International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 16
June 2018

Design and Implementation of Industrial security system using Fingerprint Authentication and IOT

Ch. Narasimha Rao & M. Rambabu
[1]PG Scholar, Dept of ECE, Chebrolu Engineering College, Guntur, AP, India, E-mail: narsimharaochch@gmail.com.
[2]Associate Professor, Dept of ECE, Chebrolu Engineering College, Guntur, AP, India.

Abstract: *Most of the present technologies gives the door locking system in industry in different methods. To increase the security of the industrial we are using the extra security as a biometric finger print module and the IoT. By using these two security elements we can efficiently access the door by using the fingerprint and IoT. These fingerprint module and the IoT are controlled by the Raspberry pi board. Along with the hardware modules viz., Wi-Fi router, Gas Sensor, Fire Sensor, Door Fringe motor sensor and evaluate our proposed methodology. By using this technique we can establish the industrial security system very well. The Raspberry pi performs very well to control both the Fingerprint Module and the IoT.*

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

I. 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 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 Industrial Automation systems. IOT industrial automation techniques are greatly improving the quality of daily chores in a house hold. Industrial IOT is integrating the usual devices required in private housing technologies. Industrial 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 industrial 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 industrial IOTs. Industrial IOT devices are usually classified into two types based on the communication ability of the devices.

They are as follows:

- **One-way Industrial IOT devices:** These devices are only used to notify the operating personnel. They cannot respond to the ascribed actions of the user.
- **Two-way Industrial 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 I: Represents the Industrial 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

Table 1 represents the Ways of industrial IOT devices, 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, there're three components enabling the user intended tasks to be accomplished. These are viz., 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 are through a smart phone [3] is delivered to the IP router via the internet. As we're talking in terms of industrial IOT, the internet here is generally a broadband connection provided by the ISP.

IP Router: This acts as a bridge between Smart Phone devices and IOT gateway. Internet we spoke of above 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 industrial 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.

II. BIOMETRIC SECURITY ELEMENTS

There are different types of security elements employing the biometric technology in industrial IoT Security [4, 5].

A. Fingerprint Recognition

This is one of the finest biometric technologies used for the security systems [6]. The fingerprint Processing includes 3 sections. They are registering, search for Sinking and erase when not needed.

only then, we can access the module. We 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 [7, 8]. 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.

III. SYSTEM DESIGN

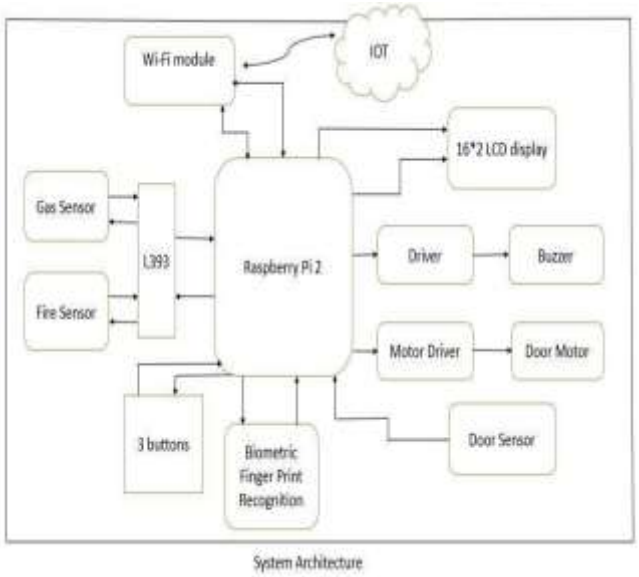

Fig. 1. represents the proposed block diagram.

The fig.1 depicts the entire block diagram of the proposed system and all the individual components are explained in the below

A. 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. the administrator has the id "0000".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 any other person except the administrator try to enter into the room without administrator permission then automatically the entire system will lock and the door will lock permanently.

B. Biometric Fingerprint Recognition

The biometric recognition module will store the administrator fingerprints [9,10]. 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.

C. 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.

E. 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 20mm then automatically the sensor will be activated and sends the information to mobile "Door sensor is activated, take care". Fig.2 depicts the Door sensor.

