ISSN: 0974-5572
IJCTA
International Journal of
CONTROL THEORY
AND APPLICATIONS
UGC APPROVED JOURNAL
ज्ञान-विज्ञान विमुक्तये
INTERNATIONAL SCIENCE PRESS
Gurgaon, Haryana (India)

International Journal of Control Theory and Applications

ISSN : 0974-5572

© **International Science Press**

Volume 10 • Number 35 • 2017

Multimodal Home Security System using IoT and Raspberry Pi

S. Neeraja[a] and N. Venkatram[b]

[a]Corresponding author, Department of ECSE, K.L. University, Green Fields, Guntur DT, AP, 522502, India. Emails: neeru8416@gmail.com
[b]Department of ECSE, K.L. University, Green Fields, Guntur DT, AP, 522502, India. Emails: venkatram@kluniversity.in

Abstract: The Security is a significant aspect in home native environments. The Security notion in native habitats like home is important because due to the increasing of thefts, fire accidents, entry of an intruder, poisonous gasses. The home security system integrated with IoT will respond dynamically like Real time application. The Biometric recognition system is playing a fundamental aspect in the home security systems. Among distinct biometric recognition systems available the fingerprint recognition system is the most suited for the enhancement of security system. The fingerprint and webcam both will result in a secured biometric system. The home security system is developed by employing Raspberry Pi 3. The information from the sensors, fingerprint and webcam that are interfaced to the Raspberry Pi 3 are monitored and manipulated by the Administrator remotely. The IR fire and temperature sensors interfaced with the Raspberry Pi 3central server provide the environmental conditions time to time. The Administrator gives permission to the person who is requesting for the door access with the help of web page. All the information from the Raspberry Pi 3 central server is available in the form of SMS and web page to the Administrator, so that administrator can remotely control the system. In comparison with the existing home security systems, this developed system greatly reduces the overall cost and can work efficiently and produce results in Real time.

Keywords: Fingerprint module, Fire Sensor, IoT, Raspberry Pi 3, temperature sensor, Webcam.

1. INTRODUCTION

The Smart home is a system which makes the home appliances available to the user via remote access. In any Smart home system while using the system, the user will get the facilities like convenient, remote access, comfort. The fundamental of IoT is to connect the devices to the user anytime, anywhere with the aid of network connectivity. The physical world and computer based systems are governed using IoT [1]. IoT employed with home devices is categorized into one-way and two-way devices. In one-way, the devices that are interfaced to the system are exclusively used to notify the administrator about their present conditions. In two-way, the devices that are interfaced with the system can both notify and respond to the Administrator instructions [2].

With the transformations made in embedded computing systems every device got the ability to be uniquely identified. Internet of Things offers advanced connectivity of device, services and covers a variety of protocols, applications. In the concept of IoT, the devices collect useful data with the help of numerous technologies and then flow the data between the devices. IoT had its impact on our lifestyle and it has lead a new dimension in the field of internet [3]. Security and interoperability are the two significant aspects in the IoT. IoT has already brought revolution over the existing technologies and it is favorably advancing in the domains of education, science, Government, Communication. In the later transformation of Internet, IoT affirms to make a huge step in its ability to obtain, process, distribute data and that process can be transformed into information, knowledge and eventually intelligence [4]. Some of the smart applications in the IoT are smart homes, smart industries, smart health care, smart transportation system [5]. IoT consolidates assorted computing devices and sensor networks to keep track of the Home environments [6]. The devices are connected in a seamless fashion, so that user utilizes their services conveniently. The smart home security system objective is to restrain the house safe from intruders or trespassers, fire accidents. The smart home security system reduces human effort by sensing and responds to the data in Real time without any delay.

In the recent years, the urge for remote control and security for the home environments is being rapidly increasing. Though many systems are available, but they are not capable of coping up with the market standards. The Home environment which is not having a security system is easily proved to be insecure. The advancements of home network infrastructures leading rise to new applications in the fields of home security and also as well as for home automation. Security has become a major concern for years to organizations, home, companies [7] - [8]. There are many advancements made in the home security system. The access control system mechanism is a significant part of an organization. The door access system limits access to the home to specific people and hence enhances security. The implementation of the smart home security system can be facilitated with the support of biometric systems and sensors [9]. The combination of biometrics and automation into a framework can enhance security. Biometric provides the ease of identifying people by their traits, these traits are distinct from person to person. Due to above specified quality biometrics gained prominent in the fields of systems ensuring privacy, identifying people, providing security, forensics. To ensure security to home environments, there exists numerous biometric identification elements like keystroke dynamics, speaker recognition, speech recognition, Iris recognition, Face recognition, Vein recognition, Fingerprint recognition. The biometric applications must follow the vital parameters like accuracy, robust, reliability.

