Title :

Privacy Risk Model (PRiMo) for SAHOMASI Lab

Full name of Speaker :

Anizah Abu Bakar*
Manmeet Mahinderjit Singh*
Azizul Rahman Mohd Shariff*
Prof Yuto Lim**

Institution :

Universiti Sains Malaysia (USM)*
Japan Advanced Institute of Science and Technology (JAIST)**

Contact : (email address)

anizah@student.usm.my (Anizah Abu Bakar)
manmeet@usm.my (Manmeet Mahinderjit Singh)
azizulrahman@usm.my (Azizul Rahman Mohd Shariff)
ylim@jaist.ac.jp (Prof Yuto Lim)

Project Title:

Background :

- As Malaysia is preparing itself in terms of social through its healthcare services and infrastructure to tackle the nation's aging society by 2030, the need to prepare our household with technology capable of tackling context changes is a must.

- It is believed that Malaysia will have nearly equal share of the young (18.6%) and older population (14.5%) in 2040. By this time, there will be three older persons for every 20 population.

- Due to the fact a current smart home was designed without any standardize communication, the adoption of smart home would be hard to be made accessible by elderly in Malaysia.

- The idea of designing a proof of concept with adopting an ECHONET Lite communication protocol, which is designed in JAPAN in 2007 is seen as an answer for a better standardization.

- We have designed a SAHOMASI (Smart Home with Ambient Intelligence using MEMS Sensors) Lab for the abovementioned purposes.

- SAHOMASI lab established in School of Computer Science, Universiti Sains Malaysia, Pulau Pinang, Malaysia is using ECHONET-Lite technology from JAIST, Japan in a newly-designed Smart Home lab known as SAHOMASI Lab which is an IoT-based Smart Home platform infrastructure with ECHONET-Lite middleware that interconnects home appliances, devices, people, systems and information resources together to improve the well-being of the elderly and disabled community.

Project Title:

Background :




- The pictures above are spaces and some of the appliances in the SAHOMASI Lab. The first picture from the left is the living room space, followed by kitchen space, fall detection wearable device, and kettle fitted with FSR Sensor.
- One major issue for any IoT-based system is the exposure of user data through application usage.
- Similarly for our SAHOMASI lab, the exposure of home occupants in term of the data accessed via SAHOMASI applications need to be secured and protected as this behavior exposes user towards privacy risk.

Targets:

- To design and illustrate the proposed mathematical model using tree structure.
- To propose a mathematical model designed using privacy calculus solution that will preserve the privacy of users in smartphone environment.

Proposed Method:

- The methods or techniques used to develop a mathematical model that quantify the privacy risk of smartphone user are graph theory knowledge and privacy calculus solution.
- In terms of graph theory knowledge, a tree structure is constructed to use as a clarification in developing the proposed model.
- The overall tree structure of privacy risk of user in a smartphone usage is shown in Figure 1.
- The tree structure is divided into 3 layers which is category of mobile application, permission levels and the related sensor data types and personal data types.
- L^1_i and L^2_j are denoted for the permission level types and sensor or personal data types level accordingly while w is the weight of the particular data size.

Proposed Method:

