e-ISJN: A4372-3114
p-ISJN: A4372-3115

ISSN: 2321-7782 (Online)
ISSN: 2347-1778 (Print)
Impact Factor: 7.327

Volume 7, Issue 5, May 2019

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Intrusion Detection and Prevention in Smart Home Using Logical Sensing

Rohit S. Ragmahale[1]
Department of Computer Engineering
D Y Patil College of Engineering, Ambi
Pune – India

Prof. Dhanshree Kulkarni[2]
Department of Computer Engineering
D Y Patil College of Engineering, Ambi
Pune – India

Abstract: ***Since last 4-5 decades the concept of home automation has been there. Peoples expectations regarding home automation and security has changed a to large extent during the course of time due to the advancement of technology and services. Different automation systems over the time tried to provide efficient convenient and safe way for home inhabitants to access their homes. Irrespective of the change in user expectations, advancement of technology, or change of time, the role of a home automation system has remained the same. This paper explains various security issues in current home automation system and proposes an algorithm based on logical-sensing to improve home security. Depending on the usage of home, system classified home access points into primary and secondary access points. This logic based sensing algorithm is developed to identify abnormal behaviour of an user, also this system considers the states of various access points. Goal is to develop smart, cost-efficient, collaborative, robust smart lock. System is using Arduino, ESP8266, proximity sensors, motion sensors and other to identify user behaviour at secondary access points and implement the logic based sensing algorithm. This whole system will act as distributed lock working in sync with primary access points lock in order to have more robust and smart locking system. This System is cost-efficient as there are smart sensors which are placed smartly at secondary access points from where intrusion may occur.***

Keywords: ***Internet of Things (IoT), Home automation, smart homes, Sensor Data.***

I. INTRODUCTION

Researchers have been experimenting and improving the concept of smart home since the late 1970s. As technology advanced with time, electronic devices and internet became more popular and affordable, so the concept of home automation and peoples expectation from a smart home has changed dramatically. Modern smart home is a sophisticated combination of various Ubiquitous Computing Devices and Wireless Sensor/Actor Networks. All these new user expectations, complicated electronics and unpredictable user behaviour brought new security challenges to the home automation front. The concept of home automation security has also evolved with time, sensors and actuators were integrated into the home to detect, alert and prevent intrusions. In the past, an average home had to deal with common slash and grab criminals, while a modern home has to deal with sophisticated and tech savvy attackers who know how to find vulnerabilities and manipulate the security devices to gain access or cause distress to the inhabitants. Despite smart home security being critical there are some vulnerabilities in the existing systems.

Over the years researchers demonstrated various security issues associated with the devices and technology used in modern smart homes. The wireless sensor networks deployed in modern smart homes for device to device communication is vulnerable to various Routing and Wormhole attacks. All these factors contributed to the rapid rise in home burglaries over the past decade and demonstrates the importance of Home Security in the modern world. Our previous works in smart home security explains

the changing role of modern home security systems and defines the role of a modern home automation system as, one capable of identifying, alerting and preventing intrusion attempts in a home at the same time preserving evidence of the intrusion or attempted intrusion so that the perpetuator or perpetuators can be identified and prosecuted. Intrusion detection functions include:

- Observing and analysing both user and system behaviours.
- Analysing system configurations and vulnerabilities
- Patterns recognition for certain type of attacks
- Analysing abnormal activity patterns
- Tracking user policy violations

A. *Novelty*

Ideal way to improve home security and defend against intrusion is to recognize a homes inhabitants and identify their position inside a home at all times without inconveniencing its inhabitants. This is extremely challenging and complex, given the unpredictable nature of human behaviour and home being occupied by guests and other trusted people. Identifying access points to a home and regulating access to them is the next logical step towards securing a home. Normal user behaviour at access points to a home adhere to a set of predictable behaviours. These user behaviours when analysed by our novel logical sensing algorithms can differentiate between normal and attack behaviours. Existing systems are able to secure the primary access point of the home (i.e. Door) but windows, balcony are always vulnerable to intrusion. To improve smart home security by using smart logical sensing mechanism at secondary access points which is integrated with smart lock of primary access point of a home.

