

Core Fundamentals of Federated Learning and Machine Unlearning - Week 1

Phoenix Asange-Harper

How FL Mitigates Privacy Risks

Federated learning provides greater privacy to users than traditional centralised training as FL ensures raw user data never leaves the device during training. The private data is processed into a model update which is sent to the server. A model update typically consists of updated weights, gradients, or the entire trained model. This method is more secure than transmitting raw data over a network, as seen in centralised systems, as model updates never contain as much information as raw data contains. Therefore, if a transmission is intercepted, a model update reveals far less information than the raw data would. Model updates are compatible with differential privacy which adds noise to the update to further obfuscate the underlying data. However, this introduces a trade-off between device privacy and model accuracy, because adding more noise increases privacy while decreasing model accuracy.

Real World FL Applications

Google – Mobile Keyboard Prediction

[https://arxiv.org/pdf/1811.03604](https://arxiv.org/pdf/1811.03604.pdf)

Google uses Federated Learning to power its mobile keyboard prediction. Mobile keyboard prediction is a complex problem because the keyboard is one of the primary interfaces of a mobile device and a mobile device has such extensive utility. This means that the most accurate prediction solution must consider many parameters which may include time of day, application that is being interacted with, person that is being messaged, among many others. To train a model based on these parameters, the data must be collected then used to train the model. Therefore, it is imperative that the data is kept private by using a decentralised training method.

University of Minnesota and Fairview - X-Ray COVID AI Model

<https://developer.download.nvidia.com/CLARA/Federated-Learning-Training-for-Healthcare-Using-NVIDIA-Clara.pdf>

The University of Minnesota and Fairview conducted a Federated Learning study that leveraged NVIDIA Clara Train to improve upon COVID-19 diagnosis using chest X-rays. In this case, it is both extremely important to develop such a model as well as keep the training data completely private. A diagnosis classifier has the potential to save countless lives, while at the same time if the private training data was exposed, it would compromise thousands of patient's private information. This is a perfect example as to the importance of Federated Learning in developing cutting-edge healthcare models. These models have the potential to be invaluable to the general population's health, while simultaneously requiring strong data privacy.