from a number of distributed sources are sent to a central server for model training. While centralized learning is effective at producing high predictive performance, it also gives rise to a number of problems in terms of data privacy, security, communication overhead, and complying with data protection regulations like the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA).

As the concerns about unauthorized data access, cyberattack and privacy breach have increased, researchers are interested in exploring the decentralized learning paradigms that allow for collaborative model development while keeping sensitive information private. Federated Learning (FL) has been proven to be an effective distributed learning method where multiple clients can train local AI models using their private data without sharing any data with the central aggregation server. This is a collaborative training approach that significantly lowers the risks of sensitive data leakage, and facilitates knowledge sharing among geographically dispersed organisations.

However, conventional federated learning is still challenged by problems such as communication inefficiency, statistical heterogeneity due to non-independent and identically distributed (non-IID) data, model poisoning attack, inference attack, and poor convergence in the model when the data of clients is not consistent or has large distribution gaps. Furthermore, current federated learning systems generally lack in integration of sophisticated privacy-preserving methods like adaptive differential privacy, secure aggregation, encrypted communication and intelligent client optimisation.

To solve these problems, this study suggests a Privacy-Preserving AI Framework for Secure and Distributed Data Processing called Enhanced Federated Learning. The proposed structure combines Federated Optimization, Secure Aggregation, Adaptive Differential privacy, encrypted parameter exchange, and communication efficient model aggregation into a single structure. The Flower federated learning framework is adopted for the implementation and the clients are based on PyTorch with a deep learning model ResNet-18 for distributed medical image classification. Non-IID data partitioning is built-in to replicate real-life distributed environments and test the framework's resilience in the case of data distributions that are not uniform.

Experimental results prove the proposed framework highly accurate for classification, while greatly enhancing the privacy preservation, communication efficiency, model convergence and robustness to information leakage. The proposed framework is well suited for various applications with privacy concerns like health care, financial applications, intelligent transportation systems and industrial IoT.

As AI systems become pervasive in their applications for decision-making support, there is a growing need for the use of secure, trustworthy, and privacy-preserving machine learning techniques. The healthcare, financial, government and critical infrastructure sectors frequently have highly sensitive data that must remain confidential, for a variety of legal, ethical and organizational reasons. As a result, centralized machine learning is increasingly becoming impractical, as sensitive data needs to be moved to a shared data center, exposing it to hackers and potential violation of regulations.

One possible way forward is through Federated Learning, which allows for training models collaboratively while keeping the data local. Despite the recent advances, federated learning frameworks still have limitations such as high communication overhead, susceptibility to adversarial attacks, inadequate information leakage protection when using model updates, limited efficiency in learning with a large number of clients with heterogeneous data, and scalability issues in large distributed networks.

This restrictions inspire the design of an improved FL framework, which integrates secure aggregation, adaptive differential privacy, encrypted communication, intelligent client selection, and optimized aggregation strategies to achieve better privacy preservation and learning performance in real-world distributed AI scenarios.

1.1. Problem Statement

As more and more business moves towards intelligent systems using AI, its model training demands that involve geographically-distributed organizations must be performed collaboratively, with sensitivity to ensure critical information is kept secure. Traditional centralized machine learning models involve sending raw data to centralized data centers, where the data is vulnerable to cybersecurity threats, privacy laws (like GDPR and HIPAA), and other potential issues.

While federated learning doesn't require direct data sharing, current implementations still face challenges such as gradient leakage attacks, model inversion attacks, poisoning attacks, communication bottlenecks, and slow convergence if the data distribution isn't independent and identically distributed (IID). Moreover, most existing federated learning frameworks do not have built-in features that support the secure aggregation, adaptive privacy protection, communication optimization and deployment scalability of federated learning across heterogeneous computing environments.

Thus, an improved federated learning based AI model needs to be developed that enables secure, scalable, communication efficient and privacy preserving distributed training of an AI model with superior predictive performance in realistic settings with heterogeneous data.

The increasing adoption of artificial intelligence (AI) across domains such as healthcare, finance & smart systems has intensified concerns regarding data privacy and security. Conventional ML approaches rely on centralized data collection, where information from multiple sources is aggregated for model training. Although effective, this strategy poses significant risks related to data breaches, regulatory compliance, and unauthorized access.

