Federated Learning for Internet of Medical Things

By: Taranatee (Tara) Khan

Background

❑ Traditional, centralized machine learning has many limitations:
- Privacy and data security issues
- One way communication
- Long training times

❑Due to the security risk, it is no longer sufficient for the rapidly growing field of the Internet of Medical Things
- Medical data is prone to malicious attacks, as it is confidential and can be sold

❑ Federated learning is a proposed alternative which decreases the risk of a data breach, as only a learning parameter is shared between the clients and server

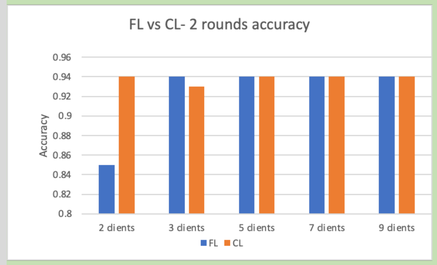
Objective

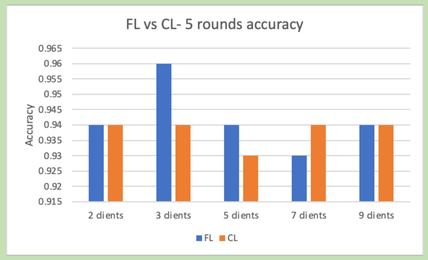
❑ Compare the performance of non federated and Federated Learning in IoT Anomaly Detection for accuracy and training time
❑ To evaluate the Federated Learning algorithm

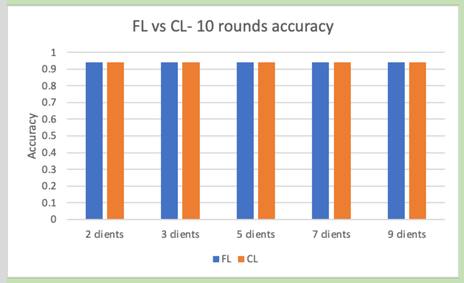
Dataset

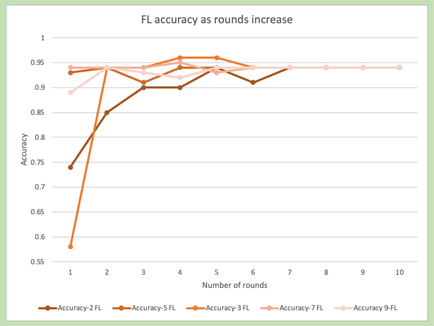
❑N-BaIoT, 9 commercial IoT devices
❑ Mirai and BASHLITE attacks (5 different types of attacks each)
❑ 115 features per data point
❑ Min-max normalization to scale down the values (done locally, using global min-max vector)

Accuracy

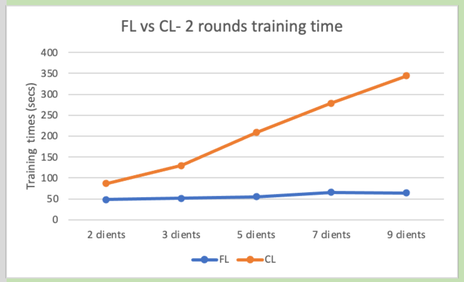


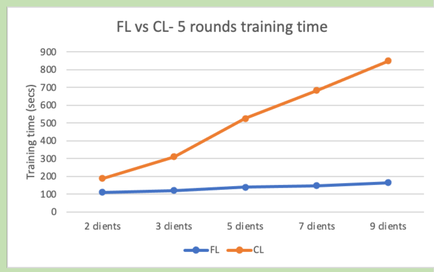


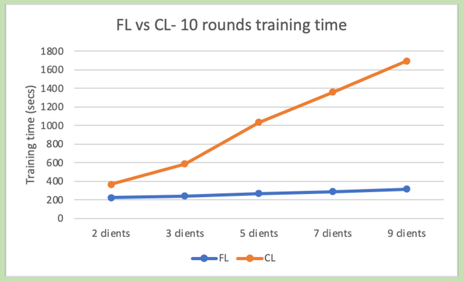




Training Time



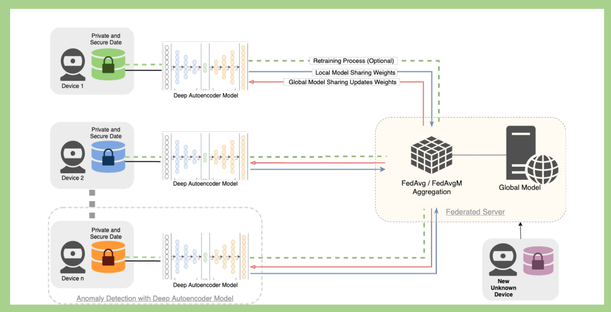




Methodology

❑ Federated Learning at the edge:
- Training occurs locally at each client
- Learning parameter sent to server from each client
- Learning parameters aggregated at server to create global model
- New global model sent to clients and process is repeated

❑ Autoencoder algorithm:
- Trained strictly on benign data
- Data is inputted, condensed, then reconstructed
- For attack data, the reconstructed input will not match the input, giving a reconstruction error.



Results

❑ Accuracy:
- Comparable between CL and FL, discrepancy decreases as number of rounds and clients increase
- For FL, tended to plateau around 5 rounds

❑ Training Time:
- FL had lower training times than CL for all trials
- Average time decrease of 67% across all numbers of clients and rounds tested