Discussion on Scalable AP-TEE for RISC-V

Ravi Sahita
11-23-2021
Trusted Computing SIG meeting

Outline (initial discussion)

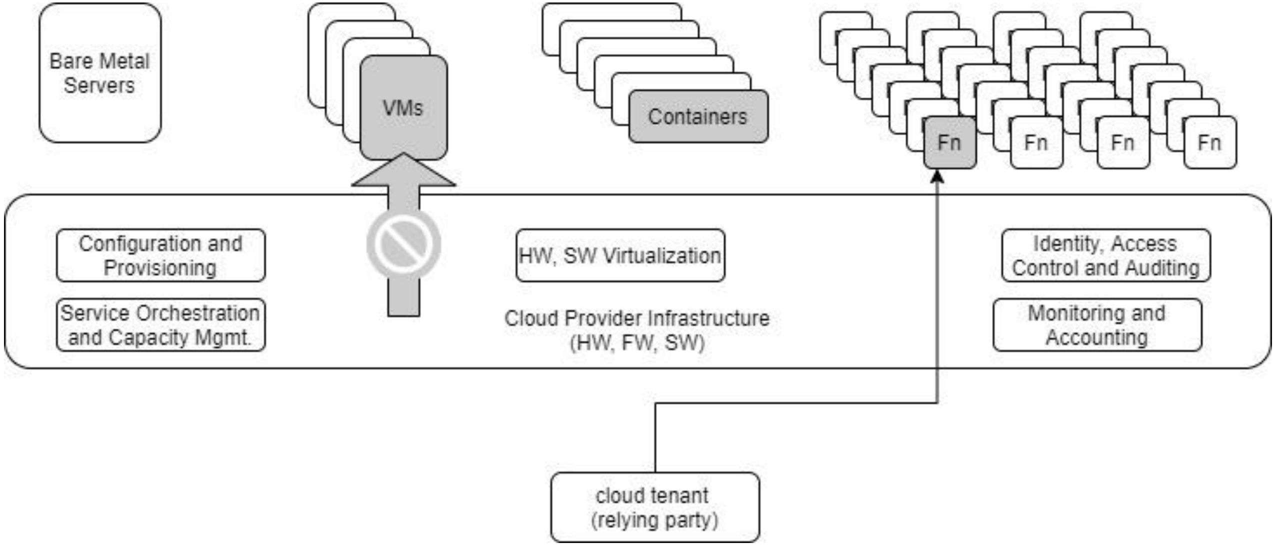
- **What is a TEE?**
- **What use cases do TEEs enable - what threats do they address?**
  - **Hosted cloud (multi-tenancy, operators)**
  - **Edge platform (untrusted physical environment)**
  - **Multi-party compute (privacy-oriented use cases)**
  - **Client platforms (IP-protection, remote workers)**
- **Security requirements of a TEE (vis-a-vis the above use cases)**
- **Other approaches (Commercial)**
- **Related**
  - **Hetero/Accelerator compute**
  - **Attestation Standards**

Trusted Execution Environment

A TEE enables isolated workloads on an application processor (or accelerator), where a hardware-attestable trusted computing base (TCB) enforces confidentiality and integrity of assets loaded within the trusted execution environment.

Use Cases

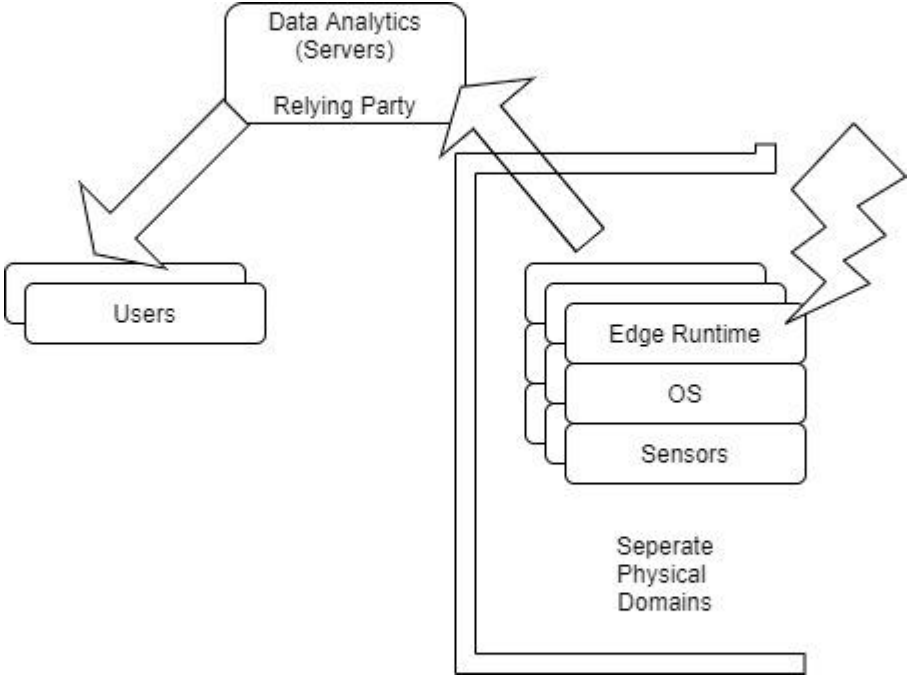
Multi-tenant hosted cloud environment


Bare Metal Servers
VMs
Containers
Fn
Fn
Fn
Fn
Configuration and Provisioning
Service Orchestration and Capacity Mgmt.
HW, SW Virtualization
Cloud Provider Infrastructure (HW, FW, SW)
Identity, Access Control and Auditing
Monitoring and Accounting
cloud tenant (relying party)

Unauthorized entities may include anyone with physical access to the hardware, including system administrators, the infrastructure owner, cloud service providers, the host firmware, operating system and hypervisor, other applications and devices on the host.

