International Journal of ChemTech Research
CODEN (USA): IJCRGG, ISSN: 0974-4290, ISSN(Online):2455-9555
Vol.10 No.14, pp 220-224, 2017

Efficient Home Security System based on Biometrics and Keypad System

R.Rohini[1]*, S.Ravi[2], G.Devi[3]

[1]Department of CSE/ Vivekanandha College of Engineering for Women, Iayampalayam, Tiruchengode - TK,Namakkal District, Tamilnadu - 637 205, INDIA
[2]Department of ECT/ Botswana International University of Science and Technology, Botswana
[3]PG Scholar/CSE/ Vivekanandha College of Engineering for Women, Elayampalayam,Tiruchengode - TK,Namakkal District, Tamilnadu - 637 205, India

Abstract : Nowadays people are facing many problems about security in all over world, at the present time security is the most important issue in the world. Security gets more significance in recent years. Door lock security has distorted a lot from the last century and will be altering in coming years. A door lock system consists of RFID reader for user authentication, touch LCD, motor module for opening and closing the door, communication module, and control module for controlling other modules. Biometric sensor is used to sense the fingerprint and is validated for authentication. If the fingerprint is matched, the door will be opened or otherwise the buzzer connected to micro controller will be activated. So the people near the surroundings will get an alert.
Keywords : Biometrics, Home Security, RFID, GSM Modem, Micro controller.

1. Introduction

The Internet of things (IoT) is the internetworking of physical devices and other devices embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. In Global Standards Initiative on Internet of Things defined the IoT as "the infrastructure of the information society. The IoT allows objects to be sensed or controlled remotely and access through network[1]. To creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit.

When IoT is enhanced with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems which also encompasses technologies such as smart grids, smart cities, industries and homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. The researcher estimates that the IoT will consist of almost 50 billion objects by 2020[2]. Internet and its applications have become an integral part of today's human lifestyle. Smart home is now becoming prevalent with the development of the Internet of things (IoT) techniques. It is aimed at providing the user with a user-friendly method to be in charge of the home appliances such as doors, lights, even in a condition of long-distance. This controlling is generally achieved by a mobile phone which can access to the Internet.

2. Related Work

The authors says that where those can easily access their information anytime and anywhere people are also faced with the threat that others can easily access the same information anytime and anywhere[3]. Generally passwords, identification cards and PIN verification techniques are being used. The most secured system is fingerprint recognition because a fingerprint of one person never matches the other. Biometrics studies universally incorporate fingerprint, face, iris, voice, signature, and hand geometry recognition and verification[4]. Many other modalities are in various stages of development and assessment. Along with these available biometric fingerprint proves to be one of the best traits providing good mismatch ratio, high accurate in terms of security and also reliable. When fingerprint module is interfaced to the microcontroller stored images will be verified with the scanned images.

IoT was initially proposed to refer uniquely identifiable interoperable connected objects with Radio Frequency Identification (RFID) technology[5]. After that researchers relate IoT with more technologies such as actuators, sensors, GPS devices, and mobile devices. Today IoT can define as "a dynamic global network infrastructure with self-configuring capabilities based on standard and communication protocols.

The OTP based door lock security having different security systems such as a digital door-lock and mechanical door-lock based system[6]. The proposed method does not need user's help to get access to the facility but the user must have the registered mobile phone to get the OTP. Then the OTP will be generated and sent to the user's mobile phone when the user requests to access facility. By entering the OTP through keypad on the door the door will open. In case if the mobile is not available or off then the option to open the door is to answer the security question ask by system and then the door will be opened.

The Smartphone application was used by end users as a centralized interface, and speech recognition was performed by connecting to a cloud Application Programming Interface (API)[7]. Each user was asked to create a set of household devices and select customized names for their appliances. Testers were instructed to issue voice commands including their selected personalized devices. Two types of acoustic models were evaluated. Acoustic models used Hidden Markov Models (HMM) to represent the temporal variability of speech, and Gaussian Mixture Models (GMM) for each HMM state. However, the second acoustic model used additional bottleneck features created by a Deep Neural Network (DNN).

The low-cost home automation system was developed with in local and mobile controls in order to control ON/OFF of appliances[8]. The first main module, the local control, is an Android-based control communicating with Arduino microcontroller interfaced with Bluetooth. And another module, the mobile control, is an Arduino attached to a GSM-based to receive command sets from a mobile phone.

