Federated Learning for Pneumonia Detection and Segmentation

Leveraging ResNet for Classification and nnU-Net for Segmentation in a Privacy-Preserving Framework

N Nagabhushanam (221CS231) N Yaswanth (221CS232)

under the guidance of **Dr Annappa B**
Department of Computer Science and Engineering
NITK Surathkal

May 9, 2025

Overview

Federated Learning: A Privacy-Preserving ML Paradigm

- Federated Learning (FL) is a decentralized machine learning technique that trains models directly on client devices without transmitting raw data.
- Enhances privacy and complies with regulations like GDPR and CCPA.
- Reduces communication overhead by sharing only model updates instead of raw datasets.
- Scales efficiently across diverse devices and organizations.
- Well-suited for sensitive domains such as healthcare and finance.
- This presentation explores FL's mechanisms, applications, and supporting technologies.
- Highlights include the Flower framework and advanced data partitioning strategies for real-world deployment.

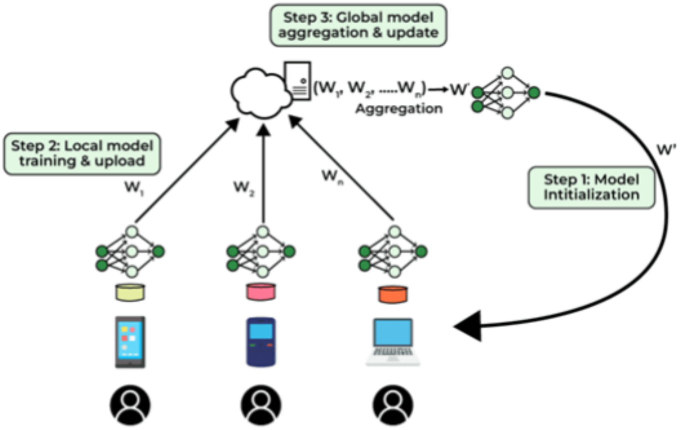


Figure: Federated Learning Workflow Diagram

How Federated Learning Works

- **Initialize Global Model:** A central server initializes the model with random or pre-trained weights.
- **Distribute Model to Clients:** The global model is sent to decentralized client devices or organizations.
- **Local Model Training:** Clients perform training on local data for limited epochs or mini-batches.
- **Aggregate Updates:** Clients send only model updates back; the server aggregates them using techniques like Federated Averaging.
- **Iterate Until Convergence:** The process repeats, progressively improving the global model across rounds.

Applications of Federated Learning

- **Healthcare:** Train diagnostic models across multiple hospitals while preserving patient confidentiality, enabling better medical insights from distributed datasets.
- **Finance:** Facilitate fraud detection collaboration across banks while complying with strict data privacy mandates, making detection more robust with federated insights.
- **Smart Devices:** Enhance AI personalization on mobile devices, such as predictive keyboards, without exposing sensitive user data.

Benefits Over Centralized Machine Learning

- **Data Privacy & Compliance:** Raw data remains on clients, fully adhering to privacy laws like GDPR and CCPA, minimizing risk of exposure.
- **Reduced Communication Costs:** Only model updates, which are much smaller than data, are communicated, leading to efficiency gains in bandwidth-constrained environments.
- **Access to Diverse Data:** Incorporates data from geographically and demographically diverse clients, enhancing model generalization and robustness.

Flower: An Open-Source Federated Learning Framework [Labs, 2023]

- **Cross-Platform Compatibility:** Supports major ML frameworks like PyTorch, TensorFlow, and JAX for versatile model development.
- **Flexible Client-Server Architecture:** Accommodates heterogeneous clients including mobile, edge, and cloud devices.
- **Simulation & Deployment:** Offers simulation capabilities on a single machine before scaling to real-world distributed environments.
- **Privacy & Scalability:** Integrates privacy measures like Differential Privacy and manages thousands of clients efficiently.

