

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

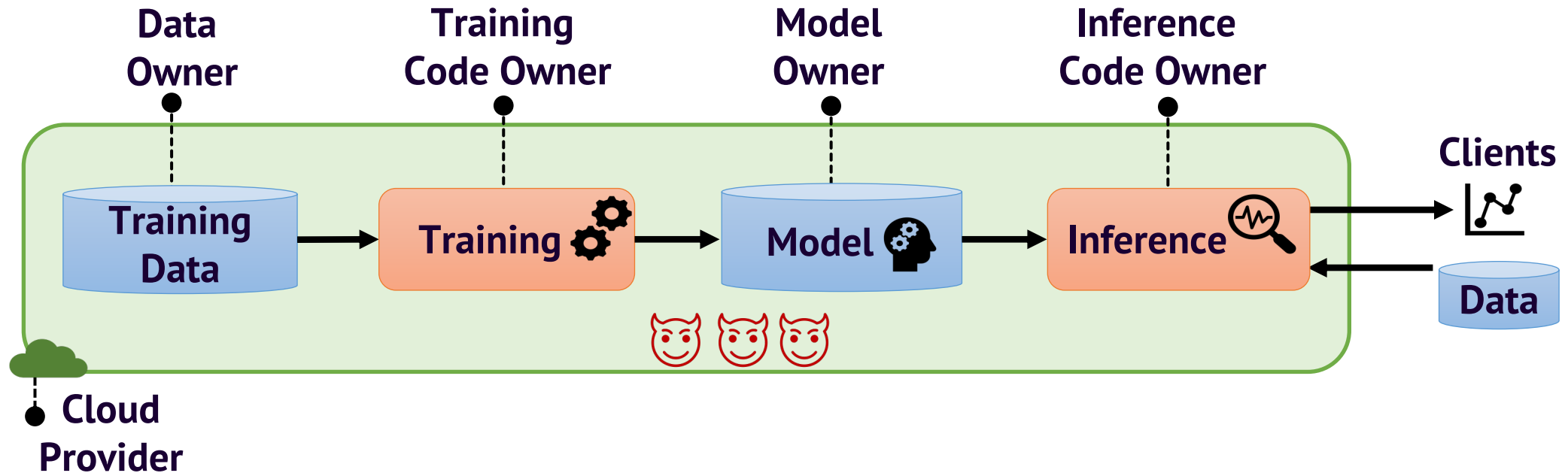


Face recognition payment



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

Article development led by [SRIJIT](#)
Legal considerations and broader implications.
BY JATINDER SINGH, JENNIFER COBBE,
DO LE QUOC, AND ZAHRA TARKHANI

Enclaves in the Clouds

TEE	Target ISA	Security Features							
TPM/vTPM	Multiple Targets	●	●	●	●	–	–	–	–
Intel TXT	x86_64	●	●	●	●	–	–	–	–
Intel SGX	x86_64	●	●	●	–	–	–	–	–
ARM TrustZone	ARM	●	–	●	●	●	●	–	–
Sanctum/KeyStone/MultiZone	RISC-V	●	●	●	●	–	●	●	–
AMD SEV	AMD x86	●	●	●	–	–	–	–	–

