SCONTAIN

# Secure Multi-Stakeholder Machine Learning using TEEs

Do Le Quoc
Huawei Munich Research Center
Email: quoc.do.le@huawei.com

# Machine Learning

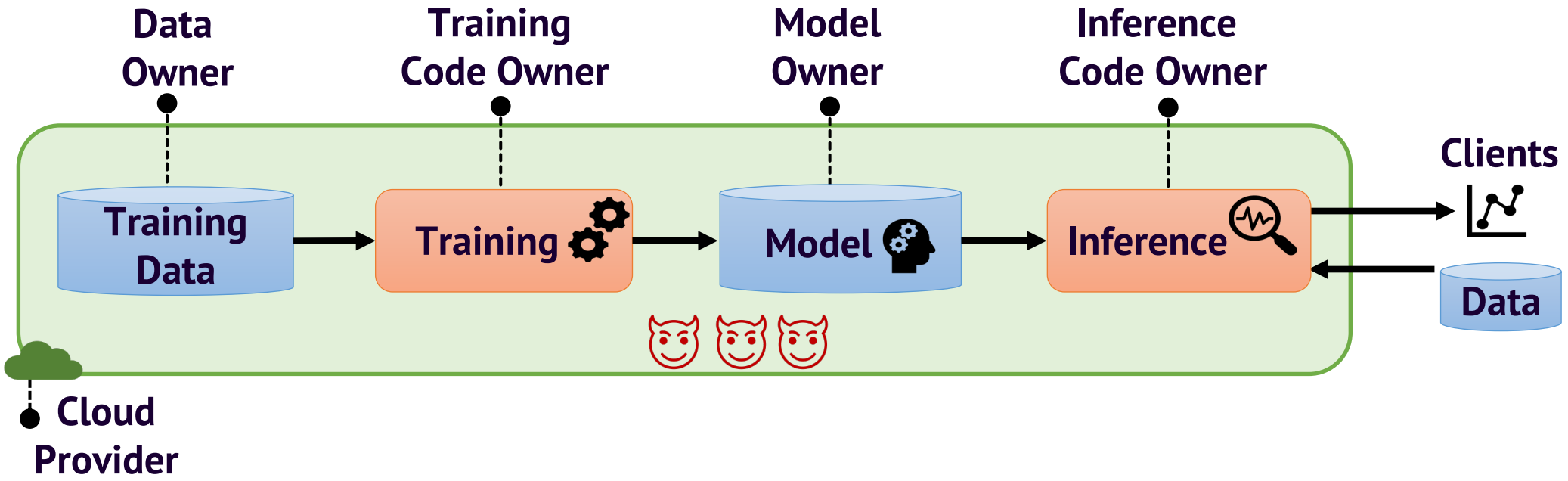

Self-driving car


Auto-translation

Face recognition payment


Medical diagnosis

# Motivation




How to enable multiple stakeholders (who do not necessarily trust each other) to still come together and perform machine learning to gain benefits of AI?

# SCONE Platform


**All data is always encrypted** - i.e., protecting all **Personally Identifiable Information** required by any privacy legislation world-wide

