Federated Learning for Image Classification in Distributed Medical Imaging Systems

Anirudh Kalva
2288613
akalva@cougarnet.uh.edu

Rakesh Chary Bangaroj
2290052
rbangaro@cougarnet.uh.edu

Sujan Chithaluri
2304283
schithal@cougarnet.uh.edu

Abstract

Medical imaging is essential for diagnosing diseases such as cancer, heart conditions, and neurological disorders, but training effective models requires access to large amounts of data. Due to the strict privacy regulations such as HIPAA and GDPR, hospitals and research centers cannot easily share patient data, which limits collaboration and makes it harder to build better diagnostic tools. This project aims to solve that problem by using Federated Learning (FL), a method that allows hospitals to work together and train machine learning models without ever sharing their actual data. Instead, each hospital keeps its data private and only shares model updates, ensuring privacy while still improving the overall performance of the model across different institutions.

1 Introduction

Traditional machine learning and deep learning techniques rely on centralized datasets for model training. This approach requires transferring data from various sources, such as hospitals or institutions, to a central server, raising significant privacy concerns. Sensitive data like medical records stored in centralized databases is particularly vulnerable to cyberattacks, increasing the risks of data breaches and reidentification of deidentified information. These limitations make centralized approaches unsuitable for privacy-critical domains like healthcare.

Federated Learning, addresses these challenges by enabling decentralized model training. As illustrated in Figure 1, FL eliminates the need for data transfer by allowing training to occur locally on client devices. Only model updates, such as gradients or weights, are sent to a central server, which aggregates these updates to build a global model. This decentralized approach significantly reduces privacy risks, mitigates the likelihood of data breaches, and leverages the computational resources of distributed devices. Initially applied in mobile applications, FL has expanded to other domains, including healthcare, where it facilitates collaborative training across institutions while ensuring patient data remains secure.

In this project, we aim to implement Federated Learning for distributed medical imaging tasks using the PathMNIST dataset. Our work focuses on exploring and evaluating three popular FL strategies—FedAvg, FedProx, and FedNova—to address challenges such as data heterogeneity and non-IID distributions across clients. By leveraging these techniques, we aim to enhance model performance while ensuring data privacy, paving the way for secure and effective collaborative learning in the medical field.

Contributions: Anirudh Kalva contributed to dataset preparation by finalizing the PathMNIST dataset and performing preprocessing, including resizing and normalization. He implemented the

FedAvg strategy, integrated Differential Privacy (DP) mechanisms for data security, and developed evaluation metrics like testing accuracy and training loss. **Rakesh Chary Bangaroj** focused on simulating data heterogeneity through IID and Non-IID setups and implemented the FedProx strategy, optimizing its hyperparameters. He also worked on the CNN model and documented performance trends and prepared sections of the methodology and results. **Sujan Chithaluri** implemented the Flower architecture for federated learning, establishing a robust client-server simulation framework to support multiple FL strategies. Implemented the FedNova strategy, and ensured effective client-server communication. Sujan also contributed to documenting the methodology and technical implementation of the client-server architecture and FedNova performance.

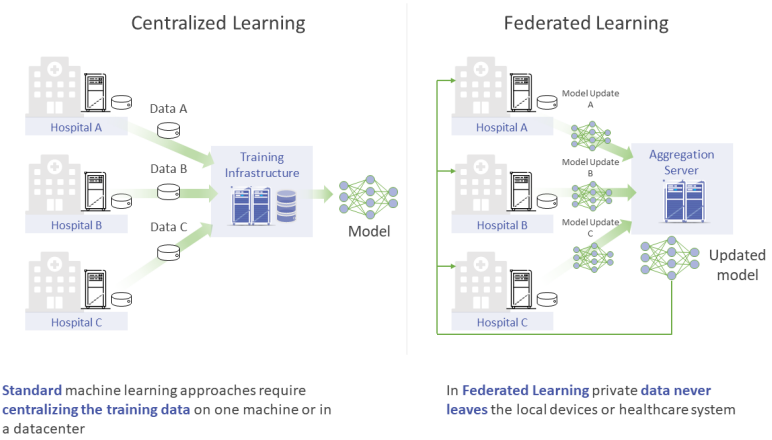


Figure 1: Comparison of centralized learning and Federated Learning. Unlike centralized learning, FL ensures that sensitive data never leaves local devices, mitigating privacy risks.

