The LNM Institute of Information Technology

B. TECH. PROJECT

FEDERATED LEARNING ON MEDICAL DATA IMAGING

Submitted by

Maulik Mathur - 22UCS121
Samarth Garg - 22UCS175
Deevanshu Garg - 22UCS060

Supervisor:

Dr. Lal Upendra Pratap Singh

Department of Computer Science and Engineering

April, 2026

ABSTRACT

MRI(Magnetic Resonance Imaging) scans are an important resource for diagnosing diseases like brain and lung tumours. We can train AI models that can detect tumours and tell us about the size and location of the tumour. So, we can pool all the hospital data and train a centralised model. However, the problem is that hospitals cannot share their private patient's data to a centralised server because of guidelines like HIPAA and GDPR. This creates the problem of data silos, which means hospitals are confined to their isolated datasets, which they cannot share. This project aims to address these issues by investigating the effectiveness of federated learning for brain tumour segmentation using the BraTS 2020 dataset and comparing it with traditional centralised training approaches. The methodology involves several key steps. First is data preprocessing, which includes various steps, such as using MinMax scaling, cropping the images, and combining the channels. So, we have cropped the images to 128x128x128. Then, we combined the channels T1ce, T2, and T2-FLAIR and ignored the channel T1. We have used MinMax scaling because it is generally seen in various competitions that the ones in the top positions have used the MinMax scaling. We cropped the images for two reasons: the first is that the brain's most important region is located at/near the centre of the images, and the rest is just the background. It is better to crop the background a little bit so that the model can focus on the necessary parts. We have implemented the simple U-Net [3] and Attention U-Net [2] architectures from scratch in PyTorch. For centralised training, the models are trained on the entire dataset for a limited number of epochs. The dataset is partitioned among simulated clients (representing hospitals) for federated learning, and federated averaging is employed to aggregate model updates over multiple communication rounds. Preliminary results suggest that while centralised training yields slightly higher segmentation accuracy, federated learning achieves competitive performance with only a modest reduction in Dice scores. The Attention U-Net consistently outperforms the standard U-Net in both settings, particularly in delineating complex tumour boundaries. These findings indicate that federated learning is a promising framework for collaborative medical image analysis, offering a viable trade-off between data privacy and model performance. In conclusion, this project demonstrates the feasibility and potential of federated learning for brain tumour segmentation in multi-institutional settings.

ACKNOWLEDGEMENT

We want to express our sincere gratitude to all those who have supported and guided us throughout this project. First and foremost, We are deeply thankful to our project supervisor, Dr Lal Upendra Pratap Singh, for his invaluable guidance, encouragement, and insightful feedback at every stage of this work. His expertise and constant support have been instrumental in shaping the direction and quality of this project. Special thanks are due to our friends and batch-mates for their collaboration, discussions, and moral support, which greatly enriched our learning experience. We are also grateful to our family for their unwavering encouragement and understanding during this endeavour.

The LNM Institute of Information Technology
Jaipur, India

CERTIFICATE

This is to certify that the project entitled “Federated Learning on Medical Data Imaging” , submitted by Maulik Mathur (22UCS121), Samarth Garg (22UCS175) and Deevanshu Garg (22UCS060) in partial fulfillment of the requirement of degree in Bachelor of Technology (B. Tech), is a bonafide record of work carried out by them at the Department of Computer Science and Engineering , The LNM Institute of Information Technology, Jaipur, (Rajasthan) India, during the academic session 2025-2026 under my supervision and guidance and the same has not been submitted elsewhere for award of any other degree. In my/our opinion, this thesis is of standard required for the award of the degree of Bachelor of Technology (B. Tech).

Date

Adviser: Dr. Lal Upendra Pratap Singh

Contents

1 Federated Learning on Medical Data Imaging

Brain tumours are among the most life-threatening forms of cancer, with gliomas being the most common and aggressive subtype affecting the central nervous system. Accurate and timely diagnosis is essential for an effective treatment plan. Magnetic Resonance Imaging (MRI) is the preferred imaging modality for brain tumour assessment due to its superior soft tissue contrast and ability to capture multiple tissue characteristics through different imaging sequences.