The HIVE system deploys three intrusion detection sensors: a passive infrared sensor (PIR), magnetic switch sensor, and load cell sensor. The first sensor, PIR sensor, detects motions in a particular area[9]. The next sensor, magnetic switch, detects the status of doors or windows. There are 2types of magnetic switch: Normally Open (NO) and Normally Close (NC).

The house-door is an important and crucial part of any smart home[10]. Where our smart phones have probably more information about us and our family, our friends, our bank accounts, where our kids go to school, and information about our lifestyle, etc. Smart-Lock-System is a complete recreation of the standard Key-Door lock .Where all the digital keys are kept in a Digital Keychain kept on the owner's phone. Encrypted and secured data in Smart-Lock-System can be connected to the Internet through internet cable or Wi-Fi.

The users can easily monitor and control all the devices through the mobile phone which can access the Internet[11]. The local access, users can enter home by making the mobile phone approach to a NFC reader which can recognize the necessary authentication information. A user Personal Identification Number (PIN) is needed to input on the mobile side for safety considerations. In the additional condition of remote access, the security is guaranteed by the PIN and the Virtual Private Network (VPN) tunnel. The VPN can establish a secure connection without the need of specialized software.

Micro controller based digital lock presented an access control system that allows only authorized persons to access the home[12]. When an authorized person enters predetermined user password via the global system for mobile communication (GSM) keypad, the stepper motor is operated for a limited time to unlatch the

solenoid-operated lock so the door can be open. If the user forgets his password, the code lock can be accessed by a unique 8 digit administrator password and the secret code can be changed any time after entering the current code[13]. To interface the microcontroller with the GSM modem and start/stop the engine by sending the predefined messages from the mobile phone to the controlling unit.

Digital door lock system is uses the digital information such as a secret code, semi-conductors, smart card, and finger prints as the method for authentication instead of the legacy key system[14]. In our system, a ZigBee module is embedded in digital door lock and the door lock acts as a central main controller of the overall home automation system. A door lock system consists of RFID reader for user authentication, touch LCD, motor module for opening and closing of the door, sensor modules for detecting the condition inside the house. The biggest improvement of our system is that it can be easily

The traditional techniques of alarm based security have gained much popularity in past decades[16]. Nowadays, embedded system is designed to provide security due to tremendous improvement in microcontroller unit and widespread applications of GSM technology. Number of security systems based on new technologies like GSM, GPRS (General Packet Radio Service), Internet, USN (Ubiquitous Sensors Network) and implemented through FPGA (Field Programmable Gate Arrays), ASICs (Application Specific Integrated circuit).

3. Experimental

The security system consists of the following stages:

RFID Reader:

When RFID tag placed on the RFID reader as it read the data and through reader its code send to the controller which access with the controller match and receives code with store code if the code is same then the security system is authorized to use and access the data. Change the tag ID in Access Control into sketch with the ID you have noted down earlier and then connect PIC microcontroller board with PC, upload the sketch into the board. After access control system the information is display on LCD and if the information is not correct the alarm will start ringing.

Biometric Finger Print:

Fingerprint is an authorized to open the locker door will be stored in the module with a unique id. To prove that the persons are authorized to open the locker door they need to scan their fingerprint images. The scanner is interfaced to pic16f877a microcontroller; this controller will be controlling the scanning process. After the scanning has been completed, user has to enter the password to open his locker with the help of a keypad. Immediately the locker will be opened. After the work has been completed if key is pressed again with help of keypad the locker door will be closed again. If an unauthorized person tries to scan his fingerprint image then an indication will be given by a buzzer which is interfaced to the controller and also if wrong password is entered by the user again indication will be given by the buzzer.

