A Survey on Security Concerns and Their Actual Solutions for using FPGAs in Cloud Computing

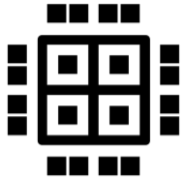
Paul D. Rosero Montalvo

IT University of Copenhagen





Agenda:



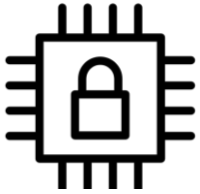
Overview about FPGAs



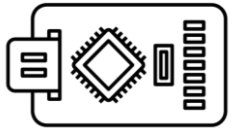
Security concerns



Security features



Trusted execution environments (TEE)



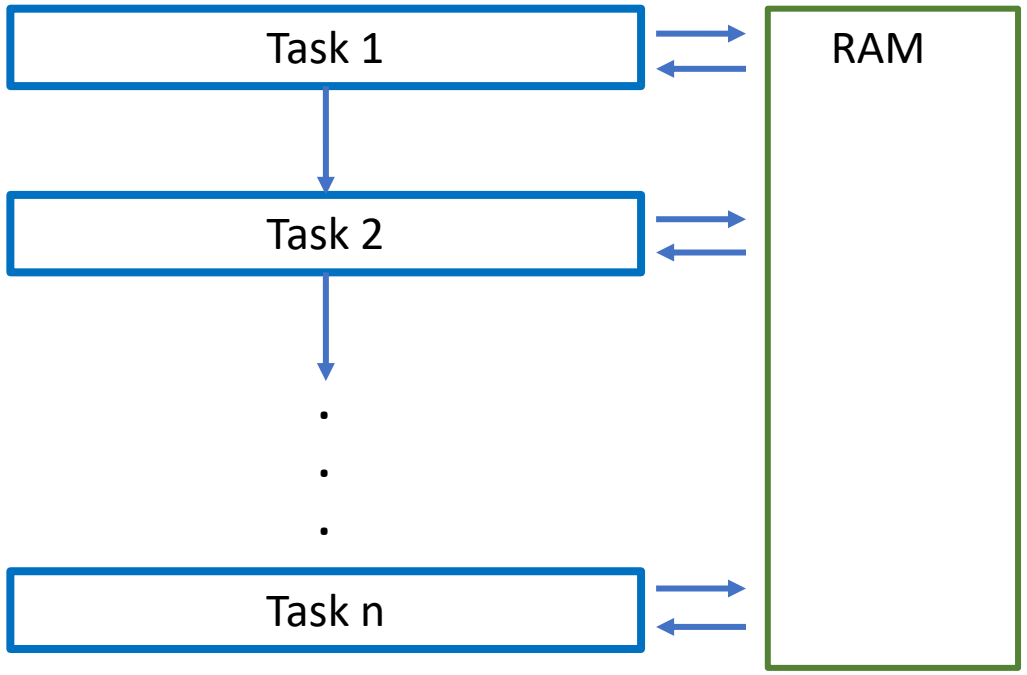
TEE only (IoT extension)

