Home Automation Security System with IoT and Embedded System

Khyati Baghel[1], Deepak Sharma[2]
[1,2]*Chhatrapati Shivaji Institute of Technology, Durg, Chhattisgarh, India*

***Abstract*— The paper explains the importance of accessing modern smart homes over the IOT and embedded system and highlights various security issues associated with it. Home automation allows us to control household appliances like lighting, door locks, heating, fan, air conditioning etc. It also provides home security and emergency system to be activated. Home automation system not only refers to reduce human efforts but also energy efficiency and time saving. The main objective of this paper is home automation and security such as access control and alarm systems in smart door locks. When connected with the internet, home devices are an important constituent of the IoT. There are number of applications addressing home automation and monitoring involving infrared/Bluetooth or Ethernet or Wi-Fi.**

***Keywords*— Wi-Fi, biometric fingerprint device, home security.**

I. INTRODUCTION

Smart homes is an emerging concept that attracts the synergy of several areas of science and technology. A lot of research has been going on for more than a decade now in order to increase the power efficiency at the consumer level of the power management system. 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 (interference). Smart home is the term commonly used to describe a residence that integrates technology and services through home networking to enhance power efficiency and improve the quality of living. The "smart home" technology is one realization of home automation ideals using a specific set of technologies. It is a house that has highly advanced automatic systems for lighting, temperature control, security, appliances, and many other functions. Coded signals are sent through the home's wiring to switches and outlets that are programmed to operate appliances (fan, light etc.) and electronic devices in every part of the house. The smart home appears "intelligent" because its computer systems can monitor many aspects of daily living and it can also provides a remote interface to home appliances or the automation system itself, via telephone line, wireless trans-mission or the internet and android application, to provide control and monitoring via a smart phone or web browser.

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 smart homes. The wireless sensor networks deployed in modern smart homes for device to device (D2D) communication is vulnerable to various routing and wormhole attacks. Popular technologies like ZigBee and 802.15.4 used in smart homes are susceptible to Replay 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. This paper mainly focuses on the security of a home when the user is away from the place. Smart home is now becoming prevalent with the development of the Internet of things (IoT) techniques. Smart door locks offer sophisticated access control features to any home or business. Proximity sensors like Bluetooth, cellular, NFC and Wi-Fi can enable a door to unlock whenever an authorized user's smartphone approaches. Users can also remotely lock and unlock the door or share access with any number of others by using mobile apps. Keypads provide a backup with many locks but are no longer the main way to let yourself in.

II. LITERATURE SURVEY

Arun Cyril Jose, Reza Malekian and Ning Ye proposed Improving home automation security; Integrating Device Fingerprinting into Smart Home. In this paper, the work explains the evolution of Device Fingerprinting concept over time, and discusses various pitfalls in existing device fingerprinting approaches. The paper proposes a two stage verification process for smart homes, using Device Fingerprints and Login Credentials, which verifies the user device as well as the user accessing the home over the internet and device Fingerprinting algorithm considers a device's geographical location while computing its fingerprint. In which it is clear that there are well documented security issues associated with implementing just password based user authentication in the home automation scenario [1].

Arun Cyril Joseand and Reza Malekian proposed Improving Smart Home Security; Integrating Logical Sensing into Smart Home. In this paper, logic based sensing is implemented by identifying normal user behavior at these access points and user position is also considered when various access points changed states. In which, 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. The paper 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 [2].

Azfarina Jaafar, Murizah Kassim and Cik Ku Haroswati Che Ku Yahya proposed dynamic home automation security (DyHAS) alert system with laser interfaces on webpages and windows mobile using Raspberry Pi. The DyHAS is developed which comprised of lasers, lights, alarm and python programmed that interfaces with webpage and Windows 10 mobile devices. Dynamics alert are triggered according to identified parameters. It is adaptively set with lights, alarm and alert messages to home owner's mobile devices and webpage. Triggers messages are updated and data are logged and adaptive bypass security can be configured if needed. The laser beams pointer with the light dependent resistors used as sensors in this system are able to trigger the lights, piezo buzzer which is the alarm and send an alert message to the webpages and Windows 10 mobile application whenever the intruders or unauthorized person crossed the laser beam connection. The remote access features implemented in this system increased the home security level and alertness of the home owner where the home owners are able to access and customize the control panel when they are far away from their home [3].