B. *Goals and Objective*

- To identify primary and secondary access points in a home based on how they are used. Detect all user actions at these access points.
- To detect and analyse user actions and behaviour after change in state of an access point.
- To identify insecure secondary access point and alert user regarding the same.
- To identify and isolate attack behaviour by analysing the user behaviour at various access points using our logical sensing algorithm. Trigger warning or raise alarms depending on the situation.
- To perform trajectory mining using sensor data to trans- formation from uncertain to deterministic trajectory data.

II. REVIEW OF LITERATURE

Now a days IoT research has grown exponentially, smart home security has improved to next level. Still there are many challenges in system:

A. *From Homeowner's Point of View*

- In many cases, money is motivation or the bottom line for the common homeowner when choosing different home automation products. People are either not aware, misinformed, or do not care enough about several security risks.
- People in home are always of different backgrounds mostly they are non technical, different age groups, guest may come to home and homeowner can not expect all these people will be careful about security mechanism in home.

- Portable devices like mobile phones, laptops uses home network and these devices goes with user wherever they go and gets connected to different networks. Attacker could make use of these devices as a gateway to home when user again connects to home network.
- There can be a case when guest may feel insulted when access gets denied to guest due to restricted access to few people. Owner has to do some change in settings to allow guests.
- There is a big difference between what user thinks is implemented of access control and the security mechanism that are actually implemented.

B. From Security Engineer's Point of View

- Unlike in companies, one can't enforce policies or security procedures that affect the convenience of people at home or their guests.
- People are careless about even simple security policies.
- Home may consist of people of different age groups e.g. Senior citizens which are not cable of understanding the technical aspect of the security system is more vulnerable to social engineering.
- An attacker who hacks a home automation network can cause a wide range of damage, including theft, vandalism, emotional harm, permanent damage to electronic devices, loss of reputation, financial damages, blackmail, environmental damages, physical harm to a homes inhabitant, granting unauthorized access to anyone.
- The mixed ownership of devices at home and guests with varying technical knowledge and different intentions compounds security issues at home.

V. Bellotti and K. Edwards, In their essay has presented a framework for designing context-aware systems that are both intelligible to their users and support the accountability of other users and the system itself. From their proposed principles, people begin to envision a set of requirements for systems designed to support context-aware computing. This is particularly true in cases where inferences about user behavior or desire are separated from the applications with the domain knowledge necessary to situate such inferences.

Alheraish discussed a home automation security system us- ing Short Messaging Service (SMS). The unauthorized access into the home is identified by monitoring the state of the home door using LED and IR sensors. He proposed system that allows legitimate users to control home lights and set the 4 digit passkey using SMS. The LED and IR sensors used to identify intrusions could easily be spoofed by a sophisticated attacker. Informing the user about an intrusion via SMS is not a good practice, as the user may not be near to the phone to receive the alert on time.

In system designed by Arun, the device fingerprint along with username/password based security proposed that enables the verification of user as well as the device used to access the home, which significantly improves home security when they are accessed over the internet. Unlike any previous approaches to device fingerprinting, thay use geolocation data in their algorithm which improves the fingerprint accuracy.

Yurur et al. proposed that context aware sensing vary depending upon user environment, prior knowledge of recent event patterns, user perception and context. Advanced sensing techniques and high processing power makes context aware sensing an expensive proposition for smart homes. In addition, during context aware computing the system handles very intimate and private information about a user and his habits, which has to be shared for the concept to be implemented successfully, this raises serious privacy issues.

Yuchen Yang and team has presented the security and privacy issues in IoT applications and systems. They pre- sented the

limitations of IoT devices in battery and computing resources, and dis- cussed possible solutions for battery life extension and lightweight computing.

