Indian Journal of Science and Technology, *Vol 9(17), DOI: 10.17485/ijst/2016/v9i17/93039, May 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Establishing Efficient Security Scheme in Home IOT Devices through Biometric Finger Print Technique

Narayanam Sri Prakash* and N. Venkatram

Department of Electronics and Computer Engineering, KL University, Vaddeswaram, Guntur District - 522 502, Andhra Pradesh, India;
prakash.sn.10@gmail.com, venkatram@kluniversity.in

Abstract

Objective: To enhance the automation of home security through biometric recognition, Finger Print in home IOT. **Analysis:** Most of the present technologies using voice recognition technologies and the pattern of security in the home environment in which it is worked by an approved client's voice key through the confirmation procedure of Speaker Recognition and voice modulation. But this procedure may not yield optimum results when the client's speech/voice is deteriorated due to an illness or undergoing through an emotional rift. **Methodology:** Instead of using voice recognition technology in IOT of home security system, we opt for implement finger print recognition technique, which overcomes the problems of existing speech recognition techniques and also greatly reduces the cost of the hardware equipment. Implementation is to be done in Raspberry Pi along with the hardware modules viz., Wi-Fi router, Gas Sensor, Fire Sensor, Door Fringe motor sensor and evaluated our proposed methodology. **Finding/Improvements:** We implement the proposed system as a stand-alone application in Raspberry Pi2 and successful in evaluating the results which support our proposed scheme, justifying the usage of Finger Print Automation is quite efficient and economical over the usage of existing voice recognition techniques in home security automation.

Keywords: Fingerprint Module, Fire Sensor, Gas Sensor, Internet of Things, Raspberry Pi 2

1. Introduction

Internet of Things (IOT) provides direct integration of physical world to computer based systems by which efficiency and accuracy of the whole system can be enhanced. The main objective of IOT is to control the devices, vehicles, buildings that are embedded with any sensors, software and network connectivity. One of the earliest interpretations of IOT by combining all the devices with machine readable identifiers is to improve the day to day life[1]. IOT finds applications in almost all the fields as it facilitates the embedded devices with restricted memory, power and CPU resources to establish their own network. Recent developments in IOT made them responsible for not just sensing rather performing.

These advancements in IOT made it to be used in almost all the daily chores. Of these, IOT plays a crucial role in Home Automation systems. IOT home automation techniques are greatly improving the quality of daily chores in a house hold. Home IOT is integrating the usual devices required in private housing technologies. Home automation of IOT is closely related to personal life even though it falls under the industrial field[2]. It covers wide areas of communications, appliances, media and MSM, Construction fields, mobile communications, energy sector, health sector and security. This greatly enhances the overall growth of the industry. There are six components present in the home IOTs. They are as follows: Wired and wired less communications, IOT communication protocols, control devices, smart phones or other smart devices, operating systems, usually in embedded form and the actual data that is being transmitted over the devices that are present via internet and the protocols defined for the system. These components need to be combined in a specific way to achieve the necessary functionalities in the home IOTs.

**Author for correspondence*

Home IOT devices are usually classified into two types based on the communication ability of the devices. They are as follows:

One-way Home IOT devices: These devices are only used to notify the operating personnel. They cannot respond to the ascribed actions of the user.

Two-way Home IOT devices: These devices not only notify the user, but also can respond to the ascribed instructions from the user. A table depicting the examples for the two types of devices is given below.

Table 1 represents the Ways of home IOT devices and the Figure 1 represents the controlling of the Existing home security system from Remote location.

Table 1. Represents the Home IoT Devices

One-way home IOT devices	Security Alarm, electricity meter, smoke detector, gas meters
Two-way home IOT devices	Light control, Gas control,Security control, Home appliances control, Room Temperature control

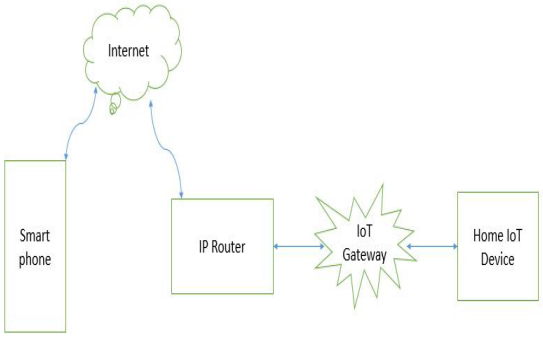

Figure 1. Depicts the existing home IOT flow of basic controls.