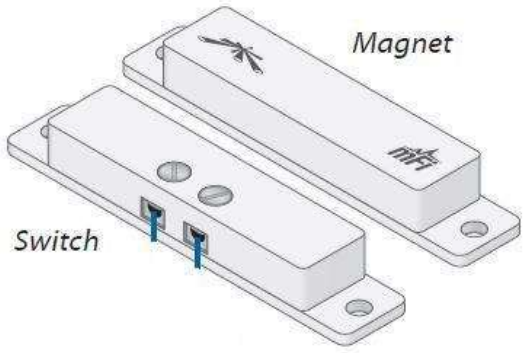

Fig. 2. depicts the Door sensor.

F. 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.

G. 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.

H. LM393 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.

I. Buzzer

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

J. 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 [11]. 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 [12]. In the raspberry pi 2 we use python language for coding.

K. 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.

L. Internet of Things

This is a latest technology through which we can access the appliances from remote locations by using the internet [13, 14]. 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.

IV. SYSTEM IMPLEMENTATION

The fig. 3 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 fig.4 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 be updated and we can access the door by using the true or false option.

Fig.3. depicts the hardware kit of the entire project.

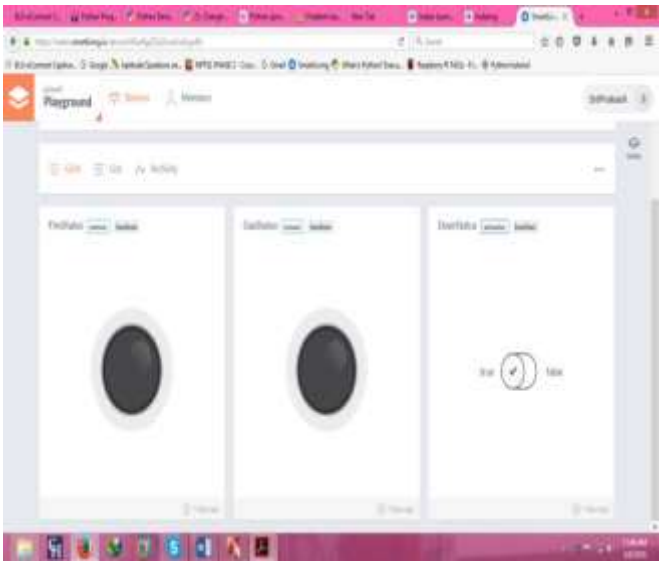

Fig. 4. depicts IOT in the Web page.

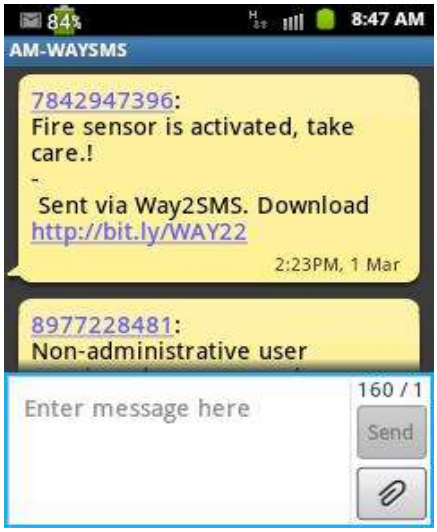

Fig.5. depicts the message getting to mobile.

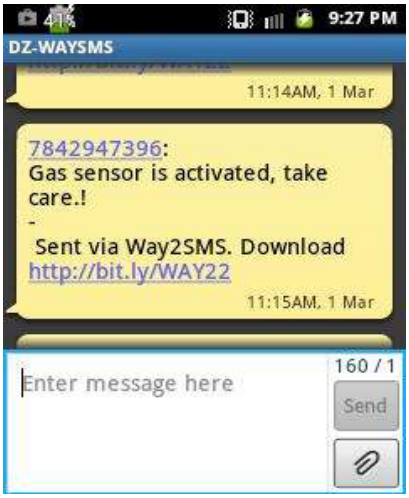

Fig.6. depicts the message getting to mobile.

If the fire sensor is activated then using the raspberry pi 2 sends the message like shown in fig.5. Similarly gas sensor will do shown in fig. 6.

