International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 4, June 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

A Secure IoT Enabled Smart Home System

Dr. B. Kedarnath[1], M. Lalitha Priya[2], G. Anusha[2], K. Vamshi[2]

[1]HOD, [2]UG Student,
[1,2]Department of Electronics and Communication Engineering,
[1,2]Guru Nanak Institute of Technology, Ibrahimpatnam, Telangana, India

ABSTRACT

Internet of Things (IoT) conceptualizes the idea of remotely connecting and monitoring real world objects (things) through the Internet. When it comes to a house, this concept can be aptly incorporated to make it smarter, safer and automated. This project presents an approach to incorporate a two level biometric based security system in deploying Internet of Things (IoT) for smart home system, together with due consideration given to user convenience in operating the system using an android based application to monitor, control the electronic appliances in the house. The objective of the proposed system is to ensure that the access to enter the house and thereby render the services of certain automated electronic applications are only by the legitimate users, and not anyone else. By using biometrics it is possible to confirm or establish an individual's identity. Biometrics has the potential to make authentication dramatically faster, easier and more secure than traditional passwords. This project adds mainly four features: security, safety, control and monitoring to home automation. This approach ensures to provide all the operations done smartly thus avoiding any manual interventions until necessary. This project differentiates itself from others as it provides a low cost-effective, compact and reliable secured home control and monitoring system with the aid of biometric fingerprint authentication and biometric face recognition systems for access and to control the equipment and devices remotely using an application over a portable Android device. The proposed system is implemented on atmega328 based arduino microcontroller board. Face recognition is achieved using matlab.

KEYWORDS: *Smart Home, Home automation, Internet of Things, Arduino, Matlab, Face detection, Mobile devices, finger print*

How to cite this paper: Dr. B. Kedarnath | M. Lalitha Priya | G. Anusha | K. Vamshi "A Secure IoT Enabled Smart Home System" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-4, June 2020, pp.537-540, URL: www.ijtsrd.com/papers/ijtsrd31010.pdf

IJTSRD31010

1. INTRODUCTION

With the growing technology, the demand for smart things is drastically increased in daily-life. The IoT (Internet of Things) is one of the major components that provides facility to interact with IoT enabled devices. In this work, a secure and efficient smart home system is proposed that enable to protect homes from theft or unusual activities. This system is developed by exploiting the features of IoT that facilitates us to monitor an IoT enabled home from anywhere anytime over the Internet when data are stored in the cloud. This system uses a pir sensor to detect any human presence from the environment where the system is deployed. It then checks for biometric authentications and grants access to enter the house only if the biometrics are verified with the database elsewhere it considers the person to be an intruder and the doors remains unlocked. This system thus avoids any human interventions unless deemed necessary.

Figure1: Smart home

2. LITERATURE SURVEY

This paper provides a simple introduction to the IoT, its application and potential benefits to the society . IoT has received much attention from scientists, industry and government all over the world for its potential in changing modern day living. IoT is envisioned as billions of sensors connected to the internet through wireless and other communication technologies. The sensors would generate large amount of data which needs to be analyzed, interpreted and utilized . Domotics System uses the technology of Internet of Things for monitoring and controlling of the electrical and electronic appliances at home from any remote location by simply using a Smartphone. Implementation of a low cost, flexible home automation system is presented. It enhances the use of wireless communication which provides the user with remote control of various electronic and electrical appliances.

3. HISTORY

Home automation system is a kind of automation systems, which are used specifically for controlling the home appliances and devices mechanically (in some cases remotely)with the help of variety of control systems. The home automation systems are used for controlling the indoor & outdoor lights, heat, ventilation, air conditioning in the house, to lock or open the doors & gates, to control electrical & electronic appliances and so on using various control systems with appropriate sensors.

Early home automation began with labour-saving machines. In 1900s,self-contained electric or gas powered home appliances came into existence with the introduction of electric power distribution resulting to the introduction of washing machines (1904), water heaters (1889), refrigerators, sewing machines, dishwashers, and also clothes dryers.

The first general purpose home automation network technology, X10 was developed in 1975. It was considered as a communication protocol for electronic devices. For the purpose of signaling and control, it primarily make use of electric power transmission wiring, here the signals will provide brief radio frequency bursts of digital data, and remains most widely available.