An operating device for the user, usually a smart phone, from which the control/manipulation commands are given by the user to the IOT devices. In between the smart phone and IOT devices the three components enabling the user intended tasks to be accomplished are: Internet, IP router and IOT gateway. Functionality of each of the components is explained below:

Internet: The control commands given as input by the user through a smart phone[3] is delivered to the IP router via the internet. In the case of home IOT, the internet is generally a broadband type provided by the ISP.

IP router: This acts as a bridge between Smart Phone devices and IOT gateway. The internet is facilitated by this router. This router is connected to IOT gateway, where the input commands from the smart phones are fed to IOT gateway.

IOT gateway: It controls all the IOT devices in the home environment. This IOT gateway based on the received command from the user, transmits the input message to the intended IOT device. In other words, IOT gateway selects the IOT device that is necessary for the task to be performed by the user, according to the given command.

2. Biometric Security Elements

There are different types of security elements employing the biometric technology in home IoT Security[4,5]. The biometric security consists of 5 types[6]. They are:

2.1 Keystroke Dynamics

It refers to identify an individual based on the rhythm of typing pattern. The basic measurements used in this technique are dwell time and flight time. The time duration to press a key is called dwell time, releasing and pressing the next key is called the flight time.

2.2 Speaker Recognition

It refers to an automated method of identifying and conforming the identity of an individual based on the voice[7,8]. The problem with this speaker recognition is anybody can imitate the actual person and breach the security.

2.3 Speech Recognition

It refers to the automated method of identifying the password[7]. The problem with this is the any-body can access the password and imitate it in the voice of the speaker, resulting in the unauthorized access.

2.4 Fingerprint Recognition

This is one of the finest biometric technologies used for the security systems[9]. The fingerprint processing includes 3 steps: Registering, search for Sinking and erase when not needed. The registration module is needed to enroll the user and then only, user can access the module. One can enroll unlimited data to access the biometric technology. If the user is trying to access the system by using the fingerprint then the system will search the data base of the particular person's fingerprint[10,11]. After searching it will give the result on the LCD display either success or failure, based on the matching with the stored finger print at the time of registration.

2.5 IRIS Recognition

The identity of a subject is done through analyzing the random pattern of the iris. The iris is the colored part of the eye. Iris recognition uses the random, colored patterns within the iris. These arrangements are unique for each individual.

The disadvantage of iris recognition is that it is very costly and it needs the perfect light intensity from beginning to the end.

2.6 Face Recognition

The face recognition uses the spatial geometry to analyze features of the face[12]. It is a technology based on computer vision that uses the face to authenticate a person[11]. The main disadvantage of the face recognition the hackers can use the mask and then lost the password.

3. Proposed Methodology

In this paper we propose a methodology for an efficient security scheme in Home IoT devices through biometric Fingerprint Technique. Figure 2 represents the proposed system.

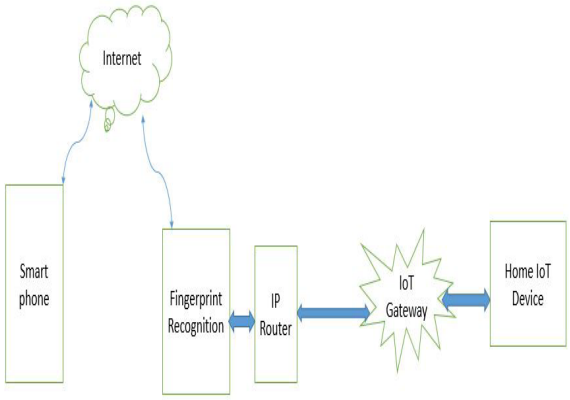

Figure 2. Explains the proposed methodology.

