Enhancing Brain Tumor Segmentation Accuracy through Scalable Federated Learning with Advanced Data Privacy and Security Measures

Faizan Ullah 1, Muhammad Nadeem 1, Muhammad Abrar 2, Farhan Amin 3,*, Abdu Salam 4 and Salabat Khan 5,*

1 Department of Computer Science and Software Engineering, International Islamic University, Islamabad 44000, Pakistan; faizan.phdcs157@iiu.edu.pk (F.U.); nadeem@iiu.edu.pk (M.N.)
2 Department of Computer Science, Bacha Khan University, Charsadda 24420, Pakistan; abrar@bkuc.edu.pk
3 Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, Republic of Korea
4 Department of Computer Science, Abdul Wali Khan University, Mardan 23200, Pakistan; abdusalam@awkum.edu.pk
5 IoT Research Center, College of Computer Science and Software Engineering, Shenzhen University, Shenzhen 518060, China

* Correspondence: farhanamin10@hotmail.com or farhan@ynu.ac.kr (F.A.); salabatkhan@szu.edu.cn (S.K.)

Abstract: Brain tumor segmentation in medical imaging is a critical task for diagnosis and treatment while preserving patient data privacy and security. Traditional centralized approaches often encounter obstacles in data sharing due to privacy regulations and security concerns, hindering the development of advanced AI-based medical imaging applications. To overcome these challenges, this study proposes the utilization of federated learning. The proposed framework enables collaborative learning by training the segmentation model on distributed data from multiple medical institutions without sharing raw data. Leveraging the U-Net-based model architecture, renowned for its exceptional performance in semantic segmentation tasks, this study emphasizes the scalability of the proposed approach for large-scale deployment in medical imaging applications. The experimental results showcase the remarkable effectiveness of federated learning, significantly improving specificity to 0.96 and the dice coefficient to 0.89 with the increase in clients from 50 to 100. Furthermore, the proposed approach outperforms existing convolutional neural network (CNN)- and recurrent neural network (RNN)-based methods, achieving higher accuracy, enhanced performance, and increased efficiency. The findings of this research contribute to advancing the field of medical image segmentation while upholding data privacy and security.

Keywords: brain tumor segmentation; computation cost; data leakage; data privacy; deep learning; federated learning; medical imaging; scalability; U-Net

MSC: 68T07, 68T01, 68W50

1. Introduction

Brain tumors are irregular growths of cells developing within the brain. These tumors can be benign or malignant and can cause severe health complications including neurological deficits and death [1]. It is very important to correctly identify and define the boundaries of brain tumors so that doctors can diagnose them accurately, plan effective treatment strategies, and keep track of how effective the treatments are [2]. To obtain a better view of brain tumors and the structures surrounding them, medical professionals often rely on imaging methods like magnetic resonance imaging (MRI) and computed tomography (CT) scans. These techniques are regularly employed to help diagnose brain
tumors and figure out the most effective treatment plan for the patient [3]. To better understand MRI and CT scans, these are divided into distinct segments, which is a practice known as brain tumor segmentation. This segmentation process corresponds to different parts of a tumor, including its necrotic core, the edema, and the enhancing tumor. This segmentation is crucial for accurate diagnosis and treatment planning as it involves the process of separating unhealthy tissues from healthy ones [4]. For many years, manual segmentation has been practiced by radiotherapists to perform these procedures. However, there was a high chance of the variability in the results between different observers and even in same observer. The process is time-consuming and can be affected by the expertise of the radiologist [5]. To overcome these limitations, automated and semi-automated segmentation algorithms have been developed.

The accurate and precise outlining of brain tumors in medical images is important for several reasons. It is a crucial part of diagnosing and determining the stage of the tumor. It helps doctors to understand how big the tumor is, where it is located, and how much it is affecting nearby tissues [6]. This information is critical for determining the prognosis and guiding personalized treatment strategies such as surgery, radiotherapy, and chemotherapy [7]. Accurate segmentation enables an unbiased and measurable evaluation of how tumors respond to treatment, reducing the subjective factors associated with manual evaluation [8]. This can help clinicians to make informed decisions about the efficacy of a particular treatment, and whether adjustments to the therapeutic plan are necessary. Precise segmentation can facilitate the development of computational models that predict tumor growth and its reaction to therapy, thus enhancing personalized medicine [9]. Such models can help to identify potential treatment targets, optimize treatment schedules, and identify patients at risk of tumor recurrence or progression. The increasing availability of medical imaging data and advancement in the technology has resulted in the development of robust and accurate computational segmentation algorithms [10]. However, the need for large amounts of annotated data brings its own challenges, i.e., the security and privacy concerns that limit the access to such data [11]. Additionally, in the context of deep learning models, the key challenge is the centralized nature of these approaches, which requires data from multiple institutions to be combined in a central repository. However, this process can present significant logistical difficulties and may also face limitations due to regulatory constraints.

To overcome the challenge of the centralized nature of deep learning (DL) and data security, the idea of federated learning (FL) is introduced that works via decentralized processing units which have their own data and model [12]. In FL, a unit does not share its data with other units, but instead, it shares the weights of the model with the centralized controller for the refinement of the overall model’s performance. Figure 1a,b show the working flow of federated learning. Such privacy and security assurance resulted in the popularity of FL in areas with significant data privacy concerns such as healthcare and medical imaging [13]. Since its inception, FL has largely been applied to such tasks, i.e., segmentation, reconstruction, and classification, with significantly reliable performance and results [14,15].
In brain tumor segmentation, FL can utilize data from multiple institutions, enhancing the performance and generalizability of segmentation algorithms. This is accomplished while maintaining the utmost data privacy and security. FL is crucial in addressing the heterogeneity of the brain tumor, which varies in location, shape, size, and intensity across patients. By leveraging data from multiple institutions, FL improves segmentation algorithms while preserving data privacy and security [16]. By allowing institutions to collaborate without sharing raw data, FL can enable the development of more robust and accurate segmentation algorithms that can better account for this variability.

However, FL also presents new challenges, such as efficient communication and model aggregation, which need to be addressed to ensure the feasibility and effectiveness of the approach [17]. In addition, the performance of FL in brain tumor segmentation has not been extensively studied, and more research is needed to understand its potential benefits, limitations, and practical implications.

In the past decade, deep-learning-based techniques have appeared as powerful tools for automated brain tumor segmentation, achieving significant performance and surpassing traditional image processing methods [18]. However, the success of these techniques is based on the availability of well-annotated, diverse, and large datasets, which are challenging to obtain due to data privacy, security concerns, and regulatory constraints. Furthermore, the centralized nature of traditional deep learning approaches may not be ideal for multi-institutional collaborations, where sharing raw patient data may not be feasible. Therefore, in this research article, the aim is to investigate the role of FL in accurate brain tumor segmentation and comparing its performance to traditional and other DL-based methods. Furthermore, this study evaluates the impact of FL on security, data privacy, and scalability in the context of medical imaging. By doing so, the aim is to deliver an in-depth understanding of FL’s potential and challenges associated with brain tumor segmentation. It will contribute to the development of more accurate, privacy-preserving, and scalable medical imaging techniques.

This research article mainly concentrates on examining the impact of FL on the accuracy of brain tumor segmentation. This paper will serve to achieve the following objectives.

- To examine the potential of FL to address the limitations by building a new model to preserve the privacy of the data while improving the accuracy of brain tumor segmentation algorithms.
- To develop an FL framework for brain tumor segmentation, including the selection of an appropriate base architecture U-Net, model aggregation methods, and communication.
- To evaluate the performance of the FL-based brain tumor segmentation algorithm using standard evaluation metrics such as the dice coefficient, sensitivity, and specificity.
- To discuss the impact of FL on data privacy and security, including the evaluation of data leakage risks and the efficiency of the communication protocol.
- To investigate the scalability of the FL approach by examining the impact of the number of clients on performance, as well as the trade-offs between computation and communication costs.