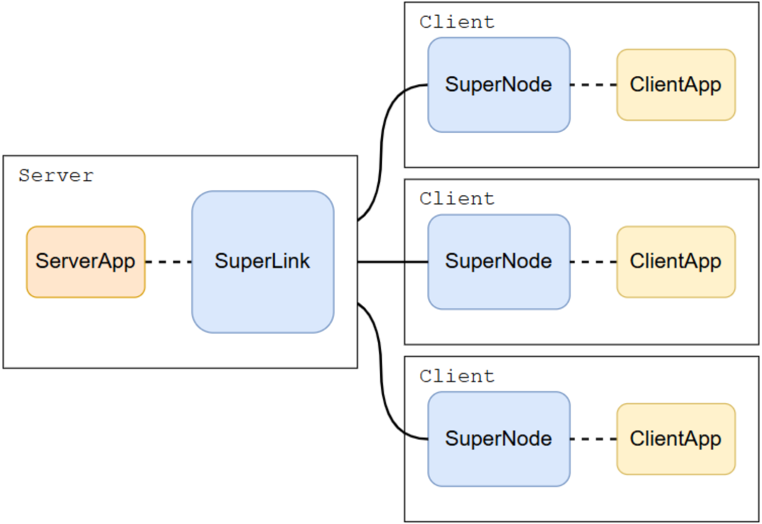


Figure: The basic Flower architecture for federated learning

Hybrid Partition in Federated Learning

- **Dirichlet Distribution:** Introduces controlled data skew by assigning varying class proportions to different clients, simulating real-world non-IID data.
- **Stratified Sampling:** Ensures every client has representation from all classes, preventing complete exclusion of certain classes in local datasets.
- **Why Hybrid Partition?:** Balances data heterogeneity and coverage to improve model generalization across non-IID and imbalanced client data scenarios.

ResNet-50: Deep Residual Learning [He et al., 2015]

- **What is ResNet-50?** A 50-layer deep convolutional neural network that uses residual connections to ease training of very deep networks.
- **Core Concept:**
  - Introduces *skip connections* or *identity shortcuts* to bypass non-linear layers.
  - Helps mitigate vanishing gradients and degradation in deep networks.
- **Architecture Highlights:**
  - Composed of a stem (Conv + MaxPool) followed by 4 stages.
  - Uses **Bottleneck blocks** (1x1 $\rightarrow$ 3x3 $\rightarrow$ 1x1 convolutions).
  - Stage configuration: [3, 4, 6, 3] bottleneck blocks respectively.
- **Applications:** Image classification, feature extraction, transfer learning for various CV tasks.

Residual Networks (ResNet50)

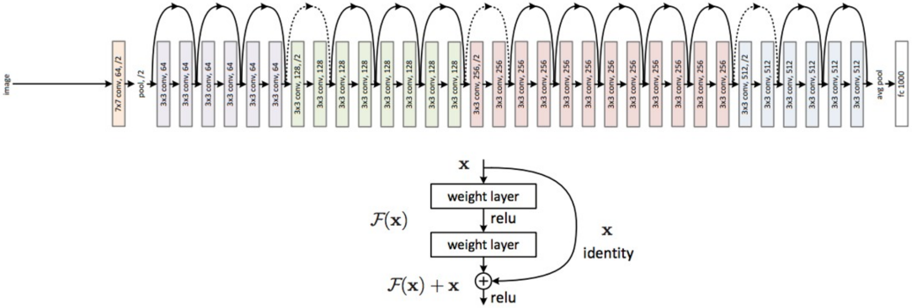


Figure: Network architecture generated by ResNet-50

nnU-Net: Self-Configuring Segmentation [Isensee et al., 2021]

- **What is nnU-Net?** A deep learning framework that auto-configures U-Net-based pipelines for biomedical image segmentation.
- **Key Features:**
  - Supports 2D/3D images with arbitrary modalities.
  - No manual tuning—analyzes dataset and adapts architecture.
  - Provides strong out-of-the-box performance on diverse datasets.
- **Use Cases:** MDS

