Secure Data Sharing in multi-user IoT systems

SWITS 2021

Marcus Birgersson marbir@kth.se

June 2-3, 2022

Abstract

IoT systems, such as in smart cities or hospitals, generate data that may be subject to different security classifications, privacy regulations, and access rights. However, popular IoT platforms do not consider data classification and security-aware data analysis. Popular platforms such as IFTTT, Zapier and Microsoft Power Automate all provide so called trigger-action platforms which can trigger an action when a particular prerequisite is full-filled. These platforms however, do not consider different classes of confidentiality and is a target for malicious developers and attackers that would like to access private data.

At the same time, the world of smart devices has big potential to solve different problems, and the popularity of above mentioned platforms is a proof that people find them useful. Therefor it is important to find solutions where one in a secure way can handle confidential data in a security-aware setting.

I will present an architecture for handling confidential data in a secure way by the means of classification labels and filtering functions that prevents unauthorized data access.

Continuing this work, I will show how this system can be made more secure by the means of trusted execution environments. Trusted execution environments show a big potential in this fields and has many strengths such as remote attestation for verifying that one executes the correct code and secure enclaves that hide the data in memory even from a malicious server provider.

Using TEE:s we will extend the above mentioned architecture to only store encrypted data in the cloud, but still being able to perform aggregations on this data without the means of any homomorphic encryption.