We extend the system explained in Figure 1 by adding the additional individual "Fingerprint Recognition Module". Whenever the user tries to access the IoT devices through IP router, the system authorizes and validates the user through fingerprint module we have added. In other words if the user fails to authorize himself through fingerprint recognition, he cannot access the IoT devices. This fingerprint module can be integrated to various IoT embedded Devices like automated Door Lock, various electronic devices and other security devices. In system implementation we have developed a biometric fingerprint security system for Door locks. From the above section, we have defined various biometric security elements, where each of the individual types have their own advantages and disadvantages.

The Reason for opting to fingerprint recognition tech among the contemporary technologies viz., Iris, Fingerprint, Face, and voice, we can observe that iris is a bit expensive, voice cannot be reliable under certain circumstances and face recognition requires balanced amount of ambient light. So obviously we are going for fingerprint recognition as our system is home security system and we cannot afford expensive devices all the time, light cannot be present in abundant in homes at nights and finally deduce that fingerprint recognition is a practical solution compare to other security systems.

Practical results obtained by implementing our system, further strengthens our argument that fingerprint recognition technology is an optimal solution among the biometric security types we have discussed in the above section.

4. System Design

The Figure 3 depicts the entire block diagram of the proposed system and all the individual components are explained in the below. And the Figure 4 depicts the flow chart of the proposed system.

4.1 Buttons

The developed system uses 3 buttons called as S1, S2 and S3. S1 belongs to the Erase, S2 Belongs to the Enroll and S3 belongs to the Search for the right one. If anyone wants to access the door, then he needs to enroll his fingerprint with the administrator. First person is administrator with the ID "0000" and the remaining persons who enrolled will be given the IDs Incrementing with 1. If a person wants to access the door then he/she hold the S3 key as far as the LCD displays "Insert Finger" then the person will give the fingerprint impression using the module. If he is the administrator, then automatically the door opens. If anybody other than the administrator i.e., valid user want to enter the room, then the hardware module will send the information to the specified mobile number by using way2sms. If the administrator is willing to open the door, then he needs to login to the IOT and then grants permission.

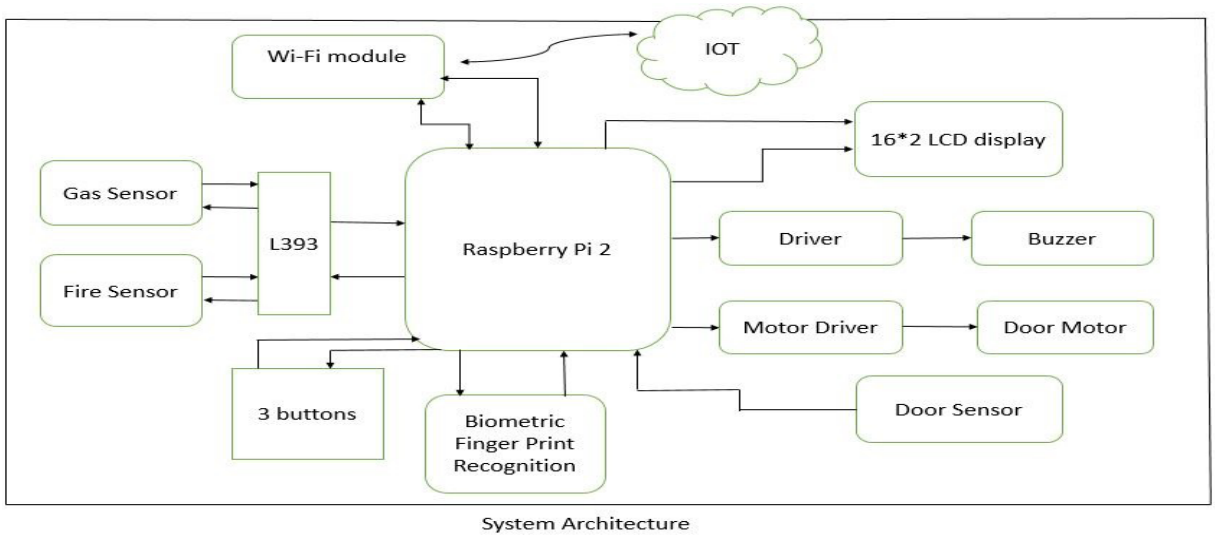

Figure 3. Represents the proposed block diagram.

