CS523 Mid-Semester Report (temporary title)

Hyun Bin Lee
Department of Computer Science
University of Illinois Urbana-Champaign
Urbana, United States
lee559@illinois.edu

Aravind Sagar
Department of Computer Science
University of Illinois Urbana-Champaign
Urbana, United States
asagar3@illinois.edu

3rd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address

***Abstract*—This document is a model and instructions for LaTeX. This and the IEEEtran.cls file define the components of your paper [title, text, heads, etc.]. *CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract.**

***Index Terms*—component, formatting, style, styling, insert**

I. Introduction

TODO

II. Background

A. Internet of Things

TODO (Can potentially include the paper exposing security holes in Samsung SmartThings)

B. Security and provacy in IoT (Blockchain paper)

TODO

C. Intel SGX

TODO

D. Related Works

Davies et. al. points out that privacy concerns could be a major factor preventing wide-spread adoption of IoT devices [1]. Over-centralization of IoT systems is identified as a critical obstacle to eliminating concern over privacy. They propose a privacy mediator which sits in between IoT devices/data and outside world. This model includes a trusted 'cloudlet', which could be a local hub or a trusted server at the edge of the cloud. They also emphasize some important characteristics that a privacy-aware IoT system should have, like exposing summarized data, user anonymity, control over inferred sensors, and ease of use. However, the model's limitation is that data storage has to happen in the sensor or the cloudlet - this could be limiting when the number of sensors increase.

Data mining and clustering of IoT related articles expose major problem areas in IoT [3]. App over-privilege, environment mistrust, LAN mistrust and weak authentication are identified as some of the problem areas that needs work. They also conclude that permissioning needs to be more fine-grained, and recommend better standards and widely-applicable systems.

III. Problem and solution

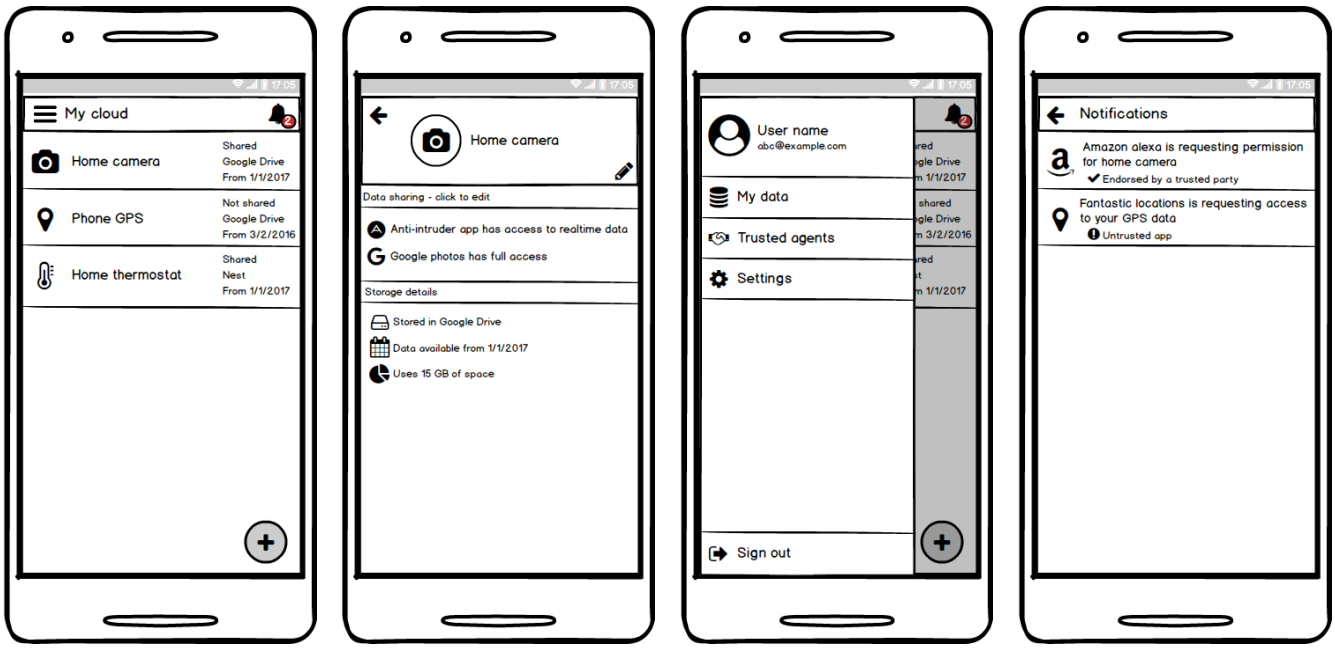
As evident from the previous sections, effectively addressing privacy concerns about the data generated by IoT devices is essential for the success of IoT. There are some proposed architectures which tackles this problem using user-oriented and decentralized systems. However, there's a lack of a user-facing component in such systems, which can effectively make the complex architectures usable to everyone. Our work is aimed at tackling this problem, which is "to build a user-facing component for a privacy-aware distributed user-centric IoT system (such as the blockchain based system described in [2]), which improves the user friendliness of the system while maintaining strong security and privacy guarantees."