● provides property

● supports partially

– does not support

In-enclave protection

Remote attestation

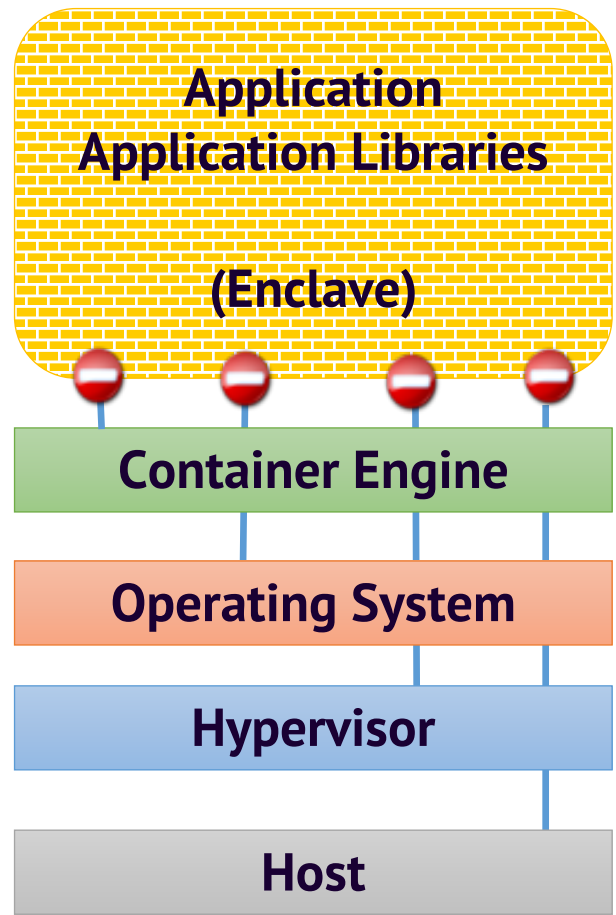
Sealing

Secure boot

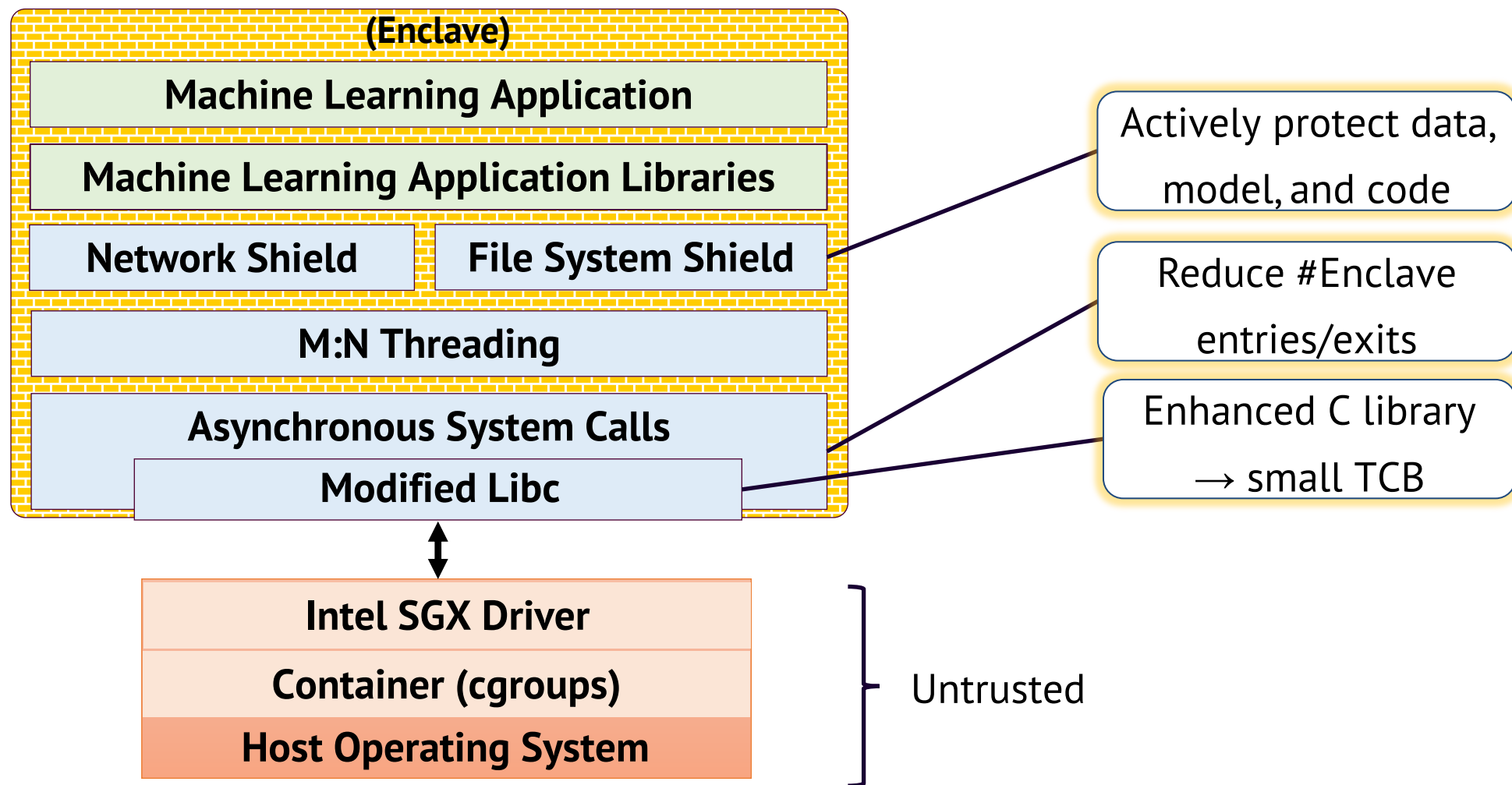
Isolated peripherals

Side-channel resistance