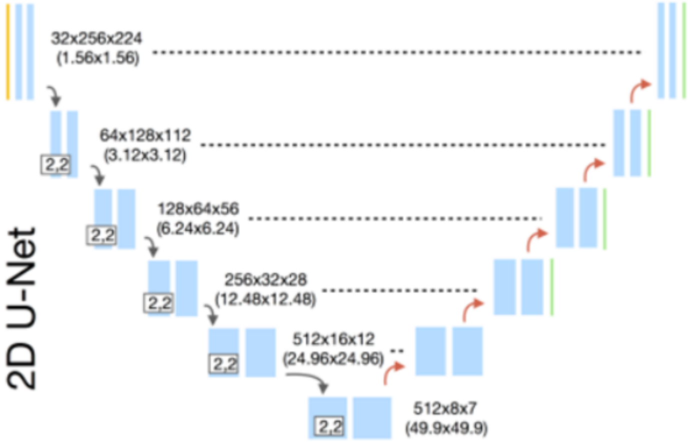


Figure: Network architectures generated by nnU-Net

Datasets Used

- **Chest X-ray Pneumonia Dataset**
  Kaggle - paultimothymooney
  Contains **5.8k images** across two classes: Normal and Pneumonia.

- **RSNA Pneumonia Processed Dataset**
  Kaggle - iamtapendu
  Contains **26k images** across two classes: Normal and Pneumonia.

Training: ResNet34 (centralized)

- **Hyperparameters:**
  - `EPOCHS = 50`
  - `BATCH_SIZE = 32`
  - `LEARNING_RATE = 0.01`
  - `OPTIMIZER = Adam`
  - `LOSS FUNCTION = CrossEntropyLoss`

ResNet34 Results

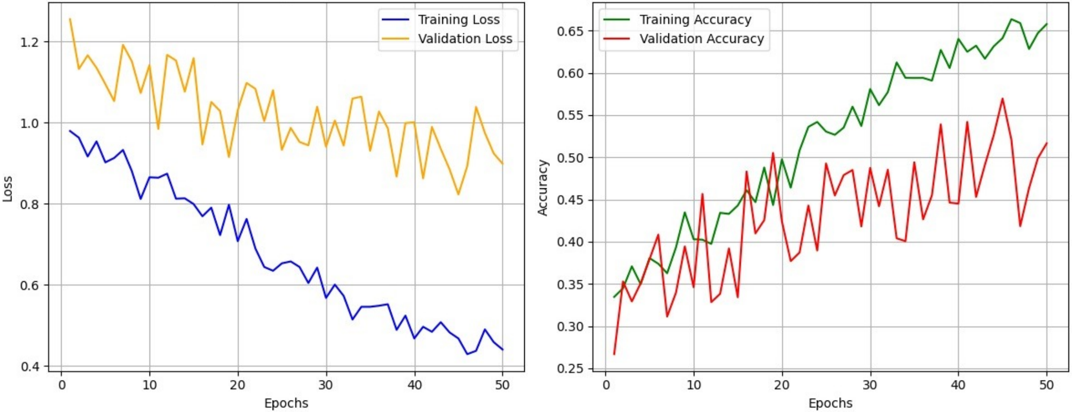


Figure: Training results with ResNet34

Training: ResNet50 (centralized)

- **Hyperparameters:**
  - `EPOCHS = 50`
  - `BATCH_SIZE = 32`
  - `LEARNING_RATE = 0.003`
  - `OPTIMIZER = SGD with MOMENTUM = 0.9`
  - `LOSS FUNCTION = CrossEntropyLoss`

