Trusted execution environments for federated learning

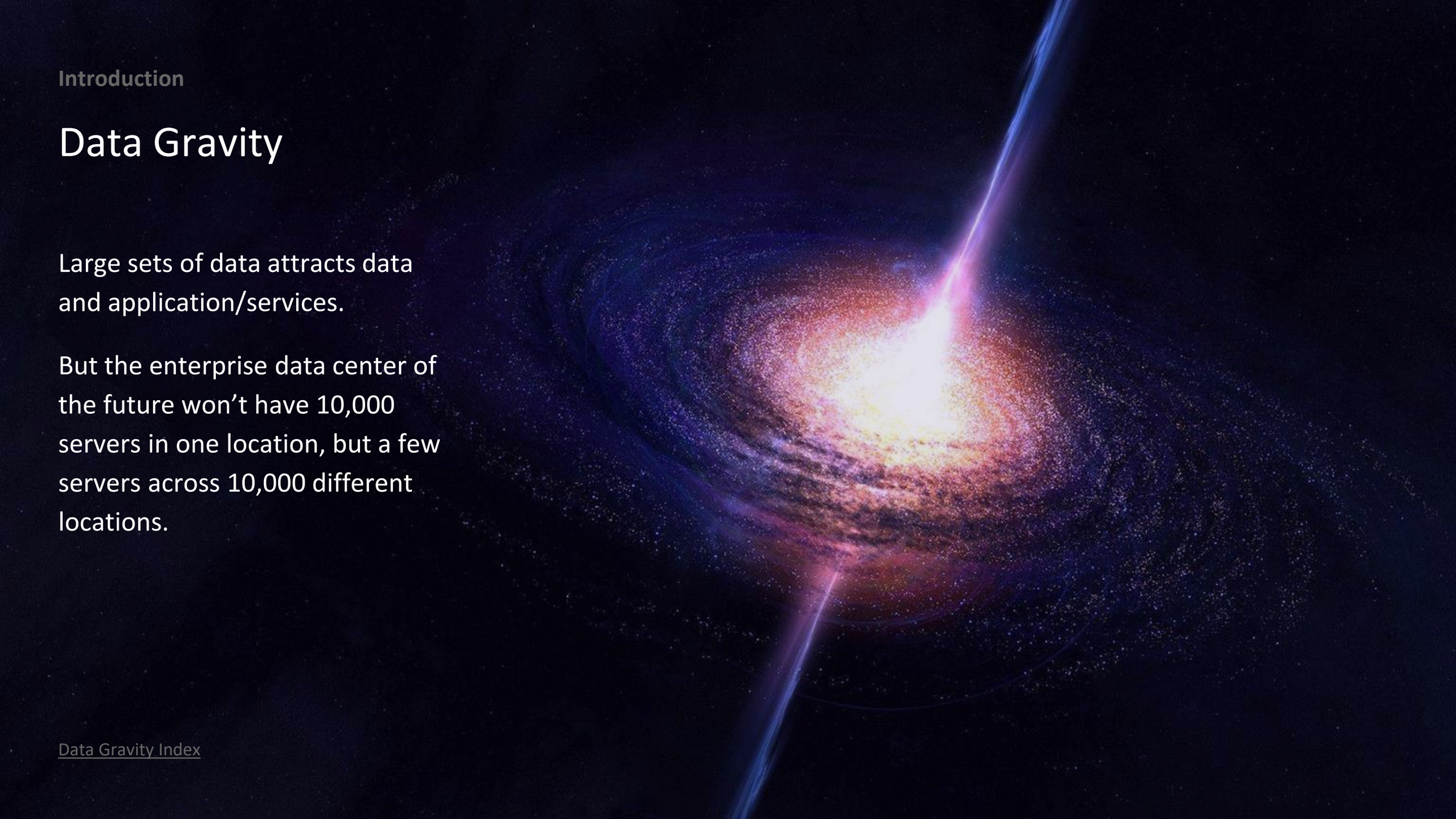
A Vinnova funded Project

Scaleout

Data Gravity

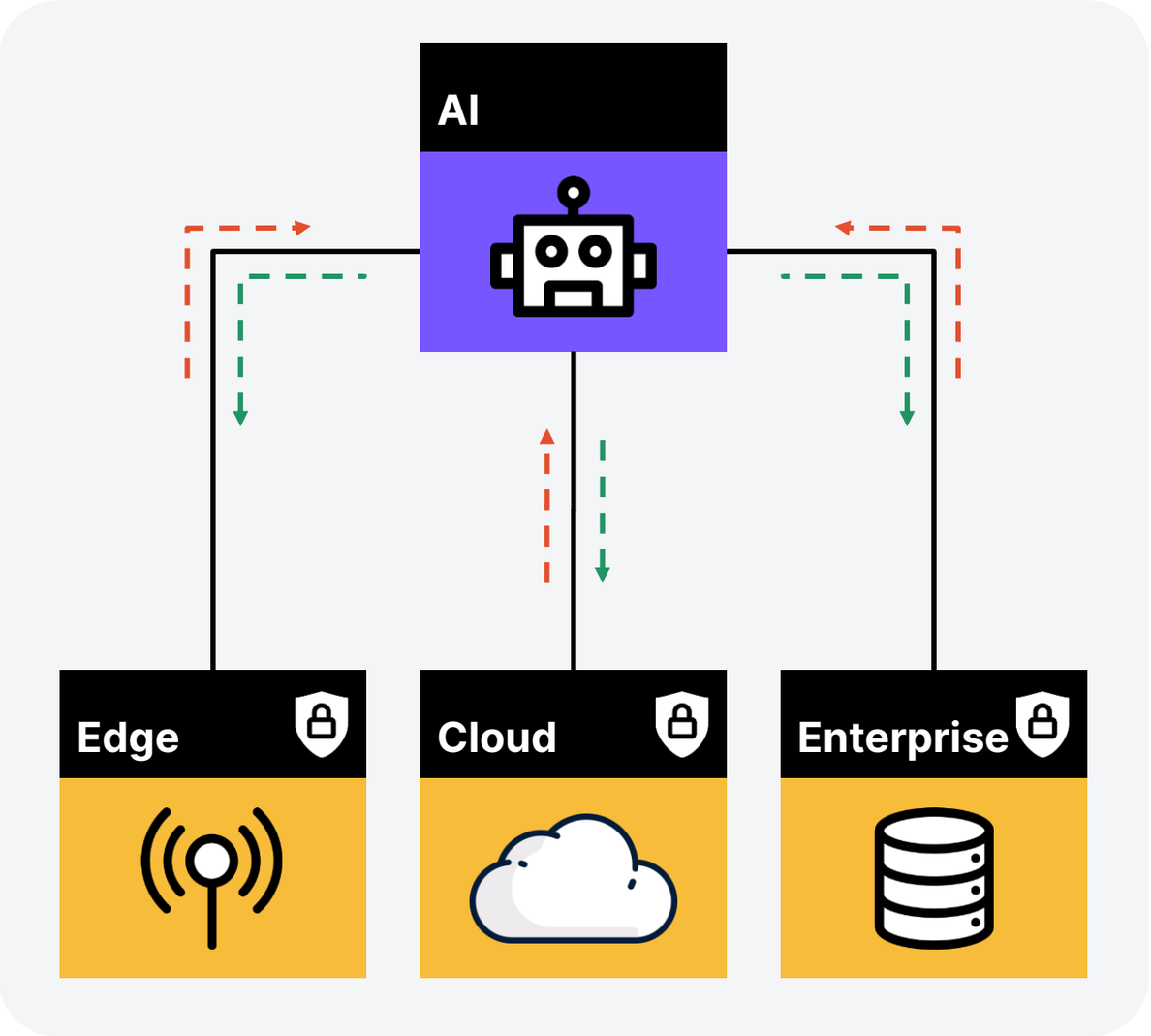
Large sets of data attracts data and application/services.

But the enterprise data center of the future won’t have 10,000 servers in one location, but a few servers across 10,000 different locations.