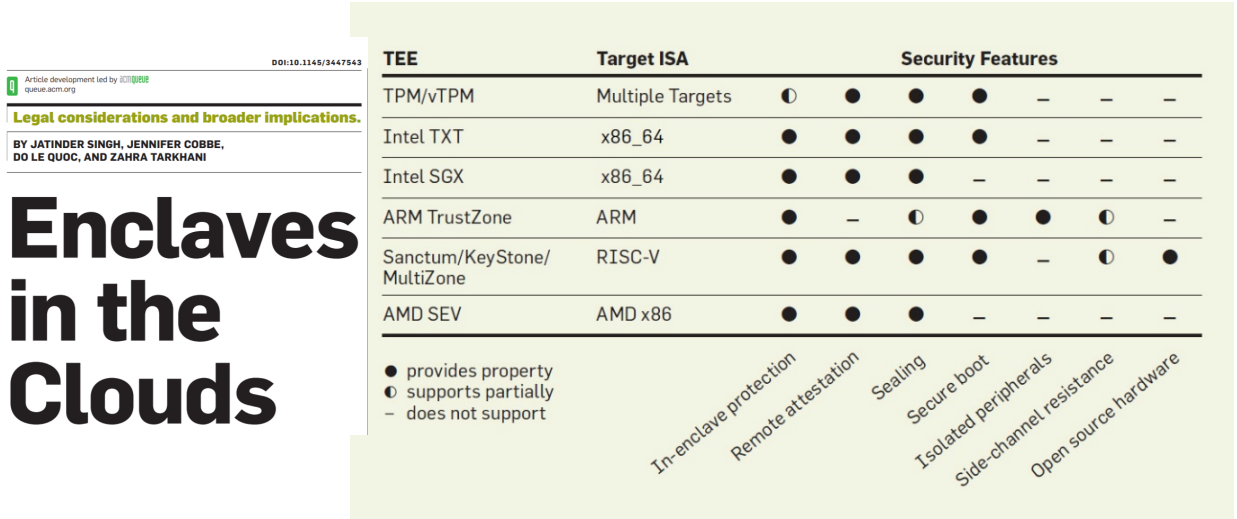
**Data**, **code** and **secrets** are only visible to **attested** and **authorized** services - improving protection and limiting the scope of security assessments

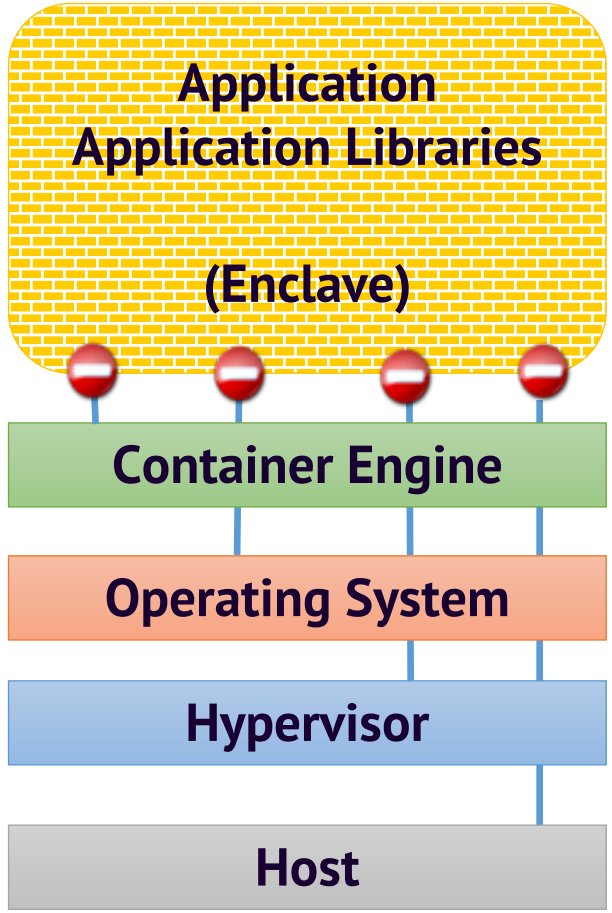
Protection against **insider attacks** - even those with root access can only see encrypted data & code & secrets