ResNet50 (Centeralized) Results

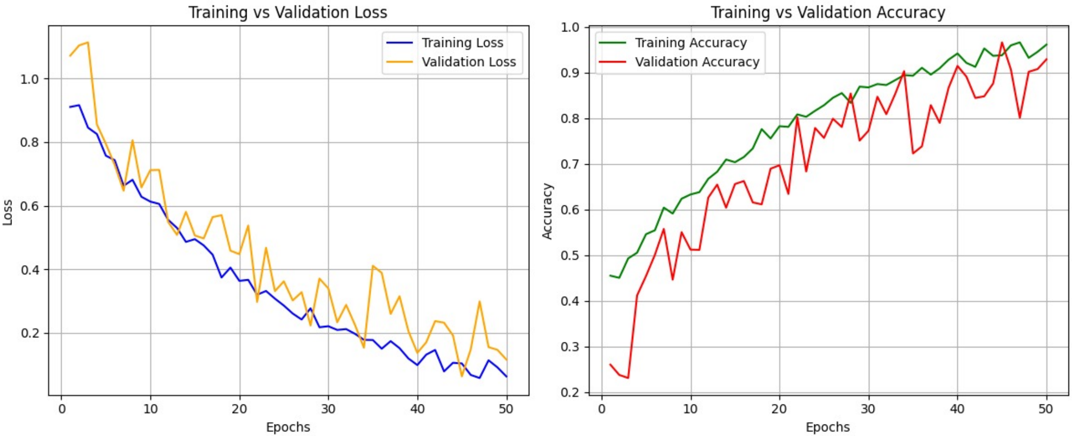


Figure: Training results with ResNet50

Training: nnU-Net (centralized)

- **Hyperparameters:**
  - `MODEL: PlainConvUNet`
  - `EPOCHS = 240`
  - `BATCH_SIZE = 12`
  - `LEARNING_RATE = 0.01`
  - `OPTIMIZER = SGD with MOMENTUM = 0.9`
  - `LR Scheduler = Polynomial decay: with exp=0.9`

$$\mathrm{lr} = \mathrm{initial\_lr} \cdot \left(1 - \frac{\mathrm{current\_epoch}}{\mathrm{max\_epoch}}\right)^{0.9}$$

  - `WEIGHT_DECAY = 3e-5`

Loss functions for nnU-Net

- **Loss Functions:**
  - Combined `Soft Dice Loss` and `Cross Entropy Loss`
  - **Soft Dice Loss:**

$$\mathcal{L}_{\text{Dice}} = -\frac{2\sum_i p_i g_i + \epsilon}{\sum_i p_i + \sum_i g_i + \epsilon}$$

  - **Cross Entropy Loss:**

$$\mathcal{L}_{\text{CE}} = -\frac{1}{N}\sum_i g_i \log(p_i)$$

  - **Combined:**

$$\mathcal{L}_{\text{Total}} = \lambda_{\text{CE}} \cdot \mathcal{L}_{\text{CE}} + \lambda_{\text{Dice}} \cdot \mathcal{L}_{\text{Dice}}$$

$$\lambda_{\text{CE}} = 1, \lambda_{\text{Dice}} = -1$$

  - Helps balance pixel-wise classification and region-based overlap, penalizing segmentation quality, ranging from ∞ to -1.