Purpose

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



Goals

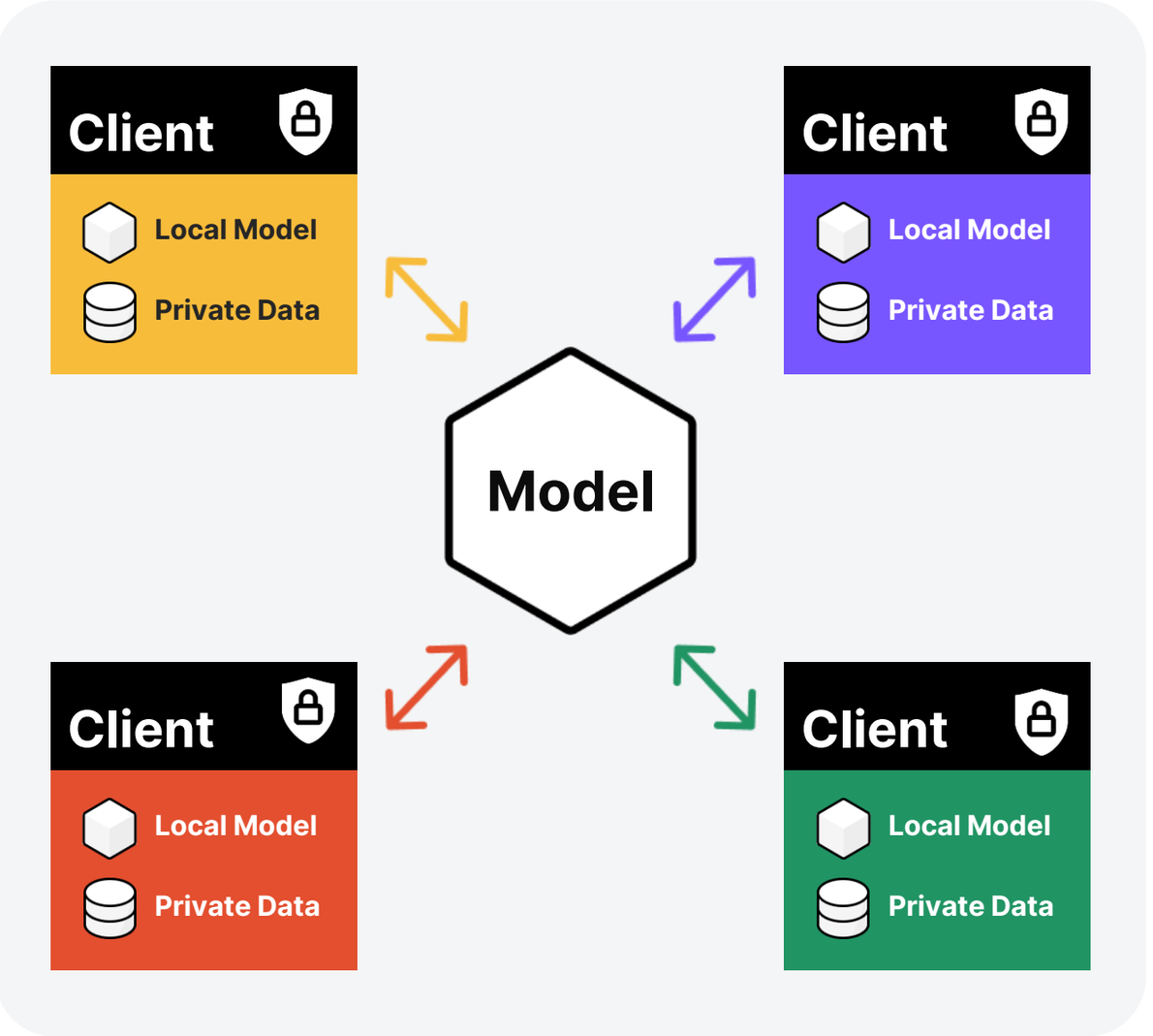
Implement and systematically evaluate secure enclave technology for federated learning

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)



