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

Mahsa Keshavarz
Mohd Anwar
North Carolina A&T State University
Problem

• Smart appliances in smart homes collect information about user.

• Sharing and obtaining information about a user might cause **privacy violation**.
<table>
<thead>
<tr>
<th>Device</th>
<th>Information</th>
<th>Sensitive/Non-Sensitive</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Smart Bed</strong></td>
<td>• Connects with Fitbits, Nest Thermostats.</td>
<td>Sensitive (PII) Medical Information</td>
</tr>
<tr>
<td></td>
<td>• sensors track heart rate, breathing and movement</td>
<td></td>
</tr>
<tr>
<td><strong>Smart Mat</strong></td>
<td>• Body weight and footprint of the user.</td>
<td>Sensitive (PII) Personal Characteristics and Weight</td>
</tr>
<tr>
<td><strong>Smart Thermostat</strong></td>
<td>• It has a small wireless sensor that keeps the heat on until it senses that room has warmed up enough</td>
<td>Sensitive (PII) Geographical Indicators</td>
</tr>
<tr>
<td></td>
<td>• By using its motion sensor it can understand when occupants leave the home or go to sleep.</td>
<td></td>
</tr>
</tbody>
</table>
Differential Privacy (DP)

- Differential privacy is a technique that we can use to remove sensitive information and release non-sensitive ones.
Differential Privacy (DP) Mechanism

X (with Bob)

Y (without Bob)

Output Perturbation

Queries

User

A(X)

A(Y)

Answers

Answers
Proposed Framework

Data Collection

1. User Request Data
2. Ask the Related Data for Replying to the Queries
3. Send Data to Machine Learning

Sensitive Information Identification

4. Classify Data
5. Check Released Information
6. Implement Differential Privacy

Implementing DP

Send Non-Sensitive Data for Sharing

User Request Data

Data Broker

Smart Central Controller

Send Data

Smart Device 1

Smart Device 2

Smart Device 3