

Secure Computations in Decentralized Environments based on Smart Contracts and Intel SGX

Michał Król, Adrian-Cristian Nicolaescu, Sergi Reñé, Onur Ascigil, Ioannis Psaras, David Oran, Dirk Kutscher

University College London, Network Systems Research & Design, Huawei

Motivation

There is a rising need for distributed computation. Currently everything is done in the cloud, but:


- Privacy issues.
- High execution cost.
- High delay.

There is a lot of unused computational power at the edge, but:

- Nodes do not trust one another.
- There are no easy mechanisms to prove result validity.
- There are no simple payment mechanisms.

Actors

 **Requestor** - submits tasks to the system

 **Execution Node** - executes tasks for a reward

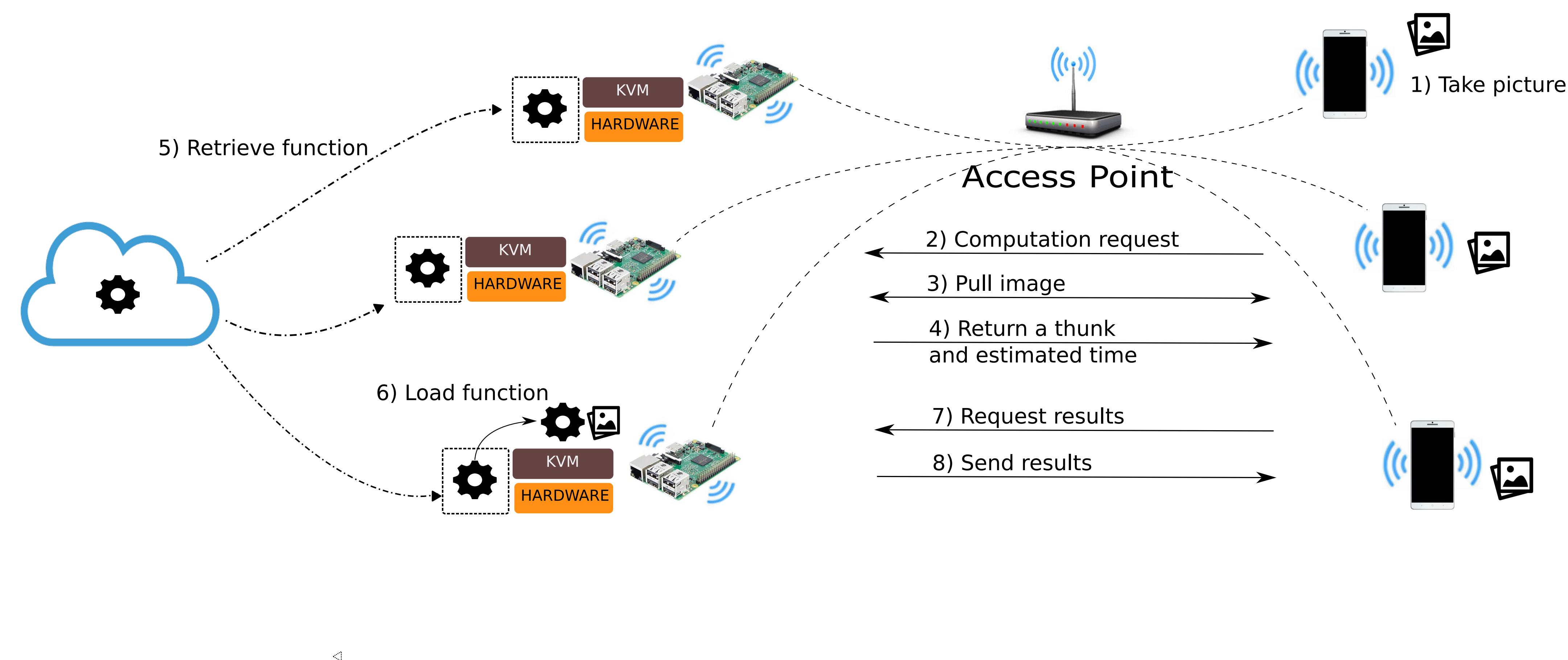
Technologies

Intel SGX

- Creates *enclaves* that are protected by the CPU against access from other OS/Hypervisor
- Remote Attestation Protocol
 - Verifies the code running on a remote node
 - Allows secure communication with the enclave

Blockchain

- Immutable, Distributed Ledger
- Smart Contracts
 - Allow to logic on top of a blockchain
 - Turing complete language (Solidity)
 - Submitted data is publicly visible



Design Goals

- **Openness** - everyone can join the system and submit or execute tasks.
- **Incentives** - *Execution Nodes* are paid for their work.
- **Result Integrity** - *Requestors* are sure that the returned result is correct.
- **Input/Output Privacy** - input parameters and result data are visible only to the *Requestor* and hidden from the *Execution Node*.

Results

- A prototype running on Ethereum Test Network.
- Orders of magnitude less overhead than the State of the Art.
- Fully automated payments and result verification.
- Operating cost lower than 1\$.
- No 3rd parties involved.
- Secure against rational attacker.

Current Limitations

- Delay imposed by the blockchain (few minutes).
- Function size limited to 100MB.
- Requires Intel hardware.
- Not secure against arbitrary attacker.