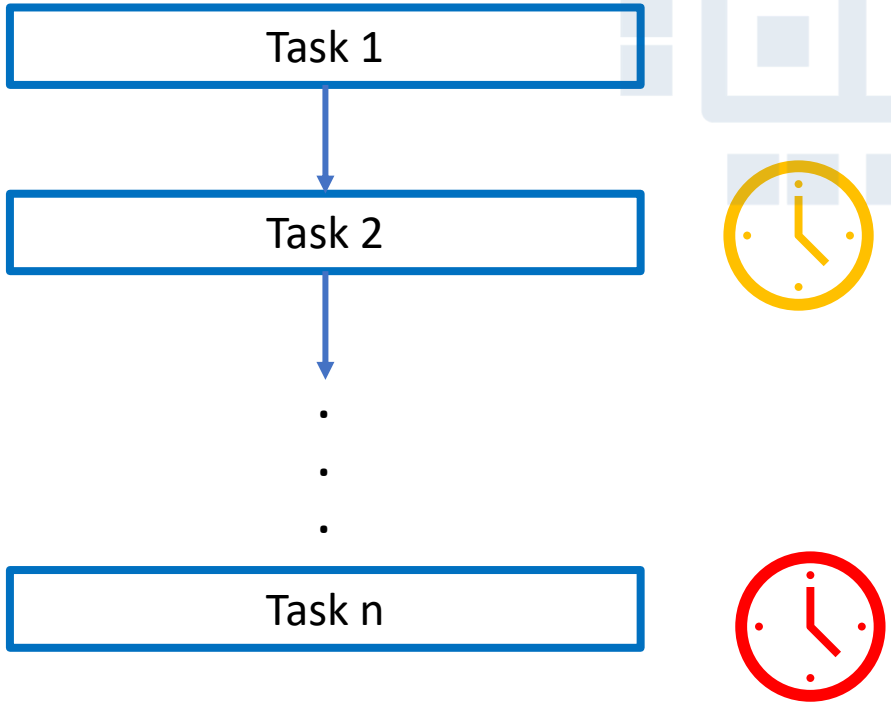


Conclusions

Overview about FPGAs

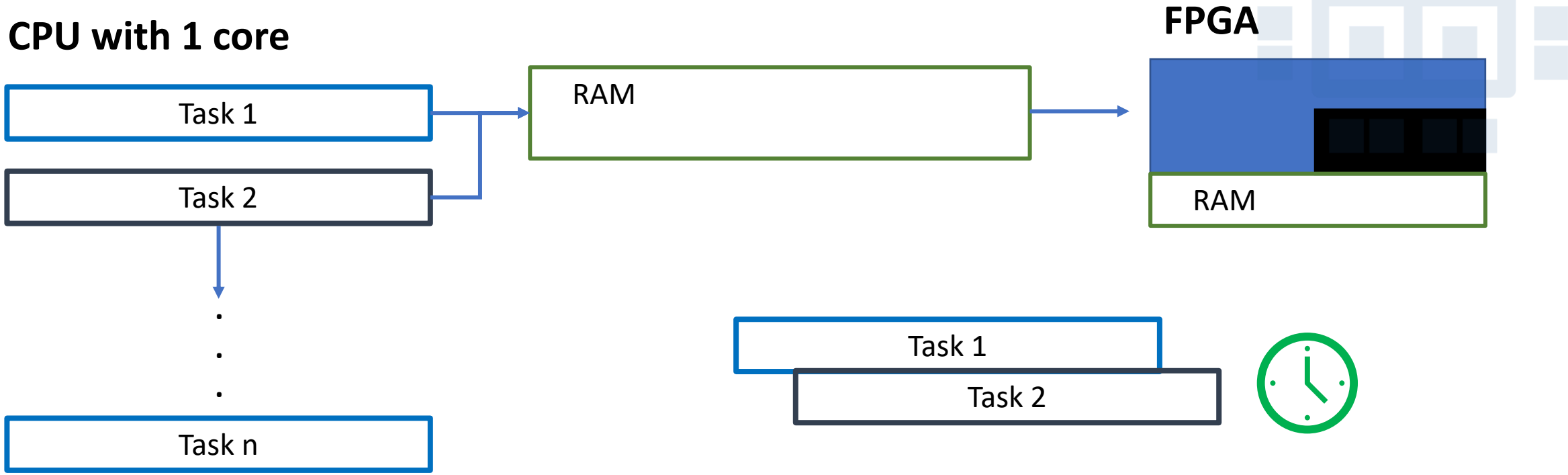
CPU with 1 core





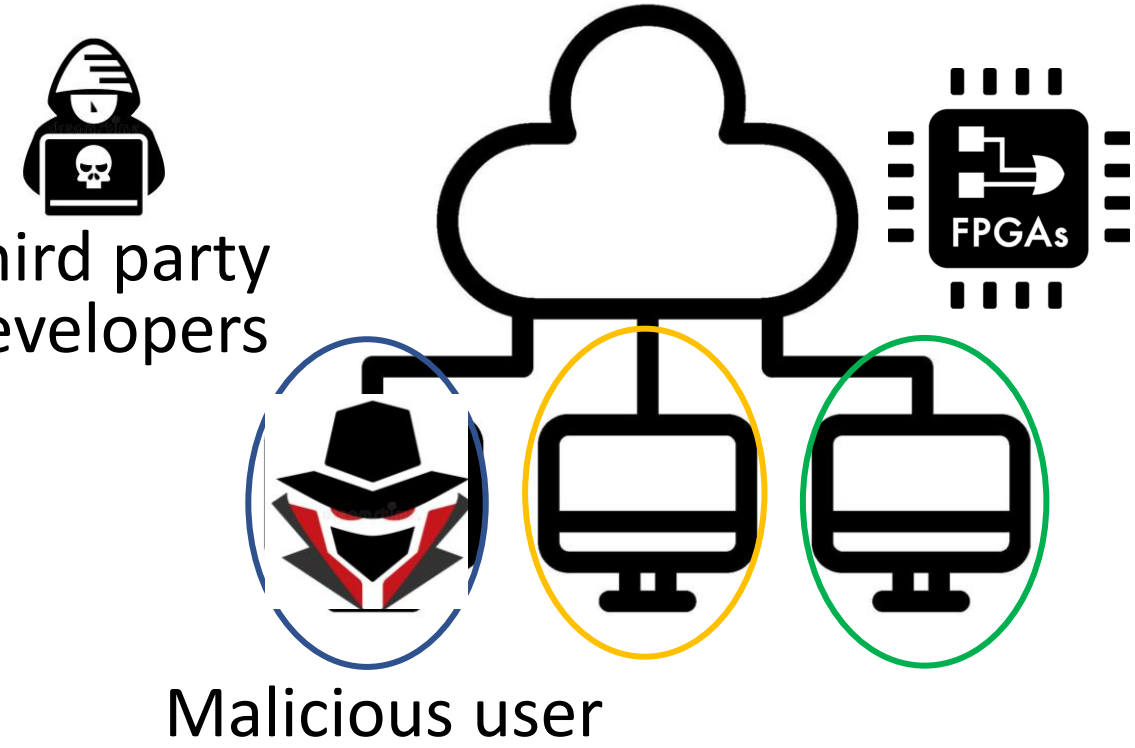
A microprocessor with one core, that's means you only can run one task o procedure. This task comes into the core, uses the RAM, and sends its result. However, if task two takes more computational resources than we expect, other tasks will be delayed, and in some cases, the CPU gets freeze.

Overview about FPGAs



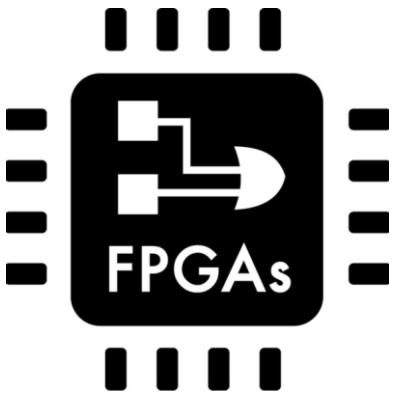
In the following scenario, the same CPU with one core has an FPGA near to it. One task comes to the core to be processed, uses the RAM, and needs more computational resources. The FPGA manages covering its needs. FPGAs do not have processing time because logic gates make them (called LUT).

Security concerns