The general operation of biometric recognition elements is the data scanned is compared with the data available in the database of the system, if both the credentials are matched then the user will get verified and get access. Fingerprint recognition system combined with the webcam suits to be the efficient biometric recognition schemes. The traditional door lock system is built with Wi-Fi, Bluetooth but due to security considerations fingerprint module is employed. The fingerprint and webcam is advantageous over existing systems because it is low cost, works accurately, reliable, uniquely identifies individuals so that’s why this approach is integrated into the smart home security system. An efficient smart home security system must work 24x7 [10].

2. LITERATURE SURVEY

The smart home security system is a prime issue because it’s not just about the monetary safety but much more than that. Everyone wants’ the happiness and protection of their dear ones and no one wants to see their family members in danger [11]. Significant reasons to utilize the smart home security system are protecting the family and home from trespassers, fire can be detected and safety measures can be taken. The challenges that smart home security system encounters are the developed system must be low cost because it must be available to all the classes of people, the system must be upgraded with the assured development team so that the system can function properly, the system’s operating procedure must be known properly, the system must be flexible, it must not consume more power, the smart home security system must not intrude into the users personal life, finally the smart home security system must function accordingly to the instructions given by the administrator.

Some of the challenges faced by biometric recognition systems are the data from the users must be sensed accurately [12]. Some recognition elements need direct contact with the user, while some recognition element doesn’t need any contact depending on the application need a specific recognition element must be chosen [13]. Biometrics operate in both stand-alone or fused mode, So issues like noise captured data, man in the middle attacks must be taken care while developing the system. Based on the application the operating scope of the recognition system is chosen.

Some of the available biometric recognition systems for smart home security are discussed below. Keystroke dynamics, specifically identify a person based on the periodicity of typing and the sequence of the words. The two parameters that keystroke dynamics follow are dwell time and flight time. The Dwell time is when the certain key is pressed and flight time is when the pressed key is released and another key is pressed. If the typing period is mismatched then the user must again repeat his actions [13]. The Speaker recognition is the automated approach of uniquely identifying a person based on the voice. The Four steps involved in speaker recognition method are voice recording, feature extraction, pattern matching, decisions [14]. The major disadvantage of this Speaker recognition system is anyone can imitate the voice and break the security. The speech recognition is the process of recognizing what is being said. An Unauthorized user can get access to the system by imitating the voice of the speaker [15]. The IRIS recognition is the method of identifying a person by the analysis of the pattern of IRIS. IRIS recognition system analyzes on the colored pattern which is unique for each individual. The IRIS recognition system cost is high, very low range is required to capture the data between the IRIS and the system [16]. The IRIS recognition system damages the eye due to the variable light intensity and produces fault results. The fingerprint recognition system is considerably known for its applications in the field of authentication on computer systems [17]. The fingerprint is distinct from person to person, no two person’s impressions will match. The basic patterns fingerprint has arch, loop, and whorl. Certain care must be taken while choosing a fingerprint reader because it must overcome the Type I and Type II error [18]. The optical reader sensor is more preferred over various readers available in the market because of its low cost, accuracy. The optical reader sensor resembles a digital camera that use visual images of the fingerprint. The Fingerprint recognition system supports the following criteria like universality, uniqueness, collectability, Acceptability, performance, Circumvention [19] - [20]. The fingerprint trait doesn’t transit unless there is physical riot due to cause of accidents which damages fingerprints.

3. HARDWARE MODULES USED FOR SYSTEM IMPLEMENTATION

The Figure 1 represents the functional block diagram of the implemented system. The modules like LM 35, PIR, IR Flame, Magnetic reed switch, Fingerprint Module, Webcam, DC motor, LCD, Raspberry Pi 3 are used for the implementation of the system are explained below.