Manual segmentation of brain tumours from MRI scans is a labour-intensive and time-consuming process and is also prone to significant inter-observer variability. The complexity of tumour morphology and multiple sub-regions (such as necrotic core, oedema, and enhancing tumour) further complicate the task. Automated segmentation using deep learning has shown promising results, but its success heavily depends on access to large, diverse, and well-annotated datasets.

2 Motivation

In real-world clinical settings, patient data is distributed across multiple hospitals and institutions, and they cannot share their data because of guidelines like HIPAA and GDPR. This makes it challenging to train data at a single site. Therefore, we use the concept of Federated learning [5]. A decentralised machine learning paradigm enables collaborative model training without sharing raw patient data, thereby addressing privacy concerns while leveraging multi-institutional data.

By using federated learning, it is possible to use the collective knowledge from distributed datasets while ensuring that sensitive patient information remains local. This approach not only addresses ethical and legal barriers but also has the potential to improve model performance and clinical applicability significantly.

3 Problem Addressed

So, we are working on the problem of image segmentation using federated learning. We are using the concept of federated learning to make a model which has comparable accuracy to the centralised training model. The goal is to evaluate whether federated learning can achieve segmentation accuracy comparable to centralised training while maintaining data privacy and accommodating the heterogeneity of multi-institutional datasets.

4 Objectives

1. Develop a privacy-preserving federated learning framework for brain tumour segmentation.

2. Achieve comparable accuracy than centralized training while ensuring data remains decentralized.

5 Mathematical Modelling of the Problem

5.1 FedAvg Algorithm

The formula below describes how weight updation happens in the global model using the FedAvg algorithm [1]. Each client locally takes one step of gradient descent on the current model using its local data, and the server then takes a weighted average of the resulting models.

This way, more computations can be added to each client by iterating the local update multiple times before doing the averaging step.

$$\forall k,\ w_{t+1}^k \leftarrow w_t - \eta g_k$$

Here, K denotes the number of clients in the subset. The symbols w_t and w_{t+1} are the weights before and after updates. The symbols η and g_k are the learning rate and gradient for a client k present in the subset.

$$w_{t+1} \leftarrow \sum_{k=1}^{K} \frac{n_k}{n} w_{t+1}^k$$

The symbol w_{t+1} is the weight of the global model in the central server after aggregation of weight updates w_{t+1}^k for each client k present in the subset.

5.2 Dice Coefficient

The Dice coefficient, also known as the Sørensen-Dice index or F1 score, is a statistical measure of the similarity between two sets. It is given by the formula below:

$$Dice = \frac{2 \times TP}{2 \times TP + FP + FN}$$

Imagine a predicted segmentation mask P and a ground truth mask G, both binary images.
Here:

- True Positives (TP) = pixels correctly predicted as foreground,
- False Positives (FP) = background pixels incorrectly predicted as foreground,
- False Negatives (FN) = foreground pixels missed.

Its value ranges from 0 to 1. The higher the value, the better the overlap between the predicted segmented mask and the ground truth.

5.3 Jaccard's Similarity

Jaccard's similarity is another metric used to measure the similarity between two sets, often compared with the Dice coefficient. It is also known as Intersection over Union (IoU). Its formula is given below:

$$J = \frac{TP}{TP + FP + FN}$$

It measures the overlap between the predicted segmentation mask P and the ground truth mask G, both binary images.
Here:

- True Positives (TP) = pixels correctly predicted as foreground,
- False Positives (FP) = background pixels incorrectly predicted as foreground,
- False Negatives (FN) = foreground pixels missed.

Its value ranges from 0 to 1. The higher the value, the better the overlap between the predicted segmented mask and the ground truth.

6 Challenges

1. Data across clients is often non-independent and identically distributed (non-IID), which can degrade model performance.
2. Unreliable or weak network connections often causes some clients to drop out during training.
3. It is susceptible to model inference attacks, model poisoning attacks.
4. Privacy of client's private data is often at risk of getting exposed to malicious clients.
5. High end hardware is required to perform federated learning for image segmentation.
6. The federated model may not be optimal enough to put into real world applications.