# Intel SGX

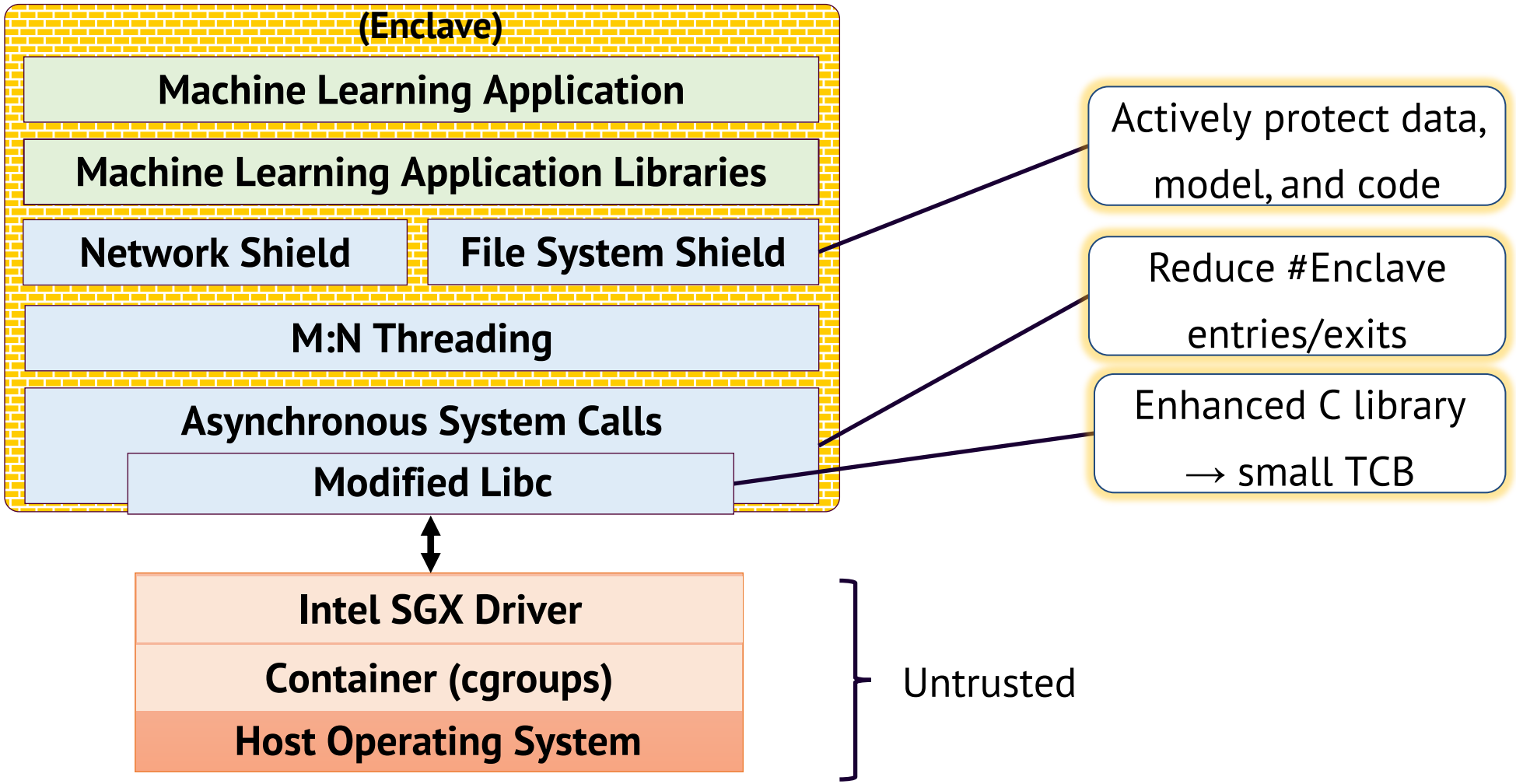
SGX (Software Guard eXtensions) is a set of processor extensions for establishing a TEE inside an application