4. SYSTEM DESIGN

A. Arduino UNO

The Arduino Uno is an open-source microcontroller board based on the Microchip ATmega328P microcontroller and developed by Arduino.cc. The board is equipped with sets of digital and analog input/output (I/O) pins that may be interfaced to various expansion boards (shields) and other circuits. The board has 14 digital I/O pins (six capable of PWM output), 6 analog I/O pins, and is programmable with the Arduino IDE (Integrated Development Environment), via a type B USB cable. It can be powered by the USB cable or by an external 9-volt battery, though it accepts voltages between 7 and 20 volts. It is also similar to the Arduino Nano and Leonardo. The hardware reference design is distributed under a Creative Commons Attribution Share-Alike 2.5 license and is available on the Arduino website. Layout and production files for some versions of the hardware are also available. The word "Uno" means "one" in Italian and was chosen to mark the initial release of Arduino Software. The Uno board is the first in a series of USB-based Arduino boards; it and version 1.0 of the Arduino IDE were the reference versions of Arduino, which have now evolved to newer releases. The ATmega328 on the board comes preprogrammed with a bootloader that allows uploading new code to it without the use of an external hardware programmer.

While the Uno communicates using the original STK500 Protocol, it differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it uses the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter.

Technical Specifications:

- Microcontroller: Microchip ATmega328P
- Operating Voltage: 5 Volts
- Input Voltage: 7 to 20 Volts
- Digital I/O Pins: 14 (of which 6 can provide PWM output)
- UART: 1
- I2C: 1
- SPPI: 1
- Analog Input Pins: 6
- DC Current per I/O Pin: 20 mA
- DC Current for 3.3V Pin: 50 mA
- Flash Memory: 32 KB of which 0.5 KB used by bootloader
- SRAM: 2 KB
- EEPROM: 1 KB
- Clock Speed: 16 MHz
- Length: 68.6 mm
- Width: 53.4 mm
- Weight: 25 g

Figure2: Arduino Uno

B. Modules and Sensors

In this project we used different modules and Sensors like

- IoT Module
- Pir Sensor
- Fingerprint Sensor
- Temperature Sensor

There are numerous definitions as to what a sensor is but I would like to define a sensor as an input device which provides an output with respect to specific physical quantity.

C. Components and Appliances

In this project we used components and home appliance devices to control using Iot are:

- Relay's
- Lcd display
- Power supply circuit

- Comparator
- Led's
- Bulb
- Cooling Fan
- Motor

5. METHODOLOGY

A. Hardware implementation

To make the desired system function we designed a block diagram that functions as per the desired functionality.

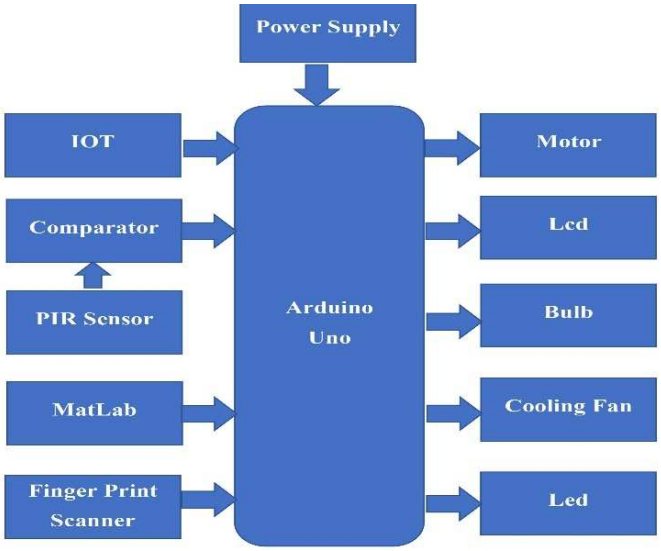

Figure 3: Block diagram of system

In hardware implementation we are using arduino Atmega328 as a controller. It has 14 digital input/output pins. The ATmega328 on the Arduino comes preprogrammed with boot loader that allows you to upload new code to it without the use of an external hardware programmer. Arduino does not have any wireless connection that's why we are using Wi-Fi module for wireless communication. ESP8266 Wi-Fi module is used for communication between android mobile app and arduino board. Arduino processes the received command and control the relay board. For electrical switches we use relay board that is connected to arduino. Here in our system we are using four relays and there are used to connect to different appliances like fan, bulb, motor. The relay is also used for switching of Rx(Arduino Rx pin) among Matlab and Iot and Tx(Arduino Tx pin) among Iot and Fingerprint circuit.