Open source hardware



SCONE Architecture



Remote Attestation & Key Management



**TRANSPARENT
ATTESTATION OF
PROGRAMS**

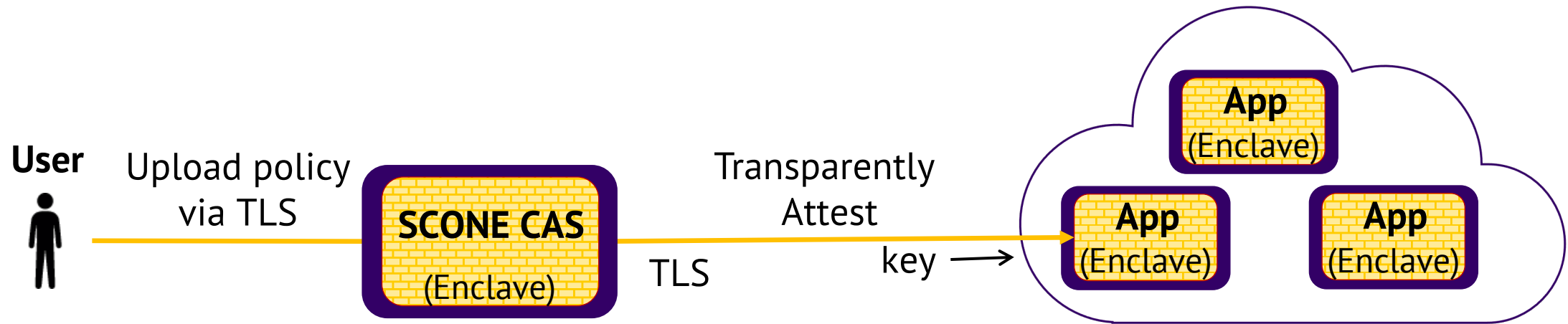


**CONFIGURATION WITH
SECRETS**



**SECRETS SHARING
WITHOUT REVEALING
