User Friendly IoT Data Management Framework

CS523 Mid-Semester Report

Hyun Bin Lee, Aravind Sagar, Zicheng Li
University of Illinois at Urbana-Champaign
Urbana, United States
{lee559,asagar3,zli135}@illinois.edu

***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.**

I. Introduction

Smaller and more power efficient processors enables almost everything in our life to collect information and access internet. This gave rise to the idea of Internet of Things (IoT). Rapid expansion of IoT devices brings new technical and privacy related challenges related to it. How do we store the vast amount of data generated by these devices? How do we manage and secure them? And, most importantly, how can we help the data owners to protect their privacy? Many research efforts have been made to address the first two challenges. Among them, Sayed Hadi Hashemi has introduced a framework that allows scalable and secure manipulation of IoT data in his paper World of Empowered IoT Devices. However, few have been done to address the last challenge. In this paper, we further improve Sayeds framework by introducing an intuitive way, in the form of a user interface, for the user to categorize and define access-control policies to his/her data. In addition, we see the trend of processing IoT data on cloud, we add SGX support to the framework to enforce data security in cloud computing environment.

Our main contributions include:

1) While most systems tag user data from the stand point of the developers, we give users the means to tag data in a way that is intuitive to them. This, combined with an easy-to use user interface, bring the security features to an accessible level to ordinary users.
2) By adding SGX support, we made the existing framework resilient to security concerns when using an untrusted cloud service platform.

II. Background

A. Internet of Things

The term Internet of Things (IoT) originated more than 15 years ago, when it was used to describe the work of the Auto-ID Labs at the Massachusetts Institute of Technology (MIT) on networked radio-frequency identification (RFID) infrastructures [9]. The definition has since expanded to beyond the scopr of RFID technologies. A lot of modern definitions have been proposed, one of them being "a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" [10].

The applications of IoT are diverse, ranging from smart industries to smart homes. In smart home area, thermostats, security systems, and energy management systems are particularly growing fast. In this paper, we focus on IoT technologies related to individual users, and these mostly fall under the smart home category, though the general principles are applicable in all areas of IoT.

Recent years have seen a rapid growth of smart devices available commercially. Ecosystems like Samsung SmartThings, Google Home and Apple Homekit are competing to become the primary player in personal IoT devices space, and for good reason - it is estimated that IoT could grow into a market worth $7.1 trillion by 2020 [11].

However, the rapid expansion of IoT market also means that many issues have been overlooked, and still need resolution. Some of the relevant issues are presented in 'Related Works'.

B. Security and privacy in IoT (Blockchain paper)

IoT data security is crucial in protecting user privacy. In the paper "World of Empowered IoT Devices" [2], a IoT data management system is proposed. This provides a user-centric, scalable, distributed and privacy-aware system to share data between the users (data owners) and third party data requesters.

In the data management protocol of this framework, user data is stored in trusted third-party entities, known as data sources. IoT users are known as data owners to the data their devices collected. Entities who are trying to get access to user data are known as data requesters.

The data owner is the only party who can grant data requesters the right, called capability, to access its proprietary data. When the data requester needs data access, it contacts the data owner for the capability. After acquiring the capability, the data requester will access data at data source. Throughout the process, the data owner has the control its data.

To ensure data transparency, all data transactions are recorded using BlockChains. After a successful data transaction, the data server broadcasts the transaction and the publishers update their BlockChain Record.

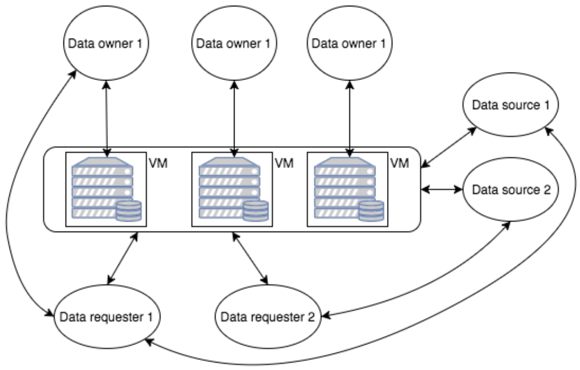

Fig. 1: Structure of the prototype framework

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, and validates permissions according to the access control policies before any data is sent out. 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. The model also does not discuss any framework for how to identify legitimate third party applications, and how to make sure that the request originates from the same application as it is claiming to be from.

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 [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 implement our solution based on Hashemi et al.'s [2] work for sharing IoT data objects. We particularly focus on their Data Management protocol to model communication between data requesters and data owners. Meanwhile, our work is not limited to this protocol as we can extend our framework to any equivalent multi-party cryptographic communication protocol. In addition to four major parties involved in their protocol, we also add one additional party named Cloud Service Providers in our model. These providers are responsible for running our server-side implementation that enforces decisions made by users to regarding approvals/denials of data object requests.

