Department of Computer Science | Lund Technical University | Date of presentation June 11 2020
Master Thesis: Federated Learning Used to Detect Credit Card Fraud
Students: Madeleine Jansson and Måns Axelsson
Supervisors: Rasmus Ros (LTH), Mehmood Alam Khan (IBM) and Peter Forsberg (IBM)
Examiner: Volker Krüger

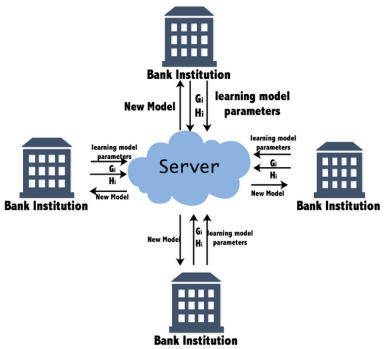
Federated Learning Used to Detect Credit Card Fraud

Popular science summary by ***Madeleine Jansson and Måns Axelsson***

Building a fraud detection system with Federated Averaging the results shows that the federated model can perform and even outperform the equivalent centralised model, Multi Layer Perceptron, when trained on the same dataset.

Machine learning has only been around for approximately 70 years, still, this learning technique is used in many different industries including for example finance, medicine, music and games. This learning technique enables to predict future outcomes and recognise patterns by analysing massive quantities of data, which was done by hand before the era of machine learning. In our thesis, we took advantage of the power of machine learning when trying to solve a problem that costs society billions of dollars every year, namely, credit card fraud. In particular, we investigated and implemented, in collaboration with IBM, a rather new machine learning model called Federated Averaging.

Since the emerge of online shopping the number of credit card fraud have risen greatly and with more money spent online there are more opportunity's available for the fraudsters to commit a crime. Today, banks train centralised models, i.e. all training is done locally and there is no collaboration between different parties. These centralised fraud detection systems would increase greatly in performance if its models had access to more training data — a problem that could be solved if banks could collaborate when trying to combat fraud. Today, using the centralised approach, the collaboration between banks is nearly impossible due to safety and privacy reasons attached to the banks data. This is where federated learning comes into the picture. With this technique banks can collectively reap the benefits of a shared model, which has seen more fraud than each bank alone, without sharing the dataset with each other. Hence, the sensitive information of the cardholders is protected.



In our thesis, we have organised the dataset into three different settings and then the Multi Layer Perceptron and Federated Averaging was trained on all of these settings. Usually, when training a fraud detection system a dataset of at least six weeks is required for proof of concept, but we only had access to two days. Due to the small size of the dataset it was difficult to draw any definitive conclusions. To our surprise, however, the results from our thesis showed that Federated Averaging could perform and even outperform the Multi Layer Perceptron on our dataset. This shows that the federated approach is an interesting learning technique for future work since it allows parties to collaborate without revealing sensitive information and still get a model with better performance than for the centralised approach. Moreover, not only can federated learning be applied in the banking industry but researchers have also seen good results when applying this learning technique to, for instance, the healthcare and keyboard predictions from an edge device.