Collaboration Without Data Sharing: The Federated Secure Computing Architecture

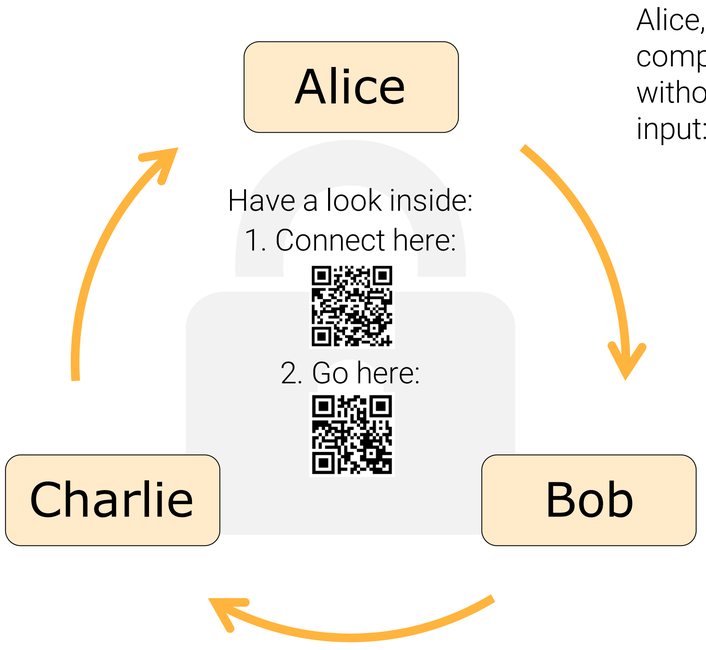
C. Goelz[1], H. Ballhausen[2]

[1] Department of Medicine I, LMU University Hospital, LMU Munich, 81377 Munich, Germany
[2] Department of Radiation Oncology, LMU University Hospital, LMU Munich, 81377 Munich, Germany

BACKGROUND

Secure Multi-Party Computation (MPC) is a cryptographic method that enables multiple parties to jointly compute a function over their inputs while keeping those inputs private. In scenarios where open data sharing is not an option due to security or privacy concerns, MPC allows participants to collaborate without revealing their individual data. Each party performs computations on encrypted data and only learns the final result, preserving confidentiality throughout the process. MPC has wide-ranging applications, particularly in sectors like finance, healthcare, and collaborative research, where privacy is critical but joint insights or outcomes are needed. [1]

Example: Secure Sum

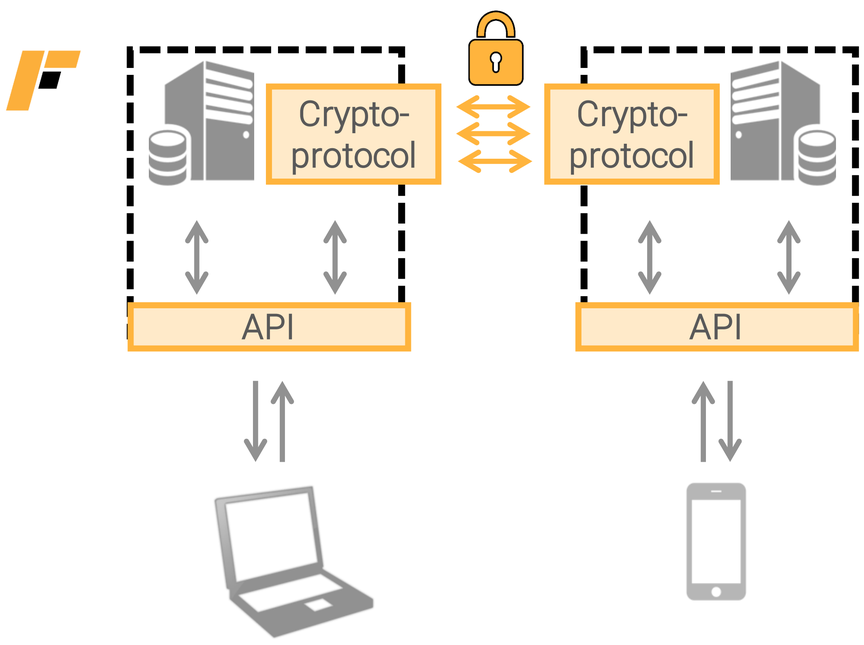


Alice, Bob and Charlie want to compute the sum of their inputs without letting the others know their input:

1. Parties submit inputs
2. Sum is computed
3. Only the result is shared

THE FEDERATED SECURE COMPUTING ARCHITECTURE

- Open-source initiative developed by LMU Munich, supported by Stifterverband. [2]
- Acts as middleware, bridging client-side business logic with server-side cryptographic backends.
- Encapsulates secure computing functions into microservices.
- Provides a simple, user-friendly API



Federated: connecting heterogenous systems from workstations to smartphones and IoT

Secure: every data owner runs their own server, all their data always remains in their control

Computing: cryptographic protocols run peer-to-peer networks to generate results without revealing input data

Find client and server libraries, examples, and documentation at **Github**

APPLICATIONS

Privacy-friendly Evaluation of Patient Data with Secure Multiparty Computation in a European Pilot Study [3]

- Successfully demonstrates the use of federated analysis in a pan-European study to address privacy concerns in clinical research, focusing on the treatment plan for a rare type of cancer. Data from LMU University Hospital in Munich, Germany, and Policlinico Universitario Fondazione Agostino Gemelli in Rome, Italy, were analyzed using MPC within the Federated Secure Computing architecture.

A Secure Median Implementation for the Federated Secure Computing Architecture [4]

- Demonstrates the implementation of a secure median, a non-trivial computation, within the Federated Secure Computing (FSC) framework. The implementation was tested on both synthetic datasets and real-world medical datasets, such as breast cancer and heart disease data in diverse technical setups from local deployment to a commercial hyperscaler.

- Pre-made Connexion/Flask app served by Uvicorn:
  e.g. start a server with:

```
$ python ./src/__main__.py --port = 55501
```

- Given a network definition a typical client side Python implementation would look like the following:

```python
import federatedsecure.client
import shared

MY_INDEX = 1  # Index for the current client in federated network
MY_URL = 'http://127.0.0.1:55501'  # URL to federated server
MY_DATA = "SOME DATA"  # Data to be processed in the federated system
NETWORK = {**shared.NETWORK, 'myself': MY_INDEX}  # Federated Network

if __name__ == "__main__":

    # Connect to the federated system
    api = federatedsecure.client.Api(MY_URL)

    # Request the Simple Multiparty computation protocol
    microservice = api.create(protocol="SIMON")

    # Perform the secure computation
    result = microservice.compute(
        microprotocol="SecureSum",
        data=MY_DATA,
        network=NETWORK
    )

    # Receive the result of the computation
    print(api.download(result))
```

References

1. Zhao C, Zhao S, Zhao M, et al. Secure multi-party computation: theory, practice, and applications. Inf Sci. 2019; 476:357-372.
2. Ballhausen H, Hinske LC. Federated Secure Computing. Informatics. 2023; 10(4):83
3. Goelz C, Vieluf S, Ballhausen H. A Secure Median Implementation for the Federated Secure Computing Architecture. Applied Sciences. 2024; 14(17):7891
4. Ballhausen H, Corradini S, Belka C, et al. Privacy-friendly evaluation of patient data with secure multiparty computation in a European pilot study. npj Digit Med. 2024; 7:280.