B. Software implementation

In this project the programming is divided into two parts:

B.A. Arduino Code

Arduino Software (IDE) - contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions and a series of menus. It connects to the Arduino and Genuino hardware to upload programs and communicate with them.

Programs written using Arduino Software (IDE) are called sketches. These sketches are written in the text editor and are saved with the file extension .ino. This code is used to control home appliances through Iot , manages the security through the fingerprint sensor and also used to perform face recognition by using matlab.

B.B Code for Face recognition:

The face recognition is done by using the Matlab software.

MATLAB (matrix laboratory) is a numerical computing environment and fourth-generation programming language. Developed by Math Works, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, Java, and Fortran. It is used in vast area, including signal and image processing, communications, control design, test and measurement, financial modeling and analysis, and computational.

6. SIMULATION AND RESULT

The person who wants to enter into the house need to confirm his identity by face recognition and Fingerprint verification. After the verification if he is an authorized person the motor turn on and the door will be opened otherwise the door remain closed.

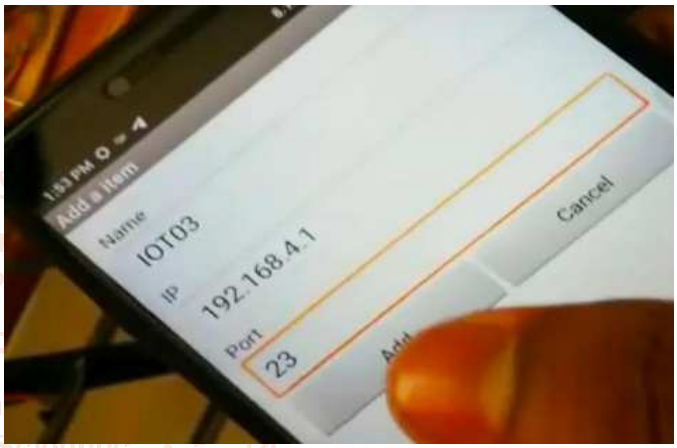

Figure 4: Adding the server in the app using Ip adress and port number

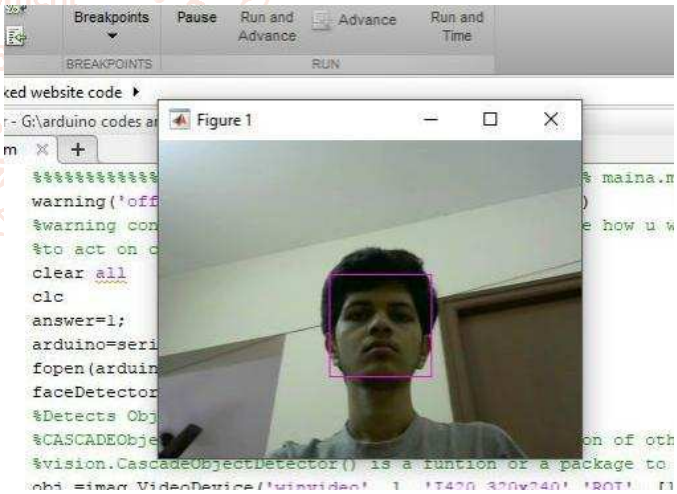

Figure 5: Face Detection Using Matlab

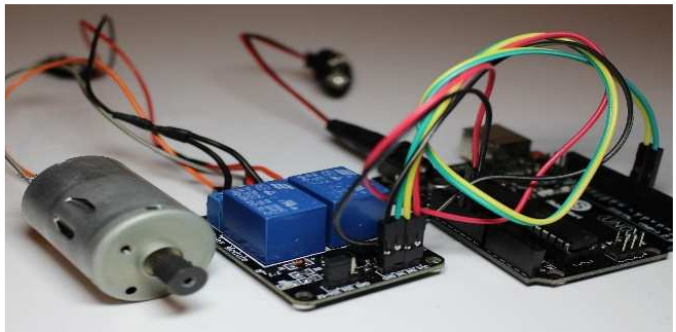

Figure 6: Motor acting as door connected with Arduino

7. CONCLUSION

Thus the proposed system is independent of the user's discretion and judgeability of the situation (whether it is a guest or an intruder entering his house) the use of a camera connected to the micro-controller helped the system to completely avoid manual interventions unless deemed necessary. In taking decisions whether to. The captured picture of the guest or intruder after face detection, can be mailed to the user. The user can further forward the same photograph to the police station if he wishes. Further the system may be made more synchronized by integrating the voice call feature within the same smart phone application through which the user can even control his home appliances without any voice call being triggered to his phone. It can also add additional features such incorporating call alerts and live video streaming for future reference and analysis.

