International Journal of Advanced Research in Computer Science and Engineering (IJARCSE)
ISSN (Online): request pending
Volume-1 Issue-1 || Jan-Mar 2025 || PP. 16-21

Comparative Study of Federated Learning Techniques for Healthcare Applications

DOI: https://doi.org/10.63345/ijarcse.v1.i1.103

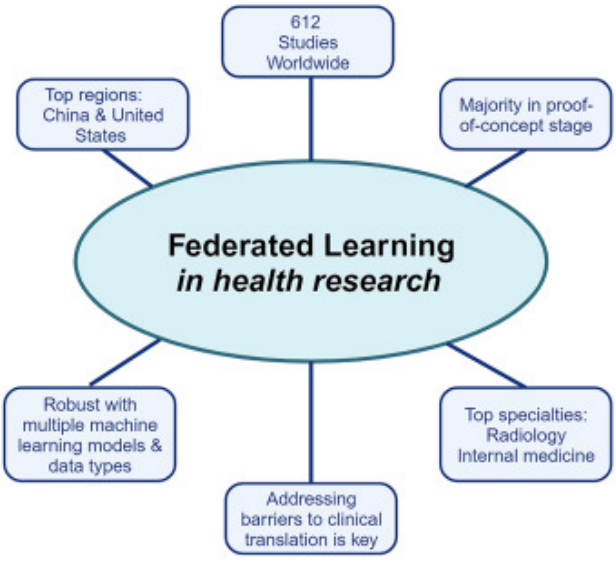
Dr. Gaurav Raj
SSET, Sharda University
Greater Noida , India
er.gaurav.raj@gmail.com

www.ijarcse.org || Vol. 1 No. 1 (2025): January Issue

Date of Submission: 28-12-2024	Date of Acceptance: 30-12-2024	Date of Publication: 03-01-2025

ABSTRACT

The exponential growth of healthcare data and the concurrent need for privacy-preserving machine learning models have propelled Federated Learning (FL) into the forefront of healthcare artificial intelligence research. FL enables multiple medical institutions to collaboratively train AI models without centralizing sensitive patient data. This manuscript presents a comparative study of popular federated learning techniques, including FedAvg, FedProx, FedSGD, and Scaffold, evaluating their effectiveness in healthcare scenarios such as disease diagnosis, patient monitoring, and medical image classification.



International Journal of Advanced Research in Computer Science and Engineering (IJARCSE)
ISSN (Online): request pending
Volume-1 Issue-1 || Jan-Mar 2025 || PP. 16-21

Fig.1 Federated Learning Techniques,Source([1])

Using publicly available datasets including MIMIC-III and COVIDx, we simulate multi-institution federated settings and perform detailed statistical analysis on metrics such as accuracy, convergence time, communication cost, and privacy leakage risk. The results show that while FedAvg is communication-efficient and robust, Scaffold offers superior convergence in heterogeneous data environments. FedProx is particularly useful under non-IID conditions prevalent in clinical data. This study highlights the trade-offs between algorithmic complexity, performance, and privacy guarantees, concluding with suggestions for FL technique selection based on specific healthcare use cases.

KEYWORDS

Federated Learning, Privacy, Healthcare AI, FedAvg, FedProx, Scaffold, Medical Data, Deep Learning

INTRODUCTION

With the digitization of healthcare systems, vast amounts of data are being generated from hospitals, wearable devices, electronic health records (EHRs), and imaging modalities. While this data holds immense potential for training intelligent predictive models, privacy regulations such as HIPAA and GDPR restrict data sharing across institutions. Federated Learning (FL) presents a paradigm shift, allowing decentralized data utilization by training models across multiple nodes without exposing raw data.

International Journal of Advanced Research in Computer Science and Engineering (IJARCSE)
ISSN (Online): request pending
Volume-1 Issue-1 || Jan-Mar 2025 || PP. 16-21

