Professur für Coding and Cryptography
Fakultät für Elektrotechnik und Informationstechnik
Technische Universität München

Forschungspraxis

Secure Federated Learning

In the initially proposed federated learning setting [1], the federator observes partial gradient computations of all clients contributing to a decentralized training procedure. However, clients might send malicious (corrupt) computations to harm the training process on purpose. Considering this model, security against malicious clients can be ensured by running statistics on the partial results [2, 3]. For example, clients' results that differ significantly from the vast majority of responses can be excluded from the training process. In recent works, secure aggregation of partial work was proposed [4]. The goal is to let the master only observe the sum of all local models, and by this to enhance the privacy level of the clients' data. These works, however, complicate the use of statistics to account for corrupt partial computations as the master only observes the aggregated result. The goal of this research internship is to review related literature on secure federated learning including their limitations, and to explore possible approaches to ensure security against potentially corrupt results while preserving privacy of the clients' data.

[1] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y. Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," vol. 54, pp. 1273–1282, 20--22 Apr 2017.

[2] P. Blanchard, E. M. El Mhamdi, R. Guerraoui, and J. Stainer, "Machine Learning with Adversaries: Byzantine Tolerant Gradient Descent," in Advances in Neural Information Processing Systems, 2017, vol. 30.

[3] Z. Yang and W. U. Bajwa, "ByRDiE: Byzantine-Resilient Distributed Coordinate Descent for Decentralized Learning," IEEE Transactions on Signal and Information Processing over Networks, vol. 5, no. 4, pp. 611–627, Dec. 2019.

[4] K. Bonawitz et al., "Practical Secure Aggregation for Privacy-Preserving Machine Learning," Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017. doi: 10.1145/3133956.3133982.

Voraussetzungen

- Coding Theory (e.g., Channel Coding)
- Information Theory

Betreuer

Christoph Hofmeister, Rawad Bitar, Maximilian Egger