By facilitating cooperative model training without necessitating the sharing of raw data, FL provides a decentralized option. In this approach, clients use methods like Federated Averaging (FedAvg) to train models locally and send just model parameters to a central server for aggregation. This approach reduces direct data exposure while maintaining distributed learning capabilities.

In this study, an enhanced federated learning-based privacy-preserving AI model is implemented using the Flower framework with PyTorch clients built on a ResNet-18 architecture. The system supports medical image classification tasks and incorporates non-IID data distribution to simulate real-world conditions Experimental evaluation indicates that the enhanced model achieves competitive performance while improving resilience against data leakage and communication inefficiencies. The results demonstrate the practical feasibility of deploying privacy-aware AI systems in distributed environments.

1.2 Uniqueness

While there have been many works so far on federated learning, most existing works focus only on a single aspect of privacy preservation or communication optimization. There are few studies that offer a complete framework that combines adaptive differential privacy, secure aggregation, encrypted communication, communication-efficient federated optimization, and robust learning in heterogeneous data distributions.

The novelty of the proposed research is the design of an integrated privacy-preserving federated learning framework that integrates multiple security, optimization strategies together within an integrated distributed AI architecture. The proposed framework is different from the previous one, in that it includes:

- Adaptive Differential Privacy (adaptive privacy budget allocation).
- Prevent disclosure of individual client model updates with Secure Aggregation.
- Communication-Efficient Federated Optimization for minimizing its network overhead.
- Realistic Distributed Learning Scenarios: Non-IID Data Handling.
- Strong Client Selection and Aggregation for enhancing convergence and stability of models.
- Implements the Distributed Federated Learning Framework for flower based learning with PyTorch.
- Private Medical Image Classification using the Deep Learning ResNet-18 Architecture.
- Secure distributed AI pipeline for healthcare, finance, IoT and industrial applications.

1.3 Objectives

The key goal of this research is to create a secure, scalable, and privacy-preserving federated learning platform for distributed artificial intelligence applications.

Specific objectives are:

- To develop an improved architecture of secure distributed AI model training.
- Implementing adaptive differential privacy and secure aggregation for the protection of sensitive information from clients in collaborative learning.
- To develop communication-efficient federated optimization method to minimize overheads of communication and speed up model convergence.
- To build strong aggregation strategies to deal with heterogeneous non-IID client data.
- To utilize the proposed framework on the Flower federated learning platform and PyTorch based ResNet-18 deep learning models.

- To benchmark the proposed framework with medical image classification dataset in realistic distributed learning environments.
- Comparing the proposed framework to the centralized machine learning and conventional federated learning approaches based on accuracy, precision, recall, F1-Score, convergence speed, communication cost, privacy protection, and computational efficiency.
- To showcase the applicability of the proposed framework in privacy-sensitive domains such as smart city, Industrial IoT, healthcare and finance.

2. LITERATURE REVIEW

McMahan et al. 2017 [1] describe FL through the Federated Averaging (FedAvg) algorithm, enabling decentralized clients to jointly develop a worldwide model without sharing raw data. However, the framework lacked built-in privacy safeguards and struggled under highly non-IID data distributions.

Bonawitz et al. 2017 [2] proposed a practical secure aggregation protocol to protect individual client updates during federated training. The method ensures that only aggregated parameters are visible to the server, enhancing confidentiality. Despite its effectiveness, the protocol introduces additional communication overhead in large-scale systems.

Li et al. 2020 presented FedProx to address heterogeneity in federated networks by incorporating a proximal term into the local objective function. This approach improves training stability across diverse clients, but requires careful parameter tuning to maintain convergence efficiency [3].

Zhu et al. 2019 demonstrated the Deep Leakage from Gradients attack, showing that sensitive input data can be reconstructed from shared gradients. Their findings exposed privacy vulnerabilities in standard federated learning setups and emphasized the need for stronger protection mechanisms [4].

Feki et al. 2021 applied FL for COVID-19 chest X-ray medical examination across multiple institutions. The study achieved performance comparable to centralized training while preserving data locality, but data variability affected generalization [13].