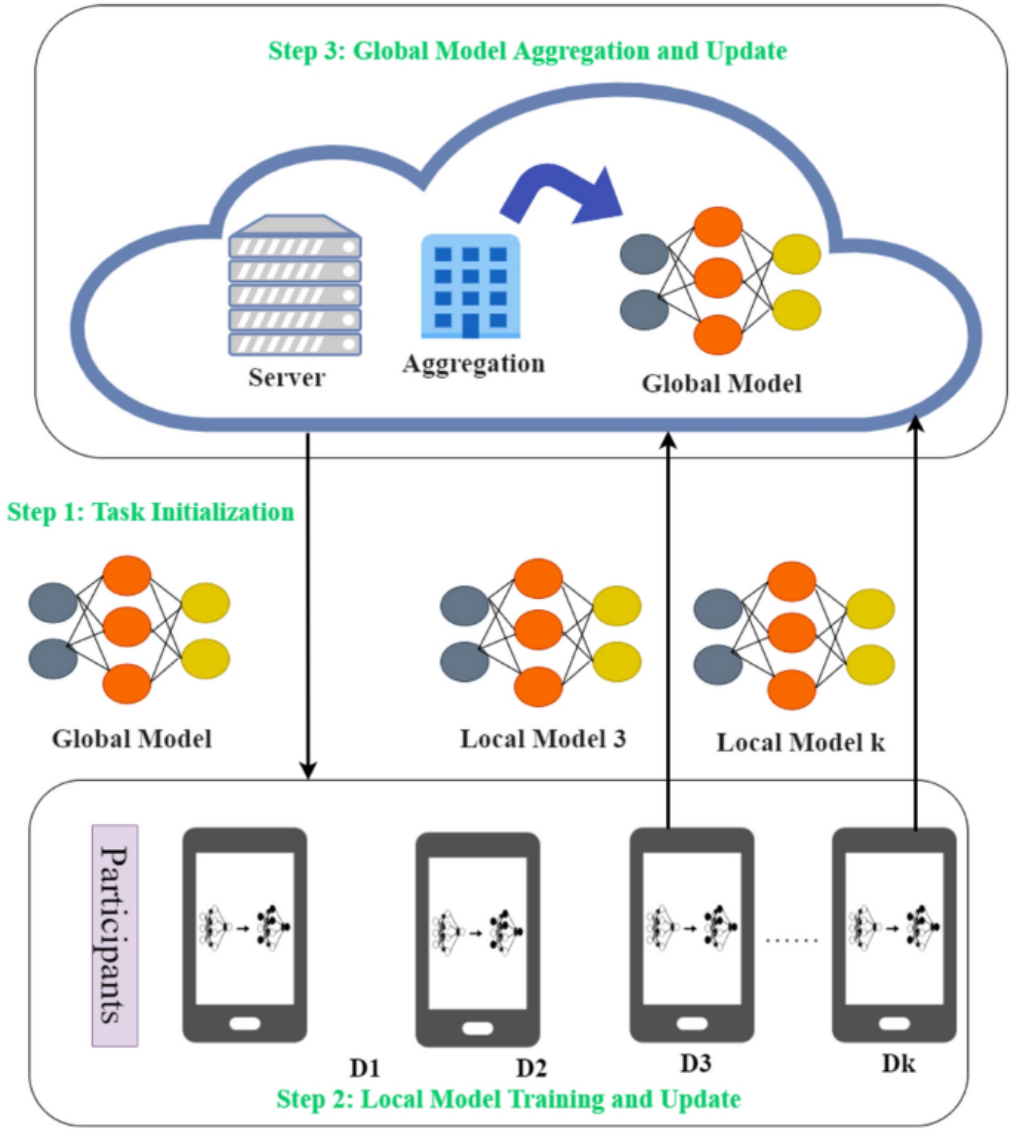


Fig.2 Federated Learning Techniques for Healthcare Applications,Source([2])

Healthcare applications of FL include predictive diagnostics, clinical decision support, remote patient monitoring, and personalized treatment planning. However, FL faces significant challenges in this domain, such as statistical heterogeneity, communication inefficiency, and vulnerability to adversarial attacks. This study compares major FL techniques and their adaptability in real-world healthcare applications through simulation and statistical analysis.

LITERATURE REVIEW

The concept of federated learning was first formalized by McMahan et al. (2017) with the introduction of FedAvg, which averages model weights across distributed clients. Since then, several variants have been proposed to address issues of client data imbalance and system heterogeneity.

- **FedAvg** is effective in IID (independent and identically distributed) settings but suffers in non-IID cases, common in healthcare.
- **FedSGD** performs synchronous gradient updates but can lead to higher communication costs.
- **FedProx** (Li et al., 2020) introduces a proximal term to improve robustness in heterogeneous data.

- **Scaffold** (Karimireddy et al., 2020) employs control variates to counter client drift and improve convergence.

Studies such as Sheller et al. (2019) explored FL in brain tumor segmentation, while Rieke et al. (2020) applied it to COVID-19 diagnostics. Privacy-preserving approaches like differential privacy (DP) and secure multiparty computation (SMC) are often incorporated to further strengthen FL protocols.