1) *Battery Life Extension:*

   a) Use Minimum Security mechanism

   b) Increase battery capacity

   c) Harvest energy from natural resource.

2) *Lightweight Computation:*

   a) In one line, conventional cryptography can not work on IoT system.

III. System Architecture/System Overview

IoT can be considered as a worldwide physical inter- connected network, in which things can be connected and controlled remotely. As more and more devices are equipped with Motion or intelligent sensors, connecting things becomes much easier.

IoT aims to connect different things over the networks. As a key technology in integrating heterogeneous systems or devices, service-oriented architecture (SOA) can be applied to support IoT.

The architectural design of IoT is concerned with architecture styles, networking and communication, smart objects, Web services and applications, business models and corresponding process, cooperative data processing, security, etc. From the technology perspective, the design of an IoT architecture needs to consider extensibility, scalability, modularity, and interoperability among heterogeneous devices.

As things might move or need real time interaction with their environment, an adaptive architecture is needed to help devices dynamically interact with other things. The decentralized and heterogeneous nature of IoT requires that the architecture provides IoT efficient event-driven capability. Thus, SOA is considered a good approach to achieve interoperability between heterogeneous devices in a multitude of way

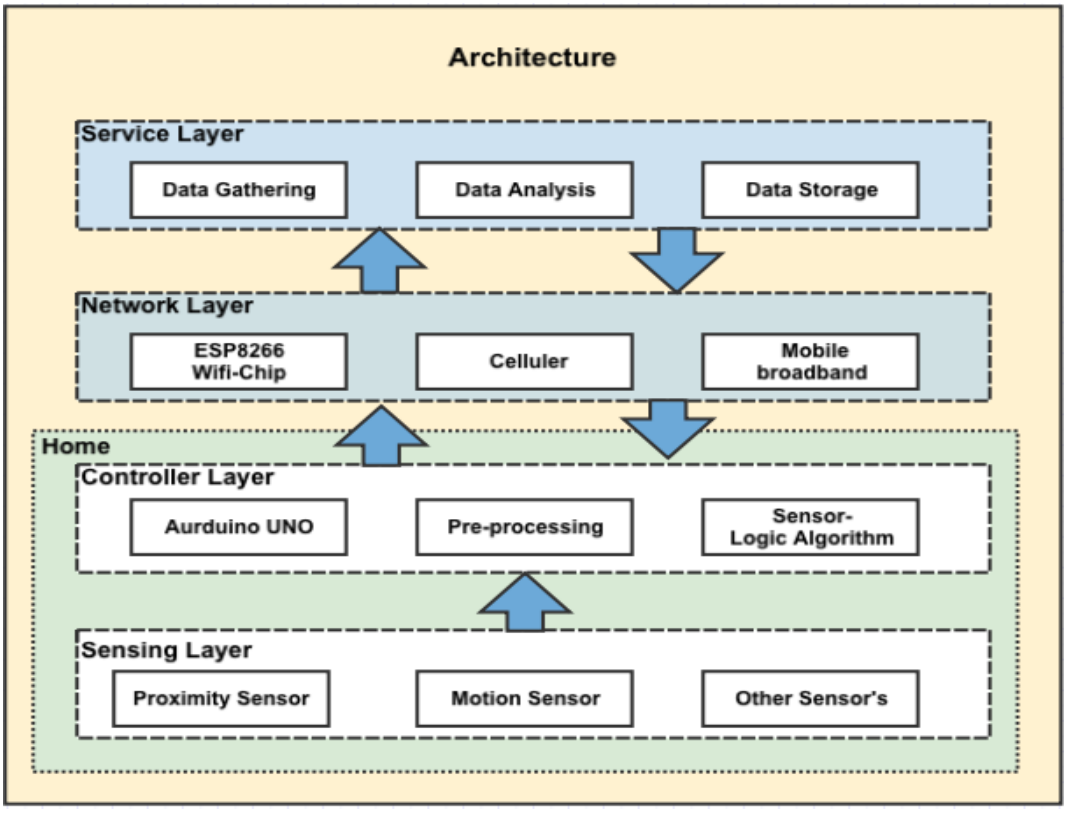

Fig. 1 SOA for Smart Home Security System

1) Sensing Layer: In the sensing layer, the wireless smart systems with tags or sensors are able to automatically sense and exchange information among different devices. These technology advances significantly improve the capability of IoT to sense and identify things or environment.