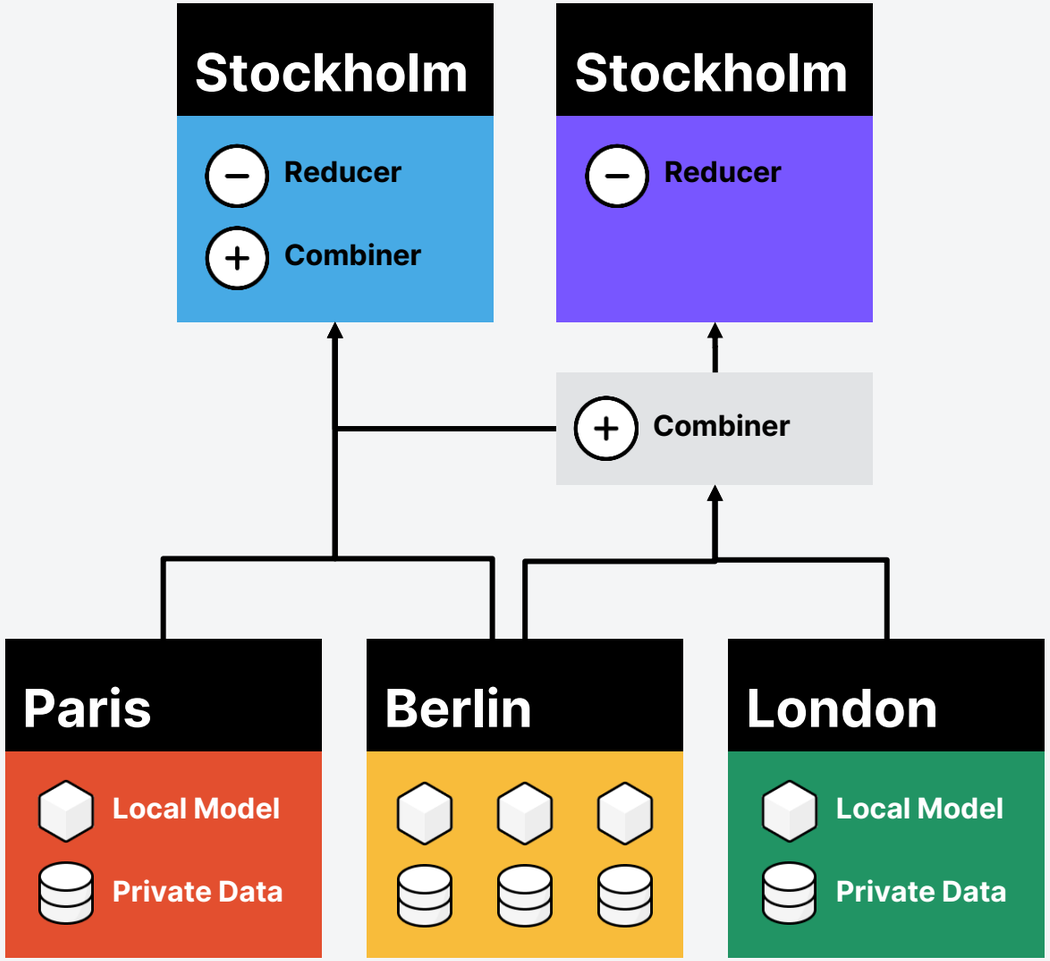
Participating parties

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

Evaluated three technical implementations

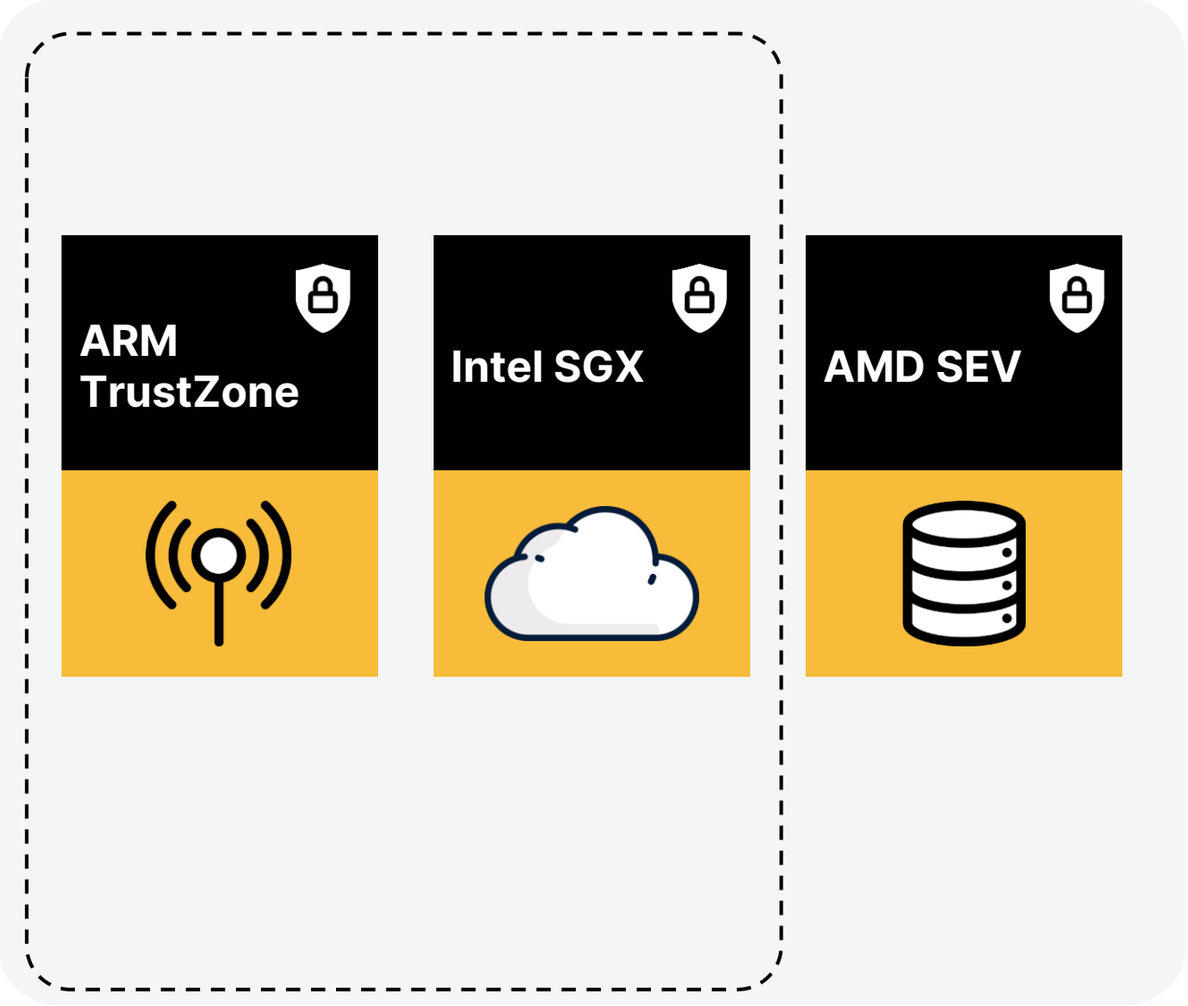
INTEL SGX, AMD SEV, ARM TrustZone

- Looked at direct interface solutions
