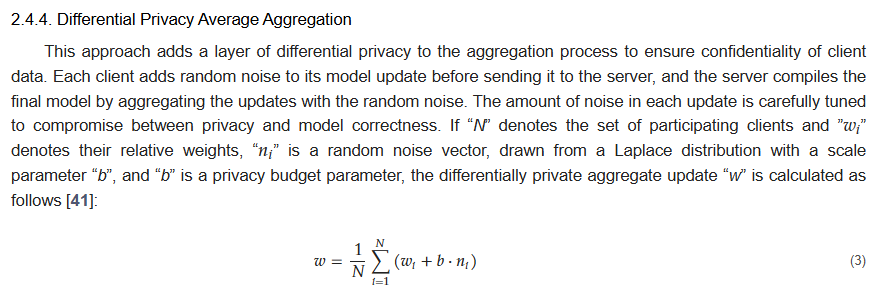
Federated Learning Notes

Implementing the federated learning method is a crucial part of this project. We aim to create a secure communication pathway for different users to train and use the same Global Model but without sharing data with other users of the same network.

It is very important to choose a correct aggregator method to update the global model. After detailed analysis of the following article, we can infer that the Differential Privacy Average Aggregation is a useful tool for our needs

https://www.mdpi.com/2079-9292/12/10/2287



Idea:

For the differential privacy average aggregation method we add random noise just like the article says so. This noise is not reversed so it affects the global model.

The idea is the following:

Create a noising function that takes as an argument a private key which we will pass throught the network as a blockchained password.

The aggregator will use this key to undo the noising and gain the actual values.

This way 100% safety is reserved