BETWEEN COMPUTATIONS**

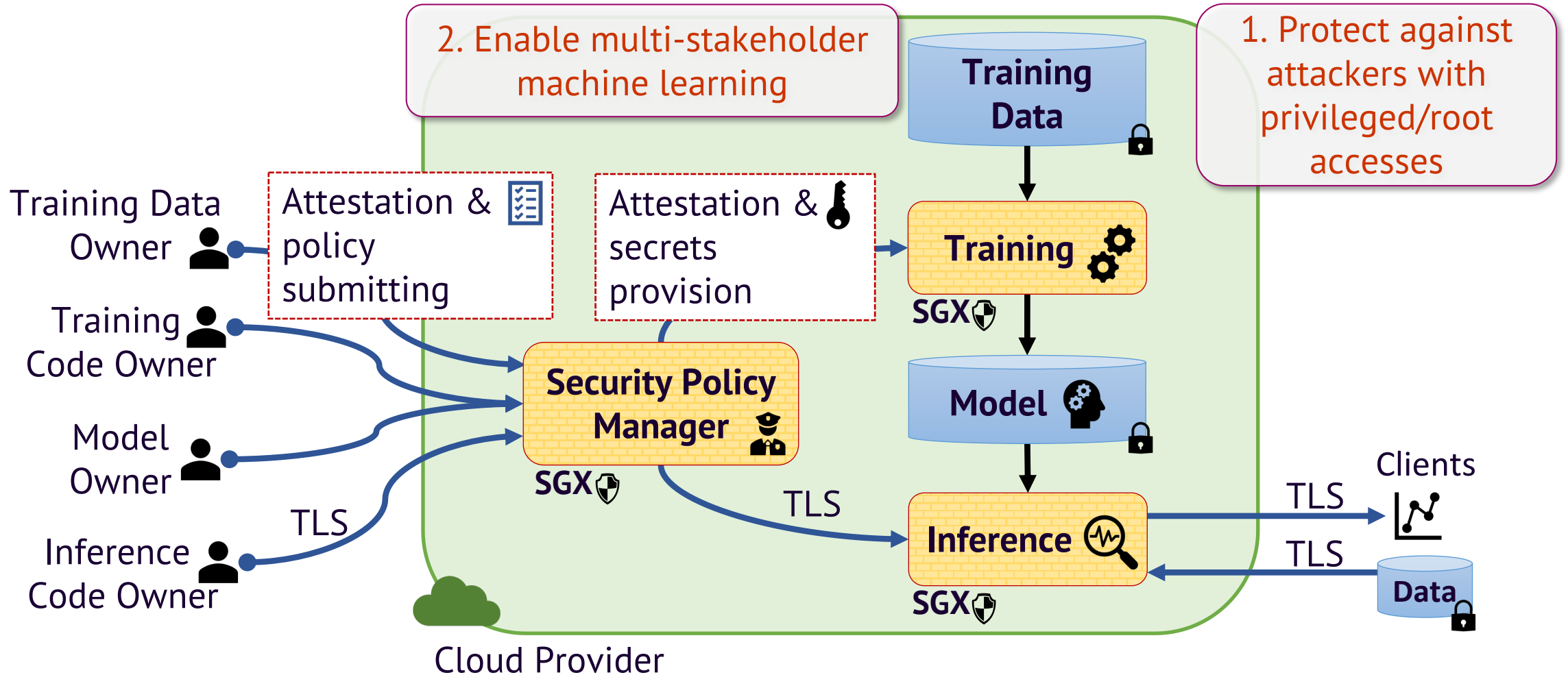
Remote Attestation & Key Management



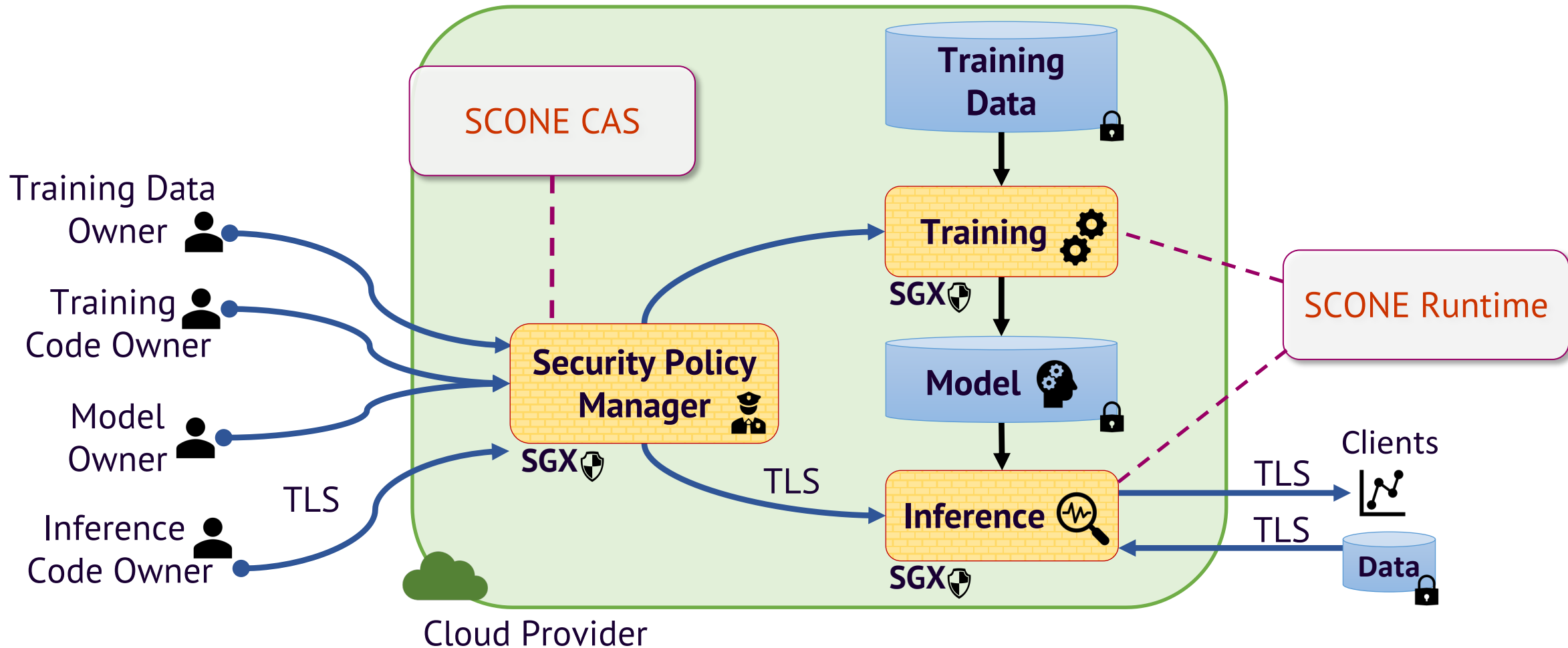
Trust Management as a Service:
Enabling Trusted Execution in the Face of Byzantine Stakeholders