Intel SGX protects the integrity and confidentiality of applications



# SCONE Architecture



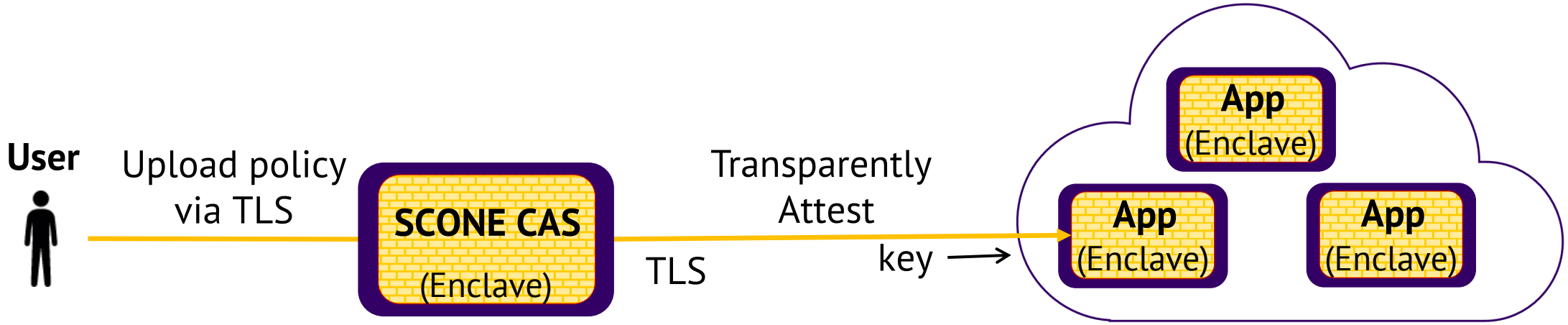
# Remote Attestation & Key Management

**TRANSPARENT ATTESTATION OF PROGRAMS**

**CONFIGURATION WITH SECRETS**

**SECRETS SHARING WITHOUT REVEALING BETWEEN