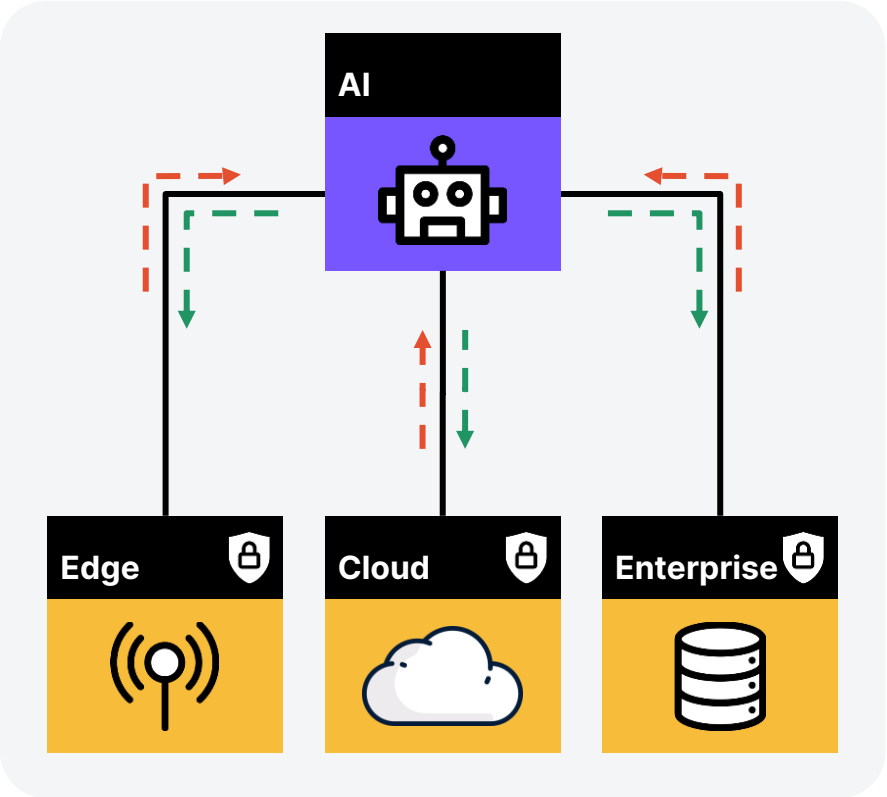
Trusted execution environments for federated learning

A Vinnova funded Project

Scaleout

Purpose

The main objective of this project is to develop a pilot implementation of TEE-empowered federated learning.



Goals

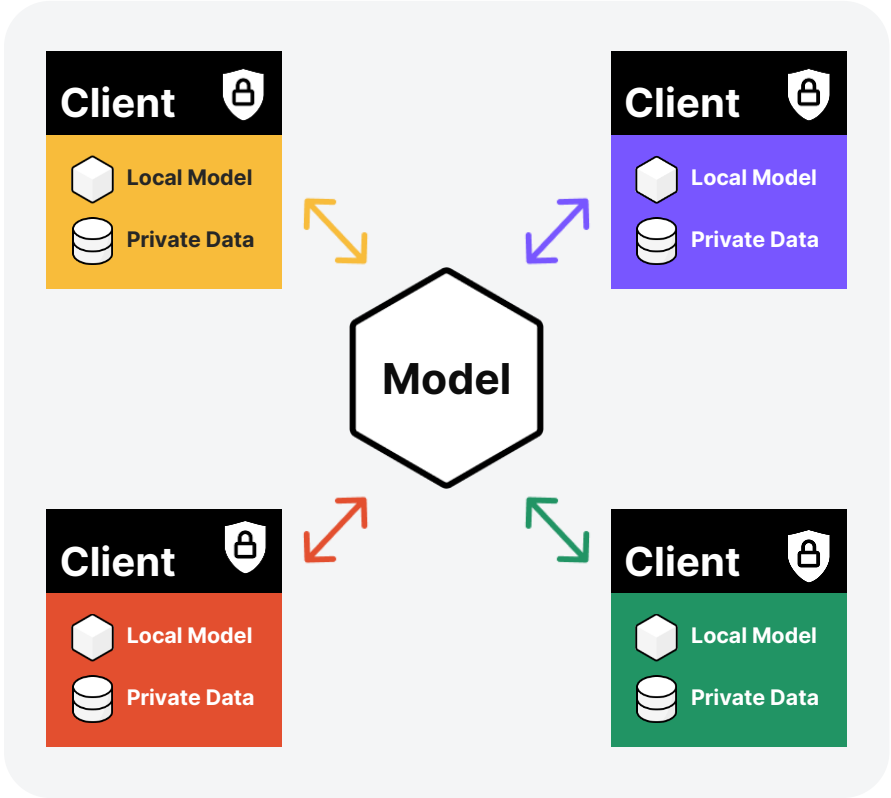
Implement and systematically evaluate secure enclave technology for federated learning

