User Friendly IoT Data Management Framework

Team 4:
Hyun Bin Lee, Aravind Sagar, Zicheng Li

Internet of Things

- Pervasive, rapid growth in recent years
- Lots of applications in home and industry
- We focus on non-commercial users (mostly owners of smart home devices)
- Estimated $7.1 trillion worth by 2020

Privacy concerns

- **Privacy** is a major concern related to mass IoT adoption [1]
- Current systems are all **centralized**. This means users need to trust a single third-party with all their data
- Users desire **user-centric** approaches, **decentralized** access control system, **fine-grained permissioning,** and **user anonymity** when sharing data with third parties[1][3]
- App over-privilege, environment mistrust, LAN mistrust and weak authentication are some of the issues with current IoT systems[3]

Related works - Hashemi et al.

- A distributed, secure and scalable framework for IoT data storage and sharing
- Data Owner: IoT device users
- Data Source: Trusted data storage provider
- Data Requester: Entity requesting user data
- Endorser: Third-party request endorser

Related works - Hashemi et al.

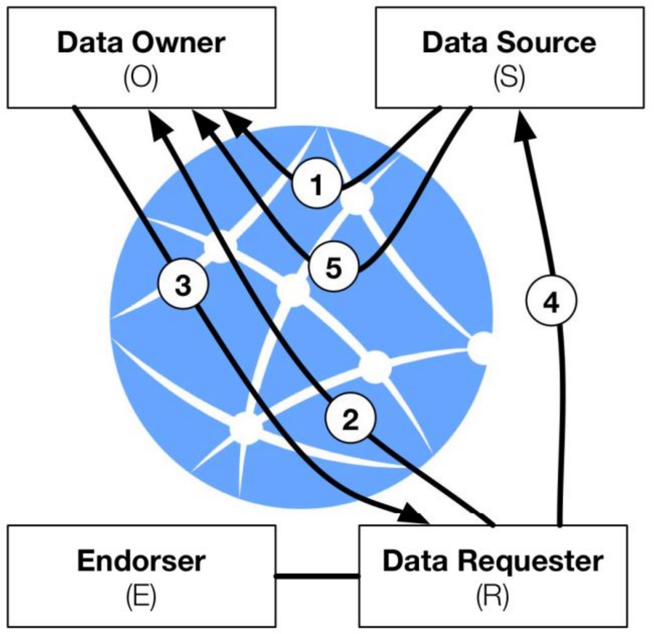


Figure by Hashemi et al.,[2]

Related works - Privacy mediators

- Davies et. al. suggests an approach based on ‘Privacy Mediators’ and ‘Cloudlets’[1]
- User-centric and distributed; emphasizes edge computing as well
- **Cloudlet architecture** - access control happens in personal hubs or trusted servers near the cloud edge
- **Privacy mediator** - Software in cloudlet that validates permissions before data is sent to outside world
- Emphasizes exposing summarized data, user anonymity, control over inferred sensors, and ease of use.
- Disadvantages:
  - Data storage in the sensor or the cloudlet
  - No mention of how to identify legitimate 3rd party apps

Problem statement

- Lack of a user-facing component in proposed privacy-aware, user-oriented, secure and decentralized IoT systems.