To accomplish this, we build the user-facing component for the blockchain based IoT architecture described in "World of empowerd IoT users [2]". Since that system is still in development, we concentrate on the user facing components of the system, and simulate some of the external components.

The proposed work consists of 2 components:

1) A smartphone app to manage IoT devices and data: Smartphones are becoming the preferred devices for internet access [4]. Hence we build a smartphone app with which users can manage their IoT devices and data. The functionality provided by the app includes:
   a) A centralized view of IoT generated data owned by them.
   b) A detailed view including the data source, access permissions and other details of this data.
   c) Permission request notifications from data requesters, and a way to accept or deny them.
   d) View, add, remove trusted parties.

   This is not a comprehensive list of the functionality, as we expect to add more as the project progresses. It also hides away some complexity from the users, like managing secure connection with the server described below, and managing user's private key etc. We also focus on the user-friendliness of the app, and expect to conduct user-research to find out what capabilities do users expect to find in such an app.
2) A trusted server which manages the access control: This is the component which actually manages access control and capability issuance in accordance to the user's wishes. This is similar to cloudlets described in



(a) Overview of user's data (b) Details of a particular device (c) Navigation drawer (d) Notifications screen

Fig. 1: UI mockup of the user facing application

[1], but with some key differences. First, we intend to leverage hardware technologies like Intel SGX to ensure that the server application can run on untrusted hosts. Second, this app does not store data within it; it simply interacts with the data owner, data sources and data requesters in accordance to the protocol outlined in [2].

IV. Threat Model

1) cellphone Trusted (we can use TrustZone based solution to be orthogonal to our solution)
2) data source Trusted
3) Endorser Trusted
4) data requesters NOT trusted
5) cloud NOT trusted
6) we are not responsible for user misassigning policies. instead we aim to minimize it

V. Experiment

We started out by experimenting with the UI of the application. We are currently developing an Android app, and apps for other mobile platforms like iOS is left as future work.

We made an initial version of the UI mockups, and ran a user survey to iterate over the design. The current design is shown in "Fig. 1". These images show only some of the important screens in the app, and are not exhaustive. The capabilities of the app include having an overall view of the devices and data (Fig. 1a), seeing and editing details pertaining to a particular device (Fig. 1b), receiving and acting upon data requests (Fig. 1d), and viewing and managing trusted parties.

User research shows that the following design choices enhance the experience.

- Overall view of the devices and data is very helpful.
- Notifications screen is well done because users can see whether the requester is endorsed and act on the notification from the same screen.
- Users also feel more comfortable with IoT devices when a privacy-control mechanism like this app is present.

We also identified some major areas of concern.

- Users need more control over what data is stored. In particular, they might want to delete data between certain time periods.
- Users want to minimize the data shared with third parties, and hence each device should expose various spatial and temporal summarizations.
- Guarantee of anonymity is a must when sharing sensitive data with third parties, especially for analytics purposes.

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

[4] (2016, Nov.) "Mobile and tablet internet usage exceeds desktop for first time worldwide." Statcounter global stats. [Online]. Available: http://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide