Finding PETs in the Real-World

Advisor: **Lukas Helminger**

Motivation

Data collection and analysis are rapidly increasing, but at what costs? There is no doubt about the potential benefits of big data. However, there is a rising concern about the individual's privacy creating an area of conflict. The question is: "Is there a way to do (economic) useful data analysis without violating the individual's privacy?"

Privacy Enhancing Technologies (PETs) try to answer this question with yes. Not only have PETs the potential to make existing applications privacy-preserving, but they could also create new data-driven business opportunities. At the IAIK, we are especially interested in PETs related to cryptography like Secure Multi-Party Computation (MPC), Homomorphic Encryption (HE), and Differential Privacy (DP).

These PETs are currently transitioning from the academic to the real-world. There is no overview of how widespread and successful these technologies are used. Your task is to document real-world deployments of these PETs in the business and the government sector. Thereby you would help to focus the research on PETs into the right direction.

Goals and Tasks

> Understand background on PETs (MPC, HE, DP)

> List, categorize, and compare the real-world deployments

> Provide portraits of individual deployments for illustration

Literature

> The Royal Society
Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis
https : / / royalsociety . org/ - /media / policy / projects / privacy - enhancing - technologies / privacy - enhancing - technologies-report.pdf 2019

Courses & Deliverables

☑ **Introduction to Scientific Working**
Short report on background
Short presentation

☑ **Bachelor Project**
Project code and documentation

☑ **Bachelor's Thesis**
Project code
Thesis
Final presentation

Recommended if you're studying

☑ CS   ☑ ICE   ☑ SEM

Prerequisites

> Interest in privacy and cryptography.

Advisor / Contact

lukas.helminger@iaik.tugraz.at