In particular, we aim to provide answers to the following specific questions

Can TEEs help verify and guarantee the **identity** of clients?

If and how can we use TEEs to ensure **veracity** of client remote execution for:

- An IoT use case (small memory footprint)
- A deep learning silo use-cases (large memory footprint)



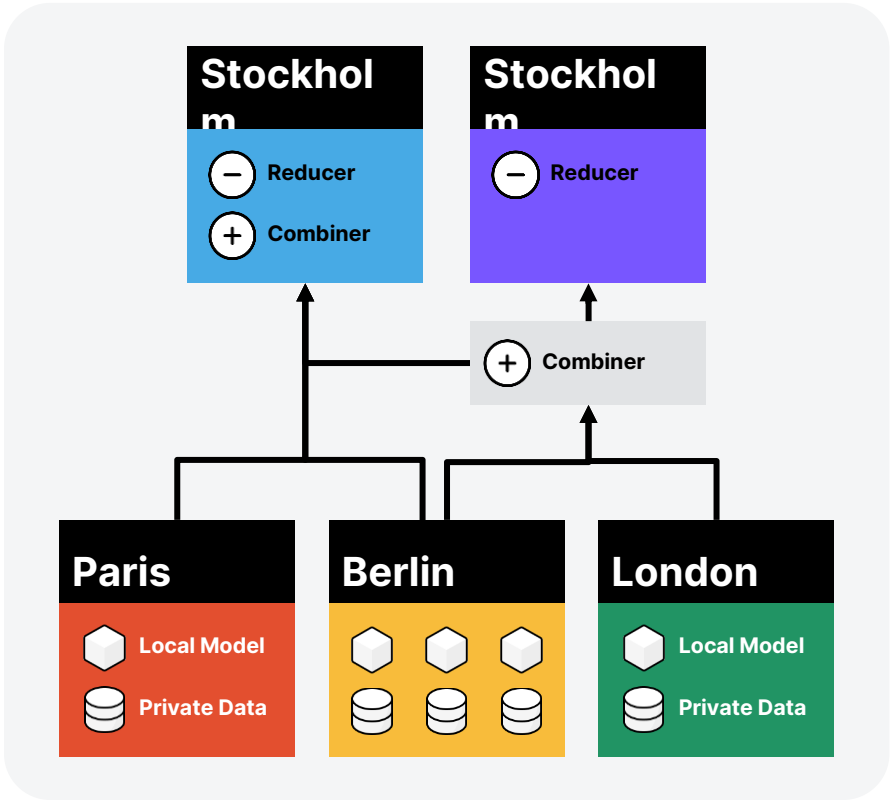
