Making a secure framework for Federated Learning

Vaibhav Gusain, Master of Science in Computer Science

University of Dublin, Trinity College, 2021

Supervisor: Aljosa Smolic

Federated learning approach was built so that we can use data which is distributed at different user devices to train a machine learning algorithm, without the data being actually transferred outside the user device. Thus facilitating the learning of the model and also not hampering the user privacy-the user data never leaves the local device. However recent approaches have shown that private user data can be exploited by using the gradients or the weights that the edge model share with the main server. In this dissertation, we would like to introduce an agent which would allow the user devices to share the weights in an encrypted way, the server would do its update on such encrypted weights and then return the updated weights to the user