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

Carnegie Mellon University

CHIMPS Lab
Computer Human Interaction: Mobility Privacy Security

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
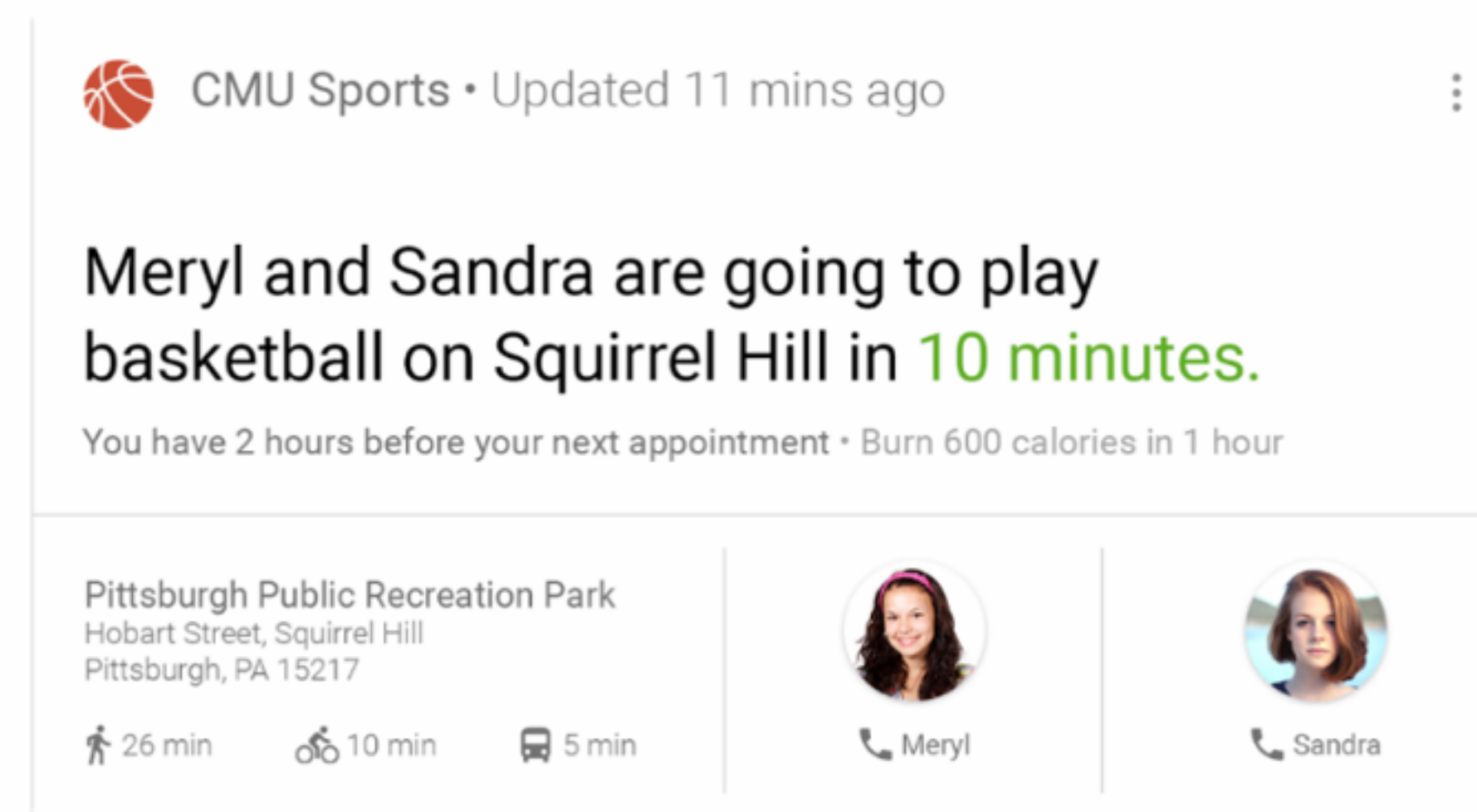
The Solution

