Confidential Computation using Trusted Execution Platforms for IoT data

SWITS 2023

Marcus Birgersson marbir@kth.se

May 29-30, 2023

Abstract

To get the full functionality from data generated by IoT applications, different devices needs to share data between them. Since many such devices are constrained in terms of storage capabilities and computing power, this data is often sent to the cloud. In addition, several applications require data generated by multiple different mutually distrusting users, where the computation must be carried out while preserving each user's confidentiality.

We present a solution that has an acceptable overhead while allowing users to be added to the system at any time without re-encrypting data. To achieve our goal, we make use of a Trusted Execution Platform, such as Intel SGX, where the computation can be validated and verified using attestation before any data is handed over.

In our solution, all data stored in the cloud is encrypted, but still gives the possibility for arbitrary computations on the data, over multiple mutually distrusting users. We do not require the user to be online during the computation, and users can be added and removed at any time. The users are themselves responsible for key generation, and hence no data can be used without the user's explicit permission.

The system is evaluated over several applications implemented using off-the-shelf software. It is compared with an equivalent system running outside a secure enclave, computing on plain data.