Enabling Computation on Encrypted Data

Scaling-up Privacy-Preserving Techniques in Healthcare AI Applications

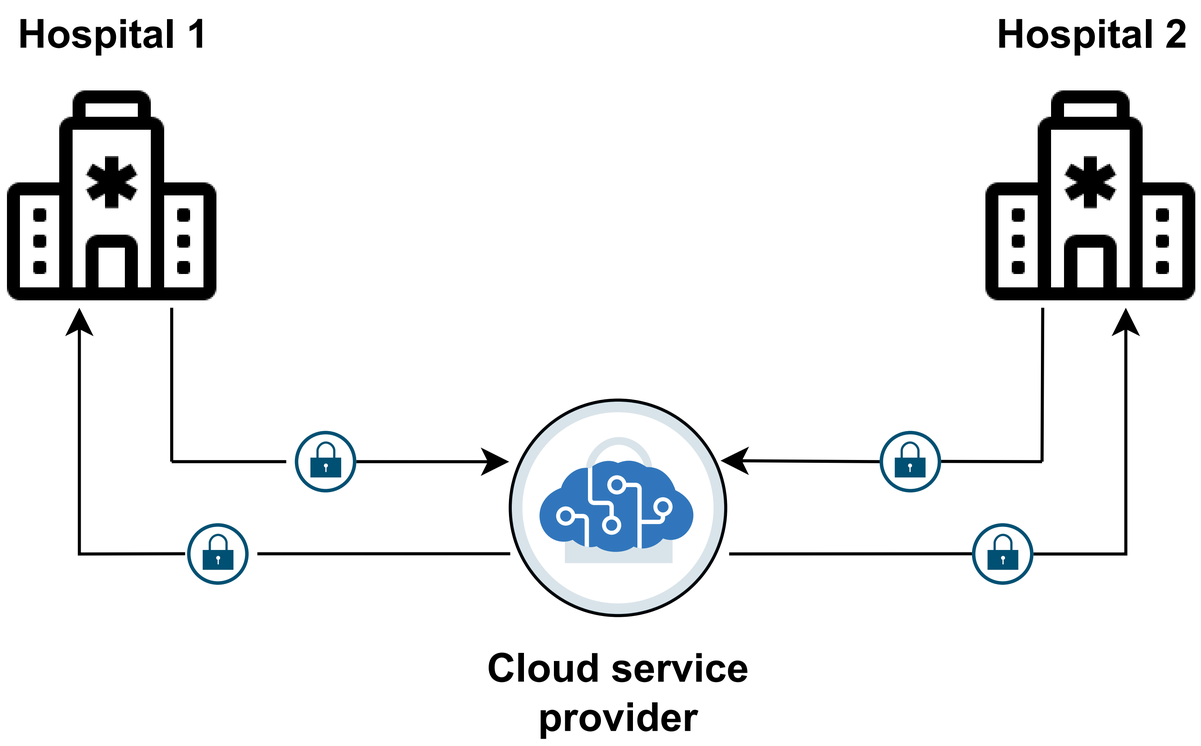
Motivation

What happens if a hospital wants to use a cloud AI application on its patients' data.

By sharing sensitive patient data with a third-party the hospital could face legal implications (GDPR) and additionally risk the privacy of the patient's data.

Cryptography offers a way to surpass these obstacles with a technique called Homomorphic Encryption (HE).

Homomorphic Encryption allows computations to be done on *encrypted* data without having to decrypt them first!



Example of hospital HE setting

- **Hospital 1** located in the Netherlands, wants to use a (collectively) trained model from various (maybe cross-country) hospitals
- **Hospital 2** located in Spain, wants to use the same model from the same cloud service provider
- **Homomorphic Encryption** enables both hospitals to train or do inference on the same model
- Even though the model is held by a third-party, **privacy** is not compromised!

What's the catch here?

Cryptography offers solutions to problems that sometimes intuitively seem impossible. But always at a cost...

The execution time overhead for operating on Fully Homomorphically Encrypted data is significant.

Even for very simple operations the execution time overhead could be **millions** of times slower, thus making real-world applications **impractical**.

How to scale-up?

Strategies to scale-up real-world FHE applications:

- Optimised implementations, usually leveraging large vector processor instructions (RISC-V "V" extension)
- Custom hardware Instruction Set Extensions (ISE)
- Implementation optimisations for specific FHE schemes, assuming an ML model and some configuration.

Take-home messages

1. **Healthcare applications** leverage Machine Learning to provide better and more accurate services but the **privacy concerns** of treating patient's data form a significant barrier.
2. Cryptography promises to remove this barrier with **Homomorphic Encryption**, a technique that allows computations to be made **on encrypted data**.
3. The **tremendous overhead** introduced by these techniques must be tackled with various methods: providing fast, **optimised implementation** leveraging large vector processor instructions, **custom hardware ISEs** and FHE **scheme-specific optimisations** for specific ML models and configurations.

Find out more

https://secured-project.eu

Acknowledgment

This project/research has received funding from the European Union's Horizon Research and Innovation Actions under the Grant Agreement No. 101095717 (SECURED). Views and opinions expressed are those of the author(s) and do not necessarily reflect those of the EU or the Health and Digital Executive Agency. Neither the EU nor the granting authority are responsible for them.

University of Amsterdam
Informatics Institute

Complex Cyber Infrastructure

SECURED EU Project

Funded by the European Union

Georgios Tasopoulos (g.tasopoulos@uva.nl)

Cyber Physical Systems School 2024
16 - 20 September 2024, Alghero, Sardinia, Italy.