A SMART MONITORING SYSTEM FOR HOME APPLIANCES USING SENSORS

[1]Prabhu K
[1]Assistant professor
[1] Department of Information Technology
[1]Sri Ramakrishna Institute of Technology, Coimbatore, India.

Abstract : This paper explains various security issues in the existing home automation systems and proposes the use of logic based security algorithms to improve home security. The work classifies natural access points to a home as primary and secondary access points depending on their use. Logic based sensing is implemented by identifying normal user behavior at these access points and requesting user verification when necessary. User position is also considered when various access points changed states. Moreover, the algorithm also verifies the legitimacy of a fire alarm by measuring the change in temperature, humidity and carbon monoxide levels, thus defending against manipulative attackers. The experiment conducted in this paper used a combination of sensors, microcontrollers, Raspberry Pi and ZigBee communication to identify user behavior at various access points and implement the logical sensing algorithm. In the experiment the proposed logical sensing algorithm was successfully implemented for a month in a studio apartment.

IndexTerms **- Home automation, Smart homes, Wireless sensor networks, Access control, ZigBee.**

I. INTRODUCTION

Using energy efficiently in smart homes saves money, enhances sustainability and reduces carbon footprint at large. Consequently, the need for smart energy management is on the rise for smart homes for smart cities in general. However, the lack of low cost, easy to deploy, and low maintenance technology has somewhat limited a large-scale deployment of such system. The sheer quantity of data collected throughout different cities of a country presents multiple challenges in data storage, organization, and analysis. Internet of Things (IoT) technology and Big Data are natural candidates to address these challenges. IoT technologies can provide a ubiquitous computing platform to sense, monitor and control the household appliances energy consumption on a large scale. This data is collected using many different wireless sensors installed in residential units. The data can be monitored, collected and analyzed using predictive analysis and advanced methods to actionable information in the form of reports, graphs and charts. Thus, this analyzed data in real time can aid home owners, utilities and utility eco-systems providers to gain significant insights on energy consumption of smart homes. The energy service providers can use the power consumption data available with analytics engine to provide flexible and on-demand supply with appropriate energy marketing strategies. The consumers, being aware of their consumption behavior and having a close interaction with the electricity utilities, can adjust and optimize their power consumption and reduce their electricity bills. In order to have an effective cost saving system, it is important to monitor and control the operation of residential loads depending on the aggregate power consumption over desired period, the peak power consumption, the effect of weather/atmospheric conditions and consumption slab rates. This is where the combination of IoT technology, Big Data analytics and BI comes into play for implementing energy management solutions on a local and national scale. Finally, as an additional advantage, the use of IoT also enables seamless remote access control of home devices where the customers get online access to the ON/OFF usage pattern of in home appliances via a personal computer or a mobile phone.

II. INTERNET OF THINGS

The process of controlling or operating various equipment, machinery, industrial processes, and other applications using various control systems and also with less or no human intervention is termed as automation. There are various types of automation based on the application they can be categorized as home automation, industrial automation, autonomous automation, building automation, etc. Home automation is the process of controlling home appliances automatically using various control system techniques. The electrical and electronic appliances in the home such as fan, lights, outdoor lights, fire alarm, kitchen timer, etc., can be controlled using various control techniques. There are various techniques to control home appliances such as IOT based home automation over the cloud, home automation under WiFi through android apps from any smart phone, Arduino based home automation, home automation by Android application based remote control, home automation using digital control, RF based home automation system and touch screen based home automation.

III. BIG DATA

The sensors, IoT, devices, and actuators in the smart grid keep generating data for carrying out functions related to operation, monitoring, control, audit, QoS, billing, etc. For having an effective operation & management of smart grid, Big data sources, monitoring and control system, data collection agents, robust ICT infrastructure and ubiquitous computing platforms play a central role. Big data is used to store and retrieve the information of home automation applications.