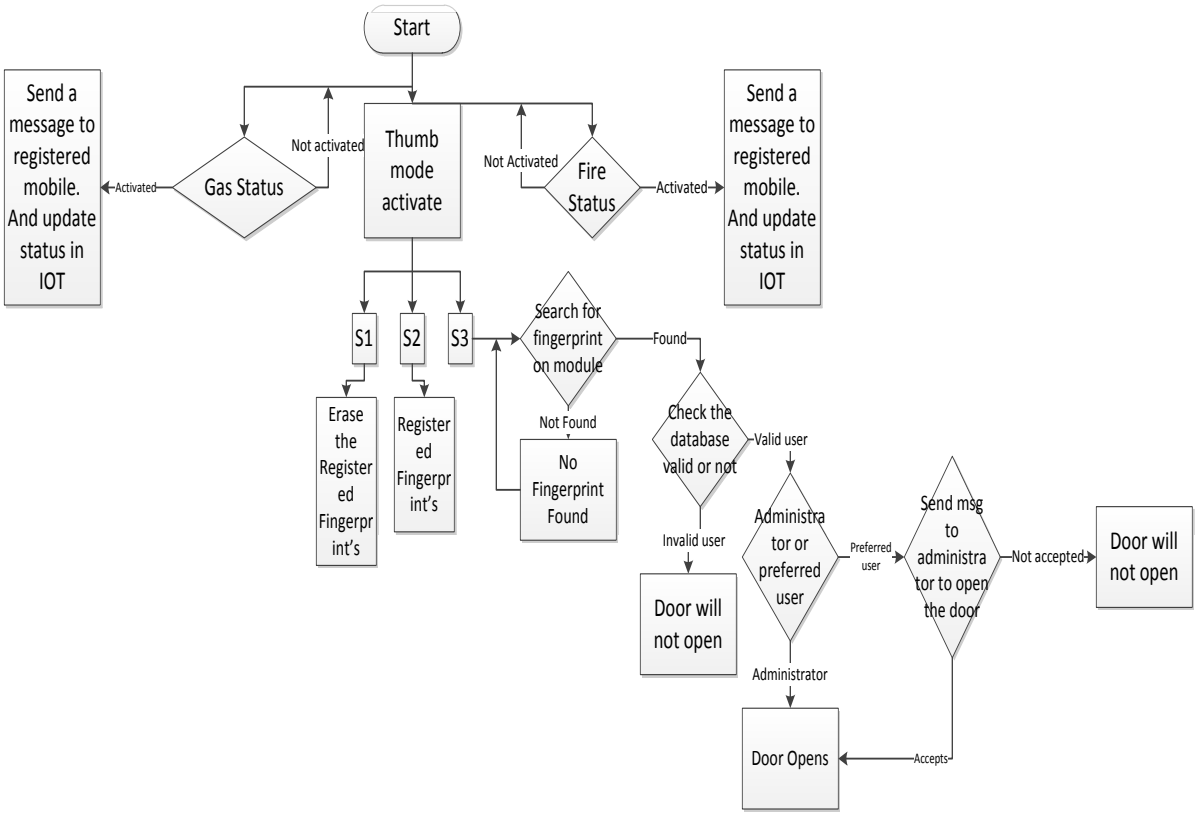

Figure 4. Represents the flow chart for the working of entire system.

4.2 Biometric Fingerprint Recognition

The biometric recognition module will store the administrator and the valid users' fingerprints[13,14]. The limit to store in a fingerprint module is 256 images. The fingerprint module will sense the image and gives the output depending on the buttons called as S1, S2 and S3. If the module senses the fingerprint then it will search the database to verify whether the image is valid or not.