Participating parties

Scaleout Systems AB

Main project driver

Industry Reference Group

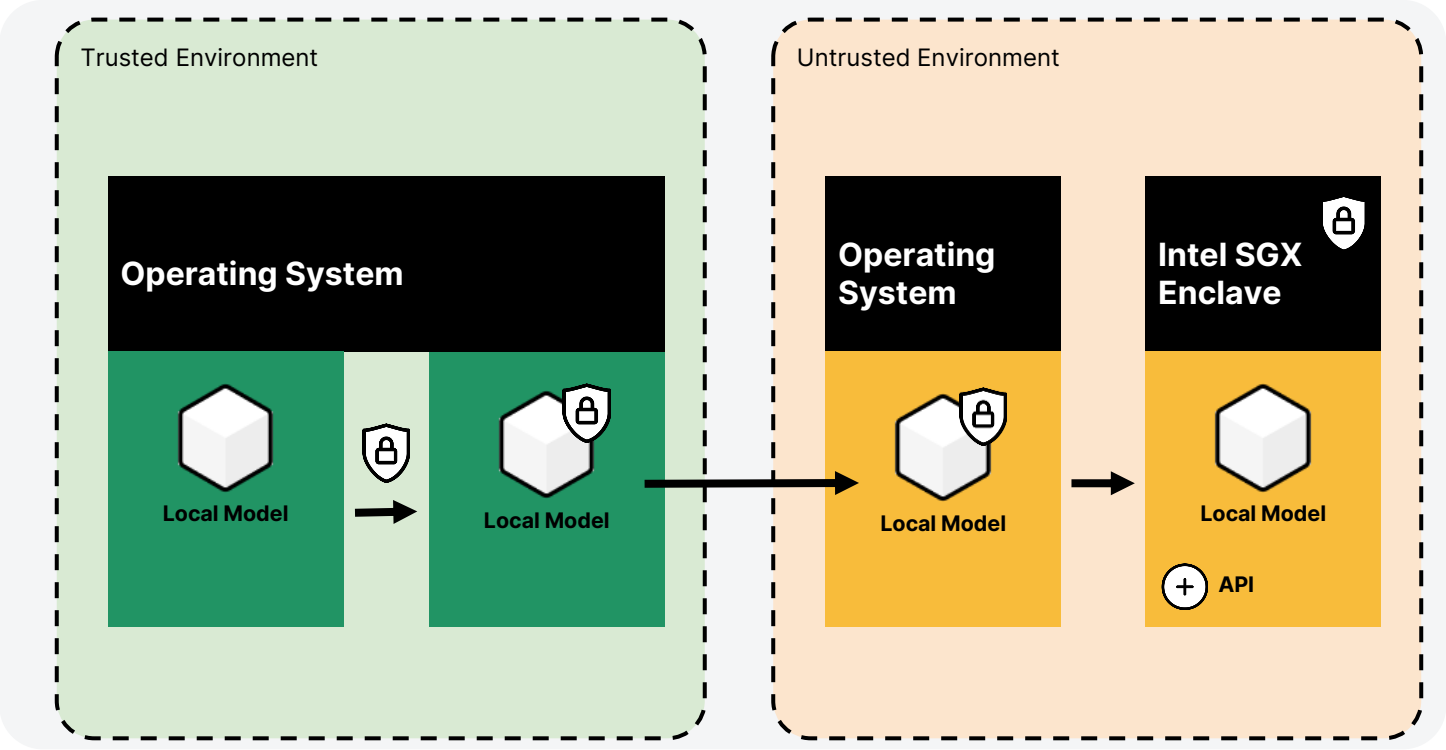
- **Javier Busto, Project Manager,**
  Product Innovation, SITA for Aircraft
- **Henrik Johansson, PhD, Senior Data Scientist,**
  Billerud
- **Andreas Johansson, PhD, Master Researcher ML**
  Ericsson