Keypad system:

In this application, all keys are used as data keys. The keypad is connected to Port. Each port is connected to the keypad, and scans the keys continuously. The columns of the keypad are pulled up with 10KΩ resistance to set them normally High. There are many methods depending on how you connect your keypad with your controller, but the basic logic is same. We make the columns as input and we drive the rows making them output, this whole procedure of reading the keyboard is called scanning. In order to detect which key is pressed from the matrix, we make row lines low one by one and read the columns

4. Result and Discussion

An RFID system consists of a reader device and transponder (tag). A transponder or tag has a unique serial number which is identified by the reader and is sent to microcontroller for checking. If an unauthorized person tries to enter then a notification will be sent to the authorized person by the GSM module which is

connected with the system. The user then has to enter his password via the keypad. The password is stored in EEPROM so that only registered user can reset it when desired. A keypad is used for inputting the password manually, which is a matrix of 4*4 elements. When one enters the code in the matrix keypad microcontroller verifies the code. The finger images are creates a template and store it in a memory slot. In the stage of matching, 1: N matching is done in which the user enters the finger print onto the optical sensor, a template is generated and is compared with all the templates stored in the memory slots. After matching the result is displayed on the screen.

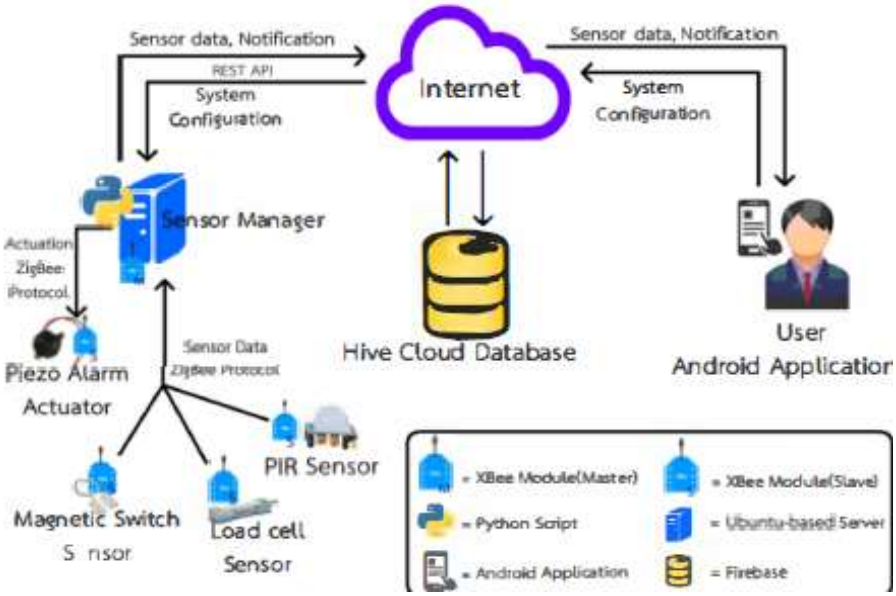

Figure 2.1 HIVE System Architecture

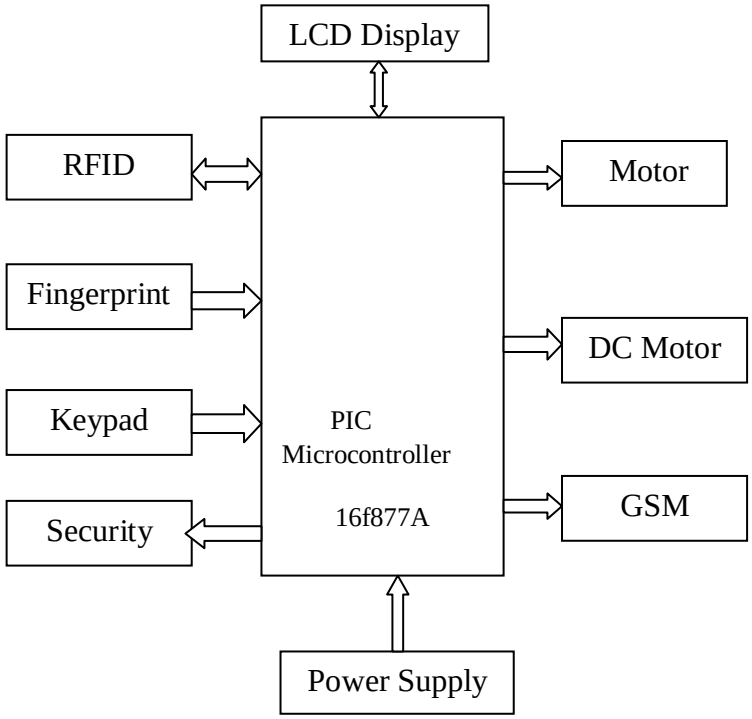

Figure 3.1 Block diagram of door locking system

5. Conclusion

GSM module can be used as a receiver, which send messages to the authorized person and notifies him mobile application. It can be useful for implementation of access control application for tracking system as well as providing the security benefits. The door lock is the physical impact of an invalid visitor and notifies the user's mobile device. The lock was designed to recover user suitability by allowing a valid visitor and open or close the door lock. The system is intellectual enough to monitor the secure environment. In addition, the user is informed about the security break through GSM network that provides a particular prospect whenever the user stays at far away from home.