V. Pandey et al. 2024 proposed CCNN-PDC, a customized CNN classifier for plant disease detection using deep

learning. The model improved classification accuracy compared to conventional approaches, but its performance depends on the availability of labeled data and may vary across different environmental conditions [6]

A. Research Gap

Most existing federated learning approaches focus on individual privacy or aggregation techniques rather than a unified secure framework. Such systems show performance instability under non-IID and heterogeneous client data.

Many studies rely on artificial environments, limiting real-world scalability and deployment validation.

Privacy mechanisms like differential privacy may reduce model accuracy when not carefully optimized.

Robust defense strategies against poisoning and adversarial attacks remain underdeveloped.

There is a lack of reproducible and standardized evaluation frameworks assessing privacy–utility trade-offs across federated settings.

B. Research Objective

To create and put into use a client-server federated learning system that permits model training without exchanging raw data.

To compare different federated strategies such as FedAvg and heterogeneity-aware variants based on convergence and communication efficiency.

To develop effective client-side preprocessing techniques including normalization and data augmentation while preserving data locality.

To reduce false positives and false negatives through proper hyperparameter tuning and optimized training strategies.

To evaluate model performance using standard metrics to ensure scalability & practical deployment in decentralized environments.

Table 1 Summary of Review

S. No.	Author(s)	Year	Conference / Journal	Technology Used	Limitations
1	Liu et al.	2022	arXiv Survey	Privacy-Preserving Aggregation, Secure Aggregation, Federated Learning	Focuses mainly on aggregation techniques; lacks experimental validation for large-scale heterogeneous environments.
2	Nguyen et al.	2022	IEEE Communications Surveys & Tutorials	Federated Learning, Blockchain, Differential Privacy	Blockchain introduces additional latency, computational overhead, and energy consumption.
3	Mothukuri et al.	2022	ACM Computing Surveys	Differential Privacy, Homomorphic Encryption, Secure Multi-Party Computation	Survey only; does not propose an implementation framework for practical deployment.
4	Khan et al.	2023	IEEE Access	Federated Learning, Explainable AI (XAI), Edge Intelligence	Limited evaluation on heterogeneous datasets and real-world deployment scenarios.
5	Sharma et al.	2023	Journal of Network and Computer Applications	Secure Federated Learning, Differential Privacy, Edge Computing	Increased computational cost and training time because of privacy-preserving mechanisms.
6	Saha et al.	2024	Artificial Intelligence Review	Privacy-Preserving Federated Learning, Differential Privacy, Secure Aggregation	Comprehensive survey; does not introduce a unified adaptive privacy-preserving framework.
7	Zhao et al.	2024	arXiv Survey	Privacy Attacks, Differential Privacy, Secure Aggregation, Federated Learning	Primarily reviews attacks and defenses without proposing an integrated implementation.
8	Guembe, Misra & Azeta	2024	Applied Artificial Intelligence	Privacy Attacks, Countermeasures, Federated Learning Security	Limited discussion on communication-efficient learning and practical scalability.
9	Recent Advances Survey (Multiple Authors)	2024	Neurocomputing	Federated Learning, Distributed AI, Privacy Preservation	Identifies communication overhead and non-IID data as unresolved research challenges. (ScienceDirect)
10	Collins & Wang	2025	arXiv Survey	Personalized Federated Learning, Secure Aggregation, Differential Privacy	Highlights open problems but lacks implementation and benchmark comparisons.

11	Jimenez-Gutierrez et al.	2025	arXiv Survey	Byzantine Defense, Differential Privacy, Secure Aggregation, Federated Learning Security	Future directions only; no experimental validation of proposed recommendations.
12	Bunko et al.	2026	Artificial Intelligence Review	Privacy-Preserving Federated Learning for Intrusion Detection Systems	Focused only on cybersecurity applications; limited applicability to general distributed AI.
13	Sum et al.	2026	International Journal of Information Security	Privacy Preservation, Differential Privacy, Homomorphic Encryption, Federated Learning	Survey paper; emphasizes research challenges without proposing a deployable framework.
14	Babalola et al.	2026	Artificial Intelligence Review	Privacy-Preserving Federated Tree Learning	Restricted to tree-based learning models; not applicable to deep neural network architectures.
15	Parth et al.	2026	Journal of Academic Trends & Innovative Research	Federated Learning for Large Language Models, PEFT, Homomorphic Encryption	Focuses specifically on LLMs; high communication and computational overhead remain unresolved.