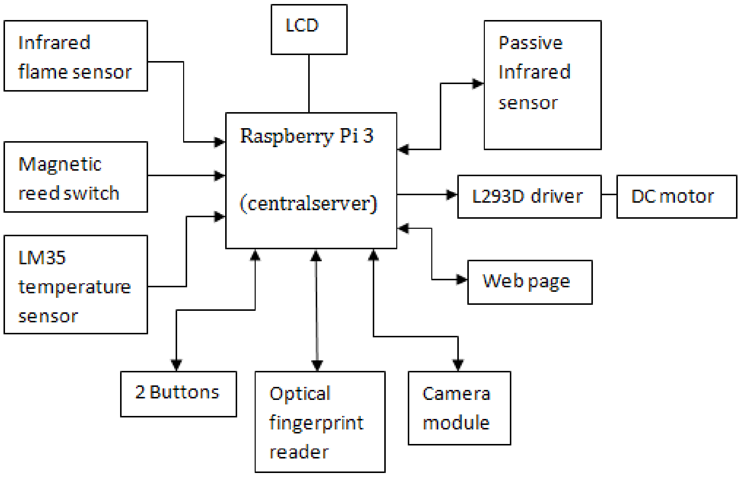


Figure 1: Block diagram of Home Security system

IR flame sensor: The fundamental of IR flame sensor is to identify and react to the existence of a flame or fire. It is a low cost module and can operate on a voltage from 3.3-5 V. The IR flame sensor is interfaced to the Raspberry Pi 3. The sensitivity is adjusted with the potentiometer available on the module. The general operating range of this sensor for high intensity flames is 3 feet. The IR flame sensor is widely utilized in the fields of industries, home, colleges.

PIR (HC-SR 501) sensor: The passive infrared sensor is made of pyroelectric sensor where varying levels of infrared radiation can be detected and it runs on a voltage of 5 V. It is also called as a motion detector. It is low cost, low power consumption and high sensitive motion sensor. The term passive reflects that PIR sensor does not emit any energy for the intent of detection. The radiated infrared energy of the object is only detected by the PIR sensor. The PIR sensor is interfaced to the Raspberry Pi.

LM 35: LM 35 is a three terminal device. It has its own importance in the field of temperature measurement and it is widely used. It is precision integrated circuit temperature sensor. It has improved performance than thermistor and it eliminates the issue of oxidation as it is a sealed device. LM 35 output voltage is equivalent to the Celsius temperature. It works at a voltage ranging from 4-30 V and can measure temperature in the range of -55°C to 150°C. The LM 35 is interfaced to pins available in Raspberry Pi 3. The temperature value produced is more precise than the various temperature measurement devices.

Magnetic reed Switches: The fundamental operation of reed switch is based on the applied magnetic field. It is a lightweight, comfortable to use, precise and has fast response. Inside the case the reeds are in disconnected state which represents that the circuit is open and no current flows, when the magnet is brought into the scope of reed sensor then the reeds get connected and forms electric switch and flows current through it. It mainly serves for the application of security.

Biometric fingerprint Optical reader: The fundamental role of fingerprint scanner is to scan the image of finger and examine with the earlier scanned images, if the image data matches then authentication will be provided. Among various readers available the optical fingerprint reader suits to be more beneficial because of its unique advantages. The optical reader can log up to 256 images. The optical fingerprint module is interfaced the Raspberry Pi 3. This module is identical to that of a digital camera.

Webcam: In the Raspberry Pi 3, there is certain zone available for interfacing Webcam. It can produce 5 MP resolution image. The webcam is interfaced to the USB ports provided on the Raspberry pi. The Raspberry Pi 3 integrated with the webcam serves efficiently in the field of security applications.

DC motor: The DC motor is utilized in the process of opening and closing the door. The DC motor directly cannot interface to the Raspberry pi 3, because Raspberry Pi 3 provides 5 V where as DC motor requires 12 V to operate. So the L293D driver is employed to drive the voltage from 5 V to 12 V to the DC motor. With one L293D driver two DC motors can be interfaced.

Raspberry Pi 3: The Raspberry Pi 3 is a low cost, efficient processor. It works on the operating voltage of 5 V. It can facilitate the user with all the features that are provided in the personal computer. The Raspberry Pi 3 acts as a central server controlling all the data. The Raspberry Pi3 is programmed using Python programming language. All the information from sensors attached to the body are interfaced to the Rasppberry Pi to achieve high computations and efficient data communication.

LCD: Liquid crystal displays are used in digital watches and many embedded systems projects. The LCD is used to display the measured data. A 16 x 2 Alphanumeric Display it can display two lines with a maximum of 16 characters in one line.