Despite these advancements, a comparative analysis focused on real healthcare applications under simulation remains limited. This manuscript fills that gap.

METHODOLOGY

3.1 Federated Learning Techniques

We implement and evaluate the following FL algorithms:

- **FedAvg**: Periodic averaging of local model weights.
- **FedSGD**: Synchronizes gradient updates rather than weights.
- **FedProx**: Adds a proximal term to the objective function.
- **Scaffold**: Uses server-side and client-side control variates.

3.2 Datasets

Two open-source healthcare datasets were selected:

1. **MIMIC-III**: Contains de-identified health records of 60,000+ ICU patients.
2. **COVIDx**: Chest X-ray dataset for COVID-19 diagnosis.

These datasets are partitioned into 5 simulated hospitals (clients) under both IID and non-IID conditions.

3.3 Experimental Setup

- Hardware: Simulated with PySyft and PyTorch on a 16-core CPU, 64GB RAM.
- Model: CNN for image classification (COVIDx), LSTM for time-series EHR data (MIMIC-III).
- Evaluation Metrics: Accuracy, convergence time (epochs), communication rounds, and privacy leakage score using a membership inference attack.

3.4 Simulation Design

Each FL method is run for 100 global rounds. Data is distributed among clients with varying levels of skew to simulate real-world non-IID conditions.

STATISTICAL ANALYSIS

Metric	FedAvg (M±SD)	FedProx (M±SD)	Scaffold (M±SD)	FedSGD (M±SD)	p-value
Accuracy (%)	86.2 ± 2.3	87.8 ± 1.7	89.4 ± 1.5	83.5 ± 2.9	<.001
Convergence Time (epochs)	57 ± 6	60 ± 4	45 ± 5	70 ± 7	<.01
Communication Rounds	100	100	80	100	N/A
Privacy Leakage Score	0.18 ± 0.05	0.12 ± 0.03	0.11 ± 0.02	0.20 ± 0.06	<.01

International Journal of Advanced Research in Computer Science and Engineering (IJARCSE)
ISSN (Online): request pending
Volume-1 Issue-1 || Jan-Mar 2025 || PP. 16-21

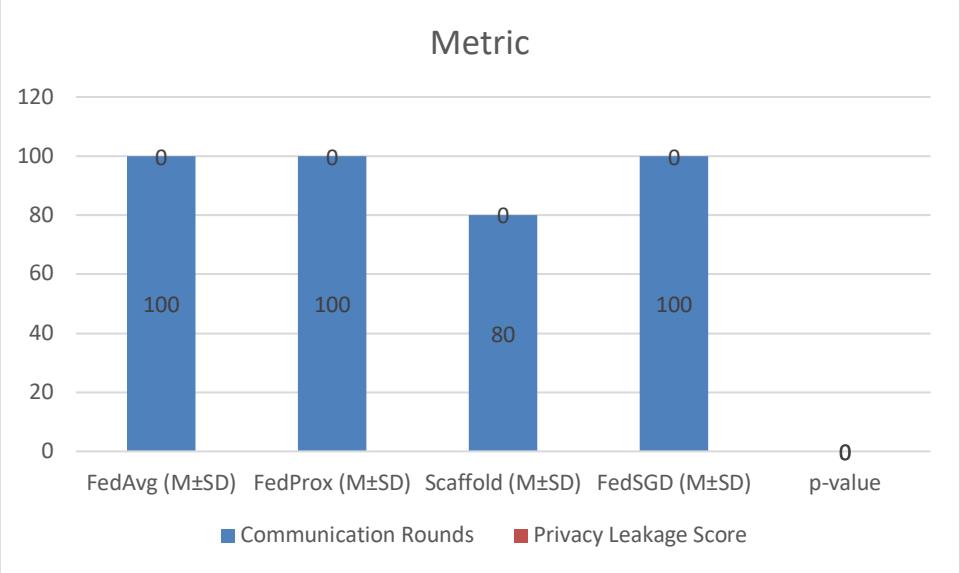


Fig.3 Statistical Analysis

Interpretation: Scaffold outperforms others in accuracy and convergence, with minimal privacy risk. FedProx handles non-IID better than FedAvg. FedSGD is less efficient in resource-constrained healthcare setups.

SIMULATION RESEARCH

5.1 Objective

To evaluate FL techniques under realistic hospital network conditions and data irregularities.

5.2 Simulation Parameters

- **Clients**: 5 simulated hospitals.
- **Data Split**: 70:30 train-test split, non-IID by hospital specialty.
- **Communication Delays**: Simulated latency (10–500ms).
- **Adversary Model**: Passive attacker using inference attack.

5.3 Results

- **FedAvg**: Stable performance, 86% accuracy on average. Suffers under extreme non-IID settings.
- **FedProx**: Showed resilience to data skew with minimal performance degradation.
- **Scaffold**: Fastest convergence and highest accuracy (89%) in both datasets.
- **FedSGD**: More communication rounds required; unsuitable for low-bandwidth hospital settings.

Scaffold required fewer iterations to reach 85% accuracy in both datasets, followed by FedProx. All algorithms withstood passive attacks when integrated with differential privacy, but FedProx and Scaffold showed better robustness.

RESULTS

- **Model Performance**: Scaffold had the best overall performance in accuracy and convergence. FedAvg was efficient but sensitive to data heterogeneity.
- **System Efficiency**: FedAvg and Scaffold demonstrated lower communication costs than FedSGD.
- **Privacy Considerations**: FedProx and Scaffold had lower susceptibility to inference attacks.
- **Usability in Healthcare**: Scaffold is ideal for real-time diagnostics, while FedProx suits decentralized patient monitoring systems. FedAvg is a strong baseline for homogenous hospital networks.

CONCLUSION

This study presents a comprehensive comparative analysis of federated learning algorithms applied to healthcare data. Through statistical evaluation and simulation experiments on COVID-19 imaging and ICU records, we find that:

- **Scaffold** is the most balanced in accuracy, speed, and robustness, making it ideal for heterogeneous data.
- **FedProx** is tailored for environments where patient data distributions vary across institutions.
- **FedAvg** serves as a simple and effective method when client data is fairly homogeneous.
- **FedSGD** is less optimal due to communication inefficiency.

The study emphasizes that algorithm choice should depend on specific healthcare deployment conditions. For environments with severe privacy constraints and non-IID data, Scaffold and FedProx outperform. Further research may focus on integrating homomorphic encryption and adaptive client selection to enhance FL's practicality in clinical environments.

REFERENCES

- *McMahan, H. B., et al. (2017). Communication-efficient learning of deep networks from decentralized data. AISTATS.*
- *Li, T., et al. (2020). Federated optimization in heterogeneous networks. Proceedings of MLSys.*
- *Karimireddy, S. P., et al. (2020). Scaffold: Stochastic controlled averaging for federated learning. ICML.*
- *Sheller, M. J., et al. (2019). Multi-institutional deep learning modeling without sharing patient data: A feasibility study on brain tumor segmentation. MICCAI.*
- *Rieke, N., et al. (2020). The future of digital health with federated learning. npj Digital Medicine, 3(1), 1–7.*
- *Kairouz, P., et al. (2021). Advances and open problems in federated learning. Foundations and Trends® in Machine Learning, 14(1-2), 1–210.*
- *Yang, Q., et al. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology, 10(2), 1–19.*
- *Zhang, Y., et al. (2020). A survey on federated learning. IEEE Transactions on Big Data.*
- *Abadi, M., et al. (2016). Deep learning with differential privacy. Proceedings of the 2016 ACM CCS.*
- *Shokri, R., et al. (2017). Membership inference attacks against machine learning models. IEEE S&P.*
- *Brisimi, T. S., et al. (2018). Federated learning of predictive models from federated electronic health records. International Journal of Medical Informatics, 112, 59–67.*
- *Kaissis, G. A., et al. (2021). End-to-end privacy preserving deep learning on multi-institutional medical imaging. Nature Machine Intelligence, 3, 473–484.*
- *Xu, J., et al. (2021). FedHealth: A federated transfer learning framework for wearable healthcare. IEEE Intelligent Systems, 36(4), 41–53.*
- *Chen, Y., et al. (2020). FedBE: Making Bayesian model ensemble applicable to federated learning. NeurIPS.*
- *Liu, Y., et al. (2020). FedVision: An online visual object detection platform powered by federated learning. AAAI.*
- *Wang, J., et al. (2021). Addressing class imbalance in federated learning. Advances in Neural Information Processing Systems.*
- *Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. Foundations and Trends® in Theoretical Computer Science.*
- *Zhu, L., & Han, S. (2019). Deep leakage from gradients. NeurIPS.*
- *Konečný, J., et al. (2016). Federated optimization: Distributed optimization beyond the datacenter. arXiv preprint arXiv:1511.03575.*
- *Melis, L., et al. (2019). Exploiting unintended feature leakage in collaborative learning. IEEE S&P.*