By accomplishing these objectives, the aim is to provide a comprehensive understanding of the potential benefits, limitations, and practical implications of FL for brain tumor segmentation.

This research will contribute to the development of more accurate, privacy-preserving, and scalable medical imaging techniques and may have broader implications for the application of FL in other medical imaging tasks and healthcare domains.

The rest of this paper is organized as follows. In Section 2, a thorough literature review is presented, focusing on traditional and deep learning techniques for brain tumor
detection using FL. Section 3 outlines the proposed methodology employed, including dataset detail, preprocessing, the FL model’s structure, and model aggregation. Section 4 presents the experimental results and discusses the model training and validation, hyperparameter tuning, and comparison of traditional and DL methods. Section 5 presents a discussion that includes the key findings of the study, implications for medical imaging and brain tumor segmentation, and the limitations of the current approach, and Section 6 concludes the paper by summarizing the key findings and their implications, and suggests potential directions for future research.

2. Related Work

Brain tumor segmentation is a critical task in medical imaging that involves identifying the location and extent of a tumor in a brain scan. The process of segmenting brain tumors can help in the diagnosis, treatment planning, and follow-up monitoring of brain tumor patients.

2.1. Traditional Brain Tumor Segmentation

Several conventional techniques have been proposed for brain tumor segmentation, including region-focused, edge-focused, and model-focused approaches [19]. While conventional brain tumor segmentation techniques have been widely used in medical imaging, they have several limitations, including sensitivity to image noise, lack of robustness to variations in image intensity and texture, and dependence on expert knowledge for parameter tuning.

The accuracy of conventional techniques depends on the specific application and available resources [20]. Thus, the choice of the most appropriate segmentation technique depends on various factors, including the image quality, the type and location of the tumor, and the clinical objectives. In recent years, deep-learning-based methods, such as CNNs, RNNs, and their variants, have emerged as powerful alternatives to conventional techniques, achieving state-of-the-art performance on various medical imaging tasks, including brain tumor segmentation. The accuracy of these techniques depends on the specific application and available resources. However, these methods require large and diverse datasets for training and the careful selection of appropriate network architectures and hyperparameters.

2.1.1. Region-Focused Approaches

Region-focused approaches have been widely used in brain tumor segmentation due to their simplicity and computational efficiency. These methods aim to segment brain tumors based on the intensity or texture differences between the tumor and its surrounding tissue. Several region-based approaches have been proposed for brain tumor segmentation, including thresholding, clustering, and region growing methods [21].

Thresholding-based methods involve setting a fixed threshold value to separate the tumor and non-tumor regions [22]. These methods are simple and fast, but may be affected by image noise and variations in image intensity and texture. Clustering-based methods use statistical clustering algorithms, such as fuzzy C-means, k-means, and expectation-maximization algorithms, to partition the image into tumor and non-tumor regions. Clustering-based methods can achieve better segmentation accuracy than thresholding-based methods, but they require the careful selection of clustering parameters.

Region growing methods start with a seed point within the tumor region and expand the region by incorporating adjacent pixels that meet specific criteria. Region growing methods can produce accurate and smooth segmentation results, but may be affected by variations in image intensity and texture, and they are sensitive to the selection of seed points. Several studies have compared the performance of region-based approaches for brain tumor segmentation. Jaglan et al. [23] compared the performance of various thresholding- and clustering-based methods and found that the Otsu thresholding method and
the fuzzy C-means clustering method achieved the highest segmentation accuracy. Charutha et al. [24] compared the performance of various region growing methods and found that a fast-marching method with an adaptive threshold achieved the best segmentation results.

Region-focused approaches have been widely used in brain tumor segmentation due to their simplicity and computational efficiency. While these methods have their strengths, they may be negatively affected by variations in image intensity and texture. Thus, they require the careful selection of parameters and domain knowledge. Advances in deep-learning-based methods have shown promising results in overcoming some of the limitations of region-focused approaches.

2.1.2. Edge-Focused Approaches

Edge-focused approaches aim to identify the boundary between the tumor and surrounding tissue by detecting edges in the image. These methods often use edge detection techniques, such as Canny or Sobel filters, to highlight the edges and then apply a segmentation algorithm to separate the tumor from the background. Edge-focused approaches can achieve better segmentation accuracy than region-based approaches, but may be sensitive to image noise and produce fragmented results. Rajan and Sundar [25] combined K-means clustering, fuzzy C-means, and active contour techniques to enhance segmentation. Similarly, Sheela and Suganthi [26] used an approach to improve accuracy, reduce processing time, and compute tumor volume for effective diagnosis and treatment. The process involves collecting images, calculating tumor area and volume, preprocessing and enhancing the images, adjusting the image intensities, clustering the images, classifying the images, extracting features, and segmenting the images. Each step in the process is important and contributes to the overall quality of the enhanced images. The process has strengths such as its ability to improve the quality of MRI images in several ways, i.e., identifying tumors, providing quantitative information about tumors, and segmenting tumors from the surrounding tissue. However, the process also has weaknesses, such as its complexity, time-consuming nature, reliance on specialized software and hardware, difficulty in automation, and sensitivity to noise in the images.

Several studies have compared the performance of edge-focused approaches for brain tumor segmentation. The performance of various edge detection methods, including Canny, Sobel, and Laplacian filters, showed that the Sobel filter achieved the highest segmentation accuracy. Und et al. [27] compared the performance of edge detection methods combined with different segmentation algorithms, such as region growing and active contour methods, and found that the Sobel filter combined with the active contour method achieved the best segmentation results.

Edge-focused approaches can be computationally intensive due to the need to detect edges in the image. Moreover, it may be affected by variations in image intensity and texture and produce fragmented segmentation results. Deep-learning-based methods, such as CNNs, have shown promising results in overcoming some of these limitations. They can also achieve better segmentation accuracy than region-based approaches, but they may be sensitive to image noise and produce fragmented results. The choice of the most appropriate edge detection method depends on the specific application and available resources. Deep-learning-based techniques have reported very significant results in improving segmentation accuracy and robustness.

2.1.3. Model-Focused Approaches

Model-focused approaches aim to model the shape, texture, and intensity-based characteristics of brain tumors and their surrounding tissue to improve segmentation accuracy. These methods often use traditional machine learning algorithms, such as random forests, decision trees, and support vector machines, to learn those features that distinguish between tumorous and non-tumorous regions [25]. Model-focused approaches can achieve high segmentation accuracy and robustness subject to the availability of high-
quality large datasets for training and may be affected by overfitting, as presented in Figure 2.

Figure 2. Model-based approach for brain tumor segmentation [28].

Several studies have conducted a comprehensive analysis of the model-based techniques used in brain tumor segmentation. Tandoori et al. [28] considered a couple of machine-learning-based models including random forests, decision trees, and support vector machines (SVMs), and reported that SVMs were the best models among all models. Similarly, Jiang et al. [29] presented a DNN model as a hybrid approach of the CNN and conditional random field and reported a very good performance.

Model-focused approaches can achieve high segmentation accuracy, but these have a substantial trade-off concerning the size of the dataset. For better performance, these models need a large high-quality dataset. However, a large dataset is also prone to data overfitting issues. Therefore, significant attention should be paid to the experimentation to obtain the best trade-off between the size of the dataset and the performance of model-focused techniques. In such cases, DL-based methods have revealed very good results in improving segmentation accuracy and robustness.

