Data classification for multi-user IoT systems

SWITS 2021

Marcus Birgersson marbir@kth.se

May 19, 2021

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.

We present a novel architecture together with a data-centric classification system for labeling and managing confidential data from IoT devices. The system is based on the decentralized label model and focuses on making sure that every data point has a classification label and that aggregated data inherits a label without leaking information. At the same time the system provides for a possibility of secure computation of third-party functions and access control based on the data label.

We present three main enforcement methods for handling data based on the classification model: 1) secure access of data by data owners, 2) secure computation using untrusted functions and 3) controlled release of data.

The architecture consists of three layers: 1) a layer for exposing labeled data to the cloud, 2) a middleware layer in the cloud and 3) a dashboard for exposing data to a user. The system is evaluated using real world inspired use cases based on both a smart city and a smart hospital. This is done based on an implementation using available open source technologies such as Web of Things, Node-RED and Grafana.

This is a joint work with Musard Balliu (musard@kth.se) and Cyrille Artho (artho@kth.se).