7 Literature Survey

Table 1: DETAILS ABOUT RESEARCH PAPERS

S. No	Paper Title, Author, Year	Method used	Limitations
1	Federated learning: Overview, strategies, applications, tools and future directions, Betul Yurdem, Murat Kuzlu, Mehmet Kemal Gullu, Ferhat Ozgur Catak, Maliha Tabassum, 2024	Discuses the various researches done on federated learning providing a comprehensive survey of it. It includes the need for it , the different types of FL algorithms and the frameworks based on it.	Does not deal with the security concerns placed with adopting federated learning.
2	Enhancing Privacy-Utility Tradeoff with Few-Round Strategy in Heterogeneous Federated Learning, Qingbin Wei and Feilong Zhang and Yuanchao Bai, Deming Zhai Junjun Jiang, Xianming Liu, 2024	Uses Federated Privacy-Preserving Knowledge Transfer (FedPPKT) which aims to enhance model performance by mitigating data heterogeneity while ensuring a certain level of privacy protection for data privacy.	It works on synthetic data which may not be robust to outliers.The use of meta-learning, generator training, and knowledge distillation adds overhead.
3	U-Net: Convolutional Networks for Biomedical Image Segmentation, Olaf Ronneberger and Philipp Fischer and Thomas Brox, 2015	It supplement a usual contracting network by successive layers, where pooling operators are replaced by upsampling operators.	Requires images with annotated labels and very high GPU power. The training time takes at least 10 hours for a NVidia Titan GPU (6 GB).
4	Federated Learning with U-Net for Brain Tumor Segmentation: Impact of Client Numbers and Data Distribution, Thu Thuy and Pham G, Nhat Truong and G, Phuong-Nam Tran and Minh Dang, Duc Ngoc, 2024	This paper proposes an FL approach using U-Net architecture for brain tumor segmentation. The authors also compare the two FL aggregation methods : FedAvg and FedSGD.	The paper does not talk about the scenario with many clients. It also does not talk about applying it to other medical imaging tasks.

Continued on next page

Table 1 – continued from previous page

S. No.	Paper Title, Author, Year	Method Used	Limitations
5	Attention U-Net: Learning Where to Look for the Pancreas, Ozan Oktay1,5, Jo Schlemper1, Loic Le Folgoc1, Matthew Lee4, Mattias Heinrich3,Kazunari Misawa2, Kensaku Mori2, Steven McDonagh1, Nils Y Hammerla5,Bernhard Kainz1, Ben Glocker1, and Daniel Rueckert1, 2018	In this paper, a novel attention gate model applied to medical image segmentation. Attention gates are added to U-Net model to automatically learn to focus on target structures without additional supervision.	The 3D model implementation required downsampling of input images to isotropic 2.0mm resolution due to GPU memory limitations. It is trained in small batches which causes gradient instability.

8 Experiment Setup

All experiments were conducted on cloud resources using Google Colab. Depending on availability, Colab Pro offers access to the following GPU types:

NVIDIA Tesla T4: 16 GB VRAM, Turing architecture
NVIDIA V100: 16 GB VRAM, Volta architecture
NVIDIA A100: 40 GB VRAM, Ampere architecture
NVIDIA L4: 24 GB VRAM, Ada Lovelace architecture

For most experiments, the Tesla T4 GPU (16 GB VRAM) was used. Deep learning models were implemented in Python 3 using the PyTorch framework, with supporting libraries including NumPy, SciPy, scikit-learn, matplotlib, glob etc. for data manipulation and visualization.

9 Dataset Description

We have used the BraTS-2020 dataset for our project. It is a multi-modal and multi-institutional brain tumour segmemntation dataset. It contains multi-modal MRI scans of patients diagnosed with gliomas. It contains 4 channels of information - 4 different volumes of the same region.