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[‡]

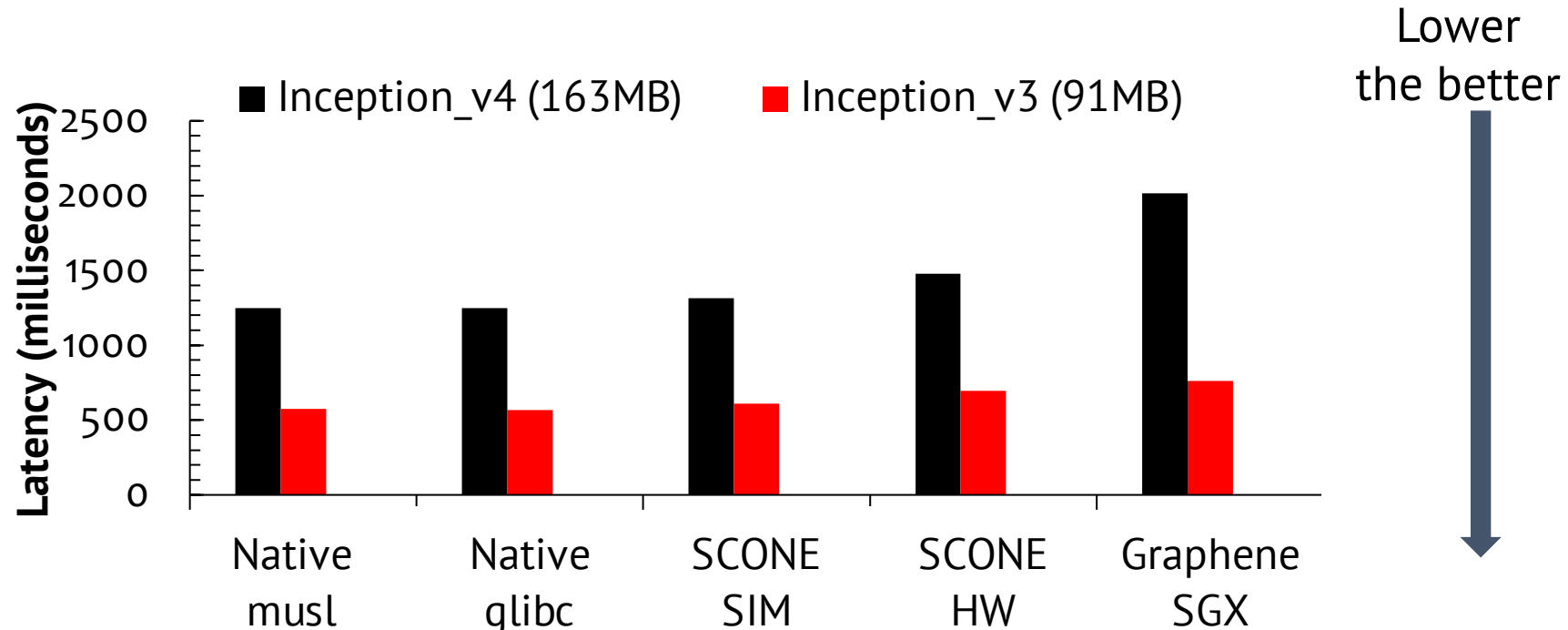
Secure Multi-Stakeholder Machine Learning