4. IMPLEMENTATION METHODOLOGY

The implementation of the smart home security system is significant because in the recent days investigators proposed that the rate of increase in robberies is not being controlled and there are also many accidents happening in the home environment like fire accidents. The smart home security system provides the facilities like potential crime can be deterred, fire can be detected and fire accidents can be prevented, improves electricity management, the home environment can be monitored remotely, Remote access can also be provided.

In this system shown in Figure 2 represents the hardware of the home security system, the developed model resembles an efficient smart home security scheme. Here two buttons S1 and S2 are provided. S1 button is used to register new user, S2 button provided is utilized to get the optical finger print module ready for the user to verify the credentials. The administrator is provided, the default ID 0000, as the users increase the ID number will incremented by one. On the LCD display the message insert your finger is displayed, then the user must place the finger on the area provided on the optical fingerprint module.

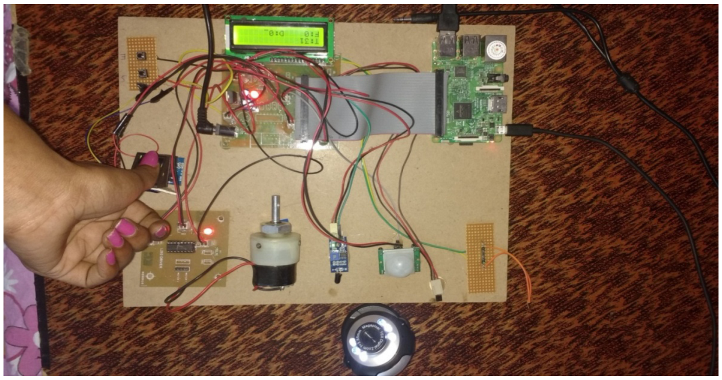
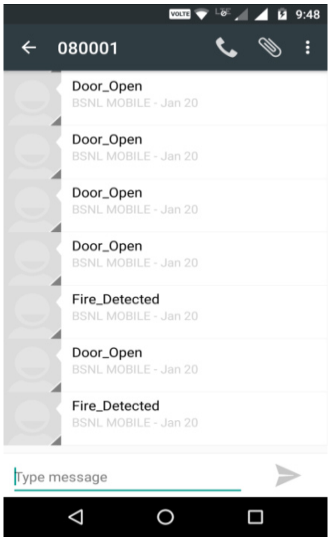


Figure 2: Implemented Hardware of the home security system

With the Optical fingerprint reader provided, the user must first enroll with the administrator for remote door access. If the user is an authorized person, the person can directly access the door by using PIR sensor, Optical fingerprint reader, webcam. The Passive Infrared Sensor is to detect whether any person is available at the door entry. The optical fingerprint reader is to scan the fingerprint of the user and the webcam is used to snap the user photo. The data from the fingerprint and the camera is uploaded to the database which is in the web server. In the database the scanned fingerprint will be compared with fingerprints already stored, if the data matches, then the access to the door is automatically provided. The door will be accessed based on the authorization provided to the user by the administrator. If the person doesn't have authorization to the door, the person must first enroll with the Optical fingerprint reader, webcam. The administrator will get a message door access requested. So that the administrator will login into the webpage and see the snapshot of the user who is requesting to access the door. Based upon the snapshot provided the administrator decides whether to give door access to the user or not and gives the instructions on the web page. The magnetic reed sensor is to check whether the door is closed or opened, if the door is opened, then the administrator will get a message that the door is opened. The LM 35 measures the temperature parameters of the room and provides the output value accurately in the form of Celsius. The administrator will be notified about the temperature in the room that is uploading the data into the web server the data is displayed in the web page and also gets notified by the SMS. The LM 35 eliminates the problem of oxidation and works efficiently. The IR Flame sensor main principle is to detect the flame or fire in the home environment and notify the administrator that fire detected take care in the form of SMS. So that the administrator can require to safeguard measurements and controls the threat. The IR flame sensor module activates when the surface of the IR is changed from black to white color due to presence of flame. The optical fingerprint reader, the webcam, the LM 35 temperature, IR flame sensor, Magnetic reed sensor, Passive infrared sensor, DC motors all the modules are interfaced to the GPIO's of the Raspberry Pi 3. The Raspberry Pi 3 is preferably programmed using Python language. The Raspberry Pi 3 acts a central server monitoring all the modules and amount of data from all the modules is sent to the administrator in the form of SMS and the administrator will also monitor the details in the web page and will remotely provide the access to the door.