References

1. Atzori.L, A. Iera, and G. Morabito, "The internet of things: A survey", Computer networks, vol. 54, no. 15, pp. 2787– 2805, 2015.
2. Gan G, Z. Lu, and J Jiang, "Internet of Things Security Analysis", IEEE Conf. on Internet Technology and Applications.
3. A. Aditya Shankar, P.R.K.Sastry, A. L.Vishnu Ram, A.Vamsidhar "Finger Print Based Door Locking System" International Journal Of Engineering And Computer Science, ISSN: 2319-7242, Volume 4, Issue 3, March 2015, Page No. 10810-10814.
4. Power D.H. and Fox C "System of Monitoring and Environmental Surveillance" http://www.dimap.es/enviromental-agriculturesservices.Html (2011). Oxford University Press, ISBN 0-8218-0531-2, 2014.
5. Suvarna Patil, TanujaLonhari, SarikaPati "Internet of Things: Current Research, Trends and Applications" International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 12, December 2015.
6. Miss. Pradnya R.Nehete & Dr. K P Rane, "OTP Based Door Lock Security System" ,International Journal For Emerging Trends in Engineering and Management Research (IJETEMR) Volume II, Issue II -21st June 2016.
7. Mahnoosh Mehrabani, Srinivas, Benjamin Stern "Personalized Speech Recognition for Internet of Things" International Conference on Future Internet of Things and Cloud.
8. Daramas A., S. Pattarakitsophon, K. Eiumtraku1, T. Tantidham N. Tamkittikhun "HIVE: Home Automation System for Intrusion Detection" 2016 Fifth ICT International Student Project Conference (ICT-ISPC).
9. Syam Krishna, J. Ravindra, January-February, 2012. Design and Implementation of Remote Home Security System Based on WSNS and GSM Technology, IJESAT, Vol. 2, Special issue 1, PP.139-14.
10. Abdallah Kassem and Sami El Murr Georges Jamous, Elie Saad and Marybelle Geagea "A Smart Lock System using Wi-Fi Security" 2016 3rd International Conference on Advances in Computational Tools for Engineering Applications (ACTEA).
11. HongleiRen, You Song, Siyu Yang and Fangling Situ "Secure Smart Home: A Voiceprint and Internet Based Authentication System for Remote Accessing", The 11th International Conference on Computer Science & Education (ICCSE 2016) August 23-25, 2016. Nagoya University, Japan
12. Ushie James Ogri, Donatus Enang Bassey Okwong, AkaisoEtim "Design and Construction of Door Locking Security System using GSM".
13. Yong Tae Park &PraneshSthapit& Jae-Young Pyun"Smart Digital Door Lock for the Home Automation".
14. Raqibull Hasan, Mohammad Monirujjaman Khan, Asaduzzaman Ashek, IsratJahan Rumpa "Microcontroller Based Home Security System with GSM Technology",Open Journal of Safety Science and Technology, 2015, 5, 55-62 Published Online June 2015 inSciRes.
15. R.Rohini, S.Ravi, "Detection of Residual Nodes in Wireless Sensor Networks by Node Weighting Algorithm " International Journal of Printing, Packaging & Allied Sciences, Vol. 5, No. 1, February 2017, ISSN: 2320-4367
16. G.Devi, R.Rohini, P. Suganya "Internet of Things: A Survey on Privacy and Security for Smart Homes", Institute of Integrative Omics and Applied Biotechnology, January 2017, ISSN: 0976 – 3104.
17. R.Rohini and R.K.Gnanamurthy, "Performance Analysis to Improve Quality of Service using Cluster Based Hidden Node Detection Algorithm in Wireless Sensor Networks", Intelligent Automation and Soft Computing, Taylor and Francis, Vol. 22, No. 2, 2016.

*****