Results so far

Model Serving

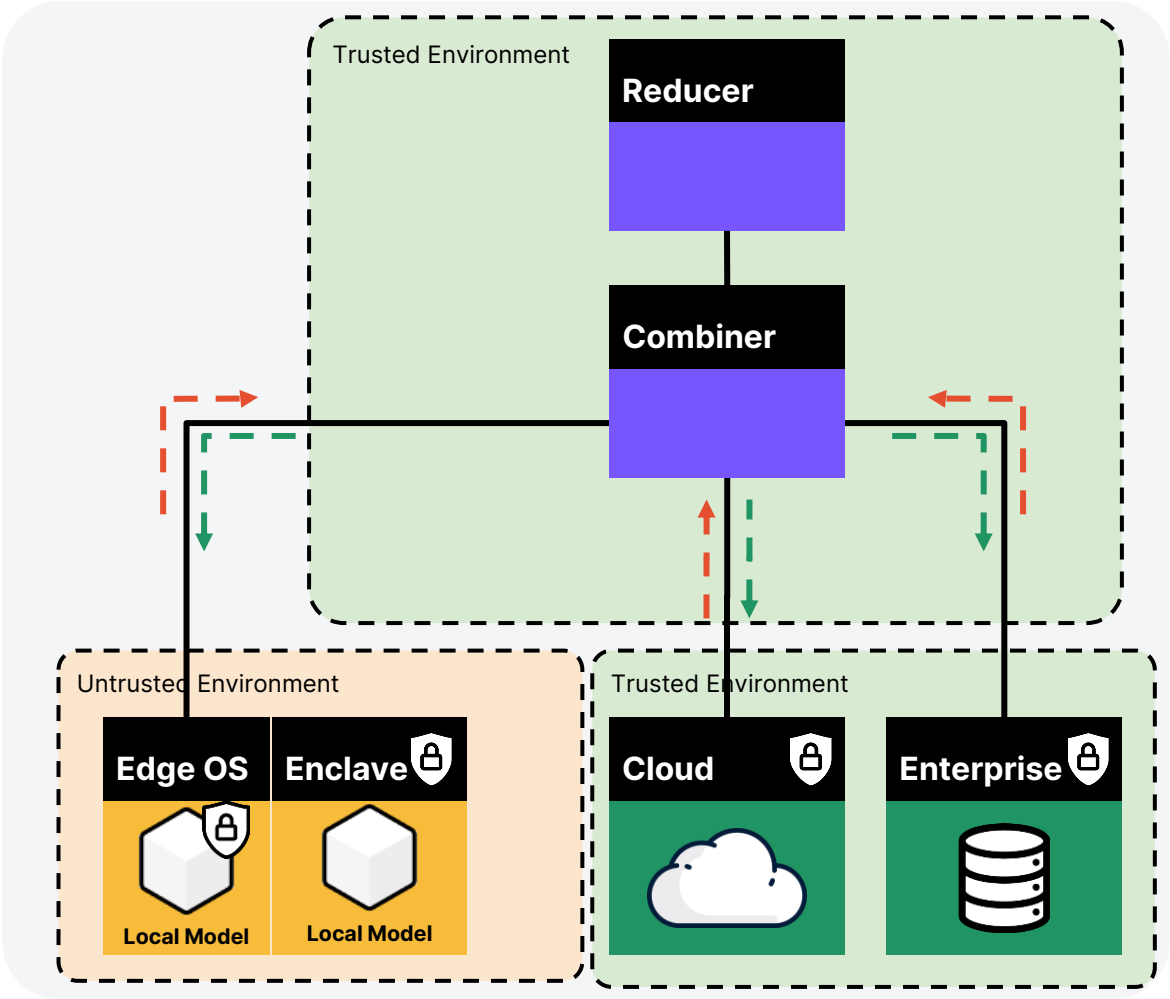
Deploying an ML model API on an untrusted cloud provider