2 Literature Review

Federated Learning has gained significant traction in recent years, particularly in applications where privacy is paramount, such as healthcare. Several works have explored the use of FL in distributed environments to solve machine learning problems between multiple stakeholders.

Sai et al.[2] propose a novel integration of FL with non-fungible tokens (NFTs) to create a secure, privacy-preserving system for medical data sharing in smart healthcare. Their model ensures decentralized data ownership while supporting intelligent diagnosis through collaborative learning. NFTs provide immutable and secure access to medical records, enhancing trust and transparency. The study emphasizes how this fusion can address privacy concerns and improve interoperability in healthcare systems. It presents a unique approach to secure data-driven diagnostics.

Bashir et al.[4] explore the role of federated learning in the evolving healthcare metaverse. They discuss concepts, applications, and challenges of integrating FL to enable seamless, collaborative healthcare solutions in virtual environments. Their study emphasizes the metaverse's potential for shared learning and diagnostics while addressing privacy and computational constraints. It also identifies critical challenges, such as scalability, security, and interoperability. This forward-looking research provides a roadmap for integrating FL into futuristic healthcare systems.

Subashchandrabose et al.[5] present an ensemble FL approach for diagnosing multi-order lung cancer with improved accuracy and reliability. Their method combines multiple federated models to enhance diagnostic performance while preserving data privacy. The study showcases the collaborative potential of FL in tackling complex medical conditions through decentralized learning. By leveraging ensemble techniques, this work provides a robust solution for precision diagnostics. It highlights the value of FL in advancing cancer diagnostics.

3 Problem Setting and Formulation

The problem is structured as a distributed multi-class image classification task using the PathMNIST dataset, which is designed for medical imaging applications. The goal is to collaboratively train a

machine learning model across multiple hospitals while addressing critical challenges such as **data heterogeneity** and **data privacy**.

3.1 Data Heterogeneity

Data heterogeneity is a significant challenge in Federated Learning (FL), where the size and distribution of datasets vary across participating clients, reflecting real-world scenarios in decentralized medical data. To evaluate these challenges, we use the **PathMNIST** dataset, which is specifically designed for machine learning applications in medical image analysis, particularly histopathology. Pathology MNIST, part of the MedMNIST dataset collection, promotes the development of AI for biomedical image analysis. It consists of histopathological images representing tissue samples, resized to smaller formats (e.g., 28×28 pixels) in RGB color. Each image is labeled into one of nine classes, as shown in Figure 2, to classify tissue samples as healthy or pathological.

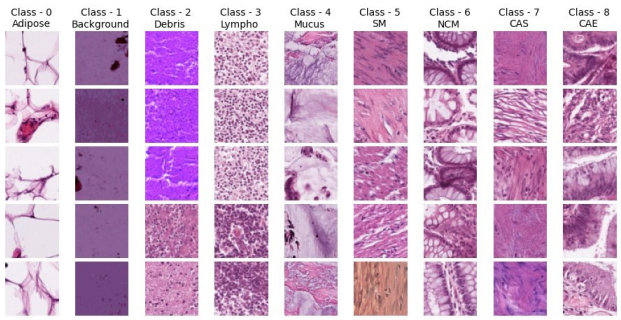
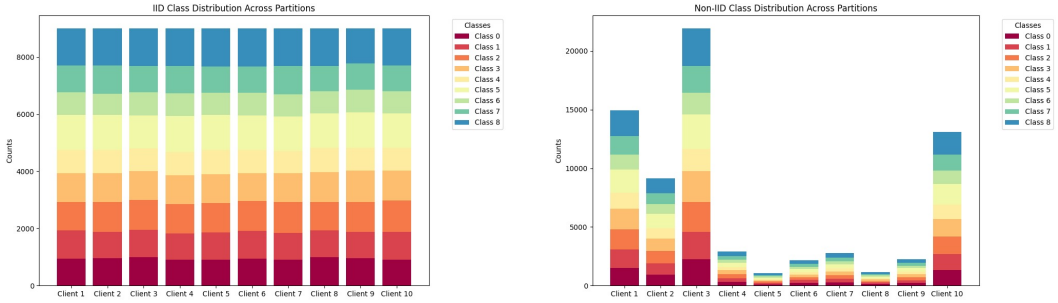