IV. EXISTING SYSTEM

The functional requirements of the system are specified as general functional requirements and specific system requirements. The general requirements are the system's functionality and specific requirements are different business processes delivered. Non-functional requirements comprise of system's attributes such as scalability, security, privacy, etc. The proposed system's functional requirements are the SoC should gather power consumption information and the ambient condition information periodically, and send it to a centralized server. The server should parse the information and transmit the readings to a central data storage system or database. The stored data should be used by analytics engine to process it and generate reports, graphs, and charts. Clients should be able to view the generated graphs through a cross-platform mobile application. Client application interacts with the server using a lightweight architectural style Web API to facilitate communication using web services. Depending on the user privileges, the application should render different services to each user such as viewing reports, device status, and remote control of device or bill payment.

The specific functional requirements can be characterized as the business processes offered by the system. To render these requirements, six divisions of business processes are follows

- Consumption Analysis for Monitoring
- Asset Efficiency Analysis
- Root Cause Analysis
- Predictive Analysis
- Remote and Local Device Controlling
- Bill Tracking Utility

The non-functional requirements of the system demonstrate that the system is scalable, reliable, secured, maintainable, easily deployed, and remotely accessible. Scalability, Security and Privacy are the three important non-functional aspects in the proposed systems which are discussed as follows Scalability of the data is collected and analysed on a national level accommodating four different levels of stakeholders Home Owner, Community Representative, State Representative and Country Representative. Each stakeholder has its respective view of the data and services offered.

The six business processes mentioned above should be applied to each stakeholder as required. To serve these levels of clients, the system should be based on an easily scalable architecture. Security of the system is important as a minor flaw in system design can lead to catastrophic disasters. Multiple levels of security such as secured web service calls using https must be implemented to ensure protected communication of the system. Privacy of the communication between server and end devices should be private. Access control using two factor authentication and proper encryption techniques should be utilized to prevent illegitimate users from prying over the data.

V. PROPOSED SYSTEM

In this paper, we analyzed 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 cannot 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. The paper proposes that, irrespective of the number and type of access points in a home, the behavior of a legitimate user at these access points can be broken down in to a set of possible events which can be predicted. Based on the purpose of the access points, the paper 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.

VI.HARDWARE AND EXPERIMENT SETUP

The proposed access monitoring and control mechanism at home is implemented using Raspberry Pi 3 which has 4× ARM Cortex-A53 processor operating at 1.2GHz, Broadcom Video Core IV graphics processor, 1GB LPDDR2 (900 MHz) built in RAM, one 10/100 Mbps Ethernet port, 2.4GHz 802.11n built in wireless adapter and a 32GB class 10 micro Secure Digital (SD) Card as the hard disk storage. The Pi works on a Raspbian Operating System (OS) optimized for Raspberry Pi.

The OS is burned on to the SD card from a laptop which is then inserted into the Pi. The algorithms are implemented using Java as the programming platform and MySQL as the database. Java 7 JDK (Java Development Kit) and MySQL are installed in the Raspberry Pi from Debian repositories using the APT (Advanced Packaging Tool) commands with root user permissions. At the access point Arduino Uno microcontroller with ATmega328P IC is used to gather data. Arduino Uno module has fourteen digital input/output pins (6 of which can be used as Pulse Width Modulation (PWM) outputs), six analog inputs, a USB connector port, a 16 MHz ceramic resonator, a power jack, an In-Circuit Serial Programming (ICSP) header, and a reset button. Arduino is flexible and offers a variety of digital and analog pins, it can be connected to a PC using USB, and it can run in standalone mode or as an interface connected to a PC. Arduino is cost effective and is an open-source project backed up by a strong online community.