Results so far

Confidential Compute Package

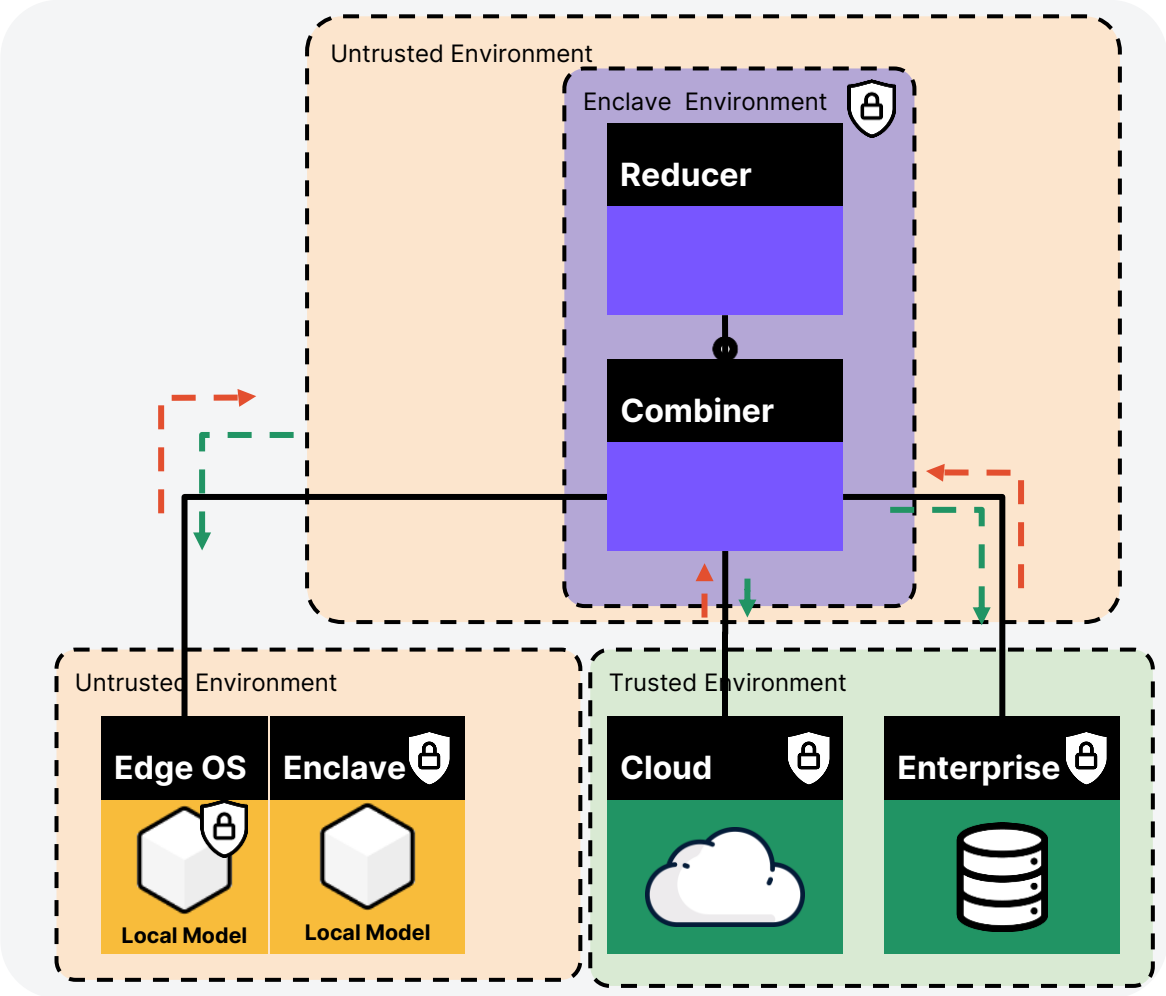
Run FEDn training with a client running on an untrusted cloud provider. Data can be encrypted and decrypted like in the previous use case.



