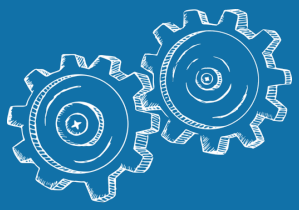


Efficient Machine learning application bench-marking for Homomorphic encryption libraries

Advisor: **Aikata**

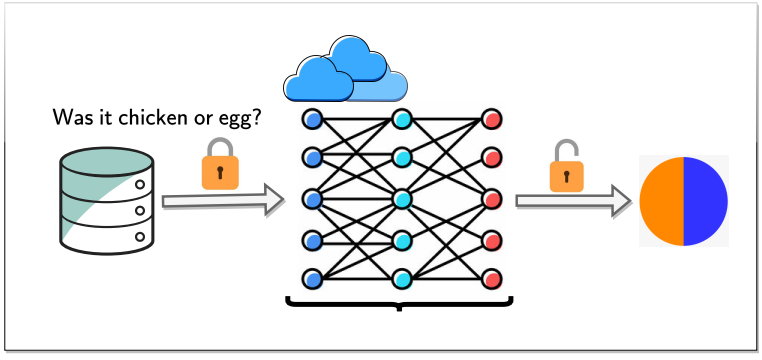
Motivation

Homomorphic encryption (HE) allows secure computation over private data [1]. There is a need for efficient machine learning models which can be easily translated to HE and aid secure evaluation. We will analyze existing machine learning models using homomorphic encryption libraries (e.g., SEAL).

The research goal is to provide efficient translations of various ML models like LeNet5, ResNet50, etc., and beat the existing results using our very own HE accelerator, *Medha* [2]. For motivation, please checkout the IDASH PRIVACY SECURITY WORKSHOP 2022 - secure genome analysis competition which focuses on these applications and will be one of the target venues for the research outcome. It can be extended to designing new HE friendly ML methods which provide the same/better accuracy with better performance.

Goals and Tasks

- Learn to use the well-defined HE libraries.
- Learn translation of ML algorithms to HE friendly level.
- Use Medha to accelerate the ML applications.



Literature

- *Machine learning on Encrypted data*

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
+ DiplomandInnenseminar (CS)
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Basic idea of Machine Learning models or Homomorphic encryption would help.
- Programming (C++ and Python)

Advisor Contact

aikata@iaik.tugraz.at