Secure Multi-Stakeholder Machine Learning



Evaluation



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

SECURETF: A Secure TensorFlow Framework

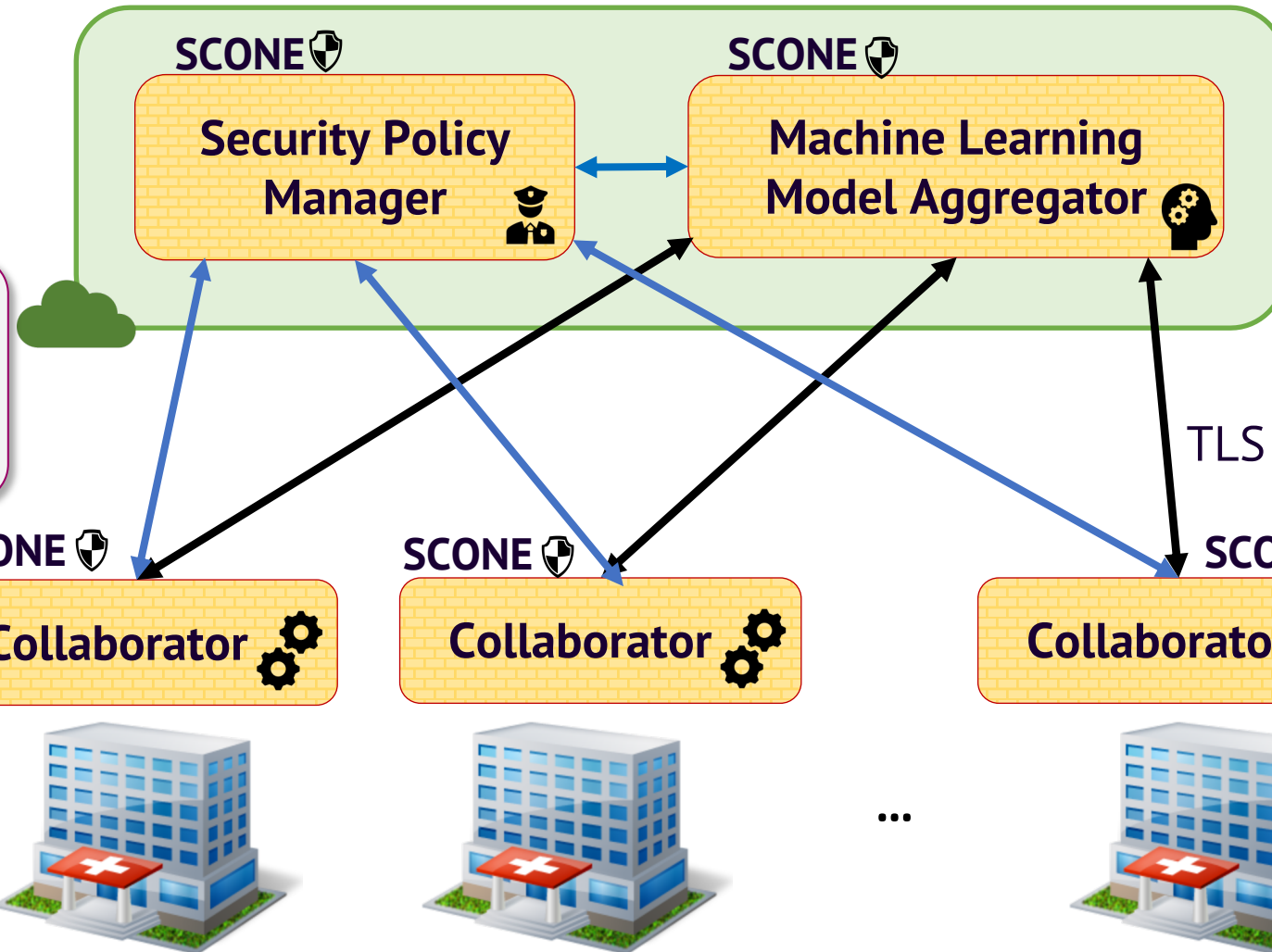
Do Le Quoc, Franz Gregor, Sergei Arnautov
TU Dresden, Scontain UG

Pramod Bhatotia
TU Munich

Roland Kunkel
TU Dresden

Christof Fetzner
TU Dresden, Scontain UG

Secure Federated Learning Architecture



2. Enable multi-parties collaborate to train ML model

1. Protect against attackers with privileged/root accesses

Demos

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



Products

<https://sconedocs.github.io>

<https://scontain.com>

Contact

info@scontain.com