2.2. DL-Based Brain Tumor Segmentation

DL-based models, particularly convolutional neural networks, have demonstrated their effectiveness in medical imaging [30]. A traditional set up of a CNN-based DL model is presented in Figure 3. CNNs are designed to automatically learn the features that distinguish between tumor and non-tumor regions by processing the image using a series of kernels, convolutional and pooling layers, activations, and loss functions. CNNs have the advantage of being able to obtain features from the input, allowing them to capture complex patterns and variations in image intensity and texture [5].
Several DL-based models have been developed for brain tumor segmentation, including V-Net, U-Net, and their variants. U-Net is a popular CNN architecture that consists of a contracting path to capture the contextual information of the input image and an expanding path to produce the segmentation map. V-Net is an extension of U-Net that includes a 3D CNN for processing volumetric data. These architectures have achieved state-of-the-art performance on various brain tumor segmentation challenges, such as the Multimodal Brain Tumor Segmentation Challenge (BRATS).

2.2.1. Neural-Network-Based Models

Several network structures, including CNNs and RNNs, have been proposed for brain tumor segmentation. CNNs are a type of deep neural network that has shown remarkable success in various image-processing tasks, including object recognition, segmentation, and classification. CNNs consist of multiple convolutional layers that extract the features of the input image and a fully connected layer that produces the segmentation map [31]. RNNs are another type of neural network that can process sequential data, such as time series or sequences of images. RNNs use feedback connections to retain information about the previous inputs and produce outputs that depend on the current and past inputs. RNNs have been applied to brain tumor segmentation by processing sequences of images and incorporating spatial and temporal information into the segmentation.

Several studies have compared the performance of different neural network structures for brain tumor segmentation. Akilan et al. [32] proposed a 3D CNN-LSTM and found that the LSTM architecture achieved the highest segmentation accuracy. Another study by Zhao et al. [33] proposed a CNN-RNN architecture that combines a 3D MRI brain tumor segmentation to improve segmentation accuracy.

CNNs and RNNs have been widely used for brain tumor segmentation due to their potential to learn intricate features from the input image and process sequential data. The choice of the most appropriate neural network structure depends on the specific application and available resources. Further research is needed to explore the potential of these structures in brain tumor segmentation.
2.2.2. Specialized Neural-Network-Based Model for Medical Imaging

U-Net and V-Net are two dedicated architectures that have been proposed for medical image segmentation, including brain tumor segmentation. U-Net is a fully convolutional neural network that involves an expanding path and a contracting path. The contracting path captures the context of the input image by reducing the spatial dimensions, while the expanding path produces the segmentation map by increasing the spatial dimensions [29].

Maqsood et al. [34] used fuzzy-logic-based edge detection and U-NET CNN classification. The approach involves preprocessing, edge detection, and feature extraction using wavelet transform, followed by CNN-based classification. The method outperforms other approaches in terms of accuracy and visual quality. Nawaz et al. [35] combine DenseNet77 in the encoder and U-NET in the decoder. The method achieves high segmentation accuracy on ISIC-2017 and ISIC-2018 datasets. Meraj et al. [36] used a quantization-assisted U-Net approach for accurate breast lesion segmentation in ultrasonic images. It combined U-Net segmentation with quantization and Independent Component Analysis (ICA) for feature extraction.

V-Net is an extension of U-Net that uses a 3D convolutional neural network for processing volumetric data. Isensee et al. [30] compared the performance of various deep-learning-based methods, including U-Net, V-Net, and other architectures, and found that U-Net achieved the best segmentation accuracy. The authors introduced a U-Net Cascade approach for large image datasets. Their approach contained two stages. Stage 1 trained a 3D U-Net on downsampled images; it enhanced the results of the image and fed it as inputs for Stage 2. Stage 2 used a second 3D U-Net for patch-based training at full resolution. Their two-stage structure is shown in Figure 4.

Several studies have compared the performance of U-Net and V-Net with other deep-learning-based methods for brain tumor segmentation. Wang et al. [37] proposed a U-Net-based method that uses a multi-scale feature extraction strategy to improve segmentation accuracy. Other dedicated architectures, such as DeepMedic, BRATS-Net, and Tiramisu-Net, have also been proposed for brain tumor segmentation. DeepMedic is a hybrid CNN that combines a multi-scale architecture with a multi-path architecture to improve segmentation accuracy. BRATS-Net is a CNN architecture that includes a cascaded network and a refinement network for processing multimodal brain images. Tiramisu-Net is a densely connected convolutional network that uses skip connections to capture the features at different scales. Thus, there are several dedicated architectures that have also shown promising results in improving segmentation accuracy and robustness. The choice of the most appropriate architecture depends on the specific application and available resources.
2.3. Federated Learning for Medical Imaging

FL is a novel machine learning technique that enables multiple parties to collaboratively train a global model without sharing their sensitive data [38]. FL has been widely used in the context of medical imaging, where privacy and security concerns are of paramount importance. In FL, each participating client trains a local model on its data and shares only the model weights with the central server. The central server aggregates the model weights and sends the updated global model back to the clients. FL allows medical institutions to collaborate and leverage their data to improve the accuracy and generalization of machine learning models while preserving the privacy and security of the data.

Several studies have demonstrated the effectiveness of FL in medical imaging tasks, including brain tumor segmentation. Khan et al. [39] proposed an FL-based framework for brain tumor segmentation that allowed multiple medical institutions to collaborate on the training of a deep learning model without sharing their data. The FL-based method achieved comparable segmentation accuracy to the centralized learning method while preserving the privacy and security of the data. Arikumar et al. [40] proposed an FL-based method for multimodal brain tumor segmentation that allowed multiple institutions to collaboratively train a global model using both MRI and histology data. The FL-based method achieved higher segmentation accuracy than the traditional centralized learning method while preserving the privacy and security of the data, as shown in Figure 5.

![Figure 5. Federated learning (FL)-based model [39].](image)

FL is a promising technique for medical tasks, including brain tumor segmentation, that enables multiple institutions to collaborate on the training of deep learning models without compromising the privacy and security of the data. Further research is needed to explore the potential of FL in medical imaging and to address the challenges related to the communication, computation, and heterogeneity of the data.

2.3.1. Data Confidentiality and Safety Concerns

Data confidentiality and safety concerns are critical issues in medical imaging, especially in the context of brain tumor segmentation, where patient data is highly sensitive and confidential. Deep-learning-based methods require large amounts of patient data for
training, and the sharing of such data among multiple institutions raises concerns about data privacy, security, and ownership [41]. Several studies have addressed data confidentiality and safety concerns in medical imaging by proposing secure and privacy-preserving methods for data sharing and machine learning. Sheller et al. [42] proposed a secure data-sharing method that uses homomorphic encryption to enable multiple institutions to collaborate on the training of a machine learning model without revealing sensitive data. It achieved comparable performance to the traditional centralized learning method while preserving the privacy and security of the data. Wang et al. [37] proposed a blockchain-based method for sharing medical data among multiple institutions while maintaining data ownership and privacy. The authors demonstrated that the method provides a secure and transparent mechanism for data sharing and machine learning while preserving the privacy and security of the data.

Moreover, several studies have addressed the legal and ethical implications of data sharing and machine learning in medical imaging. Jiang et al. [43] proposed a framework for responsible data sharing in medical research that takes into account legal, ethical, and social considerations. Data confidentiality and safety concerns are critical issues in medical imaging, especially in the context of brain tumor segmentation. Secure and privacy-preserving methods, such as homomorphic encryption and blockchain, have been proposed to enable data sharing and machine learning while preserving the privacy and security of the data. Further research is needed to explore the potential of these methods in medical imaging and to address the legal and ethical implications of data sharing and machine learning.