Figure 2: Sample images from the Pathology MNIST dataset, illustrating the 9 different tissue types commonly found in Colorectal Cancer (CRC) which includes both tumor and non-tumor tissues. Adipose (Class 0), Background (Class 1), Debris (Class 2), Lympho (Class 3), Mucus (Class 4), Smooth Muscle (Class 5), Normal Colon Mucosa (Class 6), Cancer-Associated Stroma (Class 7), and Colorectal Adenocarcinoma Epithelium (Class 8).

IID and Non-IID Data

In federated learning (FL) settings, data across participating hospitals can vary significantly in distribution and quantity, leading to distinct IID and Non-IID scenarios. In **IID** scenarios, the data is uniformly distributed across hospitals, ensuring similar proportions of features and labels, which facilitates consistent model training. Figure 3 illustrates the IID class distribution across clients, where data is evenly distributed among all participants. In **Non-IID** scenarios, the distribution varies significantly among hospitals. For instance, one hospital may have a large, balanced dataset, while another has a small, skewed dataset, reflecting real-world heterogeneity and posing challenges for model convergence. The same figure demonstrates the Non-IID class distribution, showcasing significant variations in data quantity and class representation across clients.



(a) IID Class Distribution

(b) Non-IID Class Distribution

Figure 3: Class Distributions Across Clients for IID (left) and Non-IID (right) Settings

3.2 Data Privacy

Strict regulations like GDPR and HIPAA mandate protections for sensitive medical data, restricting the sharing of raw data. Federated Learning (FL) enables decentralized model training, sharing only model updates while keeping data local. To enhance security, Differential Privacy (DP) introduces calibrated noise to updates, preventing reconstruction of individual data points. Controlled by parameters like the privacy budget (ϵ), DP ensures privacy while maintaining model performance. This approach provides a robust framework for complying with stringent data protection laws.

3.3 Mathematical Formulation

The federated learning task can be mathematically expressed as a distributed optimization problem:

$$\min_{w} \sum_{k=1}^{K} p_k F_k(w),$$

where:

- K is the total number of participating hospitals (clients).
- $F_k(w)$ is the local objective function for hospital k, representing the loss computed on its private dataset.
- p_k is the proportion of the total data contributed by hospital k, ensuring that updates are weighted based on dataset size.
- w denotes the global model weights that are iteratively updated based on aggregated client contributions.

Each hospital optimizes its local model by minimizing $F_k(w)$, typically using stochastic gradient descent (SGD) or a similar optimization algorithm. The local updates are then aggregated at the central server to update the global model:

$$w_{t+1} = w_t - \eta \sum_{k=1}^{K} p_k \nabla F_k(w_t),$$

where:

- w_t and w_{t+1} are the global model weights at the current and next iterations, respectively.
- η is the learning rate.
- $\nabla F_k(w_t)$ is the gradient of the loss function for hospital k at iteration t.

By iterating through local training and global aggregation, the model converges to a solution that reflects the combined knowledge of all participating hospitals without compromising the privacy of individual datasets. This approach balances the diverse needs of medical institutions, ensuring both privacy and effective model training.

4 Methodology and Implementation

4.1 Federated Learning Workflow

The Federated Learning (FL) process involves four key stages that enable decentralized model training across distributed clients while preserving data privacy. The workflow, as shown in Figure 4, is

Distribute Model: The central server initializes a global model w_t and distributes it to all participating clients (e.g., hospitals, devices). These clients hold local data, which remains private and never leaves their systems.