4.3 LCD Display

This is connected to the controller for displaying the status of the fingerprint module. Here we are using the

4-bit mode to use the less pins in the raspberry pi 2 board.

4.4 Door Motor

The door motor is used for closing and opening the door. Here we are using a DC motor and this motor needs 12v power supply, whereas the controller can give only 5v. For that reason we are using the external 12v power supply by using driver IC called as L293D. The L293D driver will control the 2 DC motors at a time by using two H-Bridges.

In our project we will run the motor clockwise for 0.4 seconds and stop it for 2 seconds. We continue this procedure also for anticlockwise direction. It can work by receiving instructions from both the IOT and the Fingerprint module.

4.5 Magnetic Door Sensor

This sensor is connected to the doors. It shows the status of door open/close. Here we have two types of terminals. They are Switch and Magnet. The Switch features screw terminals and attaches to the frame of the door. Magnet attaches to the movable part of the window. The space between switch and magnet must be 20mm. If the space is more than the 20 mm then automatically the sensor will be activated and sends the information to mobile "Door sensor is activated, take care". Figure 5 depicts the Door sensor.

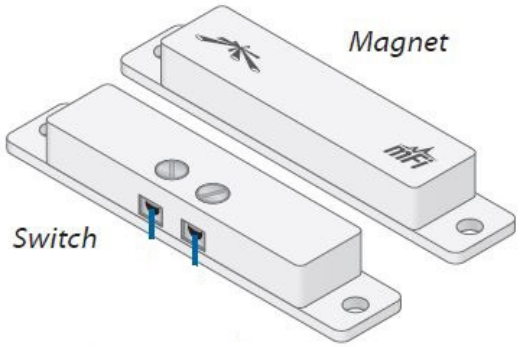

Figure 5. Depicts the door sensor.

4.6 Gas Sensor

This sensor senses the data for every pulse. If there is a gas leakage, then the sensor is activated and sends the information to the Raspberry pi 2 hardware module. This raspberry pi 2 uses the internet and sends message "Gas sensor is activated, take care", and updates the data in IOT.

4.7 Fire Sensor

This sensor also senses data for every pulse. If the Fire is detected, then the sensor is activated and sends the message to mobile, and also shows the information in the IOT.

4.8 L393 Comparator

This IC is connected to both Fire sensor and the Gas sensor. If the sensor crosses the threshold value, then the respected sensor will be activated and sends the information to the Raspberry pi2.

4.9 Buzzer

The buzzer generates a buzzing sound whenever an interrupt is occurred in the security system.

4.10 Raspberry Pi 2

The heart of the entire project is Raspberry pi 2 board. It is wallet sized CPU that plugs to monitor, Keyboard, etc[15]. The Raspberry pi 2 model B is used in this project which has more accurate processing speed than the other previous models. This raspberry pi 2 works on the basis of raspbian OS[16]. In the raspberry pi 2 we use python language for coding.

4.11 Python Language

This is a high level, object oriented scripting language. This language is similar to the C. In this programming we have two modes. They are BCM and Board. For our convenience in programming we are using the BCM mode. In this BCM mode we can directly call the Function of the pin in the Raspberry pi 2 board.

4.12 Internet of Things

This is a latest technology through which we can access the appliances from remote locations by using the internet [17,18]. Here, we need to control the door opening and closing and also we need to know about the status of the Gas and the Fire sensor.

We are using the smart living IOT application for our project. By signing up it will provide the Standard Device ID, Client Key to synchronize the data to the raspberry pi 2. After creating the sensors it will also create the specific ID'. In the Application we have gas and fire sensors as sensors

and the door as actuator i.e., to on or off. The sensors will only update the status but the actuator will allow to operate.

5. System Implementation

The Figure 6 shows the entire hardware which consists of the raspberry pi 2 board, power supply circuit, Door and Door sensor, Fingerprint module and the LCD display.

