Internship topic: Identity management for decentralized learning communities

Jan Ramon

October 2017

1 Context

Recently, internet companies collect huge amount of data of individual users. The central storage of this often sensitive data has been criticized due to the risks of abuse of the private information in a way which can't be controlled by the user.

An alternative paradigma is to avoid as much as possible to centrally collect data, while still providing similar services, while keeping the burden for the user minimal.

Important ideas there are to perform computations locally on mobile devices, and to communicate in a secure privacy-friendly way, avoiding to leak information which is not essential for the purpose of the communication.

One issue in decentralized learning is that it is necessary to be able to trust the other agents in the learning community to some extent. Many algorithms are presented in a "honest but curious" setting, which is often unsatisfactory. Briefly, agents don't want to disclose their identity, but they want to prove they are trustworthy, i.e., that their identity wouldn't be a reason to distrust them (and the contributions they make to the community calculations).

2 Objective

In this project, we want to investigate strategies to handle identities of agents participating in decentralized computations.

3 More information

The project involves the following steps:

- refine the identity-related aspects of communication and privacy models underlying typical decentralized learning algorithms.
- Study some relevant literature

- Propose a range of strategies which could be considered to better handle identities.
- Compare the several proposals according to selected relevant criteria.

4 Requirements

Knowledge of basic statistical concepts is desirable. A background in security, privacy and/or cryptography is clearly a plus.