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 objects using our Android front-end application. Securing our application against Android malwares or compromised Android OS is out of the scope of our paper, but solutions that enforce Android application security and OS security [5] can be applied as orthogonal solutions to our work.
2) **Data Source**
Although a Data Owner have a possession of data created by his Data Sources, the Data Owner may or may not manage Data Sources. We assume Data Sources are managed by trusted parties such that they honestly follow the data sharing protocol. On the other hand, enforcement of protocol on Data Sources is one of our future works.
3) **Data Requesters**
We assume data requests coming from Data Requesters to be one of the major privacy threat vectors. Data Requesters query and find data objects using the Messaging service and request those data objects to Data Owners by following the Data Management protocol. Since we assumed Data sources to be honest, Data Requesters can only obtain data objects by following the protocol. Nonetheless, Data Owners may not fully understand the risks associated with approving or denying data requests. As Hashimi et al. has mentioned, the system they have proposed is user-centric such that user has full control of access control of data. In other words, Data Owners are solely responsible for granting access to all resources. This can be a very burdensome task such that it may not be scalable as we envision IoT devices to be more ubiquitous in the future. Thus, 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. Supplementary Information provided by Endorsers regarding the data requests may help user to make correct decisions but it may also
5) **Cloud Service Providers**
Trusted third party Cloud Service Providers host back-end server applications for each Data Owner such that each front-end Android application has a corresponding back-end application. Each server application is isolated from another as each runs on a separate virtual machine. For our future work, we would like to have a stronger threat model and assume Cloud Service Providers to be untrusted as well. In such case, we could enforce security and privacy of our solution using Intel's SGX [12] 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. While, our solution provides all security guarantees that are enforced by the enclaves, attacks that target security limitations of the Intel SGX processors are out of scope in our paper. These include Cache timing side-channel attacks [6] and Denial of Service attacks. Meanwhile, we believe orthogonal approaches [7], [8] that mitigate such threats can be applied to our solution.

With guidances of our user-friendly user interface, our work protects Data Owners against data requests that may violate user privacy. We believe this is the most likely threat against ordinary IoT users as we envision complexity of IoT system to increase in the future. Our ultimate goal is to provide concise yet accurate information to users such that they make intended and autonomous decisions.

V. Challenges

There exists several challenges to implement our solution for the project.

1) simulating different parties like DR and DS (potentially simulating IoT applications as well)
2) preparing Intel SGX hardware
3) designing user interface is a hard task
4) Challenges related to user research for app interface: The challenges related to conducting a user research for the mobile app is two fold.
First, we are building an interface for which the backend is unfamiliar, and not available yet. This means that users need to know more background information about the interface for which we seek feedback. In particular, most of the IoT systems that exist now are centralized, and provides coarse-grained permissioning. By contrast, the system that we are targeting is distributed, user-centric, and fine grained in terms of third party data access permissions. Users need to know this to provide effective feedback about the interface.
Second, IoT is still in its infancy, and it's hard to find enthusiast users of IoT devices. We overcome this by treating smartphone sensors as basic IoT devices and building a story for user interaction with the application in terms of sensor data available from smartphones.

VI. 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. 2". 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. 2a), seeing and editing details pertaining

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

Fig. 2: UI mockup of the user facing application

to a particular device (Fig. 2b), receiving and acting upon data requests (Fig. 2d), 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 (Accessed Oct 24, 2017)

[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

[6] Wang, Wenhao, et al. "Leaky Cauldron on the Dark Land: Understanding Memory Side-Channel Hazards in SGX." ACM Computer and Communications Security (CCS 17), October, 2017.

[7] Yan, Mengjia, et al. 2017. "Secure Hierarchy-Aware Cache Replacement Policy (SHARP): Defending Against Cache-Based Side Channel Atacks." In Proceedings of the 44th Annual International Symposium on Computer Architecture (ISCA '17). ACM, New York, NY, USA, 347-360. DOI: https://doi.org/10.1145/3079856.3080222

[8] Rane, Ashay, et al. "Raccoon: Closing digital side-channels through obfuscated execution." In USENIX Security Symposium (2015).

[9] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

[10] (2012, Jun) "Overview of Internet of Things." ITU-T Recommendations. Available: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060 (Accessed Oct 25, 2017)

[11] (2015, Jun) "Internet of Things Market to Reach $1.7 Trillion by 2020". The Wall Street Journal. Available: https://blogs.wsj.com/cio/2015/06/02/internet-of-things-market-to-reach-1-7-trillion-by-2020-idc/ (Accessed Oct 25, 2017)

[12] Costan, Victor, et al. "Intel SGX Explained." IACR Cryptology ePrint Archive 2016 (2016): 86.