In the Figure 7 if the door status shows true then the door sensor communicating with receiver continuously. If we want to open the door then automatically we just change to false and then get back to the true, then the door will open automatically. In the first column the fire status will be update and second column Gas status will be updated. And in the third column the door status will

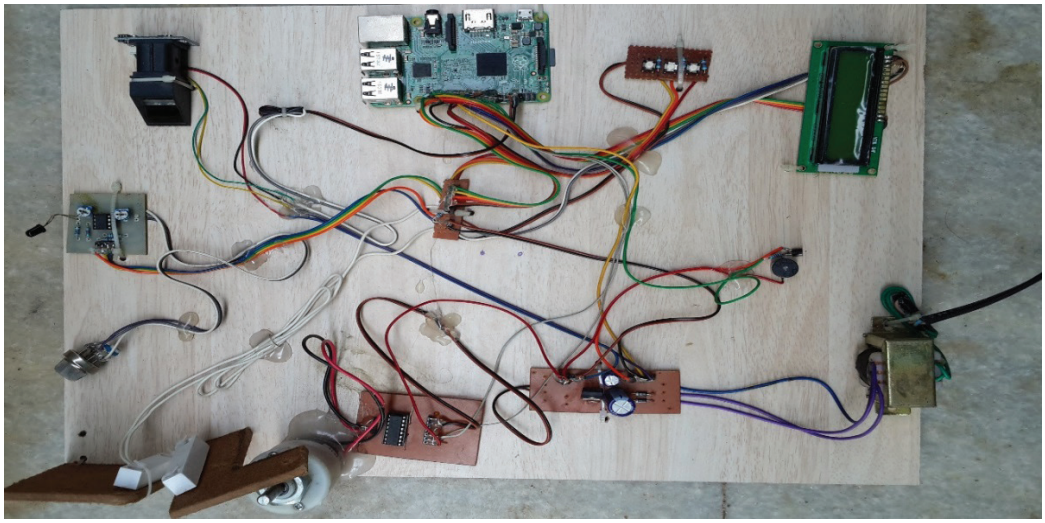

Figure 6. Depicts the hardware kit of the entire project.

