Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 07, July-2019

Person's Identity Verification using Arduino Uno

[1]Suruchi Kaushik
Assistant Professor,
Institute of Information Technology and Management,
Department of IT,
D-29,Janakpuri Institutional Area,
New Delhi-110058, India

[3] Rakshit Sachdev
Student,
Institute of Information Technology and Management,
Department of IT,
D-29,Janakpuri Institutional Area,
New Delhi-110058, India

[2] Nishant Arora
Student,
Institute of Information Technology and Management,
Department of IT,
D-29,Janakpuri Institutional Area,
New Delhi-110058, India

[4] Vaibhav Ahluwalia
Student,
Institute of Information Technology and Management,
Department of IT,
D-29,Janakpuri Institutional Area,
New Delhi-110058, India

Abstract: **Internet of things is a fast emerging technology captivating attention of information technologists, innovators and academician world over. IoT provides cost effective and reliable solutions to a variety of problems faced by human race and to the security issues which is a serious matter of concern. Existing smart home security methods use sensors and cameras to operate the connected devices in home and send an alert to the user in case of an intrusion. In case a visitor has to be identified, the conventional method for identifying a person working for an organization is the identity-card issued by the employer which is not reliable. This paper presents a model to authenticate a person's identity based on the fingerprint scan of the person followed by an OTP based authentication. The OTP is generated and sent to the device using Google's SMTP server. It uses two-stage verification for identifying the Person.**

Keywords: IOT, Fingerprint Scan, OTP authentication, SMTP

1. INTRODUCTION

Internet of Things in simple terms can be defined as a connection between the 'things' around us using internet. Today we live in a world where not only people but things are also connected to each other using the internet. The information shared between the things and the people can be as simple as notifying the temperature in a room and as complicated as controlling the temperature of air conditioner depending on the number of persons in the room.

The internet of things (IoT) is a technology in which the basic underlying principle is that the physical objects or the things are connected to the internet and communicate with the environment in an intelligent manner. Internet is a global network which connects billions of users in the world. 'Things' in internet of things are objects in the physical world which can be electronic such as smart phone or objects which we do not consider electronic at all such as a pen. Thus IoT gives a unique identity to things which can communicate with each other and collect useful information.

Kevin Ashton is known for coining the term "the Internet of Things" to describe a system where the Internet is connected to the physical world via ubiquitous sensors[1]. Using a wide variety of sensors available, communication is possible between the things and the environment. Sensors can collect data from the environment and process the data to convert it into meaningful information. Sensors can be used to monitor the air quality, temperature, humidity, heartbeat and even gestures. The interaction between all connected devices can help to identify desirable and undesirable changes in the environment and hence communicate it to the user by simply sending a notification to the user on his/her smart device. Most commonly used smart device of course is a smart phone which is used to stay connected with other people and devices. Use of smart devices has gained popularity because people can stay connected and share information anytime from anywhere. Widespread use of smart devices such as smart phones, tablets, smart watches etc. have made everyday life easier. By staying connected to these devices one can easily monitor the health and environment and manage the natural resources in an efficient way.

Today, one of the major issues of concern is security of the people and of their possessions including their personal data. Smart security and automation systems are being developed to cater to comfort and safety needs. One important aspect of smart homes is safety and security. IoT technology provides easy and less costly solutions to the issues of security in homes which can also be extended to offices and anywhere where identity of a person needs to be verified. To make sure that the concerned person is from an authentic background different ways have been used.

The Home Security Systems which exist in the market are mostly based on Camera and sensors like IR, Ultrasonic, Motion etc. Their major focus is only for the intruder alert. These systems gather input from these sensors and inform the user. The verification of an employee (Salesman, Repairman or even any Government official) is only limited to physical identification cards. Although, some of the companies/organizations are moving away from these ID cards by texting the customer at home about the details of their employees but that too is not fully secure.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 07, July-2019

2. RELATED WORK

2.1 Bluetooth based home automation system

IOT promises to improve the quality of life and make it more simple and safe. IOT technology can be used for saving time and for efficient use of resources. A home automation system based on Bluetooth technology was proposed in [2]. Arduino board and cell phone are used to control the home appliances. The implementation of the system is low cost and flexible but the Bluetooth has a short range. The main disadvantage of this design is that phone has to be in the range of 50 meters otherwise it would not be able to control the appliances**.**

2.2 Voice recognition based home automation system

Home appliances can be controlled by directly communicating with them by giving voice commands. [3] presented a voice controlled home automation system using smart phones. An Arduino UNO microcontroller is used as control unit and the connection between Arduino board and smart phone is set up by Bluetooth. This system reduces human effort as the appliances can be controlled by voice without any requirement of manual presence of someone. Voice based automation system is low cost and reliable but main disadvantage is that noise can distort the input voice signal thus interfering in the command given by a person.

2.3 Finger Print Based Systems

A finger print based door opening system was presented in [4]. This is an efficient and reliable method to provide security in homes, banks, offices etc. The identity of a person can be verified using finger print sensor and only authenticated person is allowed to enter the premises. In case the fingerprint does not match an indication is given by the buzzer.

In [5] a person's authentication is done by using a fingerprint sensor and all the information such as time and attendance is updated on the web server through ESP8266 and Wi- Fi router. This paper uses internet of things technology for time and attendance management.

2.4 Home automation and security using Node MCU

Dual aspects of home security and home automation were presented in which an intruder alert is sent through e-mail by capturing image of the person [6]. The prototype can also be used for controlling appliances such as lights and fans which are controlled by using microcontroller. Same set of sensors are used for dual problems of security and home automation. IR sensors are placed at the entrance of building to detect the motion and an image is captured and sent to the user. In case of an intruder the owner can switch ON the lights and fans to warn the intruder, or in case of a guest the user can provide access by opening the door. The main advantage of this system is that even when wi-fi services are not available 3G or 4G services can be used for sending alerts and communicating.

