Associate Professorship of Coding and Cryptography
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Forschungspraxis, Bachelor's Thesis, Master's Thesis

Private and Secure Federated Learning

In federated learning, a machine learning model shall be trained on private user data with the help of a central server, the so-called federator. This setting differs from other machine learning settings in that the user data shall not be shared with the federator for privacy reasons and/or to decrease the communication load of the system.

Even though only intermediate results are shared, extra care is necessary to guarantee data privacy. An additional challenge arises if the system includes malicious users that breach protocol and send corrupt computation results.

The goal of this work is to design, implement and analyze coding- and information-theoretic solutions for privacy and security in federated learning.

Prerequisites

- Coding Theory (e.g., Channel Coding)
- Information Theory
- Machine Learning Basics

Advisors

Christoph Hofmeister, Maximilian Egger, Rawad Bitar, Luis Maßny