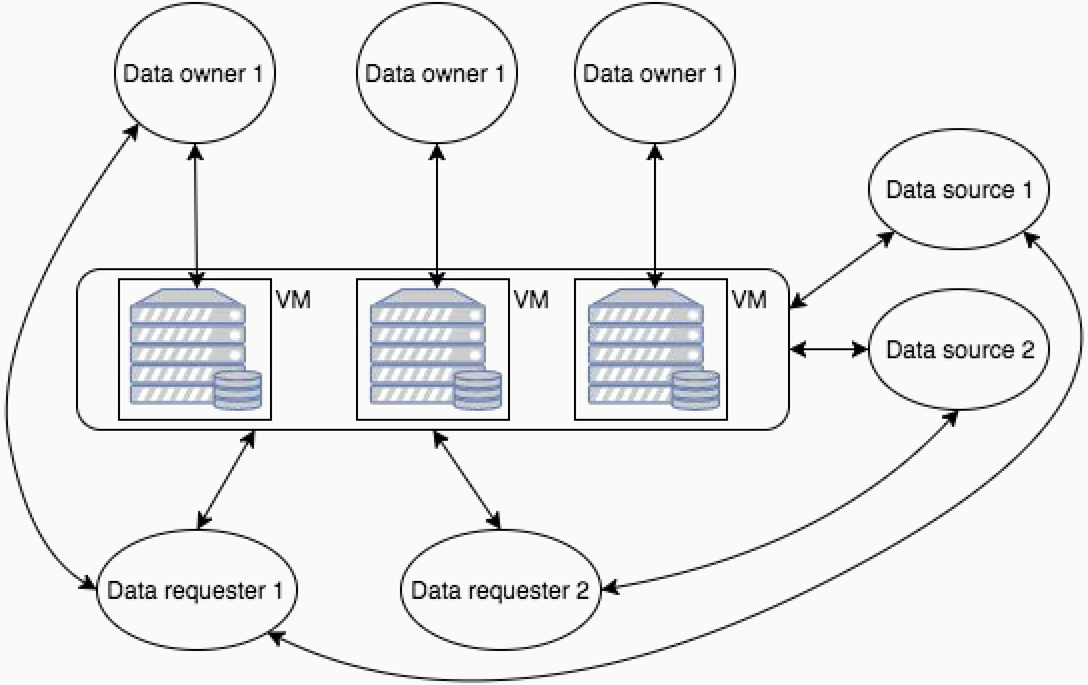
Proposed solution - Part 1

- **Smartphone app** to manage IoT devices and data
- Functionality:
  - A **centralized view** of IoT generated data owned by them
  - A **detailed view** including the data source, access permissions and other details
  - Permission request **notifications** from data requesters, and a way to accept or deny them
  - View, add, remove **trusted endorsers**
  - Provide data owner’s identity to user facing IoT apps
- Hides some complexity from users, makes the system accessible
- Focus also on **user-friendliness**

Proposed solution - Part 2

- Request handling is done on the **back-end server**
- Server periodically informs users on new data requests
- User defines privacy policies that the server can enforce
- Each server app process manages corresponding user’s data requests
- Apps are insulated by VM

Structure of the proposed framework



Threat Model

There exists four major parties involved in Hashimi et al.'s protocol.

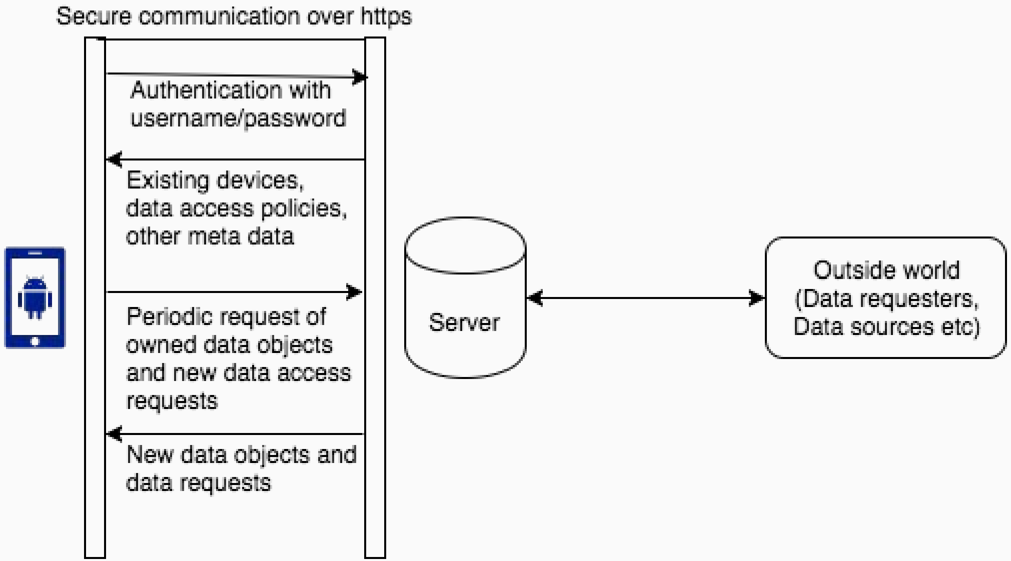
- **Data Owner**
- **Data Source**
- **Data Requester**
- **Endorser**

Our implementation also considers one additional party, **Cloud Service Providers**. We trust all parties but **Data Requesters** in this protocol.

Data Object Metadata

- Distinguish device from ‘device data summary’
- Data access request is for a particular summary
- Also stores meta-data related to Data source and Data requester names to provide friendly descriptions to the user

Solution Model


Secure communication over https
Authentication with username/password
Existing devices, data access policies, other meta data
Periodic request of owned data objects and new data access requests
New data objects and data requests
Server
Outside world (Data requesters, Data sources etc)

Demo

User Study Design

- Amazon Mechanical Turk
- Present different cases with screenshots of UI and ask

1. Which identity is asking for the data
2. What kind of data is being asked
3. Which entity has the data
4. Grant/Deny access to the data (subjective question)

What’s new?

- Central to user, while decentralized outside
- Support for temporal and spatial summarizations using ‘Device data summaries’
- Granular controls for the user, yet the option to automate many of the decisions

Challenges

- The blockchain framework is not deployed in real world.
- The effectiveness of User Interface can be subjective.
- Limited Block size for RSA

Future Works

- Verify security of communication between App and server
- Building a stronger security guarantee (against malicious cloud service provider?)
- Advanced Permission System
- Integrate our server into the publisher-subscriber network

Questions?

Thank you!

References

[1] Davies, Nigel, et al. “Privacy mediators: Helping iot cross the chasm.” Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications. ACM, 2016.

[2] Hashemi, Sayed Hadi, et al. “World of Empowered IoT Users.” Internet-of-Things Design and Implementation (IoTDI), 2016 IEEE First International Conference on. IEEE, 2016.

[3] Zhang, Nan, et al. “Understanding IoT Security Through the Data Crystal Ball: Where We Are Now and Where We Are Going to Be.” arXiv preprint arXiv:1703.09809. arXiv, 2017