Local Training: Each client k trains the global model w_t locally on its private dataset $\mathcal{D}_k$ by minimizing its local objective function:

$$F_k(w) = \frac{1}{|\mathcal{D}_k|} \sum_{i \in \mathcal{D}_k} f_i(w),$$

where $f_i(w)$ is the loss on data point i, and $|\mathcal{D}_k|$ is the size of the local dataset. The result of this training is an updated local model w_k.

Aggregation: After local training, clients send their updated models w_k to the central server. The server aggregates these updates using specific techniques to compute the new global model w_{t+1}.

Model Update: The aggregated global model w_{t+1} is redistributed to the clients, starting the next training round. This iterative process continues until the model achieves satisfactory performance.

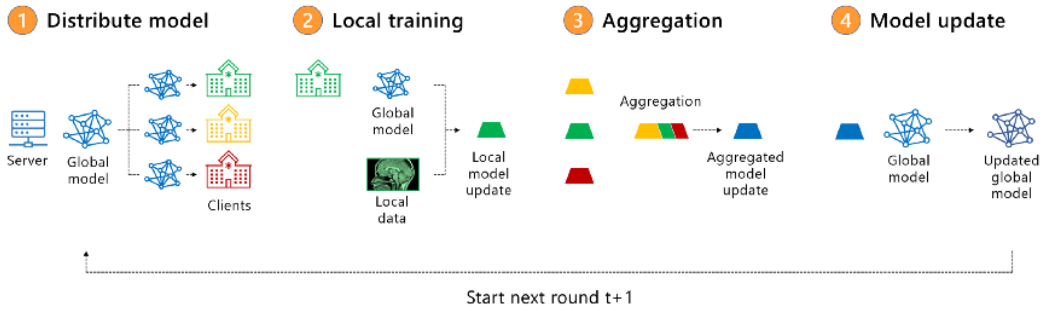


Figure 4: Federated Learning workflow: Decentralized training through model distribution, local updates, aggregation, and global model updates.

4.2 Techniques Used in Federated Learning

To address challenges such as data heterogeneity and non-IID distributions across clients, we implemented and evaluated three popular FL techniques:

4.2.1 FedAvg (Federated Averaging)

FedAvg aggregates local model updates by computing a weighted average, where the weights are proportional to the size of the local datasets. Mathematically, the global model update is given by:

$$w_{t+1} = \sum_{k=1}^{K} \frac{|\mathcal{D}_k|}{\sum_{j=1}^{K} |\mathcal{D}_j|} w_k,$$

where:

- w_k: Local model from client k,
- $|\mathcal{D}_k|$: Size of the local dataset on client k,
- K: Total number of clients.

This technique is effective for IID data but struggles with non-IID data distributions, as the weighted averaging may not capture the diversity in client data.

4.2.2 FedProx (Federated Proximal)

FedProx extends FedAvg by adding a proximal term to the local objective function, which penalizes updates that deviate significantly from the global model. The local objective function for client k is modified as:

$$F_k(w) = \frac{1}{|\mathcal{D}_k|} \sum_{i \in \mathcal{D}_k} f_i(w) + \frac{\mu}{2} \|w - w_t\|^2,$$

where:

- μ: Proximal regularization parameter,
- w_t: Global model weights at the current round,
- w: Local model weights.

This proximal term stabilizes training in non-IID settings by keeping local updates closer to the global model.

4.2.3 FedNova (Federated Normalization)

FedNova addresses the issue of imbalances caused by clients performing different numbers of local training steps. Instead of averaging updates directly, FedNova normalizes the updates from each client by the number of local training steps τ_k. The global model update is given by:

$$w_{t+1} = w_t + \eta \sum_{k=1}^{K} \frac{\tau_k}{\sum_{j=1}^{K} \tau_j} \Delta_k,$$

where:

- η: Learning rate,
- $\Delta_k = w_k - w_t$: Model update from client k,
- τ_k: Number of local training steps performed by client k.