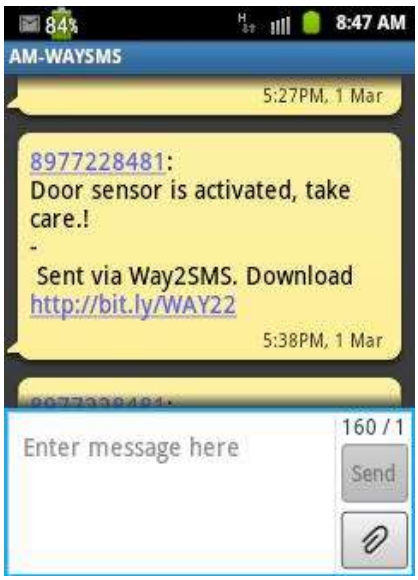

Fig.7. depicts the message getting to mobile.

If any other user except administrator want to access the door then door will lock permanently. If the thief is trying to break the door then the administrator gets the alert message shown in fig.7.

V. CONCLUSION

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

VI. ACKNOWLEDGEMENT

The constant support and encouragement of Chebrolu Engineering College, is gratefully acknowledged. This work wouldn't have been completed without the University support and we're forever thankful. My special thanks to Mr. Asso.Prof in Chebrolu Engineering College.

VII. REFERENCES

[1] Zhaoqing Peng, Takumi Kato, Hideyuki Takahashi, and Tetsuo Kinoshita. Intelligent Industrial Security System Using Agent-based IoT Devices. 2015 IEEE 4th Global Conference on Consumer Electronics.

[2] Mr. Pranay P. Gaikwadl, Mrs. Jyotsna P. Gabhane, Mrs. Snehal S. Golait. A Survey based on Smart Industrials System Using Internet-of-Things. 2015 international conference on computation of power, energy, information and communication

[3] Kovatsch M, Weiss M and Guinard D. Embedding Internet technology for industrial automation.IEEE Conference on
Emerging Technologies and Factory Automation (ETFA'10). 2010 Sep 13–16; Bilbao. IEEE. p. 1–8.

[4]Articletitle.http://www.biometric-solutions.com/ solutions/ index.php

[5]Anil K. Jain, Fellow, Arun Ross and Salil Prabhakar. An Introduction to Biometric Recognition.IEEE Transactions on Circuit and SYSTEMS for Video Technology, Vol.14, No.1, January 2004.

[6] Maltoni D, Maio D, Jain AK, Prabhakar S. In. Introduction-handbook of fingerprint recognition. Chapter 1. New York, USA: Springer Verlag; 2003 Jun.

[7]Jain AK, Prabhakar S, Hong L, Pankanti S. Filter-bank based fingerprint matching. IEEE Trans Image Process. 2000 May; 9(5):846–49.

[8] L.Hong and A.Jain, Integrating face and fingerprints for personal identification.in proc.3rd Asian Conference on ComputerVision, pages16-23, Hong Kong, China, 1998.

[9] Krishnasamy P, Belongie S, Kriegman D. Wet fingerprint recognition: Challenges and opportunities. Proc Int'l Joint Conf Biometrics; 2011 Oct. p. 1–7.

[10] P. Pakutharivu and M. V. Srinath. AComprehensive Survey on Fingerprint Recognition Systems.Indian Journal of Science and Technology, Vol 8(35), DOI: 10.17485/ijst/ 2015/v8i35/80504, December 2015

[11] M. R. Navya and Prakash Rama chandran.Development of Secured Industrial Automation using Social Networking Sites. Indian Journal of Science and Technology. Vol8 (20), DOI:10.17485/ijst/ 2015/ v8i20/79083, August 2015

[12] Article in Download the Required Operating System in http://www.raspberrypi.org/downloads/.

[13] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. The internet of things: A surveyComputer networks54.15 (2010): 2787-2805.

[14] Monu Pandey, M. Rajasekhara Babu, Javvaji Manasa and K. Avinash. Mobile Based Industrial Automation and Security System. Indian Journal of Science and Technology, Vol 8(S2), 12-16, January 2015.