REFERENCES

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

[2] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, Network Traffic Anomaly Detection and Prevention - Concepts, Techniques, and Tools, 1st ed., ser. Computer Communications and Networks Series. Springer International Germany, 2017.

[3] D. Choi, S. Seo, Y. Oh, and Y. Kang, "Two-Factor Fuzzy Commitment for Unmanned IoT Devices Security," IEEE Internet of Things Journal, vol. 6, no. 1, pp. 335–348, Feb 2019.

[4] N. Sriskanthan and T. Karand, "Bluetooth based home automation system," Journal of Microprocessors and Microsystems, vol. 26, pp. 281–289, 2002.

[5] R. Petrolo, V. Loscri, and N. Mitton, "Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms," Trans. Emerg. Telecommun. Technol., vol. 28, no. 1, pp. 1–12, 2015.

[6] S. Joshi, A. Joshi, S. Jabade, and A. Jathar, "M2M Communication Based Wireless SCADA for Real-Time Industrial Automation," International Journal of Research in Advent Technology, vol. 2, no. 4, pp. 107–109, 2014.

[7] A. C. Jose and R. Malekian, "Smart home automation security: A literature review," Smart Computing Review, vol. 5, no. 4, pp. 269–285, 2015.

[8] A. Z. Alkar and U. Buhur, "An internet based wireless home automation system for multifunctional devices," IEEE Transactions on Consumer Electronics, vol. 51, pp. 1169–1174, 2005.

[9] E. Yavuz, B. Hasan, I. Serkan, and K. Duygu, "Safe and secure pic based remote control application for intelligent home," International Journal of Computer Science and Network Security, vol. 7, no. 5, 2007.

[10] S. Das, N. Debabhuti, R. Das, S. Dutta, and A. Ghosh, "Embedded system for home automation using sms," in IEEE International Conference on Automation, Control, Energy and Systems, 2014, pp. 1–6.

[11] S. Kumar, "Ubiquitous smart home system using android application," International Journal of Computer Networks & Communications, vol. 6, no. 1, 2014.

[12] S. P. Tseng, B. R. Li, J. L. Pan, and C. Lin, "An application of internet of things with motion sensing on smart house," in IEEE International Conference on Orange Technologies, 2014, pp. 65–68.

[13] V. M. Reddy, N. Vinay, T. Pokharna, and S. S. K. Jha, "Internet of things enabled smart switch," in 13th International Conference on Wireless and Optical Communications Networks, 2016, pp. 1–4.

[14] M. Mongiello, F. Nocera, A. Parchitelli, L. Patrono, P. Rametta, L. Riccardi, and I. Sergi, "A Smart IoT-Aware System For Crisis Scenario Management," Journal of Communication Software and Systems, pp. 91–98, 2018.

Dr. B. Kedarnath currently working as a Professor and HOD in the discipline of Electronics and Communication Engineering, at Guru Nanak Institute of Technology and has a 24yrs of teaching experience in the field of 'Wireless communications'.

M. Lalitha Priya currently pursuing Bachelor of Engineering in the discipline of Electronics and Communication Engineering, at Guru Nanak Institute of Technology, Ibrahimpatnam, Hyderabad, Telangana.
E-Mail: msvnlpriya@gmail.com

K. Vamshi currently pursuing Bachelor of Engineering in the discipline of Electronics and Communication Engineering, at Guru Nanak Institute of Technology, Ibrahimpatnam, Hyderabad, Telangana. E-mail: Vamshikatterashala056@gmail.com

G. ANUSHA currently pursuing Bachelor of Engineering in the discipline of Electronics and Communication Engineering, at Guru Nanak Institute of Technology, Ibrahimpatnam, Hyderabad, Telangana.
E-Mail: anushagopathi98@gmail.com