K. Atukorala, D. Wijekoon, M. Tharugasini, I. Perera, C. Silva proposed SmartEye - Integrated solution to home automation, security and monitoring through mobile phones. In this paper SmartEye accomplishes two tasks; they are home automation and monitoring through mobile phone. Under automation it addresses turning on/off household electrical appliances such as electric bulbs, door locks etc. SmartEye uses an alerting mechanism together with security cameras to safeguard homes and also it provides an interface to monitor and control the home through mobile devices [4].

Brundha S.M.,Lakshmi P. and Santhanalakshmi S. proposed Home Automation in Client-Server Approach with User Notification along with Efficient Security Alerting system. In which a typical home automation workflow consists of 4 stages. Understanding the user environment by sensing, reporting the events to a centralized entity, centralized entity analyses and triggers the workflow. Workflow will execute and update user by any interactive channels or even exercise over a home device. The physical condition of the device can also be altered based on the user request and the home automation can be made efficient by including security factor by alerting user about an unknown person in the house. The security system alerts the user about the condition in the home by giving the notifications to the user mobile phone and a camera module is connected to the Microcontroller which captures the image of the intruder [5].

III. SYSTEM DESIGN

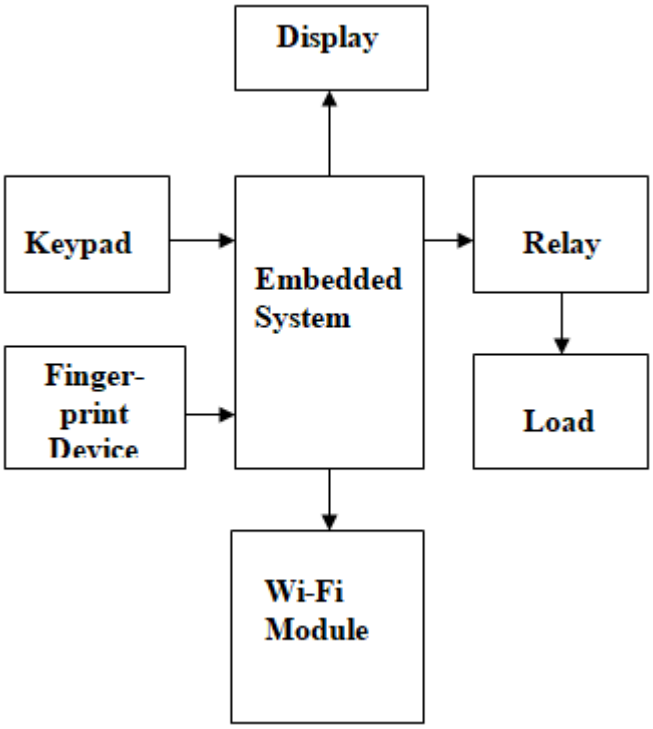

Fig. 1: Block diagram

A. Fingerprint Device

Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Biometric fingerprint reader is a scanning device on which persons of home swap their fingers for biometric identification. In order to make biometric fingerprint reader function effectively and efficiently, fingerprint of each person must be enrolled with the database. After the fingerprints are enrolled, and when a person swaps finger, the image of the fingerprint is matched with the one stored in the database. If the fingerprint matches, the biometric fingerprint reader allows access to the classified data.

B. Keypad

A keypad is a set of buttons complete with all alpha numerals and a couple of symbols. Keypads (Pinpads) for doors are either connected to a central access control system, standalone pin pads, keypads on door locks or deadbolts or IP connected pin pads but here for the purpose of time and attendance they are paired up with biometrics since PIN codes can be passed on. The lock is part of a security system, the actual lock mechanism works by needing a small electrical current to release the lock bolt. The current is generated when the proper code is entered at the keypad. For security purposes, keypad locks allow users to change the codes used to unlock them to new codes of their choosing where periodic code changes are generally encouraged as they provide added security in case someone was able to discover a previous code. The locks that are part of a larger security

system often draw their power from the security system itself, though some of these locks may use batteries as a backup power source as well.

C. Embedded system (microcontroller unit)

The control console consists of micro controller. Microcontroller is a general purpose MCU (microcontroller) with a rich set of built-in peripherals. Microcontroller is heart of the system. It has a USB host interface to connect with Android based phones. It is interfaced with relay while on the other hand it is communicating with the Wi-Fi module.