This normalization ensures that all clients contribute fairly, regardless of their computational resources or dataset sizes, improving convergence and fairness.

4.3 Implementation

4.3.1 Overview

The Federated Learning (FL) framework was implemented using PyTorch for building and training the CNN model, and Flower (FLwr) for simulating client-server communication and federated training workflows. This setup facilitated the evaluation of **FedAvg**, **FedProx**, and **FedNova** techniques in heterogeneous, non-IID scenarios. To enhance data security, Differential Privacy (DP) was integrated during the aggregation process. Key hyperparameters included a learning rate of 0.001, 10 local epochs (per client), 50 communication rounds (between clients and the server), and a batch size of 64. The pipeline was executed on a GPU-enabled system to efficiently manage computational demands.

For the **FedProx** strategy, the key parameters were a proximal term (μ) of 0.01 to stabilize updates by penalizing deviations from the global model, momentum of 0.9 to accelerate gradient descent, and weight decay of 1×10^{-5} to prevent overfitting. Similarly, for the **FedNova** strategy, momentum of 0.9 and weight decay of 1×10^{-5} were applied to improve gradient descent and maintain model generalization.

4.3.2 Dataset and Preprocessing

The **PathMNIST** dataset was used to evaluate the framework. It contains multi-class data with images of tissue types. The images were resized to 28×28 and normalized with a mean of 0.5 and a standard deviation of 0.5. The dataset was divided into 90,000 training samples, 10,000 validation samples, and 7,000 testing samples. To simulate real-world scenarios, the dataset was partitioned into non-IID subsets by assigning different classes to specific clients, creating heterogeneity across datasets. Data loaders with a batch size of 64 were created for each client to facilitate mini-batch gradient descent during local training.

4.3.3 Model Architecture

A lightweight **Convolutional Neural Network (CNN)** was employed as the base model for classification, designed to balance computational efficiency and accuracy for distributed federated learning environments. The architecture begins with two convolutional layers for feature extraction: the first applies six filters of size 5×5 to the input, followed by ReLU activation and 2×2 max-pooling for downsampling, and the second uses 16 filters of size 5×5, with similar ReLU activation and max-pooling. The extracted features are flattened and passed through three fully connected layers: the first maps the features to 120 neurons with ReLU activation, the second reduces them to 84 neurons with ReLU activation, and the final output layer contains 9 neurons corresponding to the total classes.

4.3.4 Client-Server Simulation

The **Flower** framework was used to simulate communication between clients and the server, modeling a real-world federated learning setup where devices may not always be available. The system comprised 10 clients, each representing a simulated hospital or device with its private dataset. In each

round, 50% of the clients (5 clients) were selected for training and evaluation. Clients trained locally for 10 epochs and sent their updates to the central server, which aggregated them using the different startegies. A minimum of 3 clients required for both training and evaluation in each round, and a total of 50 communication rounds between clients and the server.

4.3.5 Differential Privacy Integration

To enhance data security, **Differential Privacy (DP)** was integrated at the client side using fixed gradient clipping and noise addition, ensuring individual data privacy before updates were shared with the server. The DP mechanism employed a noise multiplier of 0.2 and a gradient clipping norm of 3, balancing privacy preservation with model utility. In each round, the updates from participating clients were clipped and perturbed with calibrated noise. This approach, controlled by the privacy budget (ϵ), prevents the inference of sensitive individual data.

4.3.6 Training Process

The federated training process was executed over **50** communication rounds, with each round involving three key steps. First, the server distributed the global model to a subset of clients for local training. During local training, clients optimized their models using stochastic gradient descent (SGD) with hyperparameters such as a learning rate, momentum, and weight decay, tailored to each FL technique. Each client iteratively computed the loss using cross-entropy and the proximal term, performed backpropagation, and updated their model parameters. Finally, the server aggregated the locally updated models using the respective FL strategy—**FedAvg**, **FedProx**, or **FedNova**—and redistributed the updated global model to all clients for the next round. This iterative process ensured model convergence while addressing challenges like data heterogeneity and client availability.

