Paper Title:
Federated Learning for Medical Image Analysis with Deep Neural Networks

Paper Link:
https://www.mdpi.com/2075-4418/13/9/1532

1 Summary

1.1 Motivation:

For medical data, along with training the model for better accuracy, preserving the privacy of those images is also a significant factor. As sharing of local medical data from various medical institutions usually has regulatory constraints, so designing a Deep Neural Network (DNN) model to only train the local data is like exploiting the full potential of the DNN. Thus, a global training approach without sharing the local data is much required. Even if data were to be trained using decentralized and collaborative approaches like Federated Learning, there are possibilities of malicious and inversion attacks. Sometimes, adding extra measures to prevent these attacks might lead to the decrease in the accuracy of the model.

1.2 Contribution:

This research briefly covers different Federated Learning methods used in different studies for medical image classification and segmentation with DNN. It is mainly based on various disease predictions with different image modalities. The study also states some directions to address Federated Learning model performance and security. As there are various challenges associated with FL methods, some research directions are given as well.

1.3 Methodology:

Based on several researches on FL for the past few years, this study proposed some privacy implementation methods based on many factors of the data. Like Homomorphic encryption for keeping values hidden when shared by participants, differential privacy by adding noise to local data and Multi-Party Computation (MPC) to compute the aggravated model without the use of a central server by providing better privacy for the model parameters.

1.4 Conclusion:

With more quantity and variations of data available for training the FL model, the biases can be minimized that arises due to differences in demographics, different equipment etc. A better model generalization can be gained as well.

2 Limitations:

2.1 First Limitation:

After analyzing, it was found that using differential privacy for security assurance comes at the cost of model accuracy.

2.2 Second Limitation:

By using Multi-Party Computation (MPC), there is still scope to recover the local training data or images and threaten the data privacy.

3 Synthesis:

With the increase in use of Federating Learning approaches, various methods to address the possible attacks and performance adaptation are to be taken into account as well. We also need to consider the location, size, type of data, number of clients participating for fine tuning the model. In case of model drift or in case more data becomes locally available, the aggravated model post training at the central server and also the model during deployment at the local server has the scope to be re-trained.