Institut für Verteilte Systeme
Institute of Distributed Systems

ulm university universität ulm

Machine Learning on Encrypted Data

Machine Learning enables great applications, such as voice assistants and image recognition. However, in most cases, it is required to send the input data to another party with powerful machine learning models and lots of computing power, in order to utilize the power of machine learning. This is a risk for privacy.

Libraries like tf-encrypted and PySyft aim to address this issue by implementing encryption mechanisms that allow machine learning on encrypted data. The goal of this thesis or project is to understand how encrypted machine learning techniques work and how they get implemented with tf-encrypted and/or PySyft. Further, it is possible to extend on this by comparing different libraries and techniques or by implementing own encrypted machine learning techniques.

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 | O27-3209

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