Reinforcing Smart Home Security System

Jennifer D[#1], Loshiga M[*2], Sowndharya Lakshmi R[#3], Vidhyalakshmi.M [#4]

[#1]*Assistant Professor & Computer Science and Engineering & Panimalar Engineering College Chennai, Tamilnadu, India*

[*234]*B.E Student & Computer Science and Engineering & Panimalar Engineering College Chennai, Tamilnadu, India*

Abstract: *With advancement of latest technology, life is getting simpler and easier in all aspects. In today's world Automatic systems are being preferred over manual system. With the rapid increase in the number of users of internet over the past decade has made Internet a part and parcel of life, and IoT is the latest and emerging internet technology. Internet of things is a growing network of everyday object- from industrial machine to consumer goods that can share information and complete tasks while you are busy with other activities. Nowadays the idea of smart home has been so prevalent; it can be viewed as intelligent or automated home where the house can be monitored remotely. This paper describes about the development of home security system based on human motion detection and remotely monitoring the home. In this proposed method fingerprint and face recognition based home security, automation and also monitoring system using arm 11 processor. This project implement to all the home members fingerprint and face images are stored in database, So easily identify the authorized user or not in this system. And also sensors are used to monitor the home status. If any unknown person is detected to receive the unknown person image to the android application.*

Keywords — *Home automation; Smart homes; Wireless sensor networks; Access control; Raspberry Pi.*

I. INTRODUCTION

A smart home security system connects to your home Wi-Fi network so you can monitor and control your devices using your Smartphone and an app. Entry-level systems typically include a couple of door and window sensors, a motion detector, and a hub that communicates with these devices using one or more wireless protocols such as Wi-Fi, or a proprietary mesh network. You can add extra door, motion, and window sensors to provide coverage for your entire house and build a comprehensive system that includes door locks, garage door openers, indoor and outdoor surveillance cameras, lights, sirens, smoke/CO detectors, water sensors, and more. Any smart security system worth its salt offers components that work together in a seamless environment and can be manipulated using customized rules. For example, you can create rules to have the lights turn on when motion is detected, have your doors unlock when a smoke alarm goes off, and have a camera begin recording when a sensor is triggered. Some systems store recorded video locally on an SD card or a solid state drive, while others offer cloud storage.

II. LITERATURE SURVEY

A. Bluetooth-based Home Automation System

Issues of using Bluetooth for home automation: Bluetooth has a maximum communication range of 100m in ideal conditions. More may be needed in a home environment. Bluetooth communication has comparatively high power consumption, so the batteries of devices need to be frequently recharged or replaced. Bluetooth technology has advanced and improved to Bluetooth Low Energy (BTLE), which provides the same range of communication. However, it has serious security concerns such as eavesdropping and weak encryption as discussed by M. Ryan Bluetooth communication should only be used on occasions where there is a need for quick short-lived network communication with little concern for security. Bluetooth looks like an attractive communication technology for creating smart homes. It is cheap, easy, and quick to set up. People are already familiar with the technology. The hardware required for establishing.Bluetooth communication is readily available. And the technology also provides the necessary bandwidth for the operation in a home. But they also have serious flaws, as discussed above.

B. GSM or Mobile-based Home Automation System

Mobile-based home automation is attractive to researchers because of the popularity of mobile phones and GSM technology. We mainly consider three options for communication in GSM, namely SMS-based home automation, GPRS-based home automation, and Dual Tone Multi Frequency (DTMF)-based home automation. Each of these three technologies is discussed below, along with their shortcomings.

III.PROPOSED

In this paper, we analysed 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.

A. Primary Access Point

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. This paper proposes the use of motion and proximity sensors to detect user behavior at primary access points. When a user leaves an occupied home, the motion and proximity sensors placed near the access point inside the home are triggered before the door is opened. Once the user stepped out and closes the door the motion and proximity sensors will not be triggered. When someone enters an empty home, they are entering from outside so, the motion and proximity sensors will not be triggered before the door is opened. Once the door is opened and the user enters the home the motion and proximity sensors placed inside the home will be triggered. Fig. 1 shows the shows the flowchart of the door state changes and sensor operations of the primary access point.

B. Secondary Access Points

The balcony door and windows form the secondary access points in a home. In a typical home, the balcony door is not used as the main access point to and from a home. Usually balcony door opens into a relatively secure and private area, sometimes even a few floors up. So, these balcony doors 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 door to gain access to the home, in order to avoid that, balcony doors must be closed when the home becomes empty. Moreover, when the home is empty the balcony door should not be opened under any circumstances. The algorithm keeps monitoring the state of the balcony door, so in an empty home when the balcony door is opened the system triggers intrusion defense mechanisms without waiting for any identity verifications.

