Institut für Verteilte Systeme
Institute of Distributed Systems

ulm university universität uulm

Machine Learning with TensorFlow Privacy

Machine learning offers great opportunities, but also comes with risks. Especially the privacy risks are becoming more prevalent in the discussions about machine learning.

Recently, Google published a machine learning library called TensorFlow Privacy. Its goal is to make it easier for developers and researchers to build privacy-preserving machine learning models. Specifically, it utilizes Differential Privacy, which mathematically guarantees that the training data to create the models is protected from being extracted.

The goal of this thesis or project is to become familiar with the TensorFlow Privacy library, to understand and be able to explain the techniques which are implemented in it, to be able to build privacy-preserved machine learning models, and possibly to implement own protection techniques that could enhance the TensorFlow Privacy library.

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