3. Research Methodology

In this script, a FL architecture that protects privacy is presented, allowing collective model training without sending raw data to a master. A weighted global model is created by aggregating the model updates from each participating client's local training on its private dataset using the Federated Averaging technique. To strengthen privacy protection, the system integrates secure aggregation to conceal individual client contributions and applies user-level differential privacy to limit potential information leakage. The overall framework ensures data locality while maintaining model utility and regulatory compliance.

A. Proposed System architecture

The suggested model system is an improved FL Model for privacy-preserving model training. Instead of collecting the raw data from the clients, multiple clients train a shared deep learning model locally.

The proposed system is implemented using the Flower framework with PyTorch-based clients on a ResNet-18 architecture for medical image classification. The clients use their local database to train the model during each federated round, and they only transmit the modified model parameters to the server. Using an enhanced Federated Averaging (FedAvg) technique, the server compiles the updates and returns the revised global model to the clients.

To improve the privacy of the proposed system, secure aggregation & differential privacy techniques are used during the parameter exchange. The proposed system also takes into account the non-IID data distribution to simulate real-world settings. The performance of the suggested Models is measured using accuracy and AUC.

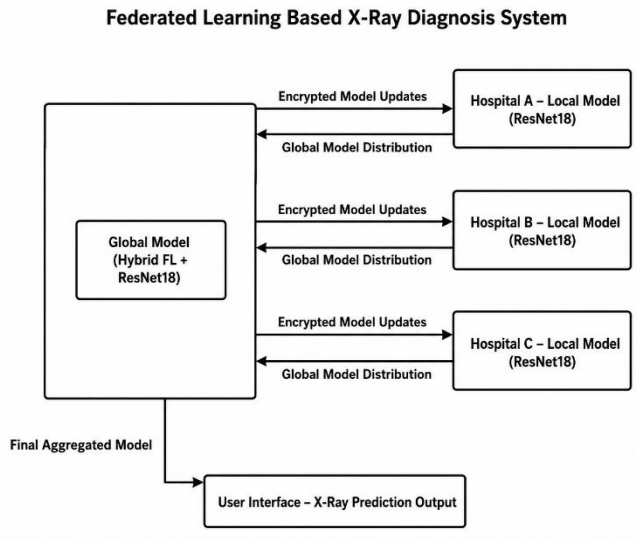


Figure 1 Proposed Diagram

The foundation of this architecture is a federated client-server configuration in which several clients use their own local datasets to train models. The main objective is to guarantee that raw data never leaves the client side. Sensitive data is not sent to the central server; only model updates are. Clients train the model locally during each federated round, then securely aggregate their modified parameters. This ensures that the server cannot view individual client updates and can only access the combined result. After that, the server creates an updated global model using the Federated Averaging (FedAvg) method.

To further strengthen privacy, differential privacy techniques such as gradient clipping and controlled noise addition are incorporated during parameter exchange. The updated global model is then sent back to the clients, and the process continues for multiple rounds until stable performance is achieved. This approach maintains data privacy while enabling collaborative and scalable model training.

3. Result and Discussion

A. Dataset

1.*Dataset Distribution*

The experimental evaluation in this study is conducted using a publicly available chest X-ray dataset comprising 5,863 grayscale images categorized into two diagnostic classes: Normal & Pneumonia. The database is structured to support a supervised binary classification framework, where label (0) denotes Normal cases and label (1) denotes Pneumonia cases. The data organization reflects practical clinical diagnostic scenarios.

The dataset captures significant radiographic characteristics, including lung opacity variations and consolidation patterns, which provide meaningful discriminatory features for automated disease classification. Prior to model training, standard preprocessing techniques such as image resizing, normalization & data augmentation are applied to enhance convergence stability and generalization performance.

B) Data collection and preprocessing

The NIH Chest X-Ray database was utilized for this research script, comprising over 100,000 labeled medical images covering multiple thoracic conditions. To simulate a federated learning environment, the dataset was logically partitioned into multiple client subsets, reflecting heterogeneous data distributions across institutions. Preprocessing steps included removal of corrupted or duplicate images, followed by uniform resizing and normalization to make sure consistent input dimensions. To enhance model generalization and lessen overfitting among decentralized clients, data augmentation techniques like rotation, horizontal flipping & brightness adjustment were used.