2.3.2. Cooperative Learning for Better Performance

Cooperative learning, also known as collaborative learning, is a method that involves multiple learners working together to achieve a common goal. In the context of brain tumor segmentation, cooperative learning has been used to improve the performance of machine learning models by leveraging the collective intelligence of multiple experts [44]. Several studies have explored the potential of cooperative learning for brain tumor segmentation. Amiri et al. [45] proposed a cooperative learning framework that combines the outputs of multiple deep learning models to improve segmentation accuracy. The authors stated that the cooperative learning framework achieved higher segmentation accuracy than individual models and traditional ensemble learning methods. Witowski et al. [46] proposed a cooperative learning method that involves multiple experts in a crowdsourcing platform to annotate brain tumor images. The authors demonstrated that the cooperative learning method achieved higher annotation accuracy and consistency than individual experts and traditional methods.

Moreover, several studies have investigated the impact of cooperative learning on the interpretation and generalization of machine learning models. Abramoff et al. proposed a cooperative learning method that involves radiologists and deep learning models to jointly interpret brain MRI images. The proposed cooperative learning method achieved higher diagnostic accuracy and interpretability than individual radiologists and deep learning models.

Cooperative learning is a promising method for improving the performance and interpretability of machine learning models in brain tumor segmentation. Further research is needed to explore the potential of cooperative learning in other medical imaging tasks and to address the challenges related to the communication, computation, and heterogeneity of the data.

2.3.3. Federated Learning Applications

FL is a novel machine learning technique that has been applied in various domains, including healthcare, finance, and the internet of things (IoT). In healthcare, FL has been used for various tasks, such as disease diagnosis, drug discovery, and medical imaging analysis [47]. Chen et al. [48] proposed an FL-based framework for personalized cancer
diagnosis that allowed multiple hospitals to collaboratively train a DL model without sharing their patient data. The FL-based method achieved higher accuracy than the traditional centralized learning method while preserving the privacy and security of the data.

Dayan et al. [49] proposed a FL-based method for predicting COVID-19 severity using chest X-ray images. The authors showed that the FL-based method achieved higher accuracy than the traditional centralized learning method while preserving the privacy and security of the data.

Moreover, several studies have explored the potential of FL for medical image analysis tasks, such as brain tumor segmentation, retinal image analysis, and skin lesion classification. Zhang et al. [50] present an FL-based method for retinal image analysis that allowed multiple medical institutions to collaborate on the training of a deep learning model without sharing their patient data. The authors demonstrated that the FL-based method achieved higher accuracy than the traditional centralized learning method while preserving data security privacy.

FL is a promising technique for various ML applications, including healthcare and medical imaging analysis. However, further research is needed to explore the potential of FL in other domains and to address the challenges related to the communication, computation, and heterogeneity of the data.

3. Methodology

This section introduces the methodology used in developing the FL framework for brain tumor segmentation. It outlines the dataset used, the preprocessing steps performed, the server–client architecture, model aggregation techniques, the U-Net-based architecture with adaptations, and the evaluation metrics employed. In addition, to reduce the communication overhead of the client data transfer, model compression is discussed, and its performance is presented.

3.1. Dataset

This research uses a standard dataset, i.e., BRATS [51] dataset, which contains MRI scans of the brain tumor. The BRATS images consist of four modalities of each MRI. These modalities are T1-weighted, T1-weighted contrast-enhanced, T2-weighted, and FLAIR [2]. The dataset provides a large and diverse set of brain tumor images for training and testing deep learning models. The detail of the dataset is presented in Table 1.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Patients</th>
<th>Imaging Modalities</th>
<th>Ground Truth</th>
<th>Tumor Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>BRATS</td>
<td>285</td>
<td>T1, T1CE, T2, FLAIR</td>
<td>Yes</td>
<td>Glioma, Meningioma</td>
</tr>
</tbody>
</table>

3.2. Preprocessing

Before training the deep learning model, several preprocessing steps on the MRI images were performed to enhance the quality and consistency of the data. First, skull stripping was performed to remove the non-brain tissues and artifacts using the FMRIB Software Library (FSL) toolbox [52]. Then, intensity normalization was performed to reduce the intensity variations between the different modalities using the z-score normalization method [53]. Next, image registration was carried out to align the images in the same anatomical space using the Advanced Normalization Tools (ANTS) toolbox [54]. Finally, a variety of data augmentation methods were applied, i.e., random rotations, translations, and elastic deformations, to increase the diversity of the dataset to prevent model overfitting.

3.3. Generic Federated Learning Model’s Structure

The FL framework consists of a server–client architecture, where the server coordinates the training process, and the clients perform local model updates using their data.
The server–client architecture allows for the training of a deep learning model on a large amount of distributed data while maintaining data privacy and confidentiality. Each client trains their local model on their local data without sharing it with the server or other clients, which reduces the risk of data leakage and ensures data privacy. Moreover, the server aggregates the local model weights from the clients using secure communication protocols, which further enhances the privacy and security of the data. Table 2 summarizes the task and description of the server and client in the context of FL architecture.

Table 2. Server and client components in FL architecture.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Manages the global model and aggregates the weights of the model received from the clients. The aggregated weights are then sent back to the client to refine their weights for improved results.</td>
</tr>
<tr>
<td>Client</td>
<td>The weight of the client’s model, or the distinction between the local and global models, is sent to the server for aggregation. In this study, local model updates using several clients were performed.</td>
</tr>
</tbody>
</table>

In this study, a central server was used to perform the model aggregation, but other FL architectures, such as peer-to-peer and hierarchical architectures, can also be used depending on the requirements of the application.

Overall, the server–client architecture is a critical component of the FL framework that enables the training of accurate and robust deep learning models for medical imaging applications while ensuring data privacy and confidentiality.

3.4. Proposed Model’s Architecture

This section discusses the development of the model’s architecture for brain tumor segmentation using FL. The process includes selecting a base architecture, adapting it for brain tumor segmentation, and choosing appropriate loss function and evaluation metrics.

3.4.1. Base Architecture

The base architecture determines the fundamental structure of the model and its ability to extract relevant features from the input data. Section 2 highlights several architectures that can be used for image segmentation tasks. These models include U-Net, V-Net, and Fully Convolutional Networks (FCNs). Among these models, U-Net has the ability to capture both local and global features from the input image [55]. This model comprises a contracting path for downsampling (via $3 \times 3$ convolutions, ReLU, and max pooling) and an expanding path for upsampling (using up-convolution, concatenation, and ReLU). Each stage doubles the feature channels in downsampling and halves them in upsampling. The final $1 \times 1$ convolution tailors a 64-component feature vector for class division. It consists of an encoder that extracts features from the input image and a decoder that generates the segmentation map, as shown in Figure 6. V-Net is a more advanced architecture that uses residual connections to improve training efficiency and stability. FCNs are another type of architecture that consist of only convolutional layers and can handle images of arbitrary size.

In this study, U-Net is used as the base architecture for brain tumor segmentation due to its proven performance in medical imaging applications.
3.4.2. Adaptations for Brain Tumor Segmentation

Adapting the base architecture to the specific task of brain tumor segmentation is essential for improving the model’s accuracy. This can include modifying the architecture’s parameters or adding additional layers to capture specific features. One common adaptation is the addition of skip connections that allow for the transfer of features from the encoder to the decoder, which helps preserve spatial information and improves the segmentation accuracy. Another adaptation is the use of attention mechanisms that focus the model’s attention on the most relevant parts of the input image.

In this study, skip connections were added to the U-Net architecture to improve its accuracy for brain tumor segmentation. The multimodal input was selected based on the input types in the dataset as there were four types of images, i.e., T1, T2, T3, and T4.

To avoid the overfitting of the model, batch normalization was used. Additionally, after normalization, the dropout was applied to further safeguard the overfitting issues. Finally, SoftMax was used to obtain the pixel-wise prediction for the brain tumor class. These are summarized in Table 3.

Table 3. Adaptations made to the U-Net architecture for brain tumor segmentation.