nnU-Net (Centeralized) Results

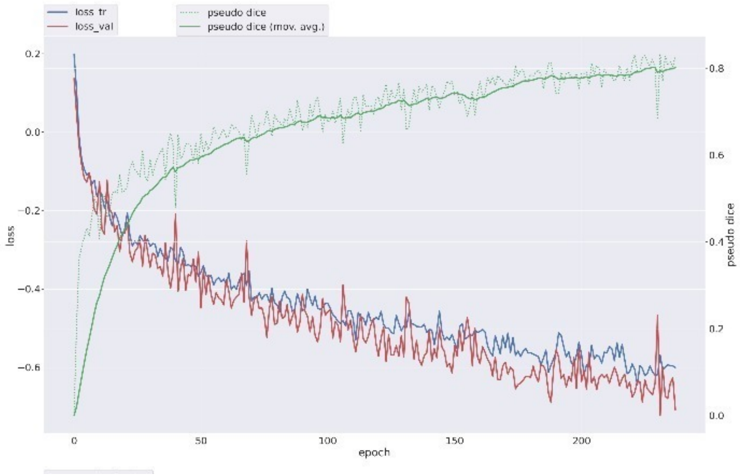
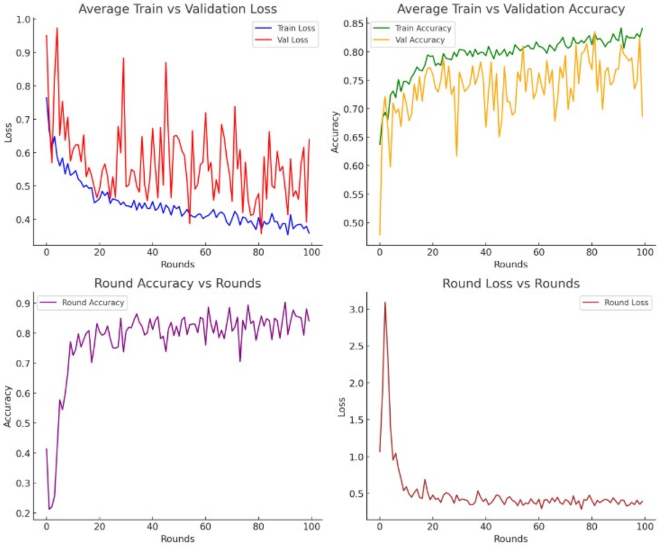


Figure: Training results with nnU-Net

Training: ResNet50 (Federated)

- **Hyperparameters:**
  - `NUM_PARTITIONS = 20`
  - `MIN_FIT_CLIENTS = 6`
  - `EPOCHS = 1`
  - `NUM_ROUNDS = 100`
  - `BATCH_SIZE = 32`
  - `LEARNING_RATE = 0.003`
  - `OPTIMIZER = SGD with MOMENTUM = 0.7`

ResNet50 (Federated) Trail-1 Results



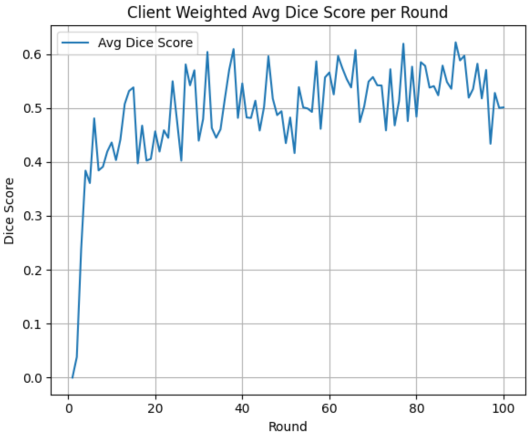
Training: nnU-Net (Federated)

- **Hyperparameters:**
  - `MODEL: PlainConvUNet`
  - `120`
  - `BATCH_SIZE = 12`
  - `LEARNING_RATE = 0.01`
  - `OPTIMIZER = SGD with MOMENTUM = 0.9`
  - `LR Scheduler = Polynomial decay (Server): with exp=0.9`

$$\text{lr} = \text{initial\_lr} \cdot \left(1 - \frac{\text{current\_round}}{\text{max\_round}}\right)^{\text{exponent}}$$

  - `WEIGHT_DECAY = 3e-5`
- **Loss Functions:**
  - Combined `Dice Loss` and `Cross Entropy Loss`
  - Designed to handle class imbalance and segmentation accuracy, ranges from $+$inf to -1