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.
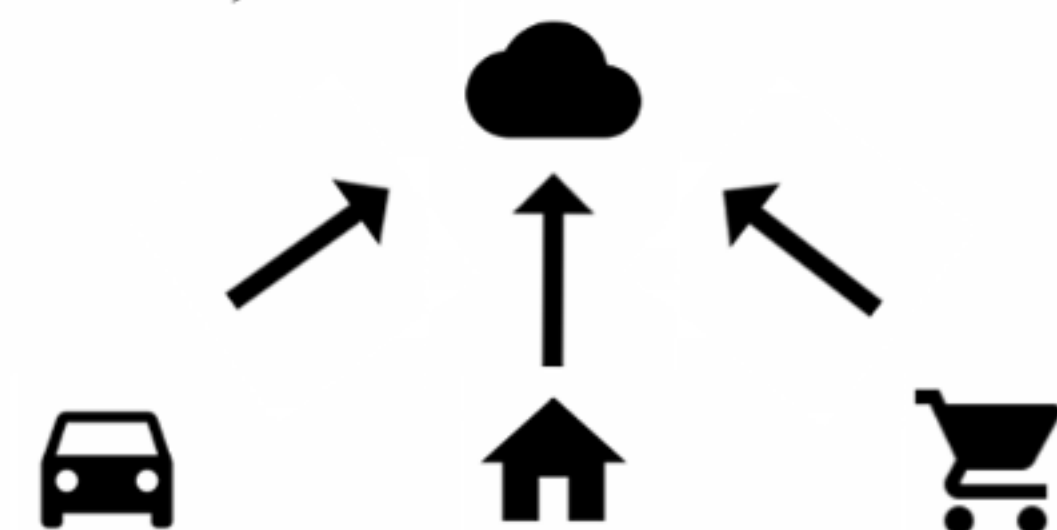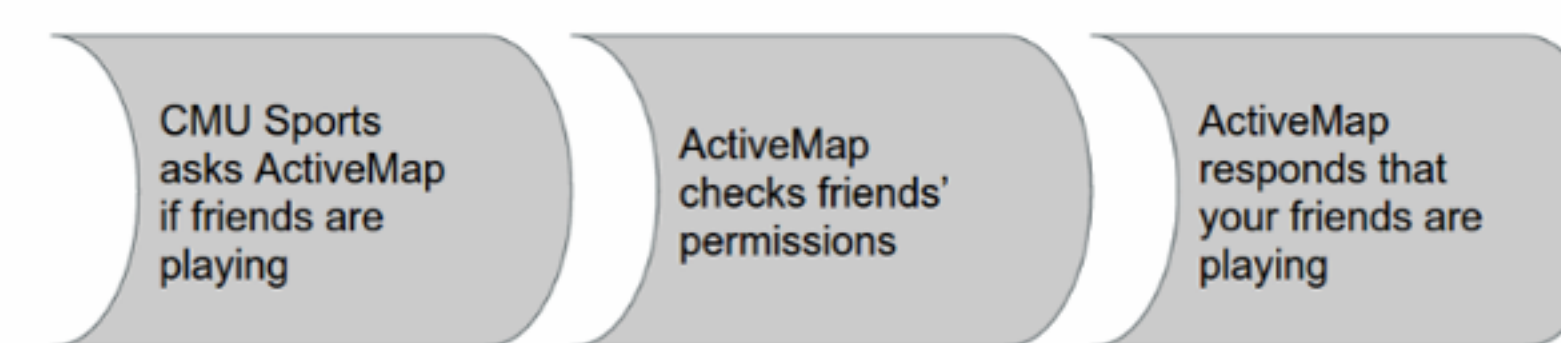
ActiveMap

Consider the following scenario that Giotto enables. We will walk through the role of ActiveMap in making this scenario possible.
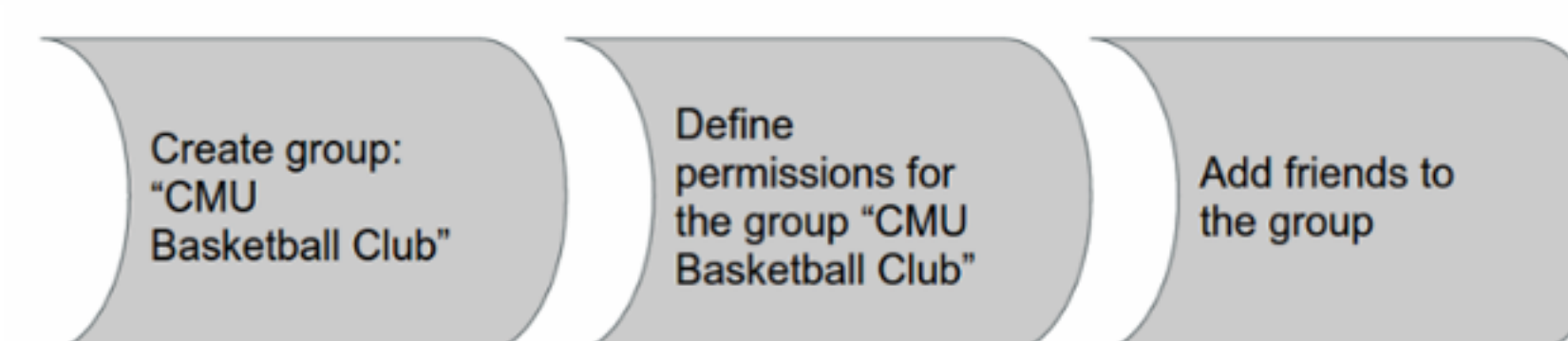
🏀 **CMU Sports** • Updated 11 mins ago

Meryl and Sandra are going to play basketball on Squirrel Hill in 10 minutes.