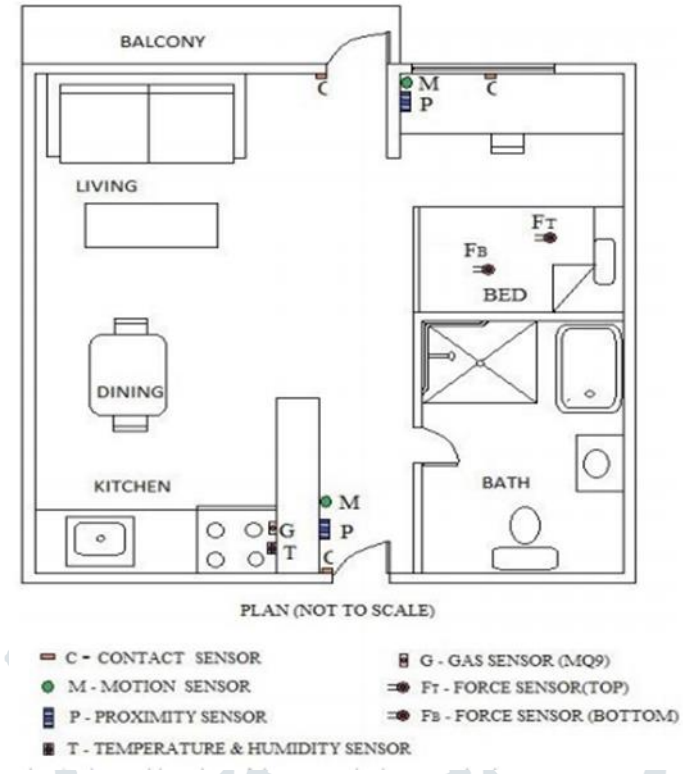

Fig.1 Implementation of Sensors in home

Each microcontroller in the experiment is connected to a PC using USB and programmed using the Arduino Interactive Development Environment (IDE). A Micro Contact/Limit Switch is used at the doors and windows to sense the state of doors and windows. Adjustable Passive Infrared (PIR) Motion Sensors and HC-SR04 ultrasonic range sensors capable of noncontact measurement from 2 cm to 400 cm are used to identify user activities inside the home near an access point.

Fig .2 Sensors, board and microcontroller deployment at Primary Access Point

Every living thing with temperature above absolute zero emits heat energy in the form of radiation this may be invisible to the naked eye but can be detected by PIR sensors. The PIR sensors implemented here has a field of view less than 180 degree.

Fig .3 Board one installation at Primary Access Point

VII. RESULTS AND DISCUSSION

The algorithm generated 14 warnings, 8 regarding the open primary access point, 3 for not securing the secondary access point before leaving the home and another 3 warnings for opening the balcony door during day when the bed was occupied. Intruder alarm was triggered 5 times during the experiment, 4 were related to primary access points while one was related to secondary access points. IVM was triggered 59 times and user successfully verified his identity 55 times. Alarm was killed using the 12 character password five times. The state change timer was activated 23 times while the user re-entered the home before the state change timer expired 15 times, so the home state changed due to state change timer expiry 8 times. The graph in Fig. 6 shows the number of state changes for primary access point, total number of warnings generated, IVM triggers, number of user identity verifications and number of alarms generated. Fig.4 shows the number of state triggers for frequently triggered states namely State 1, 4, 6, 9, 13, 17, 19 and 31.