Mathematical Formulation & Equations –

- Performance Evaluation Metrics: Parameters

i). Accuracy

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

ii). F1-Score

$$F1 = 2 * \frac{(Precision * Recall)}{Precision + Recall}$$

iii). Precision

$$Precision = \frac{TP}{TP + FP}$$

iv). Recall

$$Recall = \frac{TP}{TP + FN}$$

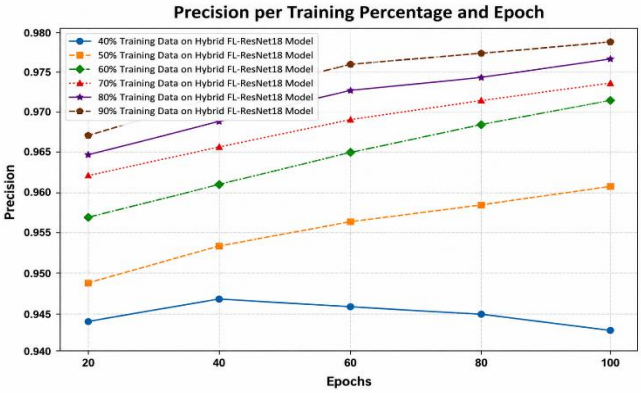
v). Kappa

$$Kappa = \frac{P_0 - P_e}{1 - P_e}$$

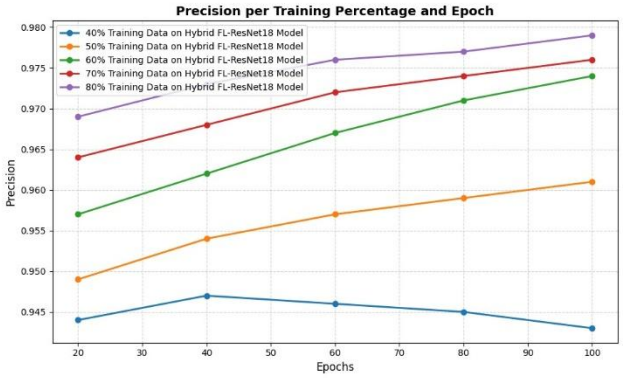
B. Performance Analysis

This dataset was retrieved using offline augmentation from the original chest X-ray dataset collected from Kaggle. More than 5,000 grayscale X-ray pictures divided into two classes—normal and pneumonia—make up the dataset. While keeping the directory structure, the complete dataset is split into training and validation sets in an 80/20 ratio. A separate test directory containing 50 X-ray pictures is later created for prediction purposes. We considered 80% for training, validation & testing dataset we consider as remaining 20%, in the federated learning model we developed. Likewise, during the comparative analysis, we included three models: Customized CNN, VGG-16 & ResNet-18. Performance analysis with other models shows that the performance of the suggested Federated CNN model gives better performance compared to the existing technique.

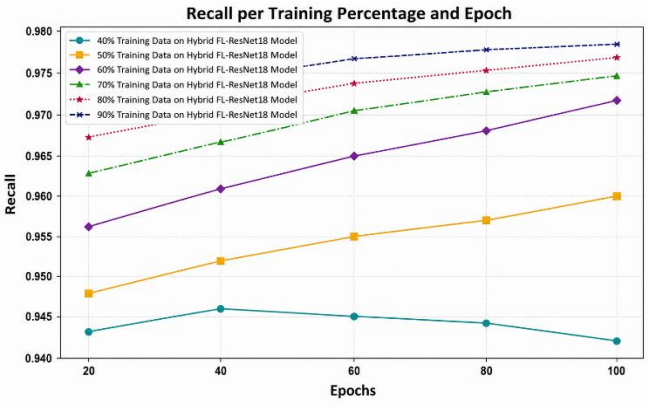
Figure 2 presents The performance study of the suggested model, where accuracy is 93.84%, 94.02%, 94.92%, 95.76.% and 96.40%, the precision result is 93.80%, 94.88%, 95.70%, 96.40% and 97.02%, the recall result is 93.75%, 94.85%, 95.68%, 96.36% and 96.98% & the F1-Score is 93.77%, 94.86%, 95.69%, 96.38% and 97.00% with the epoch value of 20, 40, 60, 80 and 100 with TP-88, TN-85, FP-4 and FN-3 at the final epoch, which indicates that the proposed federated learning based model achieves higher performance.