C. Fire Alarm

The work of B. Fouladi [2] discussed the weakness in the existing smart home architecture and demonstrated how an attacker will compromise various networked elements in a home. The easiest way to get the inhabitants out of a home is to trigger an emergency alarm like the fire alarm. When a fire alarm is triggered all the automatic locks of a home are disabled. During home fire the carbon monoxide and the ambient temperature levels in the area of the fire will go up and inversely the humidity in and around the area will go down. If there is no change in humidity, temperature or carbon monoxide levels, the algorithm warns the user about a possible attack attempt which the user can verify.

Each twelve second average of the temperature, humidity and carbon monoxide sensor readings are compared to detect fire.

IV.EXPERIMENTAL 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 VideoCore 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.

Figure 1 shows the structure of our proposed system. In this project is implemented in smart home security and automation using ARM11 processor. PIR and vibration sensors are placed to the front of the door this is used to sensing the motion of the human, if any motion is detected fingerprint sensor and camera is enabled to the microprocessor. Fingerprint was authenticated or unauthenticated suddenly taking the picture and send to the mobile app then closing the camera. At the same time camera is detecting the face fingerprint sensor is closed and recognize the face or not suddenly taking the picture and send to the mobile app. If any one is authenticated magnetic door is unlocked. At the same time sensors are collecting temperature, lpg gas is present or not, if gas is present AC loads are

turning to off. Vibration sensor is used to if any one persor try to break the door or not whendoor is breaked suddenly camera is captured to the image and send to the mobile application.

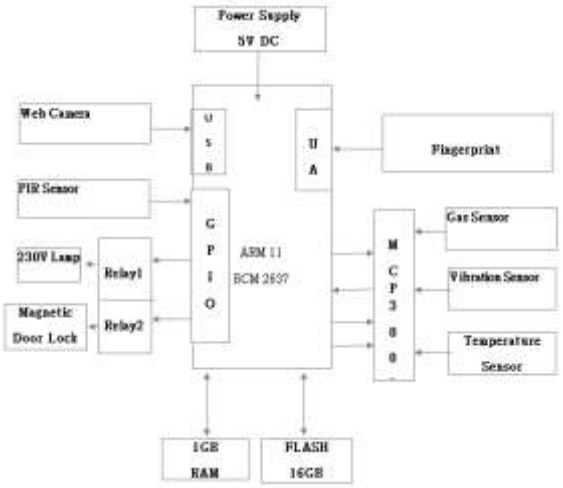

Fig.1.Block Diagram

V. EXPERIMENTAL RESULT AND ANALYSIS

During the one month period the main access point changed state 305 times. The algorithm was able to detect all these and reduce them to 190 state changes by identifying and eliminating the intermediate state changes mentioned in Table I. The most common state triggered was state 4 in Table I, it was triggered 46 times. While state 17 was triggered 33 times making it the second most popular. State 13 was triggered 20 times making it the third most triggered state. State 6 and state 1 were triggered 12 and 11 times respectively. State 31 happened 6 times, State 19 was triggered 13 times, States 9 and 16 were triggered five times; states 7, 14, and 15 were triggered four times; states 5, 11, 20, 22 and 26 were triggered thrice; states 2, 8 and 12 were triggered twice; states 3, 10, 18, 21, 27 and 32 were triggered only once during the one month time period. States 23, 24, 25, 28, 29 and 30 were not triggered during the one month time period.

States 1 to 16 occurred when the home was occupied. The most common state triggered was state 4, which happened when the home was occupied and user opened a closed primary access point from the inside triggering the motion and proximity sensors and stepped out of the home and closed the door behind him. State 4 is usually triggered when the user leaves the home. After the door was closed the algorithm waited for 15 seconds for any intermediate state changes and since door remained closed, it changed the state of the home to empty. State 1 is triggered when the user opened the home from the inside triggering the motion and proximity sensors and came back into the home leaving the door open again triggering the sensors. State 7 happened when the user closed the open door from the inside and came back into the home, motion and proximity sensors are triggered before the initial state and after the final state.

VI. CONCLUSION

The paper detects user actions at primary and 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. 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 behaviours 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 behaviours. For future works, we plan to improve user behaviour prediction by analysing various user actions inside the home to further improve smart home security.

REFERENCES (SIZE 10 & BOLD)

[1] 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.

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

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

[4] 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, Fourthquarter 2014.

[5] C. Karlof, D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures”, Ad Hoc Networks, vol. 1, pp. 293–315, 2003.

[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] D. Deadman, “Forecasting residential burglary,” International Journal of Forecasting, vol. 19, no. 4, pp. 567–578, 2003.

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