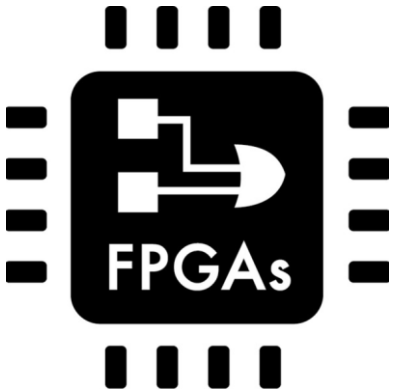
In the cloud environment, when users are isolated virtually. FPGAs have some issues with multi-tenancy. The main reason is that FPGAs share their resources fiscally. Some Cloud services providers have third-party companies for many support tasks.

Security concerns



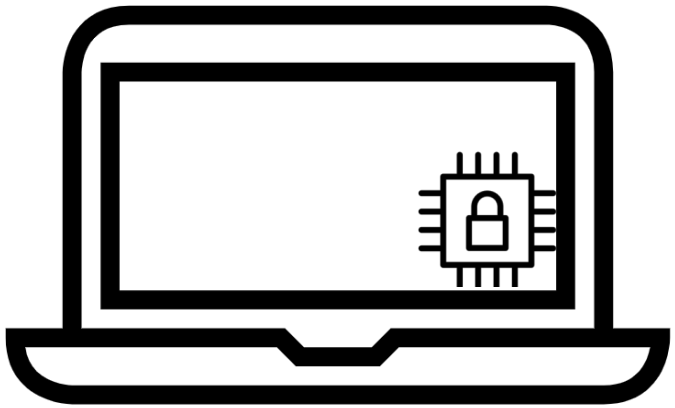
- **FPGA Genuineness** is no authentic FPGAs with security faults.
- **Hardware Trojans** are a malicious modification of the circuit to disable the security fence of a system
- **Covert-channel attacks** are a means to transfer information between users that is not allowed by the system security policy.
- **Side-channel Attacks** filtrate information by not standard digital output channels of the FPGA
- **Crosstalk** phenomenon in long wires can be exploited to launch covert channel communication as well.