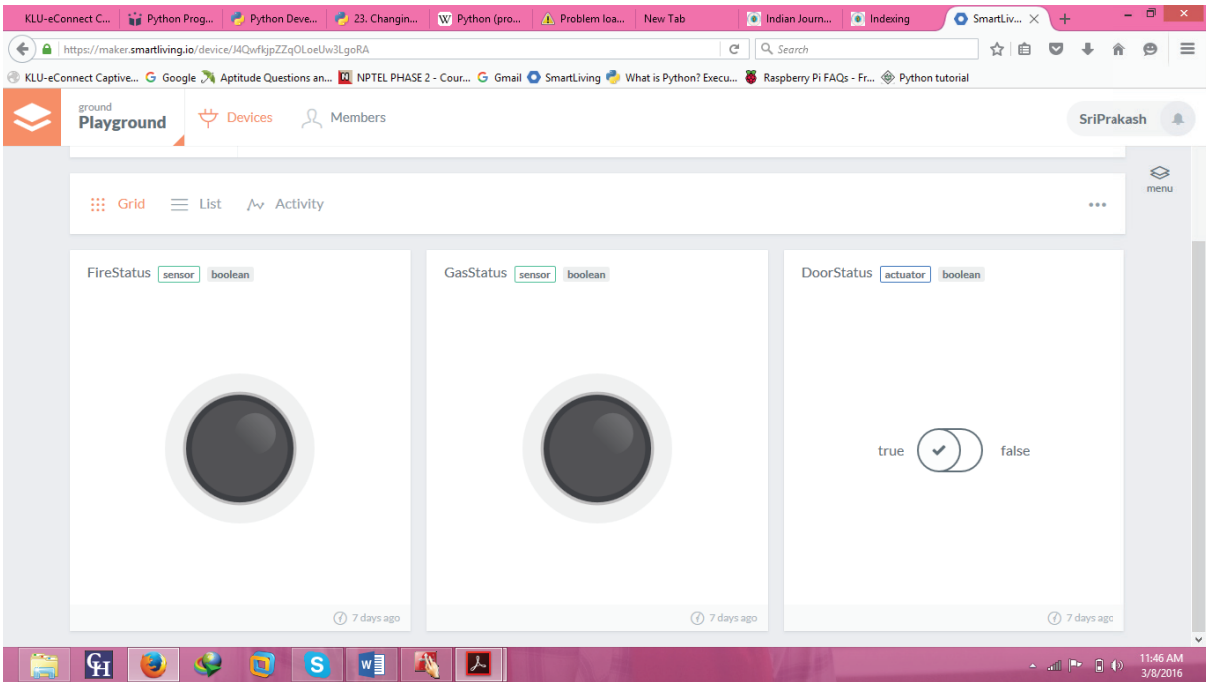

Figure 7. Depicts IOT in the web page.

be updated and we can access the door by using the true or false option.

If the fire sensor is activated then using the raspberry pi 2 sends the message like shown in Figure 8. Similarly gas sensor will do shown in Figure 9.

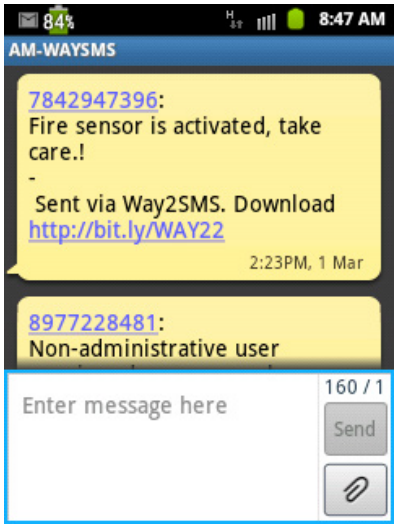

Figure 8. Depicts the message getting to mobile.

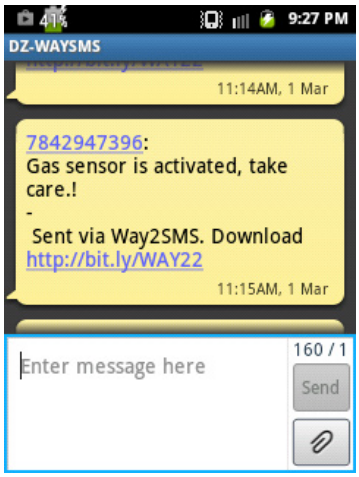

Figure 9 depicts the message getting to mobile

If any other user except administrator want to access the door then administrator gets the message showed in Figure 10. If the thief is trying to break the door then the administrator gets the alert message shown in Figure 11.

6. Conclusion

We designed, implemented and developed the home Security door locking system using the fingerprint module

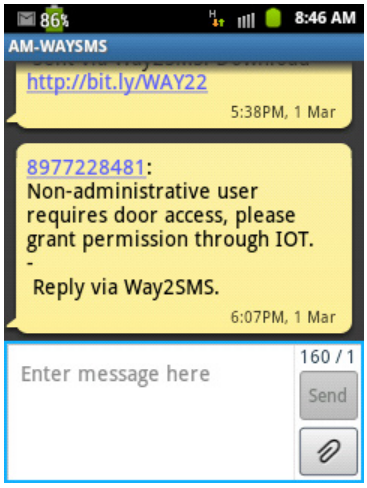

Figure 10. Depicts the message getting to mobile.

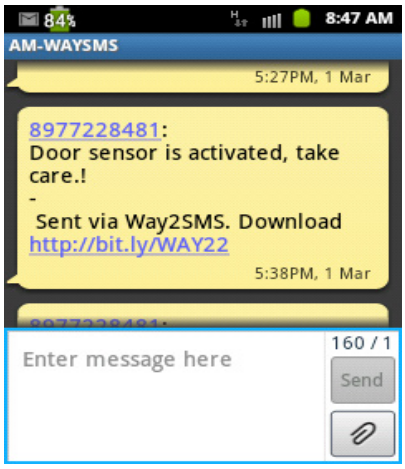

Figure 11. Depicts the message getting to mobile.

and the raspberry pi 2 board and also get the status of the Gas and the Fire. All these can be access from remote location by using the IOT.

7. Acknowledgement

The constant support and encouragement of Koneru Lakshmaih University (KLU), is gratefully acknowledged. This work wouldn't have been completed without the University support and we're forever thankful. Our special thanks to, "Embedded Systems and Sensor Networks (ESSN)" research group of KLU and "KLU Innovation Team".

8. References

1. Peng Z, Kato T, Takahashi H, Kinoshita T. Intelligent home security system using agent-based IoT Devices. 2015 IEEE 4th Global Conference on Consumer Electronics; Osaka. 2015 Oct 27-30. p. 313–4.
2. Gaikwad PP, Gabhane JP, Golait SS. A survey based on smart homes system using Internet-of-things. International Conference on Computation of Power, Energy, Information and Communication; Chennai. 2015 Apr 22-23. p. 33–5.
3. Kovatsch M, Weiss M, Guinard D. Embedding Internet technology for home automation. IEEE Conference on Emerging Technologies and Factory Automation (ETFA'10); Bilbao. 2010 Sep 13-16. p. 1–8.
4. Biometrics. Available from: http://www.biometric-solutions.com/solutions/index.php
5. Jain AK, Ross A, Prabhakar S. An introduction to biometric recognition. IEEE Transactions on Circuit and Systems for Video Technology. 2004 Jan; 14(1):4–20.
6. Ross NK, Jain AK. Handbook of multi-biometrics. Springer Science and Business Media; 2006.
7. Rashid RA, Nur H. Security system using biometric technology: Design and implementation of Voice Recognition System (VRS). International Conference on Computer and Communication Engineering; Kuala Lumpur, Malaysia. 2008. p. 898–902.
8. Mohanaprasad K, Pawani JK, Killa V, Sankarganesh S. Real time implementation of speaker verification system. Indian Journal of Science and Technology. 2015 Sep; 8(24). Doi: 10.17485/ijst/2015/v8i24/80193.
9. Maltoni D, Maio D, Jain AK, Prabhakar S. Introduction-handbook of fingerprint recognition. Chapter 1. New York, USA: Springer Verlag; 2003 Jun.
10. Jain AK, Prabhakar S, Hong L, Pankanti S. Filter-bank based fingerprint matching. IEEE Trans Image Process. 2000 May; 9(5):846–9.
11. Hong L, Jain A. Integrating face and fingerprints for personal identification. Proceedings 3rd Asian Conference on ComputerVision; Hong Kong, China. 1998. p. 16–23.
12. Ibrahim R, Zin ZM. Study of automated face recognition system for office door access control application. IEEE 3rd International Conference on Communication Software and Networks (ICCSN); Xi'an. 2011. p. 132–6.
13. Krishnasamy P, Belongie S, Kriegman D. Wet fingerprint recognition: Challenges and opportunities. Proceedings International Joint Conference on Biometrics; 2011 Oct. p. 1–7.
14. Pakutharivu P, Srinath MV. A comprehensive survey on fingerprint recognition systems. Indian Journal of Science and Technology. 2015 Dec; 8(35). Doi: 10.17485/ijst/2015/v8i35/80504.
15. Navya MR, Chandran PR. Development of secured home automation using social networking sites. Indian Journal of Science and Technology. 2015 Aug; 8(20). Doi: 10.17485/ijst/ 2015/ v8i20/79083.
16. Download the Required Operating System in ACC. Available from: http://www.raspberrypi.org/downloads/
17. Luigi A, Iera A, Morabito G. The Internet of things: A survey. Computer Networks. 2010; 54(15):2787–805.
18. Pandey M, Babu MR, Manasa J, Avinash K. Mobile based home automation and security system. Indian Journal of Science and Technology. 2015 Jan; 8(S2):12–6.