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 privacy in IoT (Blockchain paper)

Nowadays, smart devices like Android Wearables and smart phones are collecting information in every aspect of device owners and generate vast amount of data. While the sheer size and growing rate of the data present a challenge to store and process them, keeping the data secure is equally challenging and important.

The paper ”World of Empowered IoT Devices” proposes a system that aims to address these problems. In this system, user data is stored in volunteer data servers. These data servers let the data owners to name trusted entities who can access the proprietary data. A data requester can only get access to the data if it has the permission given by the data owner(IoT device user).

To ensure data transparency, all data transactions are recorded using BlockChains. A Publisher-Subscriber configuration is used to keep track and distribute the BlockChain nodes. After a successful data transaction, the data server broadcasts the transaction and the subscribers update their BlockChain Record.

Using the combination of user-granted data access and BlockChain, the system proposed by ”World of Empowered IoT Devices” provides a secure and scalable way to manage the ever-growing IoT user data.

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.

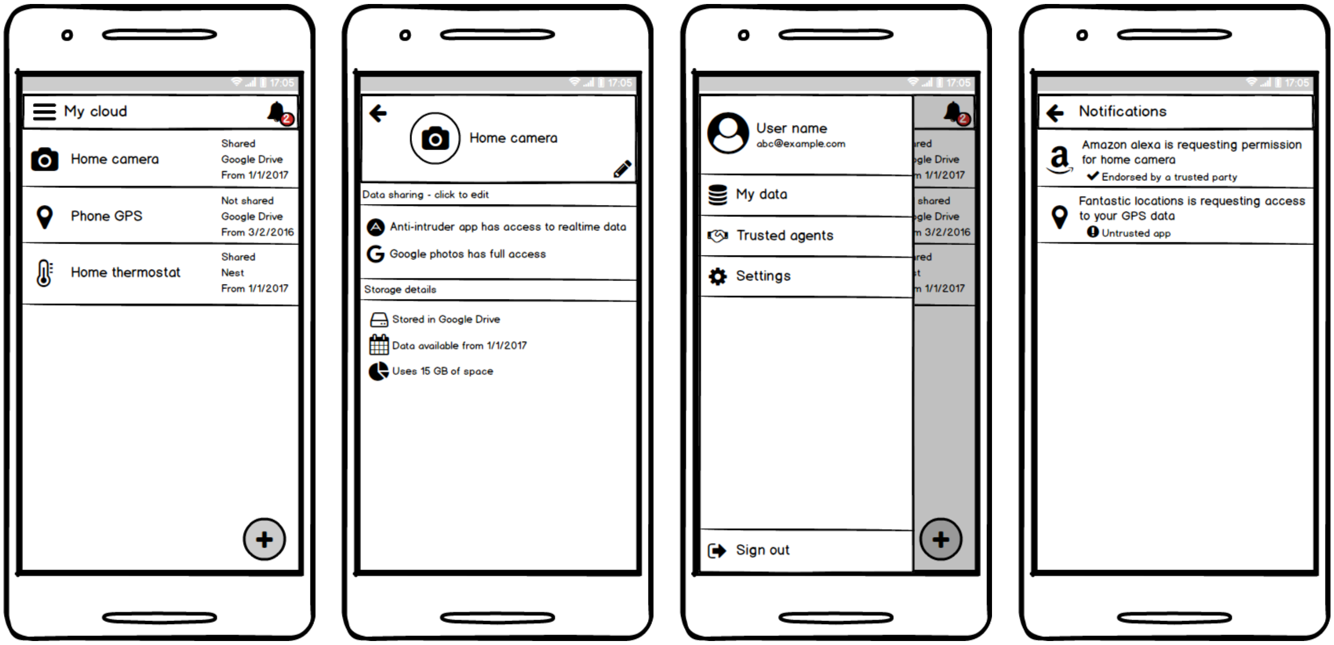
III. Problem and solution

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



Anti-intruder app has access to realtime data

Google photos has full access

Stored in Google Drive

Data available from 1/1/2017

Uses 15 GB of space

Amazon alexa is requesting permission for home camera

Fantastic locations is requesting access to your GPS data

(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

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 [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

We use Hashemi et al. [2] protocol as a main guideline for IoT sharing mechanism. Meanwhile, our work is not limited to this protocol as we can extend our framework to any data sharing protocol. In addition to four major parties involved in their protocol, we also add cloud service providers in our model. These providers are responsible for running our server-side implementation that enforces user-defined policies on data request approvals/denials.

1) **Data Owners**
Our work primarily focuses on households with a small number of IoT devices. These individuals may interact with IoT devices using IoT applications written by IoT device manufacturers or other third-party programmers. Our framework does not trust these applications as they may leak sensitive data and violate Data Owner's privacy. Users grant or deny operations related with IoT data using our Android application. Securing our application against malicious Android applications or Android OS is out of the scope, but solutions that enforce Android application security and OS security [5] can be applied as orthogonal solutions to our work.
2) **Data Source**
We assume Data Sources are managed by trusted parties such that they honestly follow the data sharing protocol.
3) **Data Requesters**
We assume data requests from Data Requesters as one of the major privacy threat vectors. Data Requesters query and find data objects using the Messaging service and request those objects to Data Owners using the protocol. Meanwhile, Data Owners may not fully understand the

risks associated with approving or denying data requests. Our solution primarily focuses on providing concise and accurate information for each data request and guiding Data Owners to make autonomous decisions.

4) **Endorsers**
In our framework, trusted Endorsers are responsible for validating identity of Data Requesters and authenticity of Requesters' requests.

5) **Cloud Service Providers**
Untrusted third party Cloud Service Providers host back-end of our framework. Note that IoT device manufacturers usually provide such service for their IoT device customers. We do not trust this computational platform and enforce security and privacy of our solution using Intel's SGX enclaves. Data Owner trusts server-side code run in the enclave, and they can validate integrity of the code using measurements provided with a cryptographic hash. Attacks that target security limitations of the Intel SGX processors are out of scope in our paper. These include Cache timing side-channel attacks and Denial of Service attacks. Meanwhile, we believe orthogonal approaches that mitigate such threats can be applied to our solution.

We primarily focus on two attack vectors. We protect Data Owners against data requests that may violate user privacy using our user-friendly User Interface. We believe this is the most likely threat against ordinary IoT users. Meanwhile, we would also like to provide transparency and resiliency of our framework by securing the back-end with Intel's SGX.

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

[5] Ahmed M. Azab, et al. 2014. "Hypervision Across Worlds: Real-time Kernel Protection from the ARM TrustZone Secure World." In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14). ACM, New York, NY, USA, 90-102. DOI: http://dx.doi.org/10.1145/2660267.2660350