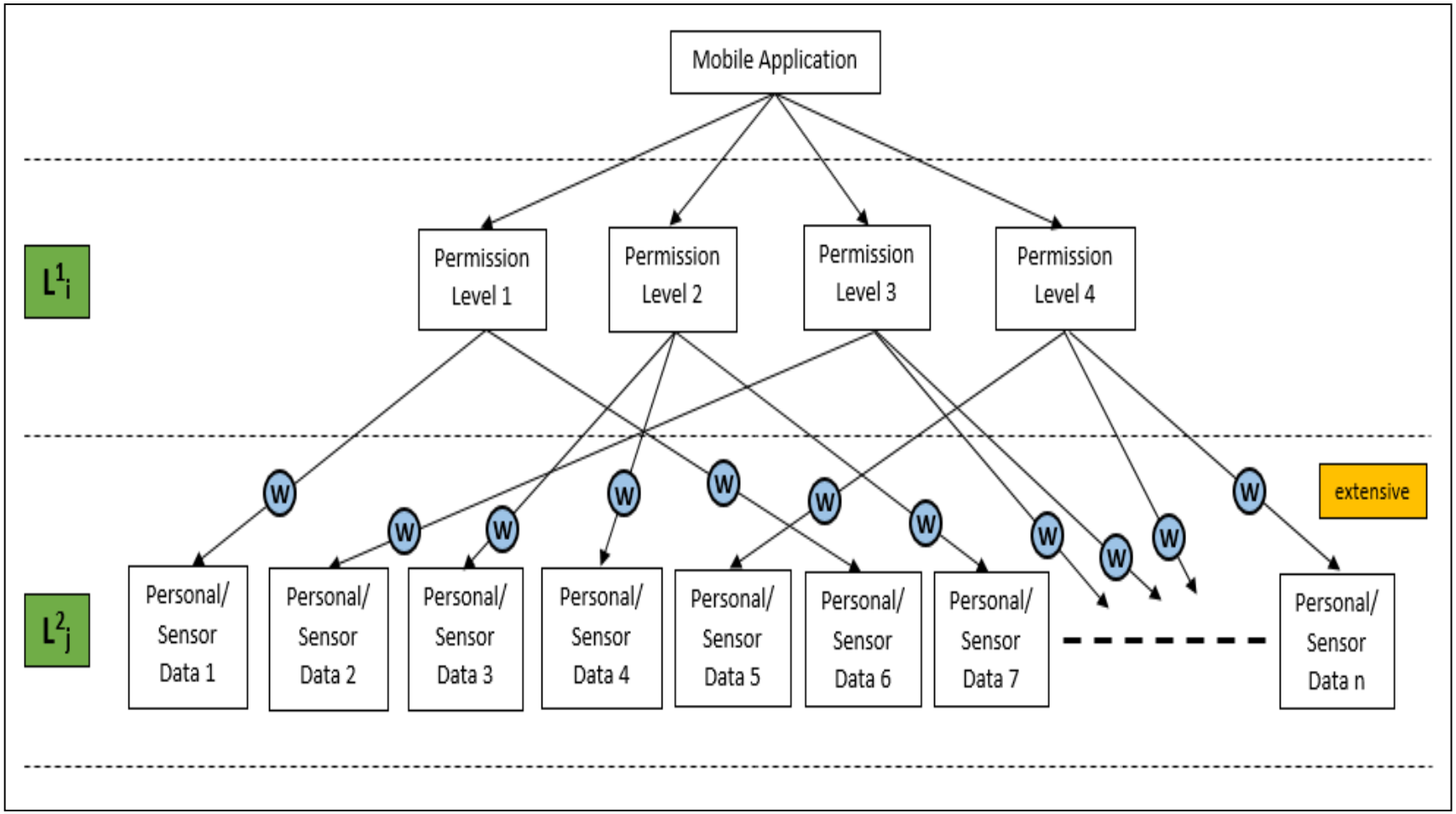


Figure 1 : Tree structure of privacy risk if user in smartphone environment

Proposed Method:

- The next method is privacy calculus solution, which is used in developing the mathematical model to quantify the privacy risk of a user in smartphone usage.

- The steps of developing the proposed model are as follows:

1. The risk in mobile application is denoted using R_A.
2. The notation used in L^1_i to denote the permission levels in mobile application is p_i where i = 0.25, 0.5, 0.75, and 1 accordingly.
3. The number of data bits generated from the sensors (sensor data types and personal data types) have weight, w and the weight are further denoted as w_j.
4. The total number of data bits generated from all the sensors is denoted as Σw_j where Σw_j is calculated using the formula shown below:

$$\Sigma w_j = w_1 + w_2 + w_3 + \ldots + w_n$$

5. The risk model is constructed as follows :

$$R_A = p_i \left(\frac{wn}{w1 + w2 + w3 + \ldots + wn} \right)$$

6. The final model is as follows :

$$R_A = p_i \left(\frac{wj}{\sum_{j=1}^{n} wj} \right)$$

Impact:

❖ The impacts of developing the proposed model are as follows :