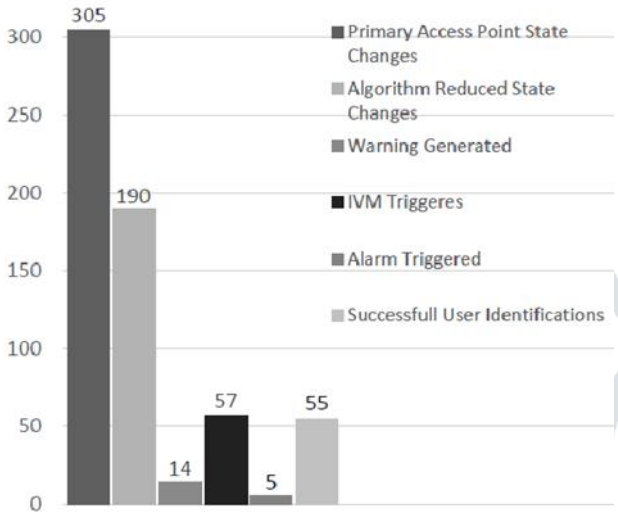

Fig.4 Graph of IVM

Secondary access points changed states 56 times; balcony door changed state 27 times and window state was changed 29 times. All of the 27 times balcony door changed state the user was at home but 3 of them happened when the user was in bed, so these 3 times warnings were generated and IVM was activated along with the identity verification timer, which was reset when the user conformed their identity. Once the open balcony door was closed due to wind, when the user was in bed, so no identity verification mechanism was initiated.

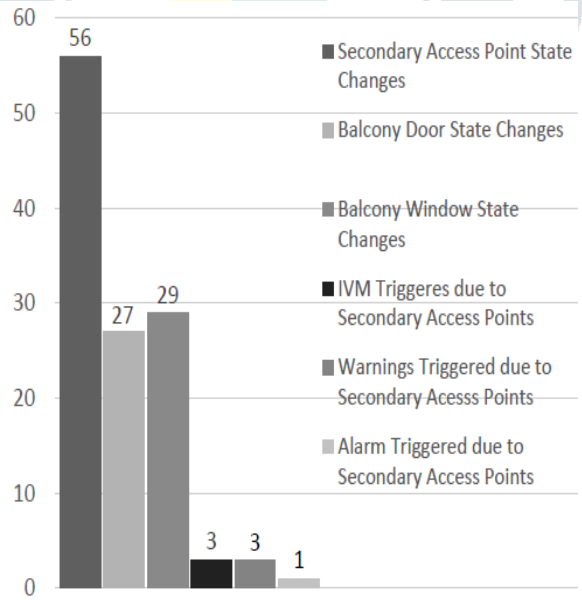

Fig.5 Graph of the secondary access point and changes in room.

The home was occupied all 29 times when the state of the balcony window was changed. Once the window was opened from the outside when the user was in bed during night; the intrusion defense mechanisms (audible alarm) were triggered without waiting for any user identity verifications. The total number of state changes for secondary access points, balcony door and window state changes, secondary access point triggered IVM, warnings and alarms generated due to secondary access points.

VIII.CONCLUSION

The proposed system detects user actions at primary and secondary access points in a home using different sensors. These detected user actions and behaviors are compared with normal user behavior at various access points to identify intrusions or intrusion attempts. In the experiment, our proposed algorithm was able to successfully identify all 305 state changes of the main access point and reduce them to 190 user behaviors while the secondary access point changed state 56 times. The alarm was triggered five times when the user failed to confirm his identity. Six of the fourteen warnings generated were regarding secondary access points while the other eight were relating to primary access point when the home became empty. In addition to identifying intrusions in home, the algorithm also warns user about imminent and live potential security vulnerabilities by identifying the status of various access points, user position and behaviors. For future works, we plan to improve user behavior prediction by analyzing various user actions inside the home to further improve smart home security.

REFERENCES

[1] Abbas javed, Hadi Larijani, Ali Ahmadinia, "Smart Random Neural Network Controller for HVAC using Cloud Computing Technology", Vol: 13, Issue: 1, 2017.

[2] C.Suh and Y.B. Ko, "Design and implementation of intelligent home control systems based on active sensor networks," IEEE Transactions on Consumer Electronics, vol. 54, no. 3, pp. 1177–1184, 2008.

[3] B.Fouladi, S. Ghanoun, "Security Evaluation of the Z-Wave Wireless Protocol," Black hat USA, Aug. 2013.

[4] Wenye Wang, Zhuo Lu, "Cyber security in the Smart Grid: Survey and challenges," Computer Networks, Volume 57, Issue 5, Pages 1344-1371, April 2013.

[5] Tianhe Gong, Haiping Huang, Ping Chen, Tao Chen, "Secure Two- party Distance Computation Protocol Based on Privacy Homomorphism and Scalar Product in Wireless Sensor Networks", Tsinghua Science and Technology, Vol.21, No.4, pp. 385-396, 2016.