- Looked at libraryOS solutions

Concluded that frameworks primarily targeted for this client implementation is ARM and SGX due to its

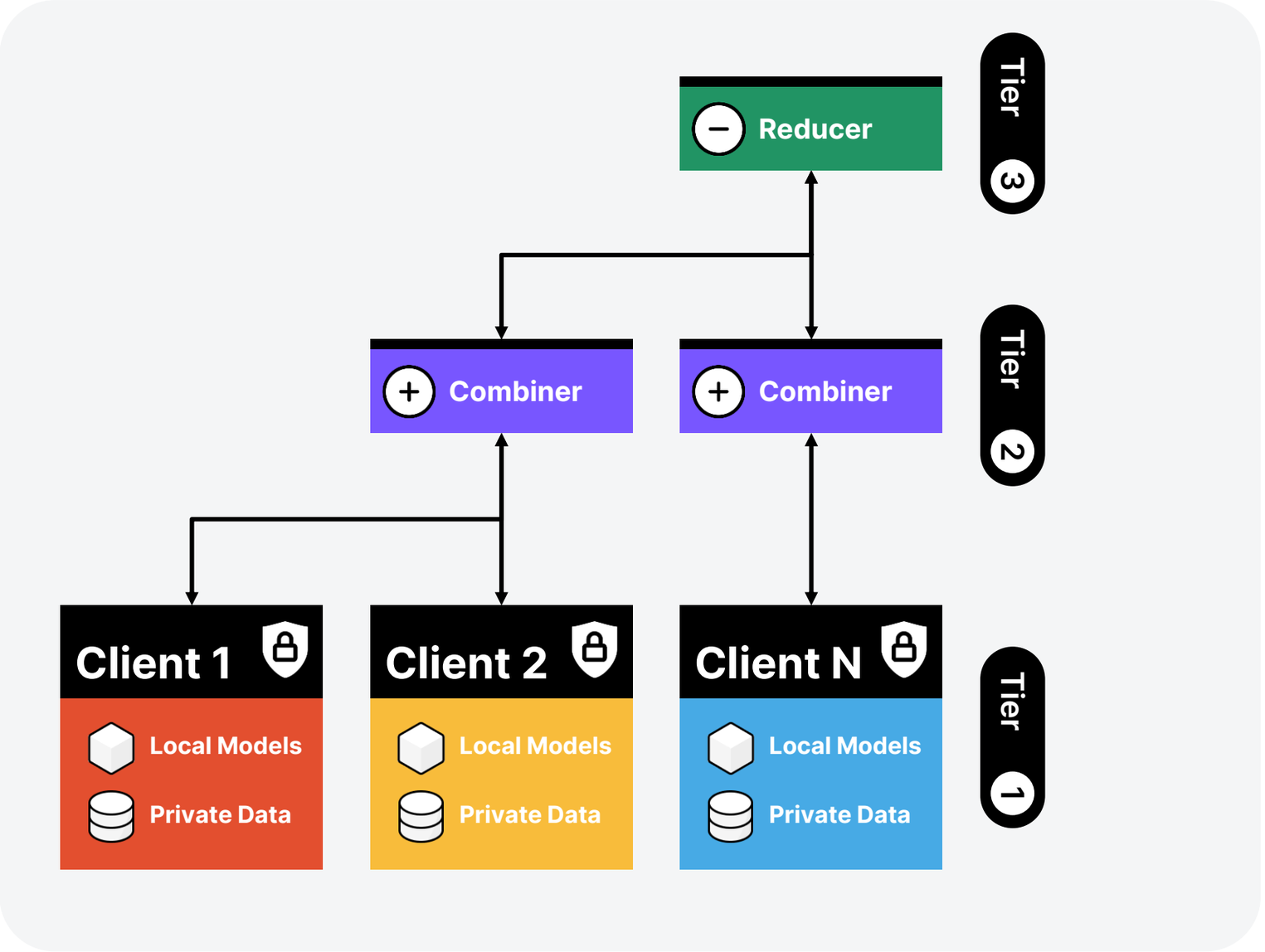
- Level of security
- Maturity
- Applicability on both silo and device