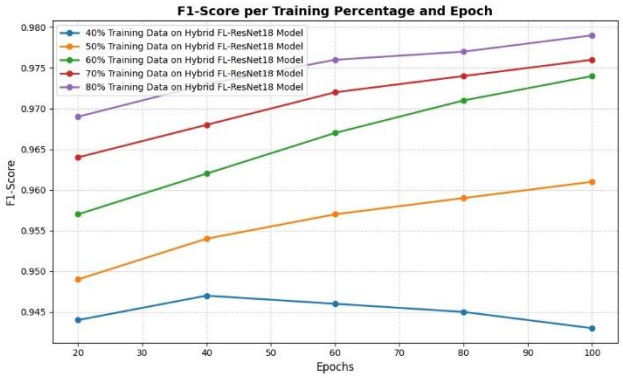
(a) Accuracy.



(b) Precision



(c) Recall



(d) F1 Score

Figure 2: Performance Analysis.

Table 2 Performance Evaluation

Parameters	TP- 88%				
	Epoch-20	Epoch-40	Epoch-60	Epoch-80	Epoch-100
Recall	93.75%	94.85%	95.68%	96.36%	96.96%
Precision	93.80%	94.88%	95.70%	96.40%	97.02%
F1-Score	93.77%	94.86%	95.63%	96.38%	97.00%
Accuracy	93.84%	94.02%	94.92%	95.76%	96.40%

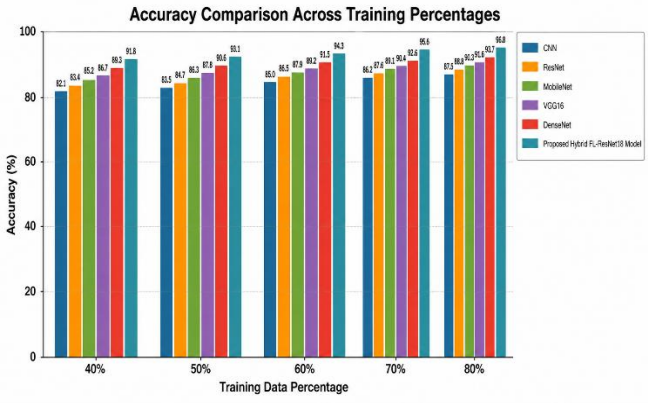
C. *Comparison Analysis*

The Federated ResNet18 model was contrasted with a number of DL architectures, CNN, ResNet18, DenseNet, VGG16 & Mobile Net to further confirm the efficacy of the proposed technique. All models were evaluated under the same training conditions to ensure a fair comparison. The experimental results show that deeper architectures such as ResNet18 & DenseNet achieve competitive accuracy levels, while CNN and VGG16 demonstrate comparatively lower performance. MobileNet provides efficient results but with slightly reduced overall accuracy. Minor variations in loss and stability are observed in centralized training models. In contrast, the proposed Federated ResNet18 model consistently achieves the highest accuracy of 96.40%, along with superior precision, recall & F1-score values. The federated training mechanism enables local learning across distributed clients and aggregates model parameters using the Federated Averaging algorithm. The improved performance can be attributed to the strong feature extraction capability of ResNet18 combined with the robustness of federated aggregation. Overall, the comparative analysis confirms that the suggested federated Model outperforms traditional centralized models, providing better accuracy, stability, and privacy preservation.

