Chair of Network Architectures and Services
School of Computation, Information, and Technology
Technical University of Munich

Thesis M.Sc.

Evaluating Quantization and Approximations Techniques for Privacy Preserving Machine Learning

Motivation

Privacy-Preserving Machine Learning (PPML) [1] allows multiple parties to train a machine learning model on their combined data without revealing their data to each other. Consider multiple hospitals that want to study adverse effects of a treatment on their patients. Clearly, training a machine learning model on their joint patient data would be beneficial. However, hospitals may not be allowed to share their patient data with each other.
A commonly used method to achieve Privacy Preserving Machine Learning is Secure Multiparty Computation (MPC) [2]. With MPC, parties can split up their data in secret shares that individually do not reveal anything about the underlying data. The model can then be trained on the secretly shared data, and the parties obtain a secret share of the trained model. The parties can use the resulting model for private inference where the model parameters as well as the input data a client submits to the model remains secret.
MPC works most efficiently for integer-based computation and non-linear functions. Therefore, PPML solutions usually train machine learning models using fixed point numbers and approximate non-linear functions such as the Softmax functions with piecewise polynomial functions [3]. These quantization and approximation techniques have different tradeoffs regarding model accuracy, training, and inference time.

Your Task

- Research quantization and approximation techniques for PPML
- Implement these techniques in a C++ based PPML framework
- Evaluate the runtime and accuracy tradeoffs of these techniques

Requirements

- Good programming skills in C++
- Experience with deep learning frameworks such as PyTorch
- Prior experience with ML quantization and approximation techniques is a plus

References

[1] https://ieeexplore.ieee.org/document/10179483
[2] https://eprint.iacr.org/2020/300.pdf
[3] https://ieeexplore.ieee.org/abstract/document/9519386

Contact

Christopher Harth-Kitzerow christopher.harth-kitzerow@tum.de