COMPUTATIONS**

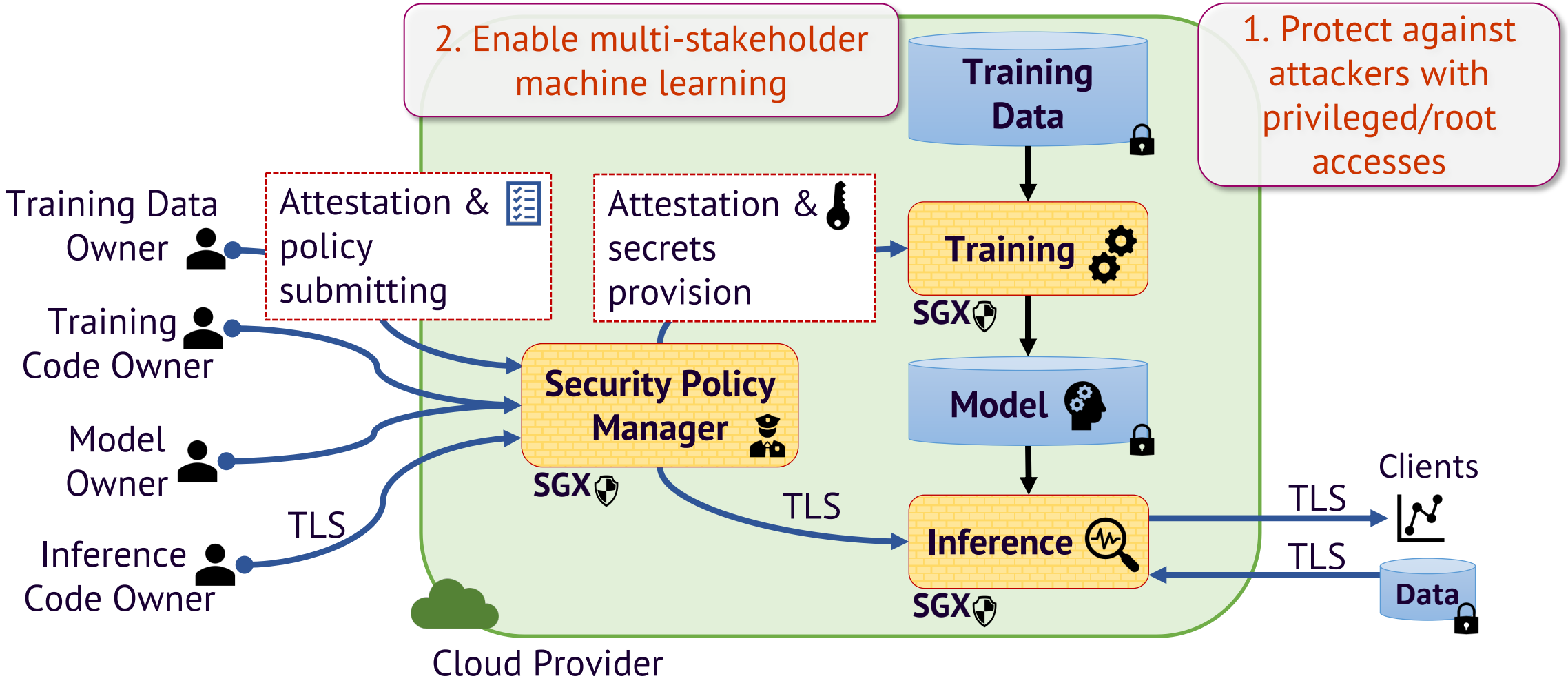
# Remote Attestation & Key Management



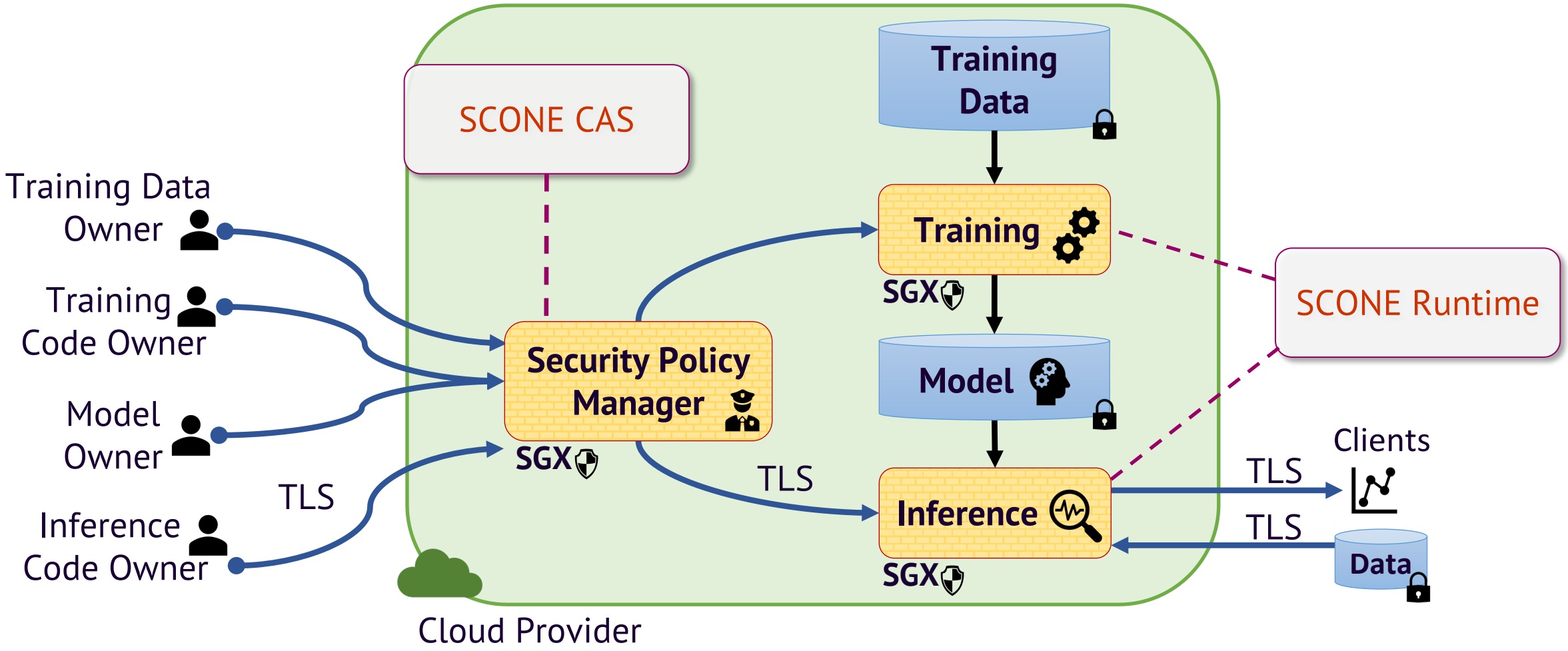

Trust Management as a Service:
Enabling Trusted Execution in the Face of Byzantine Stakeholders

Franz Gregor*, Wojciech Ozga*, Sébastien