




Machine Learning with TensorFlow Federated

To build powerful machine learning models, lots of data is required. However, obtaining the data comes with privacy risks for the people or entities that provide their data.

Recently, Google published TensorFlow Federated - an open source framework to allow machine learning on decentralized data. The approach of federated learning makes machine learning in the age of mobile devices and wearables both more efficient, as well as more privacy-friendly.

The goal of this thesis or project is to become familiar with the TensorFlow Federated framework, to understand and be able to explain the techniques which are implemented in it, to be able to build machine learning models in a federated way, and possibly to implement own enhancements of the framework.

 Master's Thesis	30 CP
 Bachelor's thesis	12 CP
 Project	8/16 CP

Suitable for students with an interest in machine learning, security, privacy and cryptography. Preliminary machine learning knowledge is helpful, but not strictly required. However, a security background on the level of the *Security in IT Systems* lecture is expected. The *Privacy Engineering and Privacy Enhancing Technologies* lecture is a recommended prerequisite.

Matthias Matousek | matthias.matousek@uni-ulm.de | 027-3209

If you are interested or you need additional details, feel free to contact me or drop by for a non-binding chat.