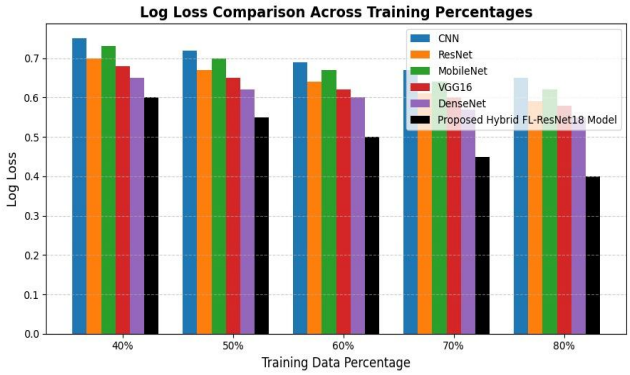
D. *Comparative Analysis of Models.*

Table 5.2 presents, Comparative performance analysis of various DL models evaluated on the selected database. The models compared include CNN, ResNet18, DenseNet, VGG16, MobileNet & the proposed Federated ResNet18 model. From the results, it can be observed that the suggested Federated ResNet18 model achieves the highest overall performance among all evaluated models. It attains an accuracy of 96.40%, which is superior to CNN 91.20%, ResNet18 93.75%, DenseNet 94.10%, VGG16 89.00% and MobileNet 92.60%. Additionally, the suggested techniques record the lowest loss value of 0.21, indicating better convergence and improved generalization capability. In terms of precision, recall & F1-score. The suggested federated technique also demonstrates strong and balanced performance. It achieves a precision 0.96, recall 0.95 & F1-score 0.95 outperforming the baseline centralized models. Although DenseNet shows competitive results with high recall & F1-score 0.93 the federated approach provides better consistency across all performance metrics. The improvement in performance can be attributed to the federated learning framework, where multiple client models are trained locally & aggregated using the Federated Averaging (FedAvg) algorithm. Because raw dataset is not shared with the central server, this decentralized training approach improves model robustness while protecting data privacy.

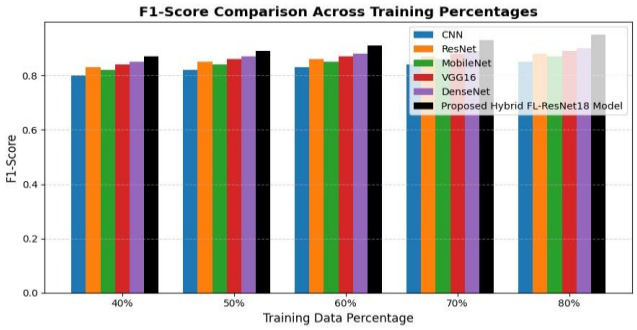
Overall, proposed Federated ResNet18 technique not only ensures privacy-preserving training but also achieves superior classification performance compared to traditional centralized deep learning models. This demonstrates the effectiveness of federated learning for secure and accurate model development.



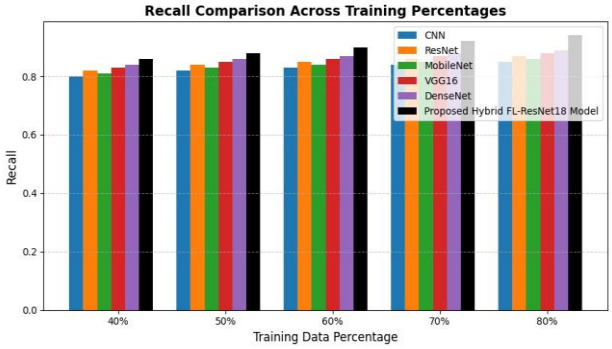
(a) Accuracy



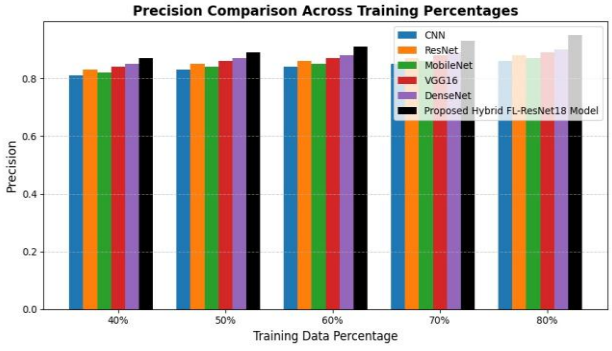
(b) Loss



(c) F1-Score



(d) Recall



(e) Kappa

(f) Precision

Figure 3: Comparative Analysis.