<table>
<thead>
<tr>
<th>Adaptations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-modal input</td>
<td>Expanded number of input channels to handle multiple MRI modalities (T1-weighted, T1-weighted with contrast, T2-weighted, FLAIR)</td>
</tr>
<tr>
<td>Batch normalization</td>
<td>Added batch normalization layers to improve generalization and mitigate overfitting</td>
</tr>
<tr>
<td>Dropout</td>
<td>Incorporated dropout layers to further prevent overfitting</td>
</tr>
<tr>
<td>SoftMax Output</td>
<td>Configured the final layer to output pixel-wise probabilities for each tumor class using a SoftMax activation function</td>
</tr>
</tbody>
</table>
3.4.3. Loss Function and Evaluation Metrics

Selecting an appropriate loss function is crucial for training a deep learning model effectively. The dice loss function is used, which is well suited for handling the class imbalance commonly observed in medical image segmentation tasks. The dice loss function is derived from the dice coefficient, a popular similarity metric for comparing the similarity of two sets and images.

In addition to the dice coefficient, other evaluation metrics such as sensitivity, specificity, and the Jaccard index were used in the literature to assess the model’s performance. Sensitivity measures the proportion of true positive detections among all actual positive cases, while specificity measures the proportion of true negative detections among all actual negative cases. The Jaccard index, also known as the Intersection over Union (IoU), calculates the ratio of the intersection of the predicted and ground truth segmentations to their union.

In this article, the researchers followed the approach used in [56,57] for parameter selection. In addition, the authors also performed extensive experimentation to fine-tune the hyperparameters that yield the best performance on the dataset. The author evaluated different parameters and their combinations and selected the ones with the best results. Hence, by carefully selecting the base architecture, making necessary adaptations, and using appropriate loss functions and evaluation metrics, the researchers developed a model architecture tailored to the task of brain tumor segmentation using FL. The complete process is summarized in Table 4.

Table 4. Key parameters and hyperparameters of the developed model.

<table>
<thead>
<tr>
<th>Parameter/Hyperparameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base architecture</td>
<td>U-Net</td>
</tr>
<tr>
<td>Skip connections</td>
<td>Yes</td>
</tr>
<tr>
<td>Number of convolutional layers</td>
<td>4</td>
</tr>
<tr>
<td>Number of pooling layers</td>
<td>4</td>
</tr>
<tr>
<td>Learning rate</td>
<td>0.001</td>
</tr>
<tr>
<td>Batch size</td>
<td>16</td>
</tr>
<tr>
<td>Number of local training epochs</td>
<td>5</td>
</tr>
</tbody>
</table>

In this study, the dice coefficient is used as an evaluation metric. The dice coefficient performs well in the image-based dataset. It calculates the difference between the actual and predicted images. The difference is between 1 and 0, where 0 refers to a mismatch and 1 refers to a 100 percent match. Besides the dice coefficient, sensitivity and specificity are also utilized in the evaluation of the model.

3.5. Model Aggregation

Model aggregation is a crucial step in the FL framework, where the server combines the model updates received from the clients to create a global model that reflects the patterns in the entire dataset. These models are used for creating one general model. This idea is identified with the collaboration mechanism. Formally, this method searches for a weights model, as shown in Figure 7.

Federated Averaging is a more advanced technique that combines the benefits of simple averaging and weighted averaging. In Federated Averaging, each client trains its local model for several epochs before sending the model update to the server. The server then aggregates the model updates using a weighted average, where the weights are determined based on the number of data points contributed by each client, as shown in Algorithm 1. The global model is then sent back to the clients for further local training and validation. This process is repeated for several rounds until the global model converges.
Figure 7. Federated learning model receiving local model weights from users.

Algorithm 1: Model Aggregation

INPUT

- GlobalModel: Initial global model with basic parameter
- NumberRounds: Number of specified aggregation rounds
- NumberLocalEpochs: Number of local training epochs per round
- Clients: List of clients

OUTPUT

- FinalGlobalModel: Aggregated global model

1. **INITIALIZATION**: (This step initializes the algorithm)
   - Initialize the GlobalModel with basic parameters

2. FOR round IN RANGE: (Loop through the specified number of aggregation rounds)
   - Server.broadcast (GlobalModel)
   - FOR EACH client IN Clients:
     - LocalModel = copy(GlobalModel)
     - NumberOfDataPoints = 0
     - FOR epoch IN RANGE (NumberLocalEpochs):
       - SampledData = Client.sample_data()
       - NumberOfDataPoints += len (SampledData)
       - LocalModel.train (SampledData)
12   Client.send_model_update (LocalModel, NumberOfDataPoints)
13   TotalDataPoints = sum ([clientpoints for_client
14   points in Clients])
15   GlobalModelUpdate = 0
16   FOR Client, NumberDataPoints IN Clients:(Loop through each client and
17   the corresponding number of data points used for training)
18   ClientUpdate = Client.receive_model_update()
19   WeightedUpdate = NumberoDataPoints/totalData-
20   Points) × ClientUpdate
21   GlobalModelUpdate += WeightedClientUpdate
22   GlobalModel.update (GlobalModelUpdate)
23   RETURN GlobalModel

In this study, Federated Averaging is used to aggregate the model updates received
from the clients. Federated Averaging has been shown to provide superior performance
compared to simple averaging and weighted averaging in various FL applications, including medical imaging.

3.6. Performance Metrics

This paper uses different evaluation methods. The dice coefficient is popular for segmenta-
tion tasks which calculate the difference between the predicted and actual seg-
ments, and the assigned values between 0 and 1.0 refer to a mismatch and 1 refers to a
perfect match. In addition to the dice coefficient, this paper uses the following evaluation
metrics.

\[
\text{Accuracy} = \frac{(TP + TN)}{(TP + TN + FP + FN)}
\]  \hspace{1cm} (1)

\[
\text{Precision} = \frac{(TP)}{(TP + FP)}
\]  \hspace{1cm} (2)

\[
\text{Sensitivity} = \text{recall} = \frac{(TP)}{(TP + FN)}
\]  \hspace{1cm} (3)

\[
\text{F1 score} = 2 \left( \frac{\text{precision} \times \text{recall}}{\text{precision} + \text{recall}} \right)
\]  \hspace{1cm} (4)

\[
\text{Dice score} = \frac{2(\sum P_{\text{actual}} \times P_{\text{predicted}})}{\sum P_{\text{actual}}^2 + \sum P_{\text{predicted}}^2 + \varepsilon}
\]  \hspace{1cm} (5)

4. Experiments and Results

This section describes the experimental setup and results used to evaluate the performance of the FL model for brain tumor segmentation. Specifically, the model’s performance was analyzed in terms of its dice coefficient, sensitivity, and specificity.

4.1. Model Training and Validation

To train and validate the FL model, a standard process of dividing the data into train-
ing and validation sets was followed, with the training set used to update the model pa-
rameters and the validation set used to assess the model’s performance. Each client trained
their local model using their respective data, with the server aggregating the model up-
dates using a weighted averaging approach. The model’s performance was evaluated with
the dice coefficient, sensitivity, and specificity.
4.2. Hyperparameter Tuning

Hyperparameters play a crucial role in determining the performance of a deep learning model. To optimize the hyperparameters of the FL model, a grid search approach was applied. This study experimented with various hyperparameters such as learning rate and weight decay. After thorough evaluation, the optimal combination was identified that resulted in the best validation performance, as outlined in Table 5.

Table 5. Summary of the hyperparameter tuning process.

<table>
<thead>
<tr>
<th>Hyperparameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimization Method</td>
<td>Grid search</td>
</tr>
<tr>
<td>Tuning</td>
<td>Learning rate, weight decay</td>
</tr>
<tr>
<td>Validation Performance</td>
<td>The combination of hyperparameters with the best validation performance was selected</td>
</tr>
</tbody>
</table>

To ensure the model’s effectiveness, hyperparameter tuning was performed, as depicted in Table 5. This involved an iterative approach and hyperparameters were systematically adjusted based on the validation performance. Through this meticulous process, we were able to strike a balance between model complexity and generalization ability, ultimately enhancing the overall performance of the proposed federated learning model.