2) Controller Layer: In the controller layer, different sensors are controlled by micro-controller e.g. Arduino. Controller processes/compare the sensor data to make certain decisions locally and sends data over network to server. It accepts data from server and set the device state accordingly.

3) Networking Layer: The role of networking layer is to connect all things together and allow things to share the information with other connected things. In addition, the networking layer is capable of aggregating information from existing IT infrastructures (e.g. business systems, transportation systems, power grids, health-care systems, ICT systems, etc.). Services provided by things are typically deployed in a heterogeneous network and all related things are brought into the service Internet.

4) Service layer: Service layer relies on the middle-ware technology that provides functionalities to seamlessly integrate services and applications in IoT. The middleware technology provides the IoT with a cost-efficient platform, where the hardware and software plat- forms can be reused. A main activity in the service layer involves the service specifications for middle- ware, which are being developed by various organizations.

IV. System Analysis

System analyses various access points in a home to identify different improbable scenarios within a smart home during its operation. Access points are inherent in the structure of a home, which can be used for entering and exiting a home. In a typical home these natural access points are front door, back door, balcony doors and windows. Even though window is not a normal access point it can be used as one, most likely by an intruder depending on the situation. Physical access to a home is only possible through these access points unless serious structural alterations are made to a home. These serious structural alterations can not be made without drawing attention to the act itself, like blasting or destroying a wall to create an entrance. So, managing access at these access points is crucial in securing a home.

Based on the purpose of the access points, the system classifies access points into primary and secondary. In a home, when an access point is used by its inhabitants as a primary means to enter and exit from their home, it is categorized as primary access point like the front door, back door etc. On the other hand, secondary access points like the window, balcony door etc. also provide entry/exit to a home but they are rarely used for that purpose because there are other convenient ways in and out of a home for a legitimate user.

1. *Intrusion Prevention Algorithm*

Front door is the primary access point to any home, inhabitants use this door as the main way in and out of their home. Depending upon the architecture and inhabitant needs, there can be one or more primary access points. Whenever a home changes state from occupied to empty the algorithm checks if the secondary access points to the home are secure. If not, it issues a warning to the user to secure the secondary access points.

Fig. 2 shows the flowchart of the secondary access point checking when the home becomes empty. In this way, using simple mechanism user can do intrusion prevention.