Concluded we will implement first iteration of client using microkernel-OS frameworks to target multiple HW implementations



Next steps

Implementing clients for execution in TEE environments.



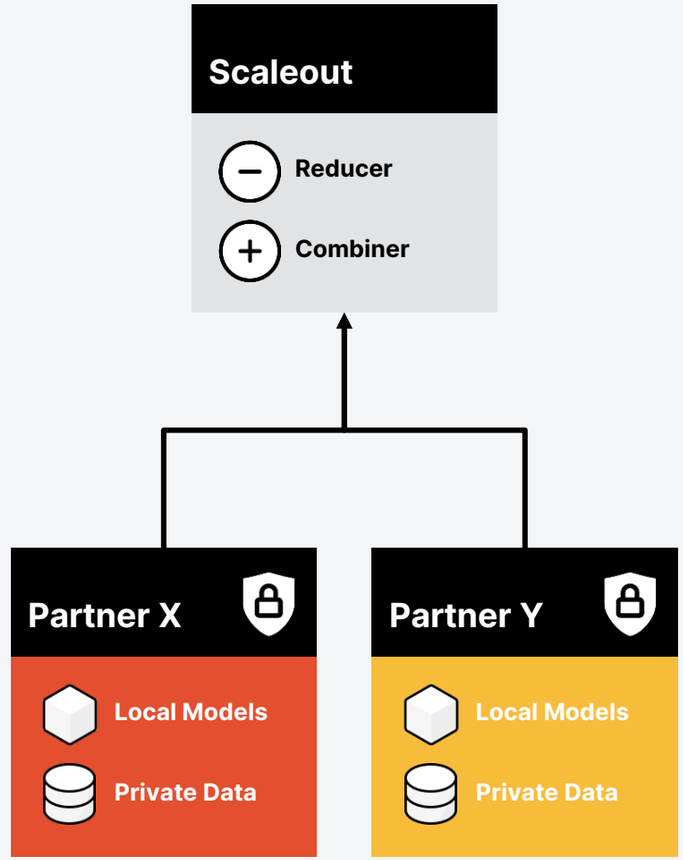
Desired collaborations

Industry applications

- Applied use cases

Hardware vendors, Cloud or IOT

- Hardware vendor collaboration
- Infrastructure provider with secure enclave capabilities



Contact persons

Morgan Ekmefjord

Role in Project - Project Manager & Tec Lead

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

Marco Cappucini

Role in Project - Machine Learning Engineer

marco@scaleoutsystems.com

+4670-65579647