The careful consideration and evaluation of these architectural choices, parameters, and hyperparameters were vital in successfully achieving the objectives of the proposed work. The improvements resulting from these modifications are reflected in the model’s accuracy, efficiency, and suitability for the federated learning setting.

4.3. Comparison with Traditional and Deep Learning Methods

To evaluate the effectiveness of the FL model for brain tumor segmentation, this study compared its performance with traditional model training approaches such as centralized learning and distributed learning. The FL model was also compared with other DL models including CNNs, RNNs, and deep neural network architectures.

First, this study evaluated the performance of the FL model on the BraTS 2019 dataset and compared it with traditional model training approaches such as centralized learning and distributed learning. Table 6 presents a summary of the performance metrics for each model.

Table 6. Performance evaluation of different learning models for medical image analysis.

<table>
<thead>
<tr>
<th>Model</th>
<th>Dice Coefficient</th>
<th>Sensitivity</th>
<th>Specificity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized Learning</td>
<td>0.84</td>
<td>0.89</td>
<td>0.92</td>
</tr>
<tr>
<td>Distributed Learning</td>
<td>0.85</td>
<td>0.88</td>
<td>0.94</td>
</tr>
<tr>
<td>Proposed FL model</td>
<td>0.87</td>
<td>0.90</td>
<td>0.95</td>
</tr>
</tbody>
</table>

As shown in Table 6, the FL model outperforms both the centralized and distributed learning approaches in terms of the dice coefficient, sensitivity, and specificity. This indicates that the FL model is effective in accurately segmenting brain tumors using distributed data without compromising privacy or security.

In addition to comparing the FL model’s performance with traditional approaches, such as centralized and distributed learning, its effectiveness against other deep learning models which are commonly used for brain tumor segmentation was also evaluated. The FL model outperformed all other deep learning models in terms of the dice coefficient, sensitivity, and specificity. This indicates that the FL approach is effective for accurately segmenting brain tumors, even compared to other sophisticated deep learning models.
As shown in Table 7, the FL model outperforms the other models in terms of the dice coefficient, sensitivity, and specificity. This indicates that the FL model is effective in accurately segmenting brain tumors using distributed data without compromising privacy or security.

Table 7. Performance evaluation of various models.

<table>
<thead>
<tr>
<th>Model</th>
<th>Dice Coefficient</th>
<th>Sensitivity</th>
<th>Specificity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federated Learning</td>
<td>0.87</td>
<td>0.90</td>
<td>0.95</td>
</tr>
<tr>
<td>U-Net</td>
<td>0.83</td>
<td>0.88</td>
<td>0.91</td>
</tr>
<tr>
<td>CNN</td>
<td>0.82</td>
<td>0.87</td>
<td>0.93</td>
</tr>
<tr>
<td>RNN</td>
<td>0.76</td>
<td>0.81</td>
<td>0.89</td>
</tr>
<tr>
<td>Other Neural Networks</td>
<td>0.80</td>
<td>0.84</td>
<td>0.92</td>
</tr>
</tbody>
</table>

As shown in Figure 8, the FL model achieves a higher dice coefficient, sensitivity, and specificity compared to other deep learning models commonly used for brain tumor segmentation, such as CNNs, RNNs, and other neural network architectures.

Figure 8. Model performance score.

Table 8 compares the performance metrics (dice coefficient, sensitivity, specificity) of federated learning with non-federated models (U-Net, CNN, RNN, other neural networks) when trained on distributed data.

Table 8. Performance comparison on distributed data (federated learning vs. non-federated models).

<table>
<thead>
<tr>
<th>Model</th>
<th>Dice Coefficient</th>
<th>Sensitivity</th>
<th>Specificity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federated Learning</td>
<td>0.87</td>
<td>0.90</td>
<td>0.95</td>
</tr>
<tr>
<td>U-Net (Distributed)</td>
<td>0.83</td>
<td>0.88</td>
<td>0.91</td>
</tr>
<tr>
<td>CNN (Distributed)</td>
<td>0.82</td>
<td>0.87</td>
<td>0.93</td>
</tr>
<tr>
<td>RNN (Distributed)</td>
<td>0.76</td>
<td>0.81</td>
<td>0.89</td>
</tr>
<tr>
<td>NN (Distributed)</td>
<td>0.80</td>
<td>0.84</td>
<td>0.92</td>
</tr>
</tbody>
</table>
Table 9 compares the performance metrics (dice coefficient, sensitivity, specificity) of non-federated models (U-Net, CNN, RNN, other neural networks) when trained on centralized data.

Table 9. Performance comparison on centralized data (non-federated model).

<table>
<thead>
<tr>
<th>Model</th>
<th>Dice Coefficient</th>
<th>Sensitivity</th>
<th>Specificity</th>
</tr>
</thead>
<tbody>
<tr>
<td>U-Net (Central)</td>
<td>0.86</td>
<td>0.89</td>
<td>0.96</td>
</tr>
<tr>
<td>CNN (Central)</td>
<td>0.85</td>
<td>0.88</td>
<td>0.92</td>
</tr>
<tr>
<td>RNN (Central)</td>
<td>0.82</td>
<td>0.85</td>
<td>0.90</td>
</tr>
<tr>
<td>NN (Central)</td>
<td>0.84</td>
<td>0.87</td>
<td>0.91</td>
</tr>
</tbody>
</table>

Table 10 presents another set of experiments and performance evaluations of the proposed FL model and three recent models from the literature. The results showed the higher performance of the FL model with dice score, sensitivity, and specificity. The improved deep learning model showed slightly lower results. Multi-Modal Fusion also yielded competitive results, highlighting the benefit of combining modalities for accurate segmentation. Each technique’s efficacy may vary based on dataset and tumor complexity. U-net with an attention mechanism performed better than other models.

Table 10. Performance evaluation of various models.

<table>
<thead>
<tr>
<th>Model</th>
<th>Dice Coefficient</th>
<th>Sensitivity</th>
<th>Specificity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved Deep Learning Model</td>
<td>0.82</td>
<td>0.88</td>
<td>0.92</td>
</tr>
<tr>
<td>U-Net with Attention</td>
<td>0.85</td>
<td>0.90</td>
<td>0.94</td>
</tr>
<tr>
<td>Multi-Modal Fusion</td>
<td>0.86</td>
<td>0.89</td>
<td>0.93</td>
</tr>
<tr>
<td>Proposed FL</td>
<td>0.87</td>
<td>0.90</td>
<td>0.95</td>
</tr>
</tbody>
</table>

The superior performance of the FL model is due to its ability to leverage distributed data from multiple sources, improving model generalization and reducing overfitting. The FL approach also provides a mechanism for maintaining data privacy and security, which is essential for medical imaging applications where patient confidentiality is critical.

The dice coefficient score of 0.87 indicates a high level of accuracy in segmenting brain tumors. In addition, sensitivity measures how effectively the model can predict non-tumorous cases. The experiments show a 0.95 sensitivity score, which is a reasonably high score. Specificity, on the other hand, measures how many of the tumorous cases are correctly identified. The experiments reported a 0.90 specificity, which means that the model has 90 percent confidence in tumor detection.

Overall, the results demonstrate the effectiveness of FL for brain tumor segmentation, with the FL model achieving a higher level of performance than traditional approaches. The high values of the dice coefficient, sensitivity, and specificity indicate the potential of FL to improve medical imaging by providing accurate segmentation of brain tumors while maintaining data privacy and security. The high performance of the FL model is likely due to its ability to leverage distributed data from multiple sources, improving model generalization and reducing overfitting.