3. PROPOSED SYSTEM DESCRIPTION

Person's Identity Verification is a System in which a user can verify identity of anyone whose biometric data is stored in the server i.e. in the database. This system is made for home security. In this system, a Fingerprint scanner, a keypad, a LCD Display and NodeMCU are used. First, the visitor puts his/her finger at the scanner present alongside doorbell. The scanner will verify if the database matches to any of the employee of the concerned company. Then generation of OTP is done after the verification of the person. A random number will be generated through random function and it will be used as OTP. After the generation of OTP is successful, the OTP is sent through an email using SMTP to the person as well as the Arduino board. The email is stored in the database. Each fingerprint has its own hash code which is linked to an email address. The user will enter the OTP which is being sent to his/her email address using a keypad which is present along with the fingerprint scanner. The keypad is connected to the Arduino Board which will verify the OTP. If the entered OTP matches to the one being sent to the Arduino, the verification will be successful. The last step is to display whether the verification is successful or not to the user inside the house on a LCD display. If verification is positive, the user will get a message so that he can let the person inside the house, otherwise he can call any emergency number for help.

Tools/ Platform Used

Hardware Used:

1. Arduino UNO R3
2. Fingerprint Module
3. Node MCU (With ESP8266)
4. 16x2 LCD Display
5. 3x3 Keypad
6. Resistors
7. Jumper Wires

Software Used:

1. Operating System
2. Arduino IDE

4. METHODOLOGY/WORKING

The Person's Identity Verification System is an Arduino based system. The core hardware component of the system is the Arduino Uno board. This board is connected to each component and acts as the control unit of the project. The other hardware components connected to it are: Fingerprint Module, Keypad, LCD Display, NodeMCU which is further connected to a database and internet server. The fingerprint module and keypad acts as the input device. These hardware components take input from the user and sends that data to the Arduino Uno board to process that. After the input is being sent to the Arduino, NodeMCU receives information from the board and updates that information on the database as well as internet server. The end user can view information through internet. The last component is the LCD Display which acts as an output module. It is connected to the Arduino Board. It displays the verification result to the user at home.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 07, July-2019

5. BLOCK DIAGRAM

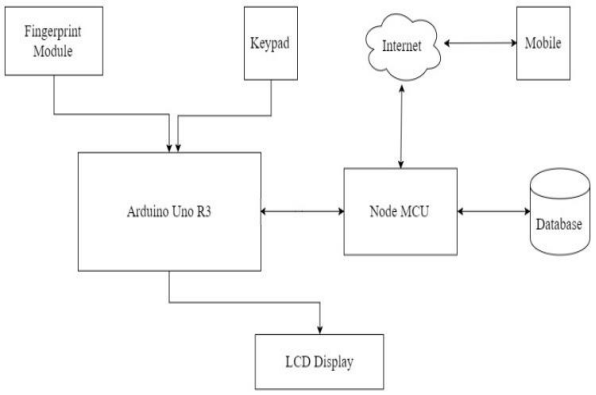

Figure 1: Block Diagram

6. FLOW CHART

The Person's Identity Verification System starts when the person first put his finger on the scanner. After the fingerprint scan, the module verifies if the scanned finger matches to the database. If there is a match, the module then sends an OTP to the person via e-mail notification using SMTP protocol. The OTP is also stored in the temporary database of the Arduino UNO. After the person receives the OTP, he/she enter that OTP through the keypad which is attached along the fingerprint scanner. If the OTP matches, the verification is successful and there is a message displayed on the LCD Display: "PIN Verified". If not, it will display: "Verification not successful".

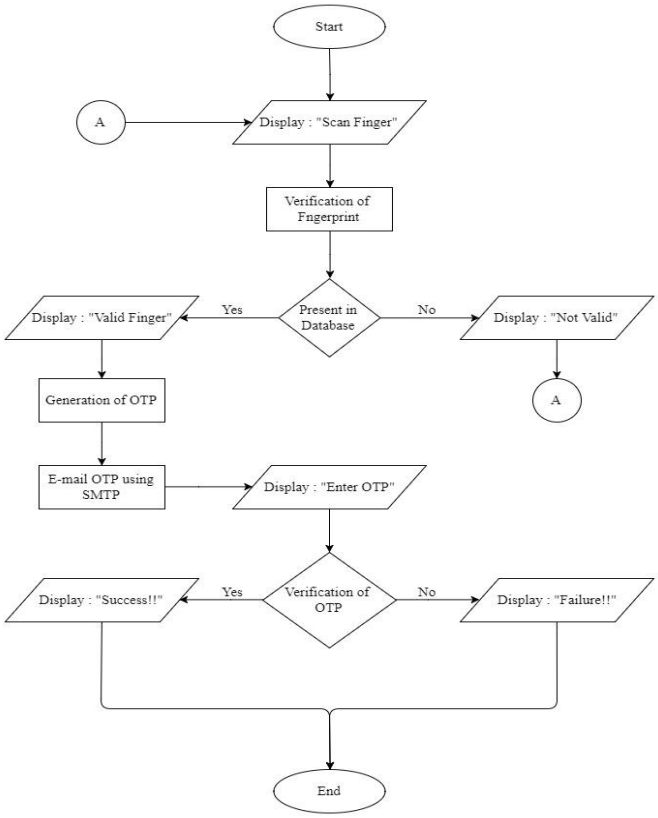

Figure 2: Flow Chart