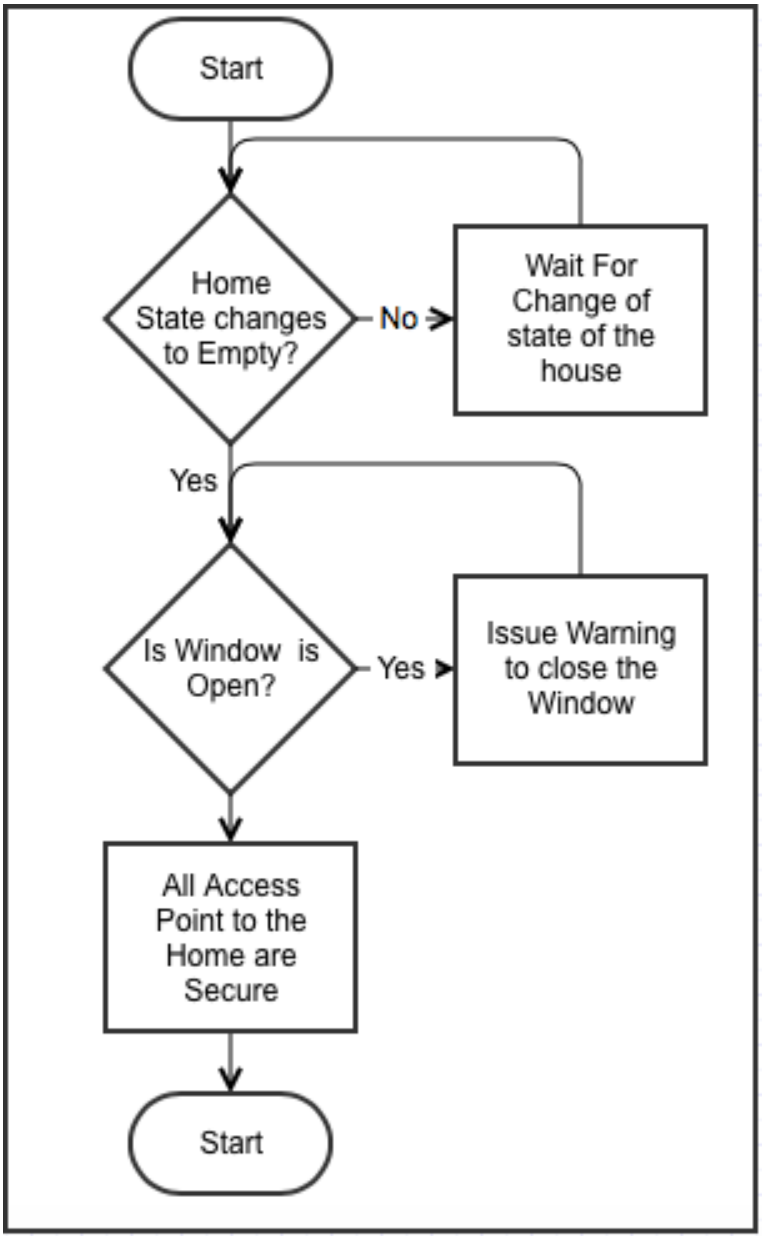

Fig. 2 Intrusion Prevention Algorithm

2. *Intrusion Detection Algorithm*

The balcony door and window form the secondary access points in a home. In a typical home, the window is not used as the main access point to and from a home. Usually window opens into a relatively secure and private area, sometimes even a few floors up. So, these window can remain open for long periods of time when the house is occupied. When the home becomes empty an observant, resourceful and proficient intruder can use this window to gain access to the home, in order to avoid that, window must be closed when the home becomes empty. Moreover, when the home is empty the window should not be opened under any circumstances.

After the initial state change the algorithm keeps observing the window for a specific interval of time called window observation time; the window state during this time is called intermediate state of the window. Fig. 3 shows the flowchart intrusion detection at the secondary access point. The algorithm observes the motion and proximity sensor values during the window observation time to identify user actions at an access point.

This system proposes the use of motion and proximity sensors to detect user behaviour at secondary access points. The motion and proximity sensors placed near the secondary access point i.e. window inside the home are triggered before the window is opened. When user opens a window from inside and goes away motion proximity sensor will be triggered before and

after the window state change. When someone enters an empty home using window, they are entering from outside so, the motion and proximity sensors will not be triggered before the window is opened. Once the window is opened and the user enters the home the motion and proximity sensors placed inside the home will be triggered. The algorithm keeps monitoring the state of the window, so in an empty home when the window door is opened from outside the system triggers intrusion detection mechanisms. The system detects user actions at secondary access points in a home using different sensors. These detected user actions and behaviours are compared with normal user behaviour at various access points to identify intrusions or intrusion attempts. Access point data is stored in a data base on cloud platform with access limited to authorized personals. This paper proposed cost-effective, Simple-to-use, Lower- maintenance, Easily adaptable security system to secure secondary access points of smart home.