Results so far

Confidential FEDn deployment

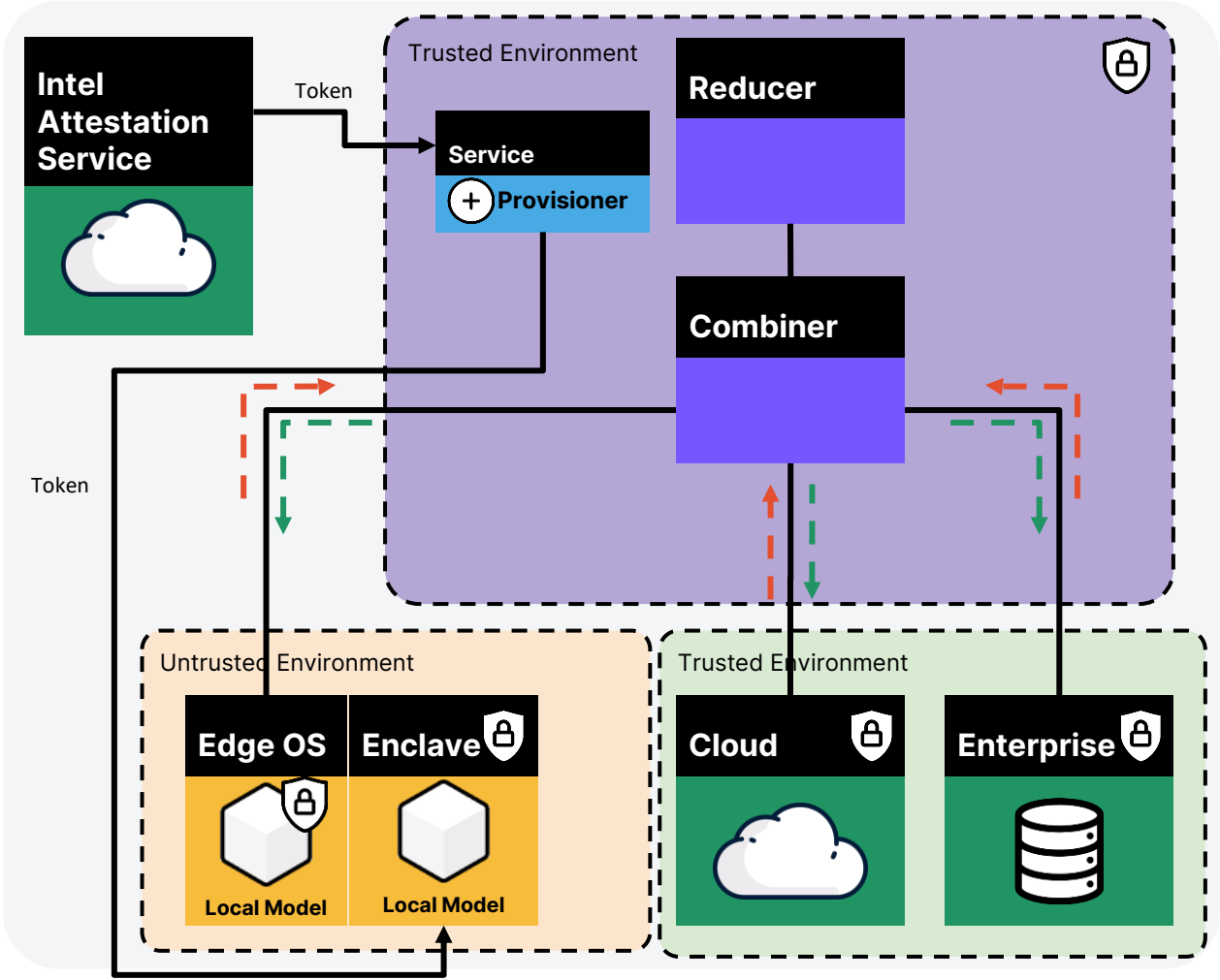
Run FEDn reducer and combiner on an untrusted environment.



