A Differential-Privacy based Framework for Preserving Privacy in Smart Homes

Mahsa Keshavarz

Advisor: Dr. Mohd Anwar

Secure and Usable Social Media & Networks (SUSMaN) Lab

Department of Computer Science, College of Engineering, North Carolina A & T State University

Email : susmanlab@gmail.com

Abstract

Smart homes are increasingly becoming popular for convenience and comfort. In smart homes, people are able to remotely control various aspects of their home environment. However, smart home appliances can pose threats to privacy. The reason is that smart appliances collect and store sensitive information, and if hackers can gain access to this information user's privacy can be breached. We propose a privacy framework to hide sensitive data and release non-sensitive data. This framework describes how we can collect data from all smart devices and separate them into two categories: sensitive and non-sensitive. The proposed framework utilizes the concept of differential privacy into the data collection and storage operations. After detecting and hiding sensitive information, the non-sensitive information can be made available for different purposes. We plan to simulate the smart home appliances to evaluate our framework for different smart home scenarios.

Background

- **Smart Home** is a dwelling incorporating a communications network that connects the key electrical appliances and services, which allows them to be remotely controlled, monitored or accessed.
- A statistic shows that in 2015 more than 60000 people search for "smart home" term per month and more than 250 companies invested in this technology.
- Homeowners want to make their homes secure, safe, and comfortable to live. These smart appliances not only provide comfort but they also provide safety inside the home.
- **Internet of Things** (IoT) is a concept to connect devices with each other and make them communicate with each other with the help of Internet and many other technologies [1].
- By 2020, the number of IoT devices is predicted to be more than 40 billion.

User Application Layer		
Kernel Layer	Agent Management	Data Transportation
	Authentication and Authorization	State Monitor
Agent Layer	Agents	
Interface Layer	Appliance Specific Service Interface	
Resource Layer (Household appliances)		

Fig1: Communication Architecture of a Smart Home [2].

- Smart homes collect data such as one's activity levels, sleeping patterns or food intake behaviors from various smart devices and share the information with health care providers or family members. However, sharing and obtaining information about a person without permission is a **violation of privacy**.
- In the context of smart home, privacy is about the controlling the content of released data.

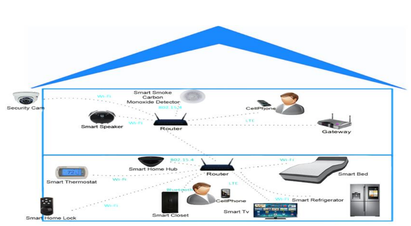


Fig 2: An Example of Smart Home Containing Different Connected Devices.

Protection of Privacy

- Our goal is to protect sensitive information of users.
- Our focus is on the privacy aspect of a smart home, where it is important to protect information about intimacies, feeling matters, physical condition and visual information such as images or video from strangers including attackers.
- These days, due to the fact of using Internet, protecting privacy is more challenging than it was in the past.
- In a survey (n = 92), 80% of respondents indicated that they care a lot about their information privacy.

How Can the Privacy be Compromised?

- Analyzing of the user behavior and activities.
- Disclosure of Personally Identifiable Information (PII). PII is any data that could release some information about a user that helps us to identify a specific individual.

Traditional Approaches for privacy protection:

- One way to protect data from hacking is deidentified that dataset.
  - There is no balance between privacy and utility.
    - Attackers can still reidentify users with enough background information. .
    - Researchers do not make many datasets available due to privacy violation.
- The other solution is using Differential Privacy.
  - Differential privacy is a technique that can be used to remove sensitive information and release non-sensitive ones [3].

Implementing Differential Privacy (DP) in Smart Home

- DP helps to minimize the chances of revealing personally identifiable information about the users and violating the users' privacy.
- Wide access to statistical information about a dataset is provided without worries of leaking of individual information. This means we provide both privacy and utility by using DP.
- If we want to change any one individual's data in dataset, the distribution of output does not change a lot.
- Differential privacy offers two parameters delta and epsilon for controlling and measuring changes in output. The smaller they are, the more privacy we can provide.

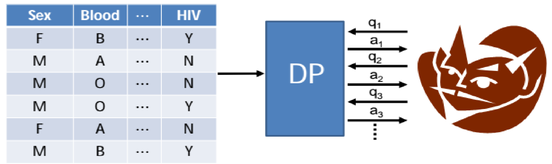
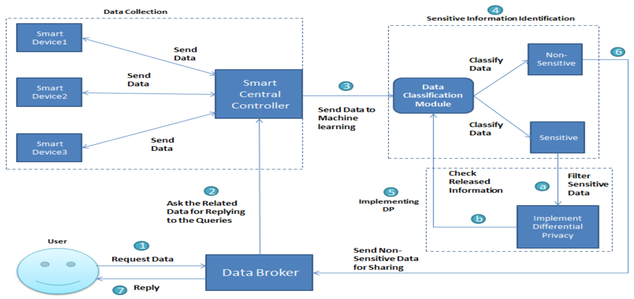


Fig. 3: Differential Privacy [4].

Accomplishment

- The framework for implementation of differential privacy model on smart home has been developed.



- **Data Request:**
  - Users ask data from data broker. Data broker analyses the requests and send the required information to smart central controller.
- **Data Collection:**
  - All of smart appliances in the smart homes send their data to smart central controller.
  - Smart central controller collects all information from all these appliances and stores all data.
- **Sensitive information identification:**
  - Smart devices collect sensitive data about users that might be dangerous.

Table 1: Sensitive Information

Device	Information	Sensitive/ Non-Sensitive
Gate Reminder	• Use RFID system to detect the users' objects. • Use a mixture of a speaker and a face identifier, and a RFID system to identify users.	Sensitive (PII) Personal Characteristics
Smart Bed	• Connects with Fitbits, Nest Thermostats. • sensors track heart rate, breathing and movement	Sensitive (PII) Medical Information
Smart Laundry	• In combination with the smart closet, future RFID-based technology will notify residents when to do laundry as well as help sort it.	None-sensitive
Smart Mat	• Body weight and footprint of the user.	Sensitive(PII) Personal Characteristics and Weight
Smart Refrigerator	• Food habit	None-sensitive
Smart Thermostat	• It has a small wireless sensor that keeps the heat on until it senses that room has warmed up enough. • By using its motion sensor it can understand when occupants leave the home or go to sleep.	Sensitive (PII) Geographical Indicators
Smart Dressing table	• Light information	Non-sensitive

- Sometimes there is a possibility of privacy violation due to the linking of multiple information sources, also known as linking attack.

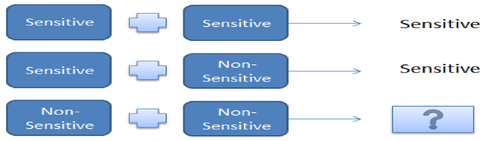


Fig 6: Data Classification Module

- We propose to employ machine learning (ML) algorithm for classification of data.

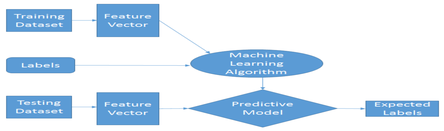


Fig 5: Composition of Information

- **Implement differential privacy mechanisms**:
  - We will use differential privacy to hide the sensitive information and release insensitive one.

Future Work

- We will simulate the smart home devices to evaluate our framework for different smart home scenarios.
- We will implement differential privacy in smart home environment.

References

1. Patel, A. and T.A. Champaneria. Fuzzy logic based algorithm for Context Awareness in IoT for Smart home environment. in Region 10 Conference (TENCON), 2016 IEEE. 2016. IEEE.
2. Han, D.-M. and J.-H. Lim, Smart home energy management system using IEEE 802.15. 4 and zigbee. IEEE Transactions on Consumer Electronics, 2010. **56**(3).
3. Dinur, I., & Nissim, K. (2003, June). Revealing information while preserving privacy. In Proceedings of the twenty-second ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems (pp. 202-210). ACM
4. Harvard University Privacy Tools Project. (n.d.). Retrieved April 21, 2014, from http://privacytools.seas.harvard.edu/differential-privacy