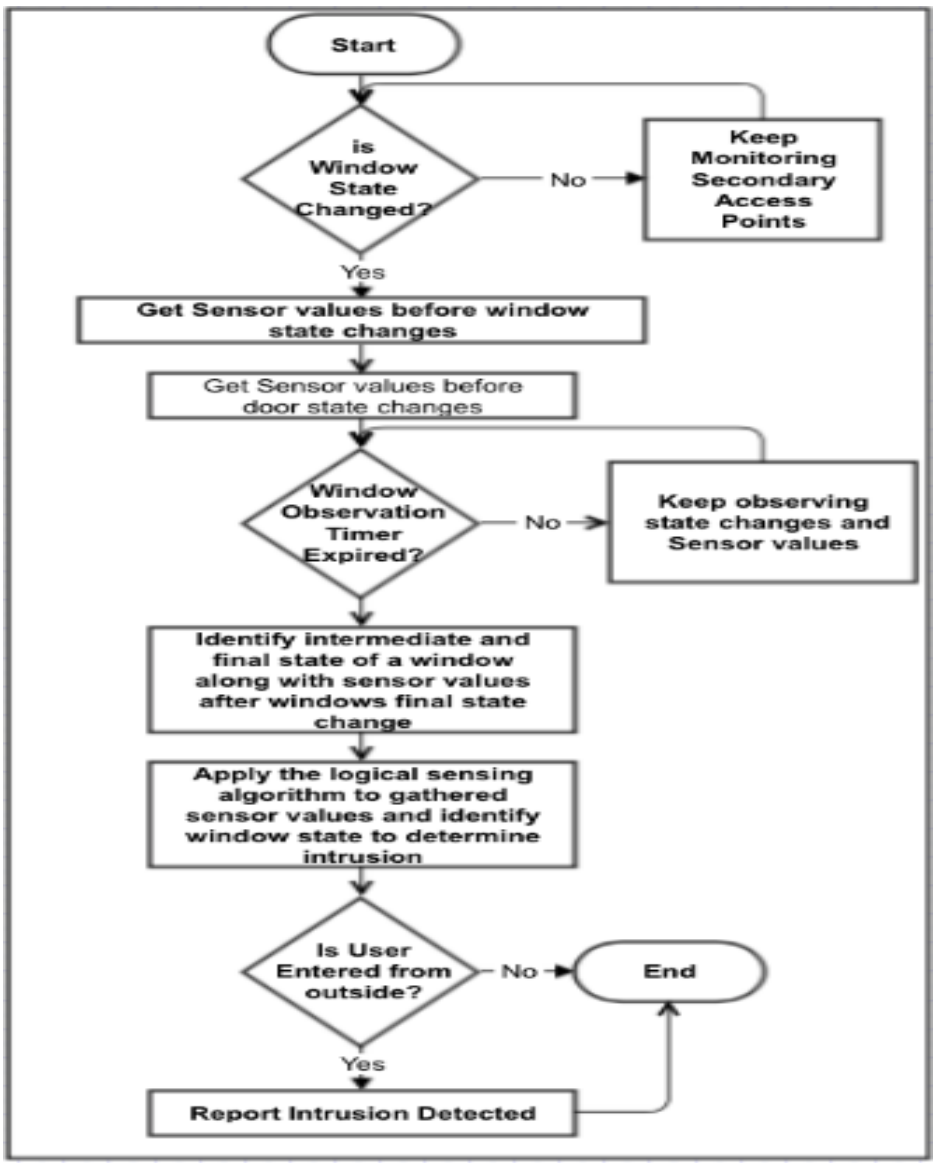

Fig. 3 Intrusion Detection Algorithm

State No	Initial State -> Intermediate State	Final State	Motion Sensor Trigger Before	Motion Sensor Trigger After	Proximity Sensor Trigger Before	Proximity Sensor Trigger After	Intrusion Detected
1	C => O	O	Y	Y	Y	Y	NO
2	C => O	O	N	Y	N	Y	Intrusion
3	C => O	O	N	N	N	N	NO
4	C => O	C	Y	N	Y	N	NO
5	C => O	C	N	N	N	N	NO
6	C => O	C	Y	Y	Y	Y	NO
7	O => C	C	Y	Y	Y	Y	NO
8	O => C	C	Y	N	Y	N	NO
9	O => C	C	N	N	N	N	NO
10	O => C	O	N	N	N	N	NO
11	O => C	O	Y	N	Y	N	NO
12	O => C	O	Y	Y	Y	Y	NO
13	C => O	O	Y	N	Y	N	NO
14	O => C	C	N	Y	N	Y	Intrusion
15	C => O	C	N	Y	N	Y	Intrusion
16	O => C	O	N	Y	N	Y	Intrusion
17	O => O	O	Y	Y	Y	Y	NO
18	O => O	O	N	Y	N	Y	Intrusion

Fig. 4 State Chart

V. Conclusion

The system detects user actions at secondary access points in a home using different sensors. These detected user actions and behaviours are compared with normal user behaviour at various access points to identify intrusions or intrusion attempts. Access point data is stored in a data base on cloud platform with access limited to authorized personals. This paper proposed cost-effective, Simple-to-use, Lower- maintenance, Easily adaptable security system to secure secondary access points of smart home.

Acknowledgement

I wish to thank all the people who gave us an unending support right from the idea was conceived. I express my sincere and profound thanks to my Guide Prof Dhanshree S. Kulkarni for their guidance and motivation for completing my work, and I am also thankful to all those who directly or indirectly guided and helped me in preparation of this paper.

References

1. Li Da Xu, Senior Member, IEEE, Wu He, and Shancang Li, Internet of Things in Industries: A Survey, IEEE TRANSACTIONS ON INDUS- TRIAL INFORMATICS, VOL. 10, NO. 4, NOVEMBER 2014