You have 2 hours before your next appointment • Burn 600 calories in 1 hour

Pittsburgh Public Recreation Park
Hobart Street, Squirrel Hill
Pittsburgh, PA 15217

🚶 26 min   🚲 10 min   🚌 5 min   📞 Meryl   📞 Sandra

There are three agents that ActiveMap manages in any given query.
- The user
- The developer
- The data (BuildingDepot)

CMU Sports asks ActiveMap if friends are playing → ActiveMap checks friends' permissions → ActiveMap responds that your friends are playing

ActiveMap also the granularity of the response they receive.

Create group: "CMU Basketball Club" → Define permissions for the group "CMU Basketball Club" → Add friends to the group

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.

Architecture
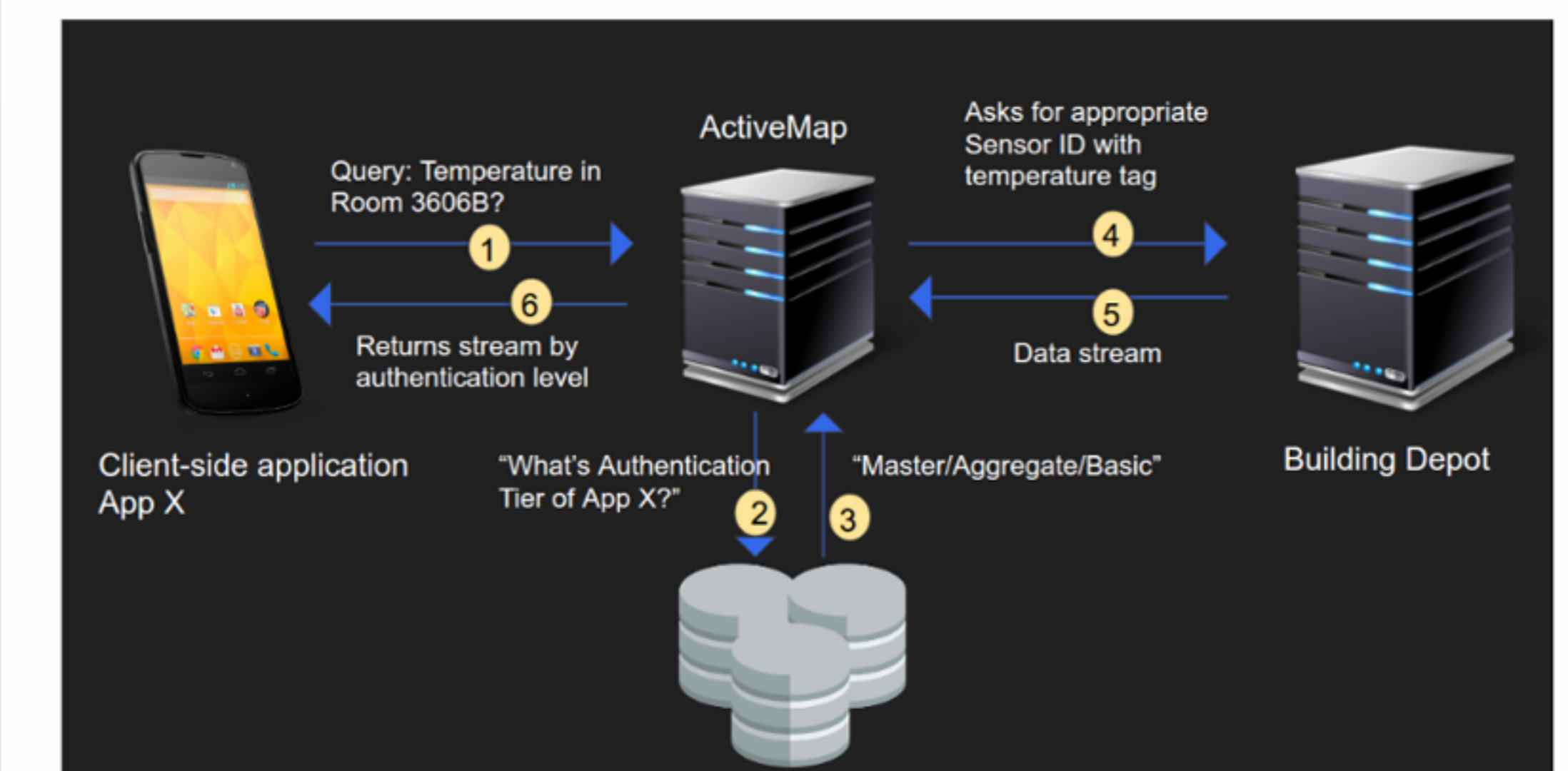
Service flow diagram

Future Work

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

Room	People	Capacity
NSH 3526	2	8
NSH 3515	Permission denied	N/A