Use Cases

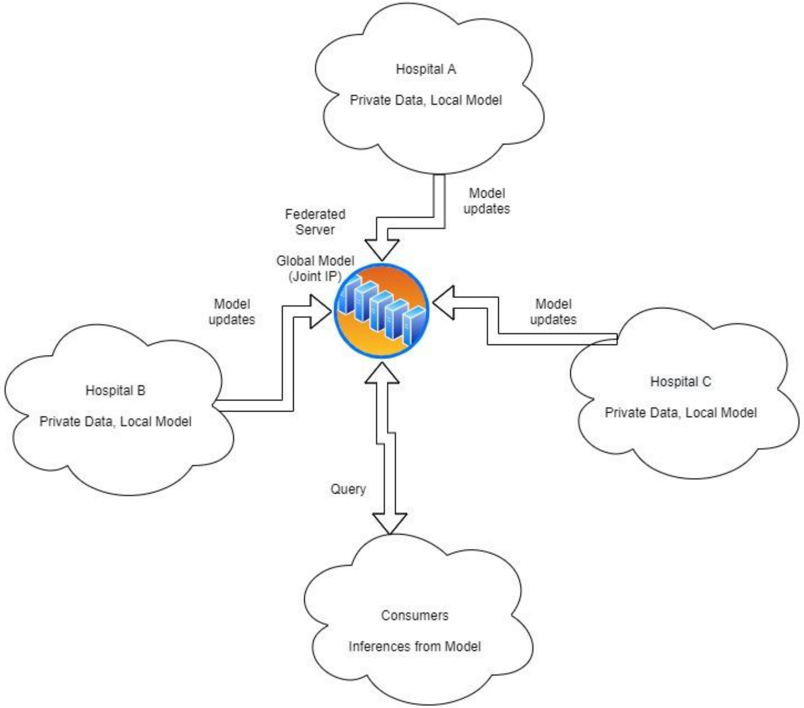
Edge cloud, IOT-based data analytics require TEE to preserve data integrity



Edge cloud and (IoT) devices are generally deemed to be under constant threat of malicious physical access.

Use Cases

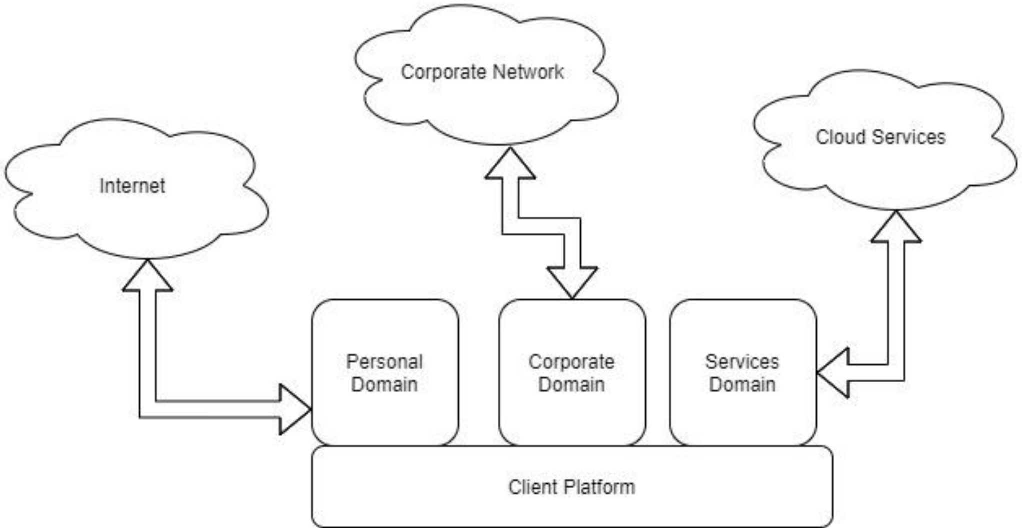
Multi-party computation on CPU/Accelerators



Multiple entities aggregating their proprietary privacy-sensitive data and collaboratively analyzing it to gain new insights (also privacy-sensitive)

Use Cases

Client Platforms



Personal computing devices used to separate personal/corporate roles (trust domains);

Analyze data and build models on the device to reduce the need for off-device processing

Security Requirements (high-level)

- Isolation
- Confidentiality
- Integrity
- Authentication
- Non-circumvention
- HW-rooted TCB
    - Attestation
    - Recovery
    - Updates
- No DoS from tenants

Non-security requirements - DoS from platform host, Availability → These are RAS/functional goals

Opens/Notes/Feedback from 11-23-2021 RVI discussion

- We should provide security targets in terms of common criteria protection profiles
- Add/expand on the multi-domain use case 4 to describe mixed-criticality domains (automotive for e.g.)
- Describe function isolation (storage, networking etc) in the multi-tenant use case
- Add non-circumvention to the high level security requirements (done)
- Clarify that availability is a functional requirement for RAS, QoS - not a security requirement