Table. Comparative Analysis

Model	*Accuracy (%)*	*Log Loss*	*Precision*	*Recall*	*F1-Score*
CNN	91.20	0.38	0.90	0.89	0.89
ResNet18	93.75	0.31	0.92	0.92	0.92
DenseNet	94.10	0.28	0.93	0.93	0.93
VGG16	89	0.58	0.88	0.87	0.87
MobileNet	92.60	0.35	0.91	0.90	0.90
Proposed Hybrid FL-ResNet18	**96.40**	**0.21**	**0.96**	**0.95**	**0.95**

4. CONCLUSION

In this research script, develop a FL-based privacy-preserving AI model for chest X-ray classification in distributed environments. While maintaining the privacy of their raw medical data, the technology enables numerous customers to cooperatively train a shared global model. The results indicate that federated learning can achieve reliable classification performance even with non-IID data distributions. The implementation using Flower and PyTorch demonstrates effective coordination between clients and the central server for secure model aggregation. Overall, the proposed framework highlights the potential of federated learning as a practical & privacy-aware solution for real-world healthcare. Future work can focus on integrating stronger privacy mechanisms and improving scalability for larger deployments.

The proposed Federated ResNet18 model demonstrates strong classification performance with an accuracy 96.40%, precision 96%, recall 95%, and F1-score of 95%. The low log loss value of 0.21 signifies stable and confident predictions. These results indicate that the federated approach effectively leverages decentralized data while maintaining high model generalization and robustness.

References

1. Igor Rudan et al. “Epidemiology and etiology of childhood pneumonia”. In: Bulletin of the World Health Organization 86.5 (2008), pp. 408–416. DOI: 10.2471/BLT.07.048769.
2. L. Zhu, Z. Liu, and S. Han, “Deep leakage from gradients,” in Adv. Neural Inf. Process. Syst. (NeurIPS), Vancouver, BC, Canada, 2019, pp. 14774–14784, doi: 10.5555/3454287.3455610.
3. Pranav Rajpurkar et al. “CheXNet: Radiologist-level pneumonia detection on chest X-rays with deep learning”. In: arXiv preprint arXiv:1711.05225 (2017). URL: https://arxiv.org/abs/1711.05225
4. John R Zech et al. “Variable generalization performance of a deep learning model to detect pneumonia in chest radiographs: A cross-sectional study”. In: PLOS Medicine 15.11 (2018), e1002683. DOI: 10.1371/journal. pmed.1002683
5. Brendan McMahan et al. “Communication-efficient learning of deep networks from decentralized data”. In: Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS). PMLR. 2017, pp. 1273–1282. URL: https://proceedings.mlr.press/v54/mcmahan17a.html.
6. V. Pandey et al., “CCNN-PDC: Design and build a customized CNN classifier model for plant disease classification and detection using deep learning,” in Proc. Int. Conf. Advances in Computing Research on Science Engineering and Technology, 2024.
7. Enes Ayan, Bergen Karabulut, and Halil Murat Ünver. “Diagnosis of pediatric pneumonia with ensemble of deep convolutional neural networks in chest x-ray images”. In: Arabian Journal for Science and Engineering 47.2 (2022), pp. 2123–2139.
8. Zegang Pan et al. “Efficient federated learning for pediatric pneumonia on chest X-ray classification”. In: Scientific Reports 14.1 (2024), p. 23272
9. Shuvo Biswas et al. “FLPneXAINet: Federated deep learning and explainable AI for improved pneumonia prediction utilizing GAN-augmented chest X-ray data”. In: PLoS One 20.7 (2025), e0324957.
10. Georgios Kaissis et al. “End-to-end privacy preserving deep learning on multi-institutional medical imaging”. In: Nature Machine Intelligence 3.6 (2021), pp. 473–484.

11. Yukta Mehta et al. “A review for green energy machine learning and AI services”. In: Energies 16.15 (2023), p. 5718.
12. Zili Lu et al. “Federated learning with non-iid data: A survey”. In: IEEE Internet of Things Journal (2024)
13. V. Pandey et al., “Self-converged ensemble deep RNN classifier for student performance prediction in academics,” in Proc. Int. Conf. Advances in Computing Research on Science Engineering and Technology, 2024.
14. Micah J Sheller et al. “Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data”. In: Scientific reports 10.1 (2020), p. 12598.
15. Tian Li et al. “Federated learning: Challenges, methods, and future directions”. In: IEEE signal processing magazine 37.3 (2020), pp. 50–60.
16. Ines Feki et al. “Federated learning for COVID-19 screening from Chest X-ray images”. In: Applied soft computing 106 (2021), p. 107330.
17. Jia Deng et al. “ImageNet: A large-scale hierarchical image database”. In: (2009), pp. 248–255. DOI: 10.1109/CVPR.2009.5206848.