D. Relay

A relay is an electrically operated switch, typically incorporating an electromagnet to mechanically operate a switch, which is activated by a current or signal in one circuit to open or close another circuit. Relays are used where it is necessary to control a circuit by a separate low-power signal or where several circuits must be controlled by one signal. Relay is interfaced with load and embedded system through relay driver are operated based on the commands received.

E. Load

Home appliances (ON and OFF devices). An automatic lock system consists of electronic control assembly which controls the output load through a password and this output load can be a motor or a lamp or any other mechanical/electrical load.

F. Wi-Fi

Wireless fidelity technology is selected to be the network infrastructure that connects server and hardware interface modules. Wi-Fi is chosen to improve system security and to increase system mobility and scalability. Most Wi-Fi devices use 2.4GHz frequency and implement frequency division multiplexing (FDM) technology.

G. Display Unit

It is used to display the name used in storing the fingerprint information of the authorized user during the registration process and to indicate that access was granted. If access is denied, it will also be shown on display unit.

IV. OPERATION

Our work utilizes device fingerprinting and legitimate login credentials (keypad) as a part of double verification process for authorized user and their device identification. Where the authorized user swap their fingers for biometric identification. The proposed system is controlled by a microcontroller which is acts as the data repository of the system. It collects information from the sensors, makes a decision and sends SMS to a corresponding number by using a Wi-Fi module. In the pattern matching the system compares the extracted features with the stored templates, which in turns generate match score. Where secure Wi-Fi technology is used by server, and hardware interface module to communicate with each other. If it finds any interruption in its sensors then microcontroller will send a SMS to the home owner. Sensors are used to detect the intruder and they are used at doors and at windows.

V. CONCLUSION

Our prime objective is home security from intruder or unauthorized person. This paper gives basic idea of how to control home appliance (door lock) and provide a security using fingerprint device along with keypad, 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 (Wi-Fi). The user can get alerts anywhere through the Wi-Fi technology thus making the system location independent.

REFERENCES

[1]. Reza Malekian, Ning Ye Arun Cyril Jose, "Improving Home Automation Security; Integrating Device Fingerprinting into Smart Home," IEEE Access 4, pp. 5776-5787, 2016.

[2]. Arun Cyril jose and Reza Malekian, "Improving Smart Home Security; Integrating Logical Sensing into Smart Home," IEEE Sensors Journal, vol. 13, no. 17, pp. 4269-4286, 2017.

[3]. Murizah Kassim and Cik Ku Haroswati Che Ku Yahya Azfarina Jaafar, "Dynamic home automation security(DyHAS) alert system with laser interfaces on webpages and windows mobile using respberry Pi," Control and System Graduate Research Colloquium (ICSGRC), 2016 7th IEEE, pp. 153-158, 2016.

[4]. D. Wijekoon, M. Tharugasini, I. Perera, C. Silva K. Atukorala, "SmartEye - Integrated solution to home automation," , 2009, pp. 64-69.

[5]. Lakshmi P. and Santhanalakshmi S. Brundha S.M., "Home Automation in Client-Server Approach with User Notification along with Efficient Security Alerting system," in Smart Technologies For Smart Nation (SmartTechCon), 2017 International Conference On. IEEE, 2017, pp. 596-601.

[6]. Jayashri Bangali and Arvind Shaligram, "Design and Implementation of Security Systems for Smart Home based on GSM technology", International Journal of Smart Home Vol.7, No.6 (2013), pp.201-208.

[7]. Deepali Javale, Mohd. Mohsin, Shreerang Nandanwar, Mayur Shingate, "Home Automation and Security System Using Android ADK", International Journal of Electronics Communication and Computer Technology (IJECCT) Volume 3 Issue 2 (March 2013).

[8]. A. Juels RFID security and privacy: A research survey IEEE Journal on chosen areas in Computing, 24(2):381– 394, February 2006.

[9]. N. Agarwal and S. G. Nayak, "Microcontroller based home security system with remote monitoring," Special Issue of International Journal of Computer Applications", pp. 38-41, 2012.

[10]. A. Tseloni, R. Thompson, L. Grove, N. Tilley, and G. Farrell, "The effectiveness of burglary security devices", Security Journal, 2014.

[11]. Sheikh Izzal Azid and Sushil Kumar, "Analysis and Performance of a Low Cost SMS Based Home Security System", International Journal of Smart Home, vol. 5, no. 3, (2011) July.