Vaucher†, Rafael Pires†, Do Le Quoc*, Sergei Arnautov‡,
André Martin*, Valerio Schiavoni†, Pascal Felber†, Christof Fetzer*
TU Dresden, Germany* — Université de Neuchâtel, Switzerland† — Scontain UG, Germany‡

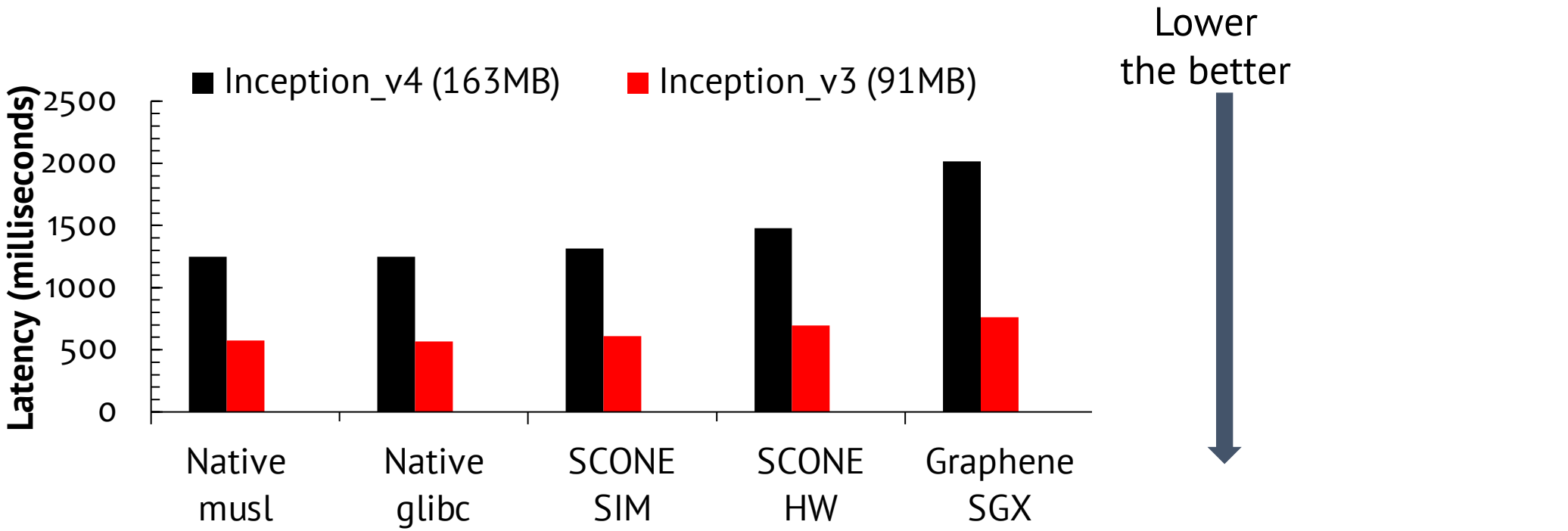
# Secure Multi-Stakeholder Machine Learning