1. The knowledge of graph theory is applied in developing the mathematical model.

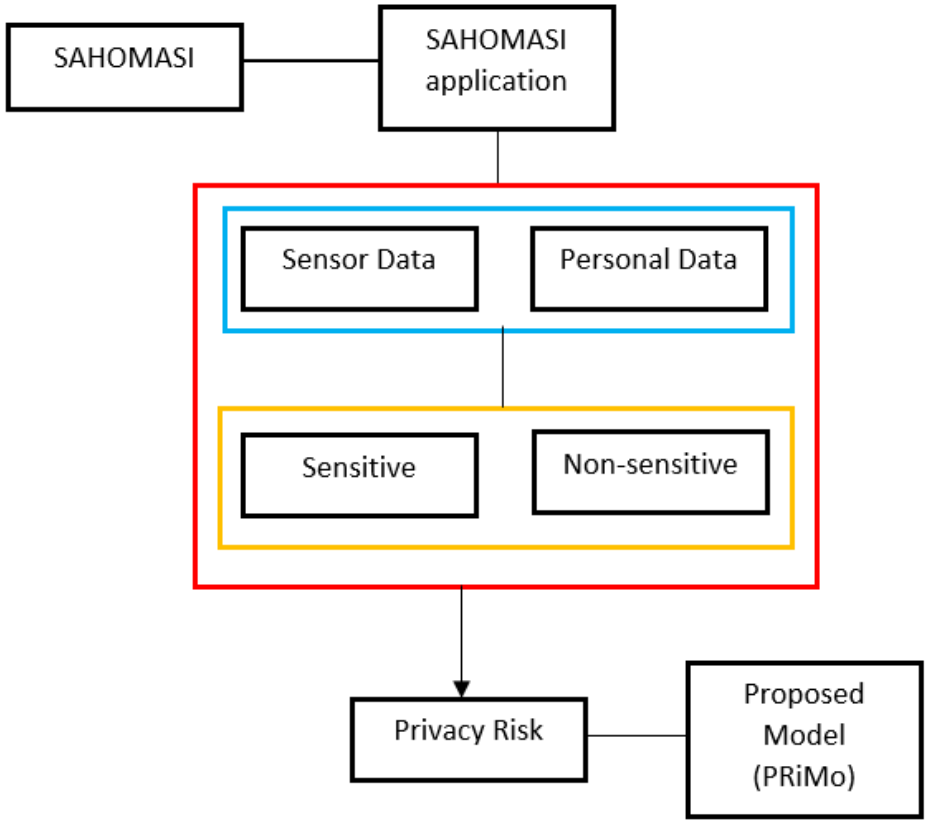
2. The proposed mathematical model is able to quantify the privacy risk of a smartphone user in smartphone usage.

3. The data of elderly or any users of smart home can be preserved and protected.

4. By using the model, users are able to realize and evaluate themselves to which level of risk they belong.

5. The usage behavior of users can be portrayed in order to create awareness about the risk that might be faced by them.

Output/Outcome:



- The figure above portrays how the proposed model used in SAHOMASI to aid in the preservation of users' data thus protects the privacy of users.

Output/Outcome:

❖ The figure is further explained as follows :

- SAHOMASI runs SAHOMASI application.
- The application collects two types of data which are sensor data and personal data.
- These data are either sensitive or non-sensitive. It may consist of private and confidential information of users.
- Thus, it will lead to privacy risk.
- The privacy risk of SAHOMASI user can be quantified using the proposed model, PRiMo to show the level of risk they are facing.

❖ The outcomes of the proposed method are as follows:

1. A novel mathematical model to quantify the privacy risk of users in smartphone usage is proposed and developed.

2. A collaboration between Universiti Sains Malaysia (USM), Penang, Malaysia and Japan Advanced Institute of Science and Technology is made.

Conclusion:

❖ The targets of this research are :

1. To design and illustrate the proposed mathematical model using tree structure.

2. To formalize and propose a mathematical model designed using privacy calculus solution that will preserve the privacy of users in smartphone environment.

❖ The methods used in developing the proposed method are :

1. Graph theory knowledge (tree structure)

2. Privacy calculus solution (mathematical model).

❖ The impacts are :

1. A novel mathematical model is proposed

2. It benefits the elderly or any smart homes users by preserving their privacy.