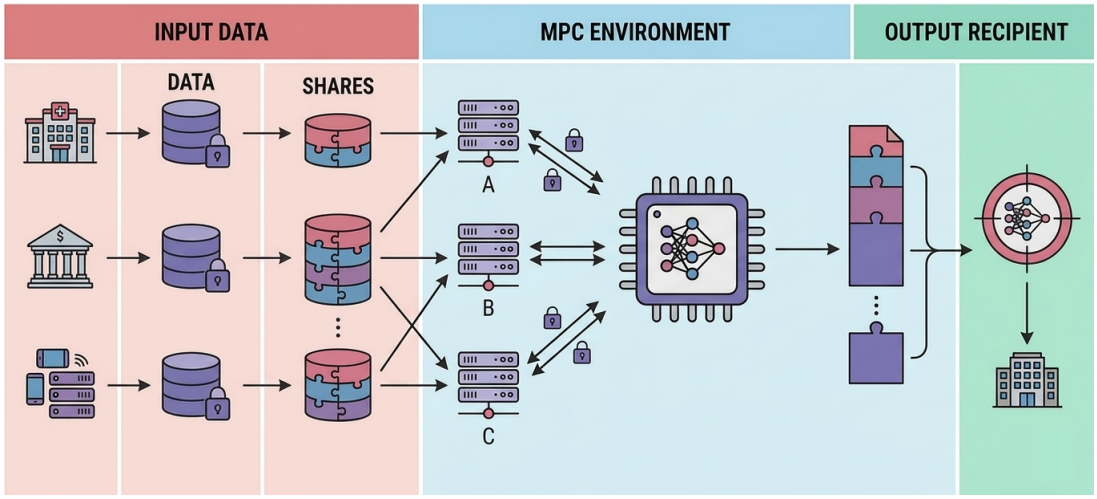
# Evaluating Practicality of Privacy-Preserving Machine Learning




Privacy-Preserving Machine Learning (PPML) enables training and deploying machine learning models on sensitive data without revealing it, using cryptographic tools like secure multiparty computation (MPC) and homomorphic encryption (HE). While the research landscape is rich, practical adoption is hindered by practical factors such as performance bottlenecks, usability challenges, and reproducibility issues.

This thesis will provide a clear map of the current PPML landscape. By evaluating a selection of PPML methods and protocols under carefully defined metrics—covering computation, scalability, and resilience to adversaries—the study will reveal which techniques are ready for real-world use and which remain research prototypes. The outcome will include a benchmarking framework to guide researchers and practitioners in selecting the right PPML approach for a given ML task and adversary models.

For a quick dive into MPC-based PPML, please check `https://eprint.iacr.org/2025/1679`.

## Practicalities


| | | | |
|---|---|---|---|
| Promotor: | Yunwen Liu | | |
| Daily supervisor: | Aysajan Abidin | firstname.lastname@esat.kuleuven.be | office 01.13 |
| | Martin Zbudila | firstname.lastname@esat.kuleuven.be | office B01.19 |


Nature of the work: 30% literature, 20% theoretical work, 50% software
Number of students: 1