Security features



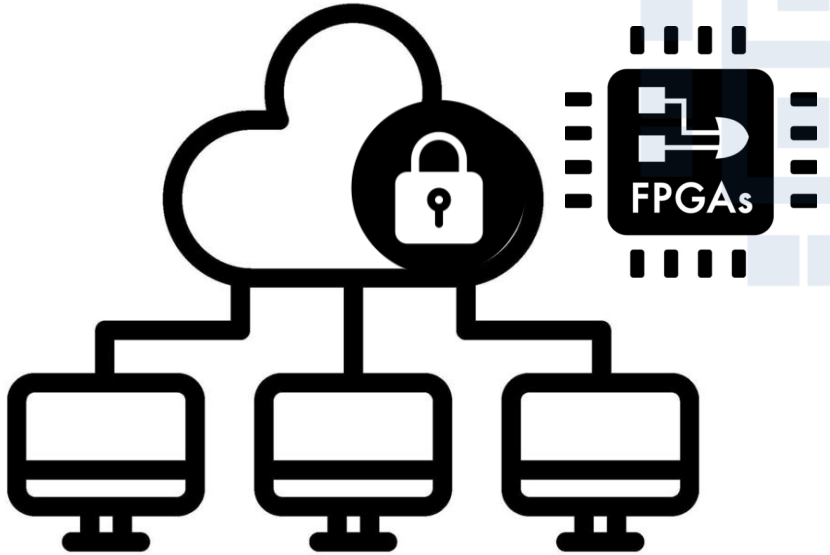
- **Memory protection:** FPGA providers have been used SRAM memory to store a bitstream
- **Bistream Decryption key Protection**: For the bit-stream protection, proposes a hard-wired logic in FPGAs for the key exchange and authentication using the Public Key Infrastructure (PKI).
- **Physical Unclonable Functions:** Hardware protection mechanism, they uses the uncontrollable manufacturing process variation of devices to generate a unique n-bit binary string identifier foreach device.

Trusted execution environment



Trusted platform module

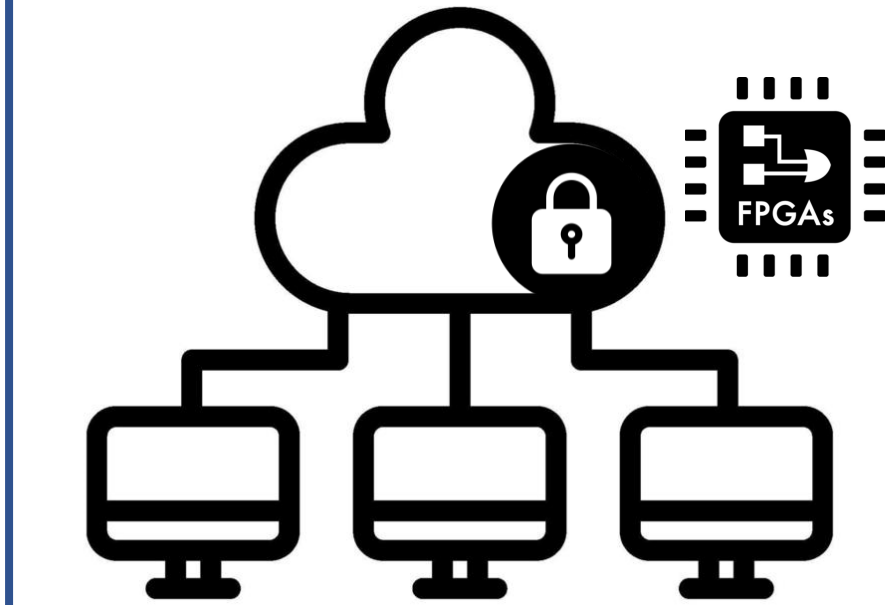
Computers have a trusted platform module (TPM) to run trusted software of the rest of the untrusted operative system. However, both share the RAM.