1. Native (T1)
2. T1 - contrast enhanced (T1 ce)
3. T2-weighted (T2)
4. T2 FLAIR volumes (T2 - FLAIR)

Annotations :

1. Label 0 : Background
2. Label 1 : Non-enhanced Tumour Core
3. Label 2 : Peritumoral Core
4. Label 3 : GD Enhanced Tumour Core

Data preprocessing includes various steps like using the MinMax scaling, cropping the images and combining the channels. So we have cropped the images to 128x128x128. Then we have combined the channels T1ce, T2, T2-FLAIR and ignored the channel T1 because T1ce is basically the contrast enhanced version of T1. So including T1 is just redundancy and does have a very significant impact in model training. We have used MinMax scaling because it is generally seen in various competitions that the ones in the top positions have used the MinMax scaling. We cropped the images because of two reasons : the first is that the most important reion of the brain is actually located at/near the center of the images and the rest is just background. So it is better to crop the background a little bit so that the model can focus on the necessary part.

10 Results (Partial)

Table 2: Comparison of Centralised and Federated Learning Models

	Centralised Model		**Federated Learning Model**	
	Simple U-Net	**Attention U-Net**	**Simple U-Net**	**Attention U-Net**
Mean Dice	0.3651	0.4143	0.2903	0.3407
Mean Jaccard	0.2873	0.3708	0.2496	0.2698
Class Wise Dice Non Enhancing Tumour	0.5304	0.5762	0.4332	0.4622
Class Wise Dice Peritumoral Edema	0.3344	0.3791	0.2701	0.3345
Class Wise Dice Enhanced Tumour	0.2306	0.2878	0.1677	0.2254

11 Scope of further work

Future work will focus on optimizing the number of rounds [4] in federated learning approach and scaling the approach to larger and more diverse datasets.

12 Conclusion

This report began by highlighting the critical challenge in brain tumour segmentation in MRI. It emphasised the need for accurate, privacy-preserving solutions that can leverage multi-institutional data without compromising patients' confidentiality. The motivation for this project stems from the limitations of centralized data collection and the promise of federated learning to collaboratively train deep learning models across distributed hospital datasets. The objectives were to implement and compare U-Net and Attention U-Net architectures for brain tumour segmentation using both centralized and federated learning paradigms. Then we described the methodologies and limitations about the papers we have reviewed for our project. The experimental setup detailed the hardware and software environment. Then we described the BraTS-2020 dataset, along with the preprocessing steps. The results shown that the centralised model is performing slightly better than the federated learning model and the Attention U-Net architecture outperforms the Simple U-Net architecture. But an important observation is that the federated learning model is not that bad as compared to the centralised model, even though we have trained it for just 2 rounds. These findings support the feasibility of federated learning for medical image segmentation tasks.

References

[1] T. T. le G, N. T. Pham G, P.-N. T. G, and D. N. Minh Dang. Federated learning with u-net for brain tumor segmentation: Impact of client numbers and data distribution. In *2024 15th International Conference on Information and Communication Technology Convergence (ICTC)*, pages 2048–2053, 2024.

[2] O. Oktay, J. Schlemper, L. L. Folgoc, M. Lee, M. Heinrich, K. Misawa, K. Mori, S. McDonagh, N. Y. Hammerla, B. Kainz, B. Glocker, and D. Rueckert. Attention u-net: Learning where to look for the pancreas, 2018.

[3] O. Ronneberger, P. Fischer, and T. Brox. U-net: Convolutional networks for biomedical image segmentation, 2015.

[4] Q. Wei, F. Zhang, Y. Bai, D. Zhai, J. Jiang, and X. Liu. Enhancing privacy-utility tradeoff with few-round strategy in heterogeneous federated learning. In *IEEE International Conference on Visual*

Communications and Image Processing, VCIP 2024, Tokyo, Japan, December 8-11, 2024, pages 1–6. IEEE, 2024.

[5] B. Yurdem, M. Kuzlu, M. K. Gullu, F. O. Catak, and M. Tabassum. Federated learning: Overview, strategies, applications, tools and future directions. *Heliyon*, 10(19):e38137, 2024.