Results so far

Attestation

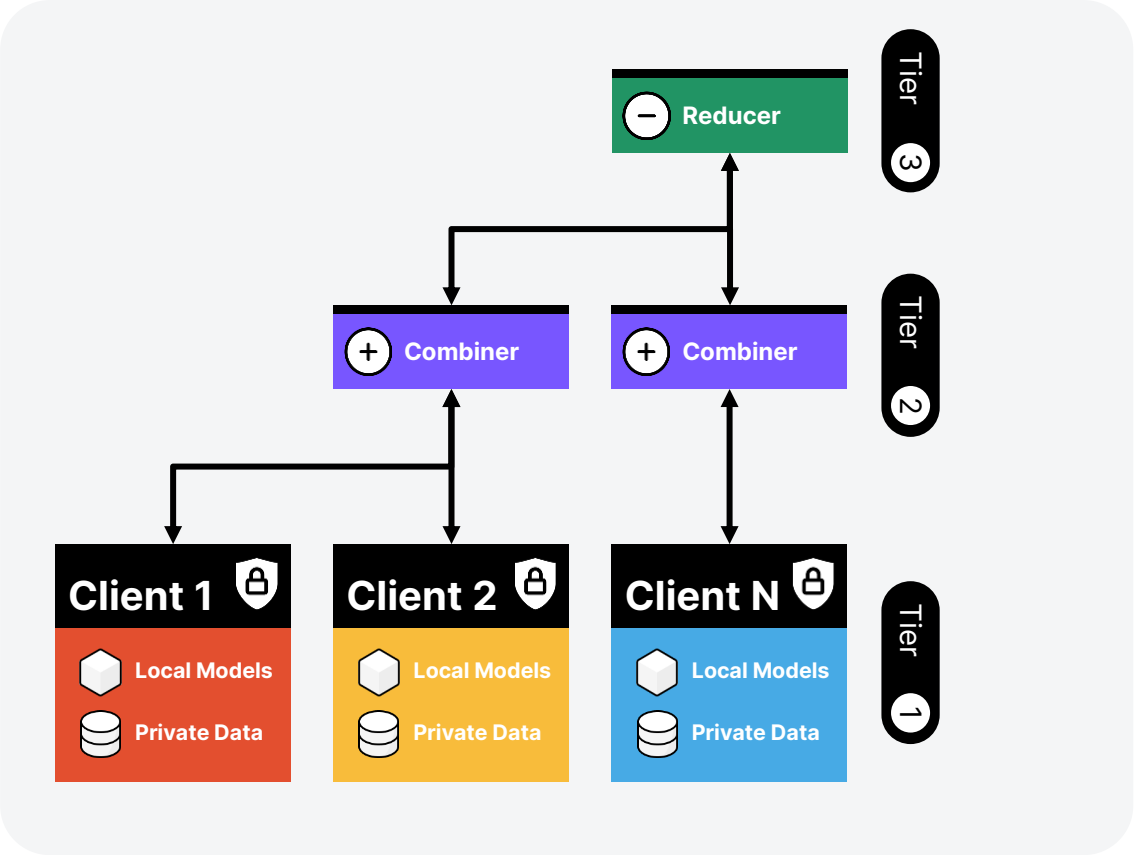
Verify that the remote client run on an up-to-date TEE with expected initial state and then provision the reducer token in the enclave.



Next steps

Evaluating, iterating on the implementing clients for execution in TEE environments.

Dissemination of results.



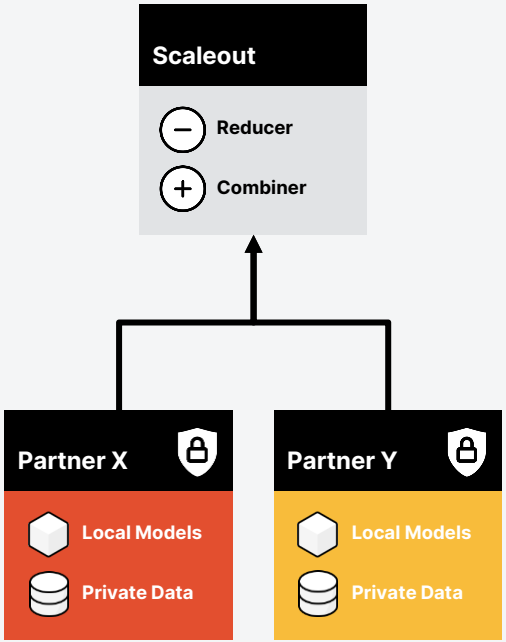
Desired collaborations

Industry applications

- Applied use cases

Hardware vendors, Cloud or IOT

- Hardware vendor collaboration
- Infrastructure provider with secure enclave capabilities



Scaleout

Trusted execution environments for federated learning

Morgan Ekmefjord

Role in Project - Project Manager

morgan@scaleoutsystems.com

+4672-22 444 64

Salman Toor

Role in Project - R&D Lead - Cloud Infra and Security

salman@scaleoutsystems.com

+4673-7031539

Andreas Hellander

Role in Project - R&D Lead - Federated Machine Learning Technologies

andreas@scaleoutsystems.com

+4670-3950447