4.3.7 Evaluation

The global model's performance was evaluated after each communication round using a centralized test dataset. The evaluation process tracked three key metrics: the **model accuracy**, calculated as the percentage of correctly classified samples, the **model loss**, measured using cross-entropy loss to assess prediction confidence, and **training stability**, analyzed by monitoring convergence trends across rounds. If the accuracy surpassed the previous best, the current model's weights were saved as the best model. This iterative evaluation provided insights into the model's improvement and ensured the retention of the most accurate global model.

5 Results

The evaluation focused on assessing the performance of the implemented Federated Learning (FL) framework under a Non-IID data setup to simulate realistic client heterogeneity. The results compare the effectiveness of different FL strategies—FedAvg, FedProx, and FedNova—based on metrics such as testing accuracy and minimum loss of the global model. These metrics provide insights into the robustness and convergence behavior of each strategy in handling decentralized data distributions.

Table 1: Comparison of Testing Accuracy and Minimum Loss for Federated Learning Strategies

Strategy	**Testing Accuracy (%)**	**Minimum Loss**
FedAvg	79.89	0.47
FedProx	81.30	0.43
FedNova	86.20	0.39

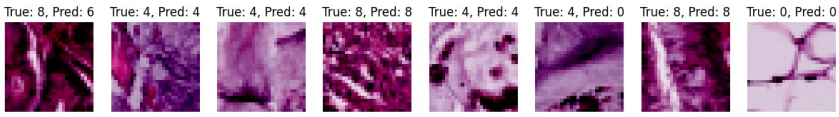
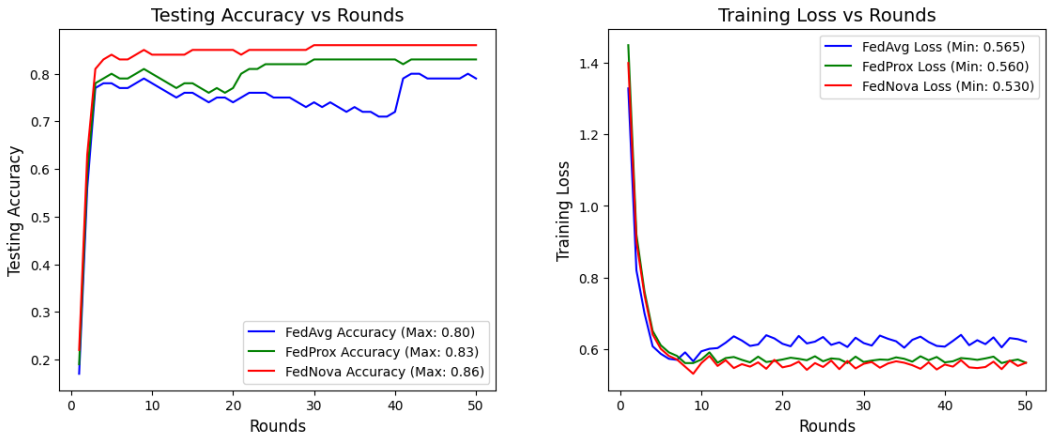


Figure 5: Few examples of the predictions from the PathMNIST dataset. The labels on each image indicate the true class (True) and the predicted class (Pred) for the corresponding sample.



(a) Testing Accuracy

(b) Training Loss

Figure 6: Testing Accuracy and Training Loss for Federated Learning Strategies

The evaluation results highlight that **FedNova** outperforms other strategies in both minimizing loss and accuracy. As shown in Figure 6b, **FedNova** achieves the lowest minimum loss compared to **FedAvg** and **FedProx**, demonstrating superior optimization stability. Additionally, Figure 6a shows that **FedNova** achieves the highest testing accuracy at 86.2%, followed by **FedProx** at 81.3% and **FedAvg** at 79.89%. Furthermore, classification analysis in Figure 5 illustrates that the **FedNova** model accurately predicts most true labels from the testing dataset, further confirming its effectiveness in handling non-IID data scenarios.