5. RESULTS AND DISCUSSIONS

The Implemented Home security system provides the Administrator the facility to remotely monitor and control the home in the form of Web pages and SMS. Figure 3 shows the message Fire_Detected and Door_Open sent to the Administrator whenever Fire is detected and door is opened in the home environment. Figure 4 shows the message Over_temperature and Unauthorized person trying to access sent to the Administrator whenever the temperature is above the threshold value and also whenever unauthorized person is trying to access the door in the home environment.



Door_Open
BSNL MOBILE - Jan 20

Door_Open
BSNL MOBILE - Jan 20

Door_Open
BSNL MOBILE - Jan 20

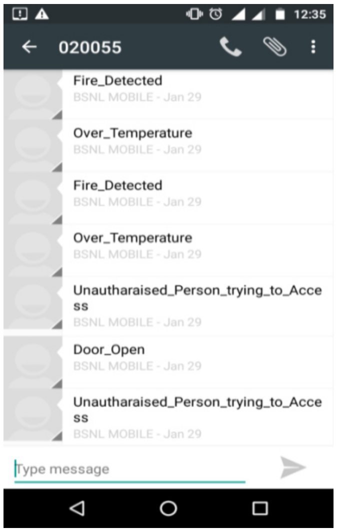
Door_Open
BSNL MOBILE - Jan 20

Fire_Detected
BSNL MOBILE - Jan 20

Door_Open
BSNL MOBILE - Jan 20

Fire_Detected
BSNL MOBILE - Jan 20

Figure 3: Fire Detected and Door is Opened SMS received on Mobile.



Fire_Detected
BSNL MOBILE - Jan 29

Over_Temperature
BSNL MOBILE - Jan 29

Fire_Detected
BSNL MOBILE - Jan 29

Over_Temperature
BSNL MOBILE - Jan 29

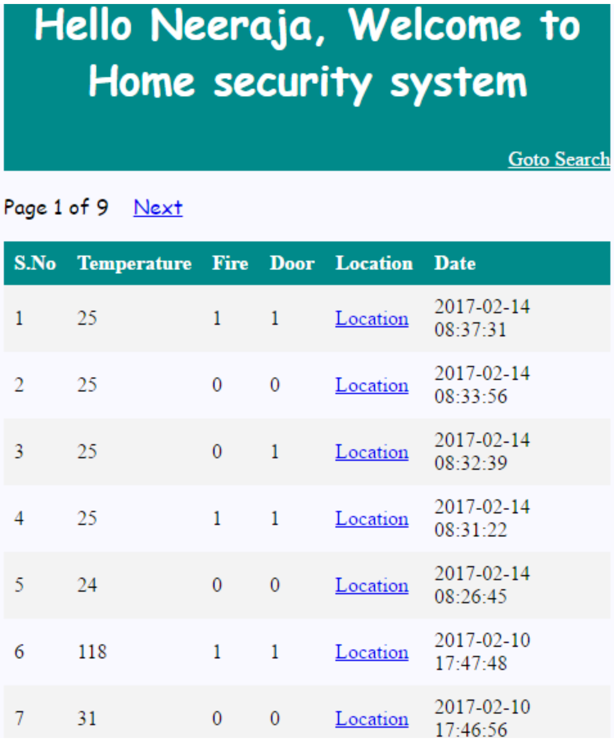
Unautharaised_Person_trying_to_Access
BSNL MOBILE - Jan 29

Door_Open
BSNL MOBILE - Jan 29

Unautharaised_Person_trying_to_Access
BSNL MOBILE - Jan 29

Figure 4: Over temperature and Door request SMS received on Mobile

Figure 5 shows the parameters in the web page and can be viewed by the Administrator. Here 0's and 1's are displayed on the web page for fire and door status. The 0's represent that the fire sensor is not activated and 1's represent that the fire sensor is activated and the user will receive a SMS that Fire_Detected. The 0's represent that the door is closed and 1's represent that the door is opened an immediate SMS will be sent to the user that Door_open and required action can be taken. The temperature recorded by the LM 35 is also displayed on the web page with all the respective timestamps.



Hello Neeraja, Welcome to Home security system

Goto Search

Page 1 of 9 Next

S.No	Temperature	Fire	Door	Location	Date
1	25	1	1	Location	2017-02-14 08:37:31
2	25	0	0	Location	2017-02-14 08:33:56
3	25	0	1	Location	2017-02-14 08:32:39
4	25	1	1	Location	2017-02-14 08:31:22
5	24	0	0	Location	2017-02-14 08:26:45
6	118	1	1	Location	2017-02-10 17:47:48
7	31	0	0	Location	2017-02-10 17:46:56

Figure 5: Parameters results on Web page

The web cam serves for the purpose of capturing snapshots of the users. The web cam takes the snapshots of every individual. The Figure 6 shows the photo captured by the web cam of the user having Door access.