Table 11 presents the descriptive statistics which show the spread of the values in the experimental results. Even though the mean shows that all the models perform reasonably well, the proposed model outperformed the other models by a 5.7% margin. The same is true for sensitivity, where the proposed model outperformed the other models on a means basis by 4.5%, and 2.8% on the specificity measure.

Table 11. Performance evaluation of various models.

<table>
<thead>
<tr>
<th>Model</th>
<th>Dice Coefficient</th>
<th>Sensitivity</th>
<th>Specificity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Additionally, a statistical significance test was conducted to find out whether the results were statistically significant, or random chance. Thus, a one-way ANOVA test was applied, and the results are presented in Table 12. The table shows that the results are statistically significant for the dice coefficient where the p-value is 0.040. Similarly, the sensitivity results were also found to be statistically significant with the p-value 0.044. But, the results of specificity are not significant, with a slight margin of 0.000239%. However, at the 90% significant level, all results were found to be significant.

Table 12. Performance evaluation of various models.

<table>
<thead>
<tr>
<th></th>
<th>Dice Coefficient</th>
<th>Sensitivity</th>
<th>Specificity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observations</td>
<td>4.000</td>
<td>4.000</td>
<td>4.000</td>
</tr>
<tr>
<td>Mean</td>
<td>0.813</td>
<td>0.855</td>
<td>0.923</td>
</tr>
<tr>
<td>Standard Deviation</td>
<td>0.046</td>
<td>0.039</td>
<td>0.025</td>
</tr>
<tr>
<td>Minimum</td>
<td>0.760</td>
<td>0.810</td>
<td>0.890</td>
</tr>
<tr>
<td>25%</td>
<td>0.790</td>
<td>0.833</td>
<td>0.913</td>
</tr>
<tr>
<td>50%</td>
<td>0.810</td>
<td>0.855</td>
<td>0.925</td>
</tr>
<tr>
<td>75%</td>
<td>0.833</td>
<td>0.878</td>
<td>0.935</td>
</tr>
<tr>
<td>Maximum</td>
<td>0.870</td>
<td>0.900</td>
<td>0.950</td>
</tr>
</tbody>
</table>

* means there’s strong evidence against the null hypothesis, but there’s still a small possibility (5%) that the observed result is due to random chance. ** means there’s very strong evidence against the null hypothesis, with an even smaller possibility (1%) that the result is due to chance.

### 4.4. Impact of Federated Learning on Data Privacy and Security

FL offers a solution to the challenges of maintaining data privacy and security in medical imaging applications. This section discusses the impact of FL on data privacy and security, including an evaluation of data leakage risks and the efficiency of the communication protocol.

#### 4.4.1. Evaluation of Data Leakage Risks

One of the key advantages of FL is its ability to maintain data privacy and security by allowing model training locally on client devices without the need for data to be transmitted to a central server. This approach minimizes the risk of data leakage or unauthorized access to patients’ sensitive data.

To evaluate the risk of data leakage in the proposed FL framework, a threat analysis was conducted to identify potential vulnerabilities in the system. Two primary risks were identified: the risk of model inversion attacks and the risk of membership inference attacks.

Model inversion attacks involve attempting to reconstruct or extract sensitive data from a trained model. Attacks using membership inference try to discover whether data from a specific person was used to train the model. To mitigate these risks, several techniques were applied, including differential privacy, encryption, and secure aggregation protocols.

The experiments showed that the proposed approach, with appropriate security measures in place, can effectively mitigate the risk of data leakage and preserve the privacy of patient data.

#### 4.4.2. Efficiency of the Communication Protocol

One potential limitation of FL is the need for frequent communication between the clients and the server, which can be affected by factors such as network bandwidth and
latency. This section evaluates the efficiency of the communication protocol used in the proposed FL framework.

A weighted averaging approach for model aggregation was used, which involves computing the weighted average of the local model updates from each client device. This approach is computationally expensive for large datasets, as it requires transferring large amounts of data between the clients and the server.

To mitigate the computational overhead, several techniques were applied, including model compression and sparsification, i.e., quantization and L1 regularization to reduce the amount of data that needed to be transferred. The experiments showed that these techniques can effectively reduce the computational overhead of the communication protocol, making it more efficient for FL.

The evaluation of data leakage risks and the efficiency of the communication protocol indicate that FL is a viable approach for medical imaging applications where data privacy and security are critical. Further research can explore alternative techniques for improving the efficiency of FL, such as more efficient model aggregation protocols or novel compression and sparsification techniques.

4.5. Scalability of the Approach

Scalability is a critical consideration in the application of FL to large datasets or when increasing the number of participating clients. The section discusses the impact of the number of clients on performance and the trade-offs between computation and communication costs.

4.5.1. Impact of the Number of Clients on Performance

The number of clients participating in the FL framework can have a significant impact on the overall performance of the model. As the number of clients increases, the model must be trained on increasingly diverse and distributed data, which can lead to improved generalization and performance. However, more clients also increase the computational overhead of the model aggregation process.

To evaluate the impact of the number of clients on performance, experiments with varying numbers of clients, ranging from 10 to 100, were performed. The results showed that increasing the number of clients led to improved model performance, as measured by the dice coefficient, sensitivity, and specificity, as shown in Table 13.

<table>
<thead>
<tr>
<th>Number of Clients</th>
<th>Dice Coefficient</th>
<th>Sensitivity</th>
<th>Specificity</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0.85</td>
<td>0.89</td>
<td>0.93</td>
</tr>
<tr>
<td>50</td>
<td>0.87</td>
<td>0.91</td>
<td>0.94</td>
</tr>
<tr>
<td>100</td>
<td>0.89</td>
<td>0.92</td>
<td>0.96</td>
</tr>
</tbody>
</table>

As shown in Table 11, increasing the number of clients led to improved model performance, with the FL model achieving a higher dice coefficient, sensitivity, and specificity. However, as the number of clients increased, the communication and computation costs also increased, leading to longer training times and increased overhead.

4.5.2. Trade-Offs between Computation and Communication Costs

The FL approach involves a trade-off between communication and computation costs. To ensure privacy and security, the data must remain on the client’s devices, necessitating frequent communication between the clients and the server. This can lead to significant communication costs, especially with large datasets or when there are many participating clients.

To minimize the communication costs, several techniques were applied, including model compression and sparsification, to reduce the amount of data that needed to be
transferred. However, these techniques can increase the computational overhead of the model aggregation process, leading to longer training times.

As shown in Table 14, increasing the level of model compression and sparsification led to reduced communication costs but increased computation costs. The experiments showed that the optimal balance between computation and communication costs depended on the dataset’s size and the number of clients.

Table 14. Impact of model compression and sparsification on communication, computation, and test accuracy.

<table>
<thead>
<tr>
<th>Model Compression Level</th>
<th>Model Sparsification Level</th>
<th>Communication Cost (kB)</th>
<th>Computation Cost (ms)</th>
<th>Test Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Low</td>
<td>500</td>
<td>100</td>
<td>0.85</td>
</tr>
<tr>
<td>Low</td>
<td>Medium</td>
<td>750</td>
<td>150</td>
<td>0.89</td>
</tr>
<tr>
<td>Low</td>
<td>High</td>
<td>1000</td>
<td>200</td>
<td>0.92</td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
<td>750</td>
<td>120</td>
<td>0.87</td>
</tr>
<tr>
<td>Medium</td>
<td>Medium</td>
<td>1000</td>
<td>180</td>
<td>0.91</td>
</tr>
<tr>
<td>Medium</td>
<td>High</td>
<td>1250</td>
<td>240</td>
<td>0.93</td>
</tr>
</tbody>
</table>

The communication cost and computation time for synchronous and asynchronous protocols were compared. Synchronous protocols are those in which all nodes in the network are synchronized, and each node waits for the others before proceeding to the next step. Asynchronous protocols, on the other hand, allow nodes to operate independently and without coordination from other nodes.

