Individual Privacy Preservation in Federated Learning

Sudipta Paul, Vicenç Torra

Abstract

From a privacy point of view, to keep data local and only share it when appropriate is just better than sending them to a central entity for their processing. That is why decentralized machine learning and federated learning(FL) can be seen as a better approach than standard centralized machine learning. Nevertheless, the fact that data is kept local does not avoid inferences from both what is sent and from the machine learning model that the central entity computes. Data privacy constraints need to be added to other constraints typical of decentralized approaches (heterogeneous devices with e.g. different computation/communication capabilities). Our research focuses on machine learning for decentralized environments taking into account 'individual privacy requirements'.

To achieve this goal, we introduce a new federated learning framework Tópos-FL on the basis of subspace and correlation analysis upon the layers of the machine learning models. It mitigates several drawbacks of FedAvg. In particular, data reconstruction and membership attack. In our approach, a conjugated view of the layers is being transferred to the central server where the update is subject to maximizing the correlation between the global and the local models. We experimented using the MNIST, BOB-ROSS-PAINTINGS, CIFAR10 and Wine Quality dataset on a simulated space to test our approach.