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

Forschungspraxis

Secure Record Linkage via Multi-Party Computation

Processing a massive amount of collected data by means of machine learning algorithms often becomes infeasible when carried out on single machines. To cope with the computational requirements, distributed cloud computing was introduced. Thereby, a large computational task is split into multiple parts and distributed among worker machines to parallelize the computations and thereby speed up the learning process. However, since confidential data must be shared with third parties and the outcome is threatened by potential corrupt computations, privacy and security has to be ensured. This is particularly critical in medical environments, in which we deal with individual patients' information.

To motivate the study of these challenges, a competition called iDash privacy and security workshop is hosted every year [1]. This year, the task is to develop a framework that securely links similar patient related entries being stored on different datasets without comprising privacy - for example to avoid double considerations in further processing steps. During this research internship, the student should use multi-party computation tools to develop a framework that complies with the aforementioned requirements.

[1] http://www.humangenomeprivacy.org/2022/competition-tasks.html

Prerequisites

- Coding Theory (e.g., Channel Coding)
- Linear Algebra
- Information Theory (optional)

Advisors

Rawad Bitar, Christoph Hofmeister, Luis Maßny, Maximilian Egger