[6] Y. Hu, A. Perrig, D. Johnson, "Wormhole attacks in wireless networks", IEEE Journal on Selected Areas in Communications, vol. 24, no.2, pp. 370–380, Feb. 2006.

[7] Y. Mo and B. Sinopoli Secure control against replay attacks 2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, pp. 911-918, 2009.

[8] N. Komninos, E. Philippou and A. Pitsillides, Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures in IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1933- 1954, Fourth quarter 2014.

[9] UNODC, "International Burglary, Car Theft and Housebreaking Statistics," United Nations Office on Drugs and Crime (UNODC), Technical Report, 2015.

[10] A.C Jose, R. Malekian, N. Ye, Improving Home Automation Security; Integrating Device Fingerprinting Into Smart Home, IEEE Access, vol. 4, October 2016.

[11] A.C Jose, R. Malekian, "Smart Home Automation Security: A Literature Review", Smart Computing Review, Vol. 5, No. 4, pp. 269-285, August 31, 2015.

[12] B. Schilit, N. Adams, R. Want, "Context-Aware Computing Applications," WMCSA '94 Proceedings of the 1994 First Workshop on Mobile Computing Systems and Applications, pp. 85-90, 1994.

[13] Jonghwa Choi, Dongkyoo Shin and Dongil Shin, Research and implementation of the context aware middleware for controlling home appliances IEEE Transactions on Consumer Electronics, vol. 51, no. 1, pp. 301-306, Feb. 2005.

[16] O. Yurur, C. H. Liu and W. Moreno, A survey of context-aware middleware designs for human activity recognition IEEE Communications Magazine, vol. 52, no. 6, pp. 24-31, June 2014.

[17] S.R. Das, S. Chita, N. Peterson, B. Shirazi, "home automation and Security for Mobile Devices," IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), pp. 141-146, 2011.

[18] Tianhe Gong, Haiping Huang, Ping Chen, Tao Chen, "Secure Two- party Distance Computation Protocol Based on Privacy Homomorphism and Scalar Product in Wireless Sensor Networks", Tsinghua Science and Technology, Vol.21, No.4, pp. 385-396, 2016.

[19] Z. Alkar, U. Buhur, "An Internet Based Wireless Home Automation System for Multifunctional Devices", IEEE Transactions on Consumer Electronics, vol. 51, no. 4, pp.1169-1174, Nov. 2005.

[20] A. De Santis, A. G. Gaggia, U. Vaccaro, Bounds on entropy in a guessing game, IEEE Transactions on Information Theory, Vol. 47, Issue. 1, pp. 468 - 473, Jan 2001.

[21] D.C. Feldmeier, P.R. Karn, UNIX Password Security - Ten Years Later, Lecture Notes in Computer Science, Vol. 435, pp 44-63, 1990.

[22] E.I Tatli, Cracking More Password Hashes With Patterns, IEEE Transactions on Information Forensics and Security, Vol. 10, Issue. 8, pp. 1656 - 1665, April 2015.

[23] S.R. Das, S. Chita, N. Peterson, B. Shirazi, "home automation and Security for Mobile Devices," IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), pp. 141-146, 2011.

[24] S. Saha, "Consideration Points: Detecting Cross-Site Scripting", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

[25] M.R Faghani, U.T Nguyen, A Study of XSS Worm Propagation and Detection Mechanisms in Online Social Networks IEEE Transactions on Information Forensics and Security, Vol. 8 (11). pp. 1815 - 1826, 2013.

[26] K. Atukorala, D. Wijekoon, M. Tharugasini, I. Perera, C. Silva, "SmartEye - Integrated solution to home automation, security and monitoring through mobile phones," Third International Conference on Next Generation Mobile Applications, Services and Technologies, NGMAST '09, pp. 64-69, Sep. 2009.