SECURED Tutorial: Privacy-Enhancing Technologies (PET)

Francesco Regazzoni, Apostolos Fournaris, Paolo Palmieri

Data Privacy?

- Cryptography is an old science (more than 3'000 years!)
- The diffusion of digital devices and network connectivity boosted the amount of information shared
- We encrypt the communication, but not the processing!
- How to access / provide services respecting privacy?

An Example: Zero Knowledge Proof (ZKP)

- Goal: to prove that the assertion “a” is true without revealing information on why it is true (actually, without revealing any additional information at all)
- ZKP is not a 100% proof, but gives a very high probability
- Satisfies thee main criteria: *Soundness*, *Completeness*, and *Zero-knowledge*

Example: Ali Baba cave

- Peggy (prover) and Victor (verifier)
- Peggy knows the magic word to open the door in the cave
- Victor wants to know if Peggy indeed knows the word
- Label the paths from “A” and “B”
- Victor, randomly select the path
- Repeating the experiment, Peggy can always return from the correct path only if she knows the the magic word

Example: Ali Baba cave

- Sound: Answer based on valid reason (if Peggy was guessing, the correct path would be selected only 50% of the time
- Complete: Probability of Peggy correctly guessing is lower
- Zero-knowledge: Victor does not know anything additional

Other Privacy Preserving techniques

- Differential privacy
- Distributed learning
- Private computation

Differential privacy

Goal: preserve output privacy

- Adversaries can reconstruct input data analyzing the statistics of the output data
- Differential privacy **reduces** the risk to reconstruct input data by adding noise to the data (input or output data)
- The amount of information that can be recovered is **bounded**
- Noise is added to guarantee this bound

Distributed learning

- Protocols to train a model keeping the data private
- Two main protocols: **Federated Learning** and **Split Learning**
- Federated Learning: each party has a copy of the network to train; each perform training locally and send the gradient to an authority; the authority agregates the gradients and provide updates for the local networks
- Split Learning: the full network is split at a specific layer into smaller portions that are trained separately on the central authority and at each party with local data. Parties perform forward propagation up to the split and send the result to continue the forward propagation,and the back propagation up to the cut, where the gradients are sent to the parties for updating their networks.

Private computation

- Techniques to compute on data securely
- **Secure Multiparty Computation** (SMPC)and **Homomorphic encryption** (HE)
- HE allows to perform computation on encrypted data.
- SMPC are usually based on “secret sharing”: each party holds a piece of computation that they use to perform their larger computation.

Homomorphic encryption: CKKS

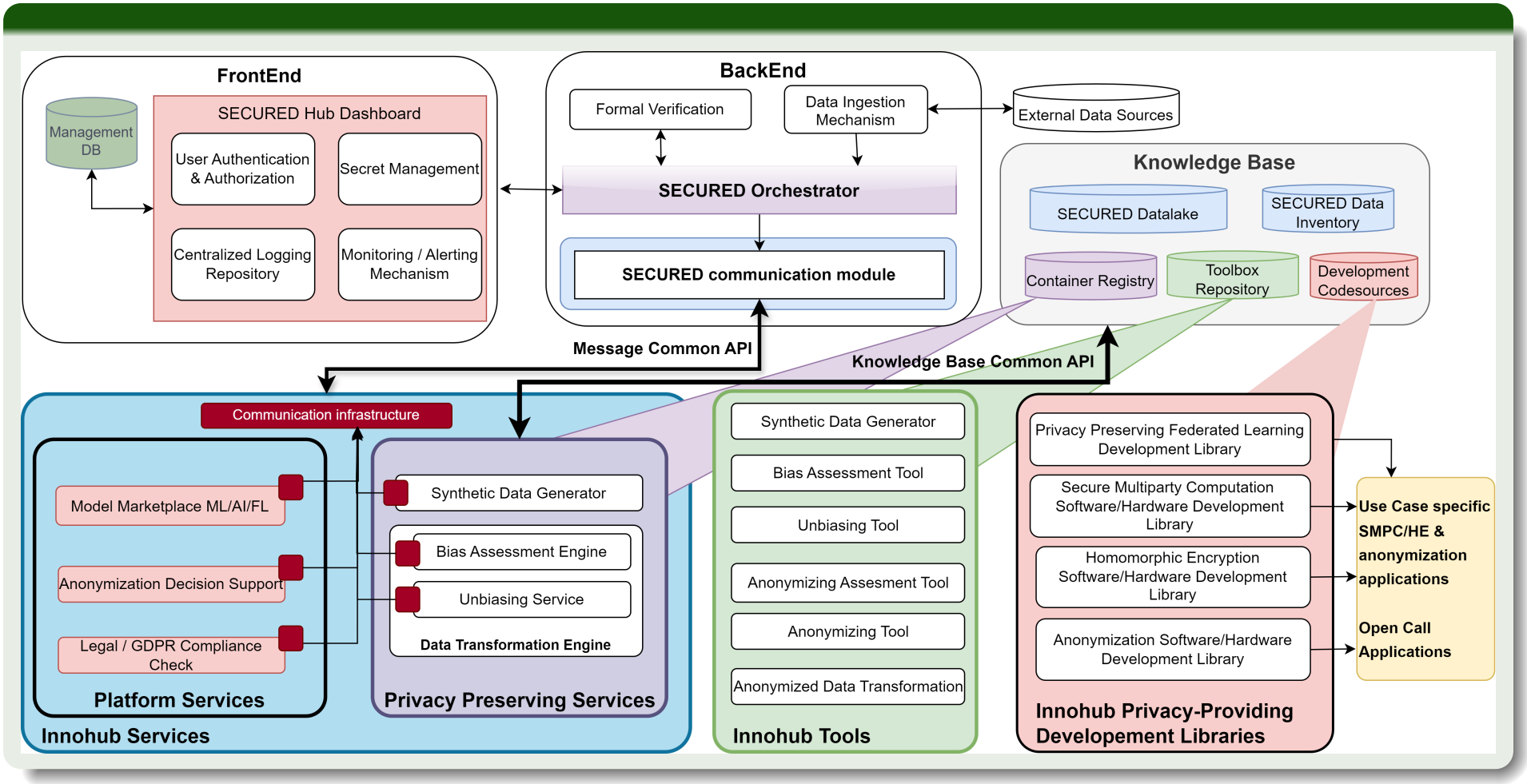
- Encode a vector of values into a plaintext polynomial
- Encrypt using a public key
- CKKS provides: addition, multiplication and rotation
- Build a “circuit” to compute using the operations provided
- Creating correct and efficient circuits **is not** straightforward, but **theoretically** there is no limit to the computations
- Perform the computation
- Decrypt the results with the secret key will give us the resul of the function

Homomorphic encryption: TFHE

- Fast Fully Homomorphic Encryption Library over the Torus
- The security of the scheme is based on a hard lattice problem called Learning With Errors
- Very fast **bootstrapping**
- No restriction on the number of gates or on their composition.
- Suitable with either manually crafted circuits or automatically generated ones

SECURED

SECURED Key Components Architecture



Contacts

Francesco Regazzoni: f.regazzoni@uva.nl; francesco.regazzoni@usi.ch

Apostolos Fournaris: fournaris@isi.gr

Paolo Palmieri: p.palmieri@cs.ucc.ie

Funded by the European Union

Questions?

Thank you for your attention!

SECURED

Scaling Up secure Processing, Anonymization and generation of Health Data for EU cross border collaborative research and Innovation

website: https://secured-project.eu/

Funded by the European Union