2. ArunCyrilJose1andRezaMalekian2,SmartHomeAutomationSecurity: A Literature Review Human-Comput. Smart Computing Review, vol. 5, no. 4, August 2015
3. N. Komninos, Member, IEEE, E. Philippou and A. Pitsillides, Senior Member, IEEE, Survey in Smart Grid and Smart Home Security: Issues, Challenges and Counter- measures, IEEE COMMUNICATION SUR- VEYS TUTORIALS, VOL. 16, NO. 4, FOURTH QUARTER 2014.
4. A.Alheraish,Design and implementation of home automation sys- tem,IEEETrans. Consum. Electron., vol. 50, no. 4, pp. 10871092, Nov. 2004
5. ARUN CYRIL JOSE1, REZA MALEKIAN1, (MEMBER, IEEE), AND NING YE, Improving Home Automation Security; Integrating Device Fingerprinting Into Smart Home IEEE Access, August 29, 2016
6. V. Bellotti and K. Edwards, Intelligibility and accountability: Human considerations in context aware systems, Human-Comput. Interaction, vol. 16, no. 2, pp. 193212, Dec. 2001

7. O. Yurur, C. H. Liu, and W. Moreno, A survey of context-aware middleware designs for human activity recognition, IEEE Commun. Mag., vol. 52, no. 6, pp. 2431, Jun. 2014
8. S. Saponara and T. Bacchillone, Network architecture, security issues, and hardware implementation of a home area network for smart grid, J. Comput. Netw. Commun., vol. 12, Nov. 2012, Art. no. 534512
9. Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao, A Survey on Security and Privacy Issues in Internet-of-Things IEEE INTERNET OF THINGS JOURNAL, VOL. 4, NO. 5, OCTOBER 2017
10. A. Z. Alkar and U. Buhur, An Internet based wireless home automation system for multifunctional devices, IEEE Trans. Consum. Electron., vol. 51, no. 4, pp. 11691174, Nov. 2005.
11. UNODC International Burglary, Car Theft and Housebreaking Statistics