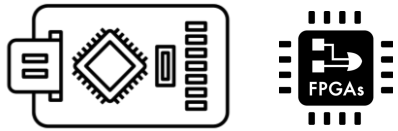
Trusted execution environment

A trusted execution environment in the Cloud environment term refers to building a secure authentication user to share software and hardware resources like FPGAs without TPM

TEE only (IoT extension)



Trusted execution environment

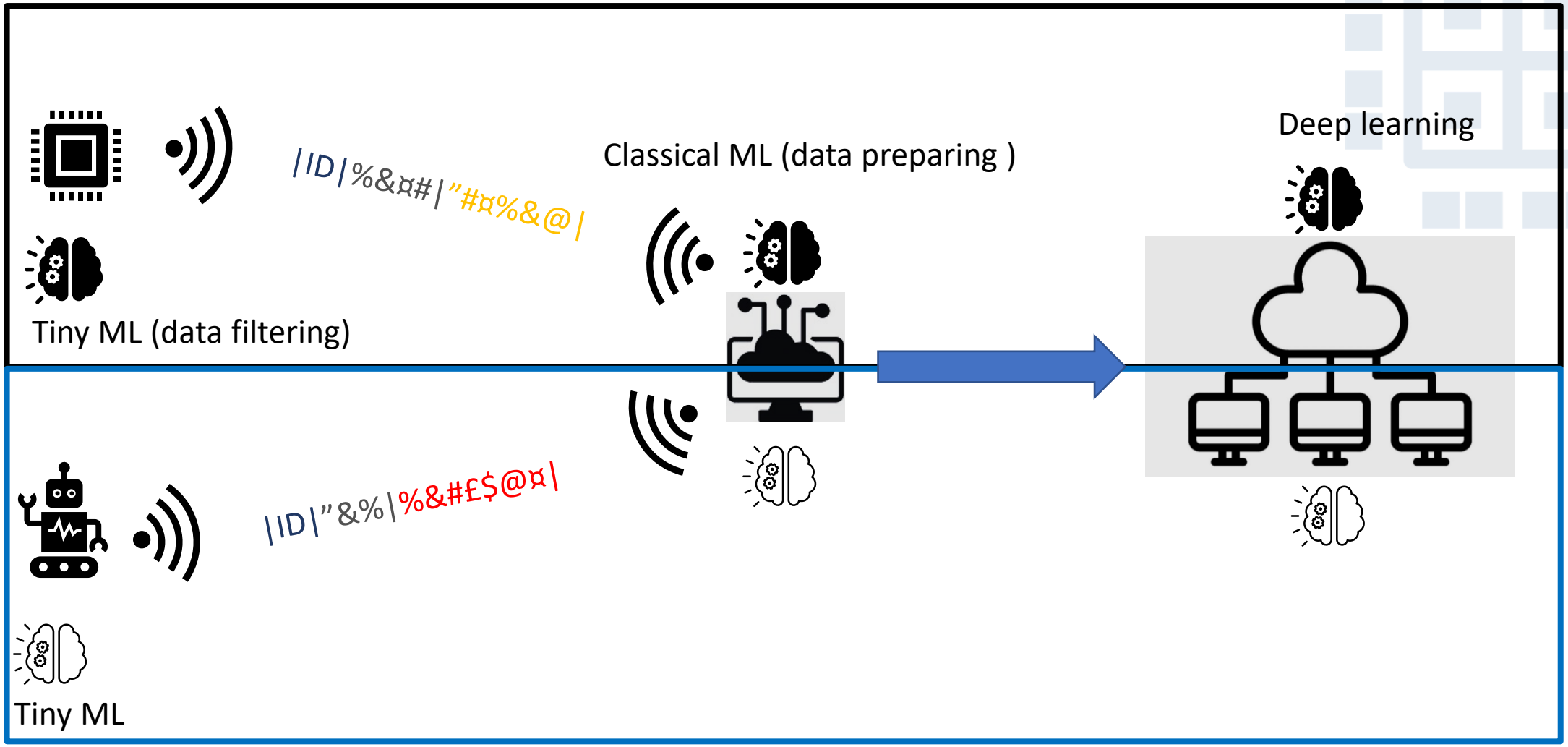




IoT: Extension of TEE

Internet of Things devices can be an extension of the secure Cloud. The first try is to determine how RAM the IoT device needs to run the entire application with the help of the Cloud. Second, we define some assumptions to ensure the channel, the data, the sensors are trusted.

TEE only (IoT extension)





Conclusions

- FPGAs have been a powerful tool for hardware accelerators in the cloud. However, these devices are not designed to work with multiple tenants and present many security issues that have been mentioned.

- A hybrid architecture between FPGA and SoC provides the opportunity to build a secure and trusted execution environment.

- What will be the next generation of trusted IoT devices?

THANKS..!!

https://paulrosero-montalvo.com/

http://teeonly.paulrosero-montalvo.com/

paur@itu.dk