# Secure Multi-Stakeholder Machine Learning



# Evaluation




**SECURETF: A Secure TensorFlow Framework**

Do Le Quoc, Franz Gregor, Sergei Arnautov
TU Dresden, Scontain UG

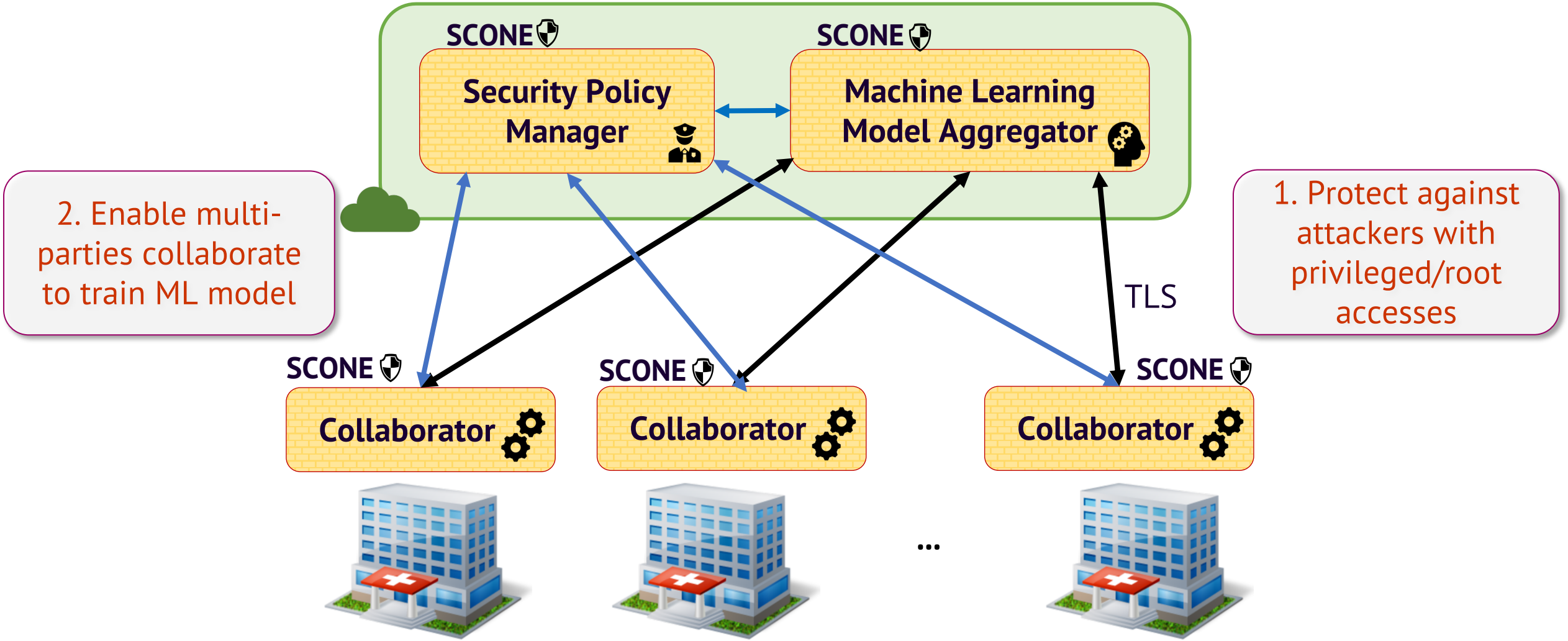
Roland Kunkel
TU Dresden

Pramod Bhatotia
TU Munich

Christof Fetzer
TU Dresden, Scontain UG

**SCONE** based system:
incurs ~5% in **SIM mode**, ~22% overhead in **HW mode** compared to **native versions**
~1.1X – 1.4X faster than **Graphene-SGX** based system

# Secure Federated Learning Architecture



# Demos

- Secure multi-stakeholder machine learning using SCONE: https://youtu.be/K3DtUdYXd7Y?t=1181
- Secure federated learning using SCONE: https://youtu.be/J3tQcjrX3Jk

# SCONTAIN

Products
https://sconedocs.github.io
https://scontain.com

Contact
info@scontain.com