nnU-Net (Federated) Trail-1 Results



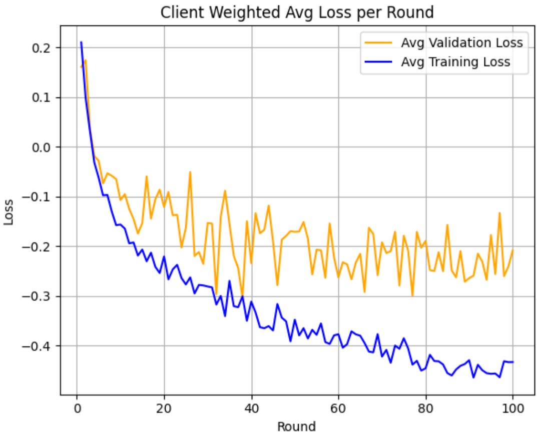


Figure: Client-side average loss and Dice score

nnU-Net (Federated) Trail-1 Results

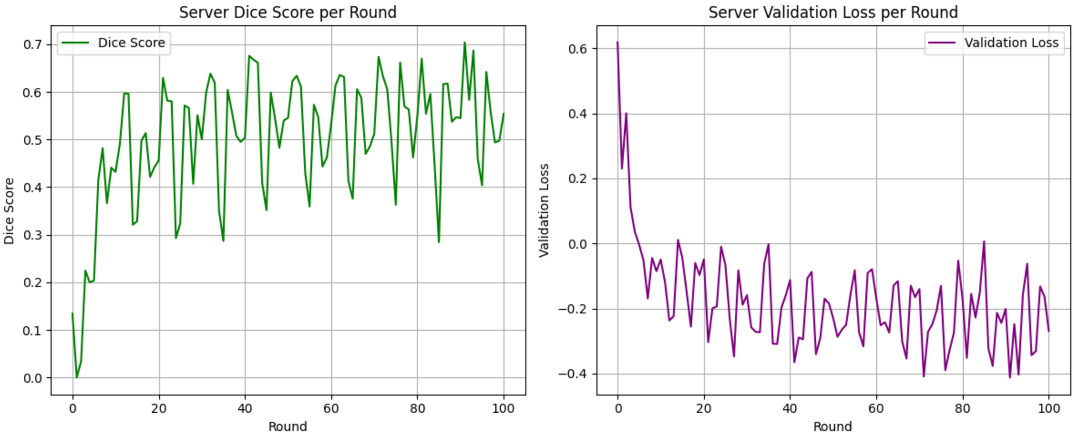


Figure: Server-side loss and Dice score

nnU-Net (Federated) Trail-2 Results

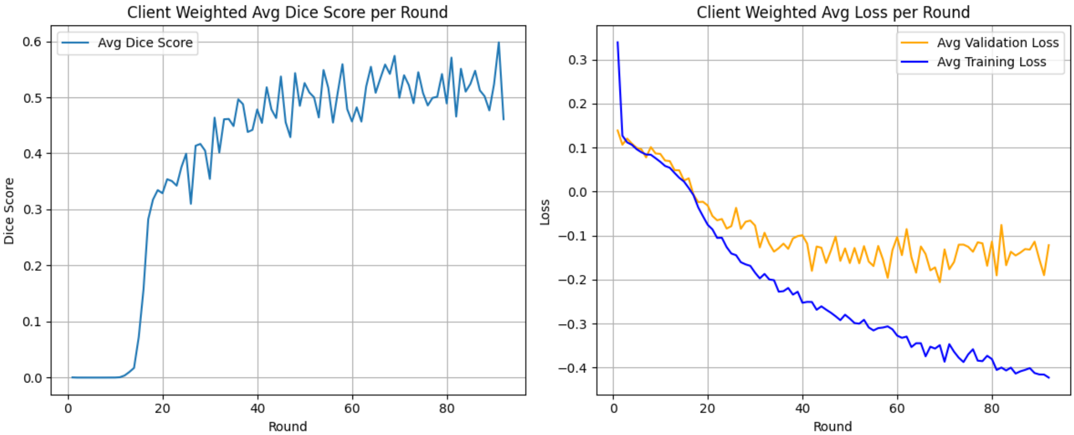
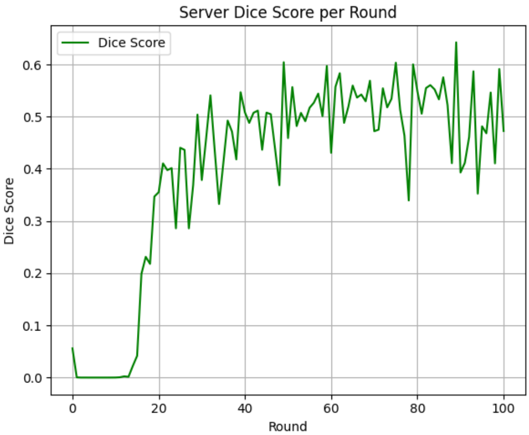