Figure 6: Picture captured by webcam of the user having door access

Figure 7 shows the picture captured by the webcam who is not having door access. To get the door access, the picture will be sent to the administrator and the administrator will decide whether to provide the door access or not.

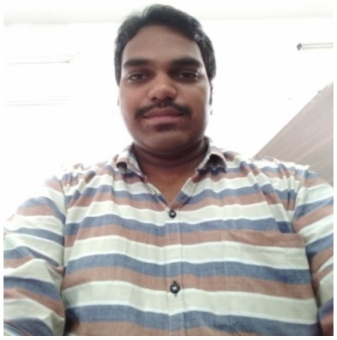


Figure 7: Picture captured by webcam of individual who is requesting the door access

6. CONCLUSION

In this paper, we designed and developed a novel smart home security system. The developed system significantly aims at the door lock system and home protection with the help of Internet of Things. The developed system can be extended to multi-room environments and will be able to satisfy the user in all provided security aspects. This system is not just limited to experimental setup, but can also accomplish its task in real world applications. Finally the developed smart home security system is low cost, highly efficient compared with the existing methodologies. Hence this system can be further enhanced and can provide its service in all applications.

Acknowledgment

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

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, Vol. 54, No. 15, pp. 2787–2805, 2010.

[2] 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.

[3] M. N. N. A. Asghar, M.H., "Principle application and vision in internet of things (iot", *Communication Technologies (GCCT) 2015 Global Conference on*, may 2015.

[4] K. Xu, Y. Qu, and K. Yang, "A tutorial on the Internet of Things: From a heterogeneous network integration perspective," IEEE Netw., Vol. 30, No. 2, pp. 102–108, Mar./Apr. 2016.

[5] A. Zanella, "Internet of Things for Smart Cities", *IEEE Internet of Things J.*, Vol. 1, No. 1, pp. 22-32, Feb. 2014.

[6] N. R. Yang, H. S. Choi, J. Y. Lee, Y. J. Kim, W. S. Rhee, "GOMs: Generic ontology models to process context information in IoT environment", *TENCON 2014 IEEE Region 10 Conference*, pp. 1-6, October 2014

[7] H. Huang, S. Xiao, X. Meng, and Y. Xiong, "A remote home security system based on wireless sensor network and gsm technology," in Networks Security Wireless Communications and Trusted Computing(NSWCTC), 2010 Second International Conference on, Vol. 1. IEEE, 2010, pp. 535–538.

[8] S. L. Keoh, S. S. Kumar, H. Tschofenig, "Securing the Internet of Things: A Standardization Perspective", IEEE Internet of Thinas J., Vol. 1, No. 3, pp. 265-75, June 2014.

[9] 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.

[10] Y. Sun, T.-Y. Wu, G. Zhao, and M. Guizani, “Efficient rule engine for smart building systems,” IEEE Trans. Comput., Vol. 64, No. 6, pp. 1658–1669, Jun. 2015.

[11] S. R. Das, S. Chita, N. Peterson, B. A. Shirazi, and M. Bhadkamkar,“Home automation and security for mobile devices,” in Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on. IEEE, 2011, pp. 141–146.

[12] 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.

[13] Biometrics. Available from: http://www.biometric-solutions.com/solutions/index.php.

[14] 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.

[15] Urmila Shrawankar and Vilas Thakare, “Techniques for Feature Extraction in Speech Recognition System : A Comparative Study”,Dept. of Computer Science, SGB Amravati University, Amravati, 2013.Systems 51, On page(s): 394 – 404 (2011).

[16] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, “Face recognition:A literature survey,” ACM computing surveys (CSUR), Vol. 35,no. 4, pp. 399–458, 2003.

[17] Hong L, Jain A.“Integrating face and fingerprints for personal identification” Proceedings 3rd Asian Conference on Comp uterVision;HongKong,China.1998. p.16–23.

[18] 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.

[19] 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.

[20] Mohamed Haghighat, Saman Zounouz, Mohamed Abdel, “CloudID: TrustWorthy Cloud Based and cross-enterprise biometric identification”, *Elsevier- Expert Systems with Applications*, Vol. 42, No. 21, pp. 7905-7916.