6 Conclusion

Due to numerous privacy and confidentiality issues, hospitals' extensive clinical data archives contain a wealth of knowledge that is largely untapped. As a potential approach to learning from decentralized medical data, such as pathology images, we implemented federated learning integrated with differential privacy in this work. Federated learning allows training models without explicitly sharing patient data, thus mitigating some confidentiality and privacy issues associated with clinical data. This is enhanced by differential privacy, which provides quantitative limits on the privacy offered. Using non-IID data distributions to simulate real-world scenarios, we evaluated different techniques, with **FedNova** emerging as the best-performing model due to its ability to handle client heterogeneity effectively. Private federated learning achieved comparable results to conventional centralized training and demonstrates potential as a viable solution for distributed training on medical data.

7 Future Work

In future work, we aim to extend this study by incorporating advanced optimization algorithms, such as adaptive learning rate techniques, to further improve model convergence in non-IID scenarios. Additionally, integrating communication-efficient strategies, such as model compression or sparsification, could reduce the overhead of transmitting updates between clients and the server. We also plan to explore more robust privacy-preserving mechanisms, such as Secure Multiparty Computation (SMC) and Homomorphic Encryption, to enhance security beyond Differential Privacy. Finally, expanding the framework to support other complex medical datasets and tasks, such as segmentation and detection, could further demonstrate the practical applicability of Federated Learning in real-world healthcare environments.

8 References

1. Tripathy, S.S., Sujit, B., Lal, C.C., Mukherjee, T., Kim, S., Jana, S., Fazal, I.M. (2024). *FedHealthFog: A federated learning-enabled approach towards healthcare analytics over fog computing platform*. Heliyon, 10(5):e26416.

2. Sai, S., Hassija, V., Chamola, V., Guizani, M. (2024). *Federated learning and NFT-based privacy-preserving medical-data-sharing scheme for intelligent diagnosis in smart healthcare*. IEEE Internet of Things Journal, 11(4):5568–5577. https://doi.org/10.1109/JIOT.2023.3308991.

3. Ullah, F., Srivastava, G., Xiao, H., Ullah, S., Lin, J.C.-W., Zhao, Y. (2023). *A scalable federated learning approach for collaborative smart healthcare systems with intermittent clients using medical imaging*. IEEE Journal of Biomedical and Health Informatics. https://doi.org/10.1109/JBHI.2023.3282955.

4. Bashir, A.K., et al. (2023). *Federated learning for the healthcare metaverse: concepts, applications, challenges, and future directions*. IEEE Internet of Things Journal, 10(24):21873–21891. https://doi.org/10.1109/JIOT.2023.3304790.

5. Subashchandrabose, U., John, R., Anbazhagu, U.V., Venkatesan, V.K., Thyluru Ramakrishna, M. (2023). *Ensemble federated learning approach for diagnostics of multi-order lung cancer*. Diagnostics, 13:3053. https://doi.org/10.3390/diagnostics13193053.

Federated Learning for Image Classification in Distributed Medical Imaging Systems

Anirudh Kalva
2288613
akalva@cougarnet.uh.edu

Rakesh Chary Bangaroj
2290054
rbangaro@cougarnet.uh.edu

Sujan Chithaluri
2304283
schithal@cougarnet.uh.edu

Abstract

Medical imaging is essential for diagnosing diseases like cancer, heart conditions, and neurological disorders, but training effective models requires access to large amounts of data. Due to strict privacy regulations like HIPAA and GDPR, hospitals and research centers can't easily share patient data, which limits collaboration and makes it harder to build better diagnostic tools. This project aims to solve that problem by using Federated Learning (FL), a method that allows hospitals to work together and train machine learning models without ever sharing their actual data. Instead, each hospital keeps its data private and only shares model updates, ensuring privacy while still improving the overall performance of the model across different institutions.

1 Literature Review

Federated Learning has gained significant traction in recent years, particularly in applications where privacy is paramount, such as healthcare. Several works have explored the use of FL in distributed environments to solve machine learning problems across multiple stakeholders.