Figure: Client-side average loss and Dice score

nnU-Net (Federated) Trail-2 Results



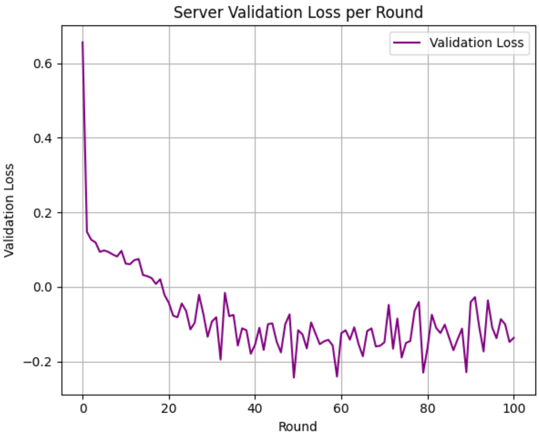


Figure: Server-side loss and Dice score

nnU-Net (Federated) Trail-3 Results

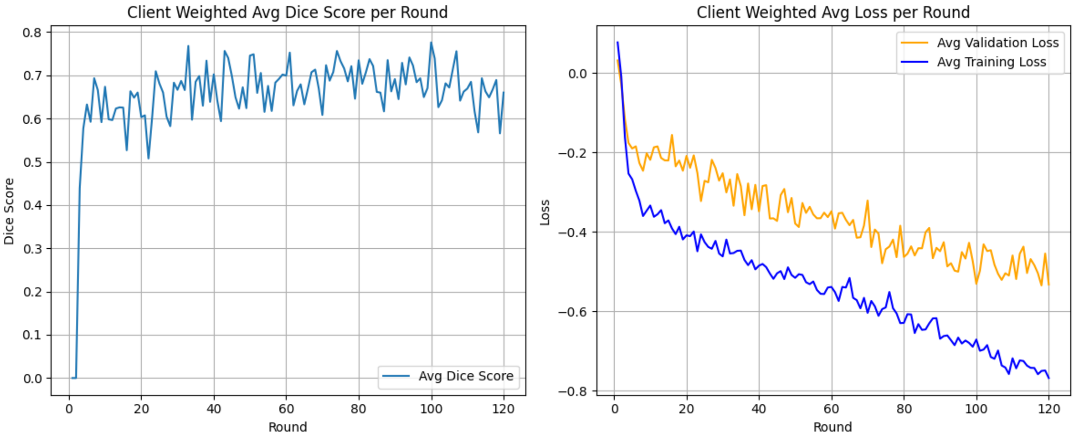


Figure: Client-side average loss and Dice score

nnU-Net (Federated) Trail-3 Results

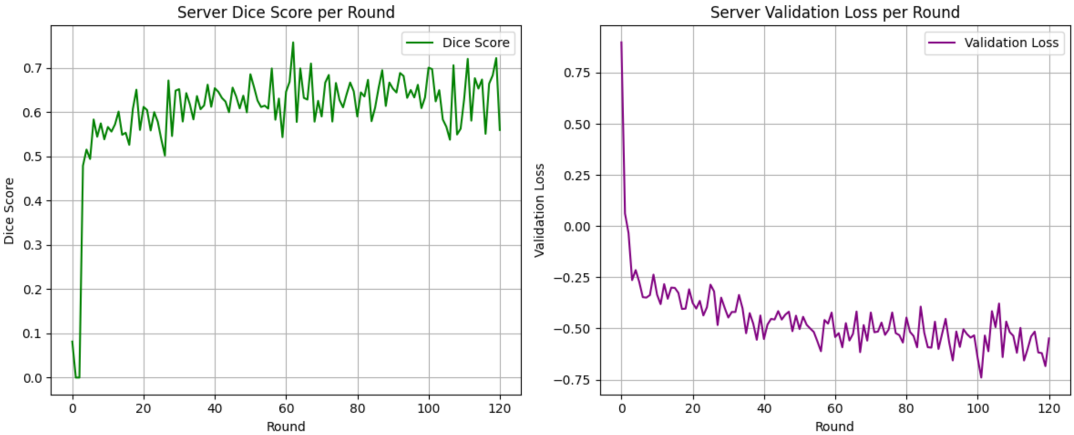
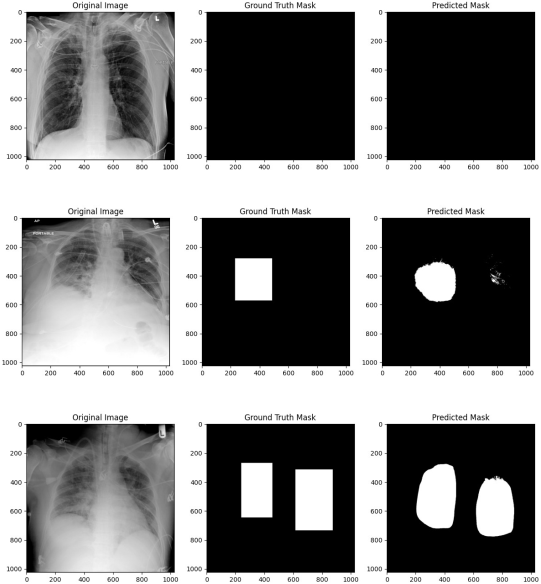


Figure: Server-side loss and Dice score

nnU-Net (Federated) Results



Centralized vs Federated Performance

Model	Centralized Accuracy/Dice	Federated Accuracy/Dice
ResNet50	96% / -	91% / -
nnU-Net	- / 0.824	- / 0.74

Table: Performance comparison between centralized and federated learning

Key Observations

- **Model Performance:**
  - ResNet50 outperformed ResNet34 in both centralized and federated settings.
  - Federated ResNet50 showed promising accuracy, though slightly lower than centralized due to data heterogeneity.
- **Segmentation Quality:**
  - nnU-Net demonstrated better Dice scores and generalization capability in both training modes.
  - Federated training showed minor performance drops but maintained consistent trends across clients.
- **Partition Strategy:**
  - Hybrid partitioning balanced non-IID distribution and class diversity effectively.

Conclusion

- Federated Learning enables privacy-preserving model training for pneumonia detection and segmentation.
- Flower framework effectively simulated FL on multiple clients with scalable and flexible configurations.
- ResNet and nnU-Net adapted well to federated settings, proving that high-performing medical models can be trained without centralized data.
- Hybrid partitioning strategy helped bridge the gap between real-world data distribution and training stability.

Future Work

- Integrate Differential Privacy for stronger privacy guarantees.
- Expand the number of clients and evaluate real-world FL deployment across hospitals.
- Automate hyperparameter tuning using tools like Optuna in a federated context.

References

He, K., Zhang, X., Ren, S., and Sun, J. (2015).
Deep residual learning for image recognition.
arXiv preprint arXiv:1512.03385.

Isensee, F., Jaeger, P. F., Kohl, S. A., Petersen, J., and Maier-Hein, K. H. (2021).
nnu-net: Self-adapting framework for u-net-based medical image segmentation.
https://github.com/MIC-DKFZ/nnUNet.

Labs, F. (2023).
What is federated learning? - flower tutorial series.
https://flower.ai/docs/framework/tutorial-series-what-is-federated-learning.html.