5. Discussion

5.1. Key Findings of the Study

This study has shown that FL is a promising approach for accurate brain tumor segmentation while preserving data privacy and security. The key findings of this study are below.

5.1.1. FL Improves Model Performance

The experiments conducted in this study demonstrated that FL led to improved model performance, with the model achieving a higher dice coefficient, sensitivity, and specificity compared to traditional and other deep-learning-based methods.

The experimental results conclusively showcase that the FL approach substantially elevated the dice coefficient, sensitivity, and specificity compared to traditional centralized learning methods and other deep-learning-based models. The improvement observed across these metrics indicates that FL effectively enabled our model to achieve a more accurate segmentation of brain tumors.

By leveraging data distributed across various sources, FL facilitated the model to improve generalization to diverse data patterns, ultimately enhancing segmentation accuracy. The decentralized nature of FL allowed for a broader and more representative dataset, reducing biases that might be present in a centralized dataset.

In summary, the adoption of federated learning played a pivotal role in significantly enhancing the performance of our brain tumor segmentation model. The improvements in the dice coefficient, sensitivity, and specificity metrics underscore the effectiveness of FL in accurately segmenting brain tumors while addressing data privacy concerns, further establishing its potential for broader applications in medical imaging.

5.1.2. FL Preserves Data Privacy and Security

This study has shown that FL effectively mitigates the risk of data leakage and preserves the privacy of patient data with appropriate security measures in place. Differential
privacy and encryption techniques were applied to prevent model inversion attacks and secure aggregation protocols to prevent membership inference attacks.

5.1.3. FL Is Scalable

This study demonstrated that FL is a scalable approach for brain tumor segmentation, with the potential to improve performance with increasing numbers of clients. However, the trade-offs between communication and computation costs highlight the need for efficient model aggregation and communication protocols.

This study also demonstrates the potential of FL for accurate brain tumor segmentation while preserving data privacy and security. The scalability of the approach highlights its potential for large-scale medical imaging applications, where data privacy and security are critical considerations. Further research can explore alternative techniques for improving the efficiency and scalability of FL, such as more efficient model aggregation protocols or novel compression and scarification techniques.

5.2. Implications for Medical Imaging and Brain Tumor Segmentation

The results of this study have several implications for medical imaging and brain tumor segmentation. First, FL has the potential to enhance the accuracy of brain tumor segmentation, which can have a significant impact on patient outcomes. Accurate segmentation is critical for treatment planning and monitoring, as well as for assessing treatment efficacy.

Second, FL can help to address the challenges related to data privacy and security in medical imaging. The use of patient data for research purposes is subject to stringent regulations, and FL provides a promising approach for researching while preserving data privacy and security.

FL has the potential to accelerate the development and adoption of AI-based medical imaging applications. The scalability of the approach makes it well suited for large-scale medical imaging datasets, and the privacy-preserving nature of the approach makes it a viable option for research collaborations across institutions.

5.3. Limitations of the Current Approach

Despite the promising results of this study, there are several limitations to the current approach that need to be addressed in future research.

First, the computational and communication overhead of FL can be significant, especially when scaling to larger datasets or increasing the number of participating clients. More efficient model aggregation and communication protocols are needed to address these challenges.

Second, the performance of FL can be highly dependent on the quality and diversity of the data contributed by the participating clients. More research is needed to explore methods for ensuring data quality and diversity in FL-based medical imaging applications.

Finally, the current approach assumes that the participating clients are trustworthy and do not have malicious intent. However, this assumption may not hold in all cases, and more research is needed to explore methods for detecting and mitigating the risk of malicious clients in FL-based medical imaging applications.

In conclusion, FL has significant potential for improving the accuracy and privacy of brain tumor segmentation in medical imaging. However, further research is needed to report the restrictions of the current approach and to develop more efficient and effective FL-based medical imaging applications.
5.4. Opportunities for Future Research

The FL is a comparatively new era and therefore there are open challenges that need to be addressed. Federated learning (FL) holds promise for decentralized machine learning but presents various challenges and limitations. Inconsistencies between datasets across devices pose difficulties in aggregating models effectively, leading to biased outcomes. Communication overhead in FL, required for frequent device–server interactions, can slow down training and escalate computational demands. Privacy concerns arise during model aggregation, risking information leakage from individual devices. Data and model heterogeneity among devices with different hardware and software configurations make ensuring model compatibility a challenge. The absence of centralized control in FL complicates monitoring and fairness enforcement. Imbalanced data distributions across devices may yield biased models. Additionally, FL’s prolonged convergence process and resource constraints on edge devices hinder model updates and may compromise accuracy.

FL has potential for accurate brain tumor segmentation while preserving data privacy and security. There are several opportunities for future research in this area.

First, there is a need for more research on the optimization of FL algorithms for medical imaging applications. More efficient model aggregation and communication protocols are needed to address the computational and communication overhead of FL when scaling to larger datasets or increasing the number of participating clients.

Second, more research is needed to explore methods for ensuring data quality and diversity in FL-based medical imaging applications. The performance of FL is highly dependent on the quality and diversity of the data contributed by the participating clients. Methods for assessing and improving data quality and diversity are needed to ensure the accuracy and generalizability of FL-based medical imaging applications.

Third, more research is required to explore the potential of FL for other medical imaging applications beyond brain tumor segmentation. FL has the potential to enhance the accuracy and privacy of a wide range of medical imaging applications, such as image classification, object detection, and segmentation.

Finally, more research is needed to explore the potential of FL in combination with other emerging technologies, such as blockchain, to improve the privacy and security of medical imaging data. Blockchain-based solutions can provide additional security and transparency to FL-based medical imaging applications, enabling the more efficient and secure sharing of medical imaging data for research purposes.

FL has significant potential for improving the accuracy and privacy of medical imaging applications, and more research is needed to explore the optimization of FL algorithms, methods for ensuring data quality and diversity, the potential for other medical imaging applications, and the combination with other emerging technologies.

6. Conclusions

This study investigated the role of federated learning (FL) in accurate brain tumor segmentation while preserving data privacy and security. The experiments demonstrated that FL is an effective approach for brain tumor segmentation, achieving high levels of accuracy while preserving data privacy and security.

Specifically, the performance of FL was compared to other deep learning models such as U-Net, CNN, and RNN in Table 7. It was found that FL outperformed all these models, achieving a higher dice coefficient, sensitivity, and specificity. These results were tested for statistical significance in Table 10, and it was found that the results are significant with 90 and 95 percent significance levels. This suggests that FL is a promising approach for improving the accuracy of brain tumor segmentation.

The impact of FL on data privacy and security was also evaluated. It was found that FL can effectively preserve data privacy and security, even when training with a large
dataset. This is because FL does not require data to be centralized, which minimizes the risk of data leakage.

Overall, the findings of this study suggest that FL is a viable approach for accurate brain tumor segmentation while preserving data privacy and security. FL has the potential to revolutionize the field of medical imaging, and this study encourages further research in this area.

**Author Contributions:** Validation, M.N.; Resources, M.A.; Data curation, A.S.; Writing—original draft, F.U.; Visualization, F.A.; Project administration, S.K. All authors have read and agreed to the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** The datasets analyzed during the current study are available on the BraTS Website (https://www.med.upenn.edu/sbia/brats2018/data.html, accessed on 9 February 2023). The detailed description, online repository, and references [51] are provided in Table 1.

**Acknowledgments:** We thank our families and colleagues who provided us with moral support.

**Conflicts of Interest:** The authors declare no conflict of interest.

**References**


**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.