Giotto: Privacy Systems and Permissions in the Internet of Things

Bharadwaj Ramachandran
Advised by: Jason Hong
Special Thanks: Adam Yee, Sharon Rajkumar, Joonho Park, Yuvraj Agarwal, Sudershan Raghavan, Jineet Doshi

The Problem

Current paradigm for IoT:
- Sensors collect streams of information from devices
- Phones, cars, microwaves, lightbulbs, etc.

The storage, privacy, and security of streams of user data is key.

Case 1: No privacy policy
- Too privacy invasive for users
- If user privacy is compromised, user adoption will stall
- The IoT platform will not have a critical mass of users

Case 2: Uncompromising privacy policy
- Not much data is available to IoT application developers
- Platform does not solve interesting use cases

The Solution

We create two services to investigate IoT privacy policies

- **BuildingDepot**: Stores streams of information with relevant metadata and generates virtual sensors to answer IoT queries.
- **ActiveMap**: Allows the Giotto stack to provide context-aware responses that can open up new application domains to developers and end users while enforcing a user-defined privacy policy. Keeps track of relationships between people, places, and IoT objects.

ActiveMap

Consider the following scenario that Giotto enables. We will walk through the role of ActiveMap in making this scenario possible.

ActiveMap also provides the granularity of the response they receive.

In addition, the developer also needs to have their query verified by the Giotto stack. In this case, CMU Sports would define the purpose of their query, and Giotto would confirm a legitimate reason to query for a user’s data.

Future Work

We are making an interface that maps out people, places, and things for the purpose of visualization and future testing.