- Tripathy et al. [1] proposed a Federated Learning (FL) model on a fog computing platform, using a greedy heuristic technique with a radio access network to select the optimal fog node for global aggregation, improving the efficiency of the aggregation process in healthcare applications.
- Sai et al. [2] introduced FL for intelligent diagnosis in smart healthcare, incorporating blockchain-based incentive mechanisms and non-fungible tokens (NFTs) for privacy-preserving medical data sharing. The Polyak-averaging technique was used to aggregate local models into a global one, ensuring data privacy and secure sharing.
- Ullah et al. [3] developed a scalable FL framework for interactive smart healthcare systems, using data augmentation to equalize datasets and enhance the scalability of local model training across healthcare environments.
- Bashir et al. [4] explored FL integration within a healthcare metaverse, combining cloud-edge computing, IoT, blockchain, and semantic communication. Their approach enhanced privacy, interoperability, data management, and cross-model usage in healthcare systems.

Despite these advancements, there remains a need for a secure and scalable FL system that can handle the challenges of data heterogeneity and privacy in medical imaging.

2 Proposed Solution

To address this problem, this project proposes a Federated Learning (FL) framework for distributed medical image classification, tackling challenges related to privacy, security, and data heterogeneity. Key contributions and solutions include:

- Federated Learning with Privacy and Security: The project will develop a FL system where hospitals collaborate to train a medical image classification model (for X-rays, MRIs, etc.) using the FedAvg algorithm. To ensure privacy, Differential Privacy (DP) will be integrated, adding noise to model updates to protect sensitive patient data. Secure aggregation methods, like RSA and homomorphic encryption, will also be used to ensure that model updates are encrypted, so the central server only sees the combined results without accessing individual hospital data..
- Considering Medical Datasets: Publicly available datasets, such as the NIH Chest X-rays or COVID-19 Radiography dataset or Brats2020, will be used to simulate a distributed hospital environment [5]. These datasets will allow testing of the FL framework's effectiveness on real-world medical data.
- Evaluation Metrics: Performance will be measured through accuracy, precision, recall, and F1-score, along with the privacy-accuracy trade-offs introduced by DP. Scalability will be tested by simulating more clients and evaluating communication efficiency, model convergence, and computation time.

This solution promises collaborative learning, allowing medical institutions to harness the power of machine learning without compromising patient confidentiality. By integrating privacy and security techniques, the proposed framework addresses both the technical and ethical challenges associated with data sharing in healthcare, making it a viable solution for real-world medical applications.

3 References

[1] Tripathy, S.S., Sujit, B., Lal, C.C., Mukherjee, T., Kim, S., Jana, S., Fazal, I.M. (2024). *FedHealthFog: A federated learning-enabled approach towards healthcare analytics over fog computing platform*. Heliyon, 10(5):e26416.

[2] Sai, S., Hassija, V., Chamola, V., Guizani, M. (2024). *Federated learning and NFT-based privacy-preserving medical-data-sharing scheme for intelligent diagnosis in smart healthcare*. IEEE Internet of Things Journal, 11(4):5568–5577. https://doi.org/10.1109/JIOT.2023.3308991.

[3] Ullah, F., Srivastava, G., Xiao, H., Ullah, S., Lin, J.C.-W., Zhao, Y. (2023). *A scalable federated learning approach for collaborative smart healthcare systems with intermittent clients using medical imaging*. IEEE Journal of Biomedical and Health Informatics. https://doi.org/10.1109/JBHI.2023.3282955.

[4] Bashir, A.K., et al. (2023). *Federated learning for the healthcare metaverse: concepts, applications, challenges, and future directions*. IEEE Internet of Things Journal, 10(24):21873–21891. https://doi.org/10.1109/JIOT.2023.3304790.

[5] Subashchandrabose, U., John, R., Anbazhagu, U.V., Venkatesan, V.K., Thyluru Ramakrishna, M. (2023). *Ensemble federated learning approach for diagnostics of multi-order lung cancer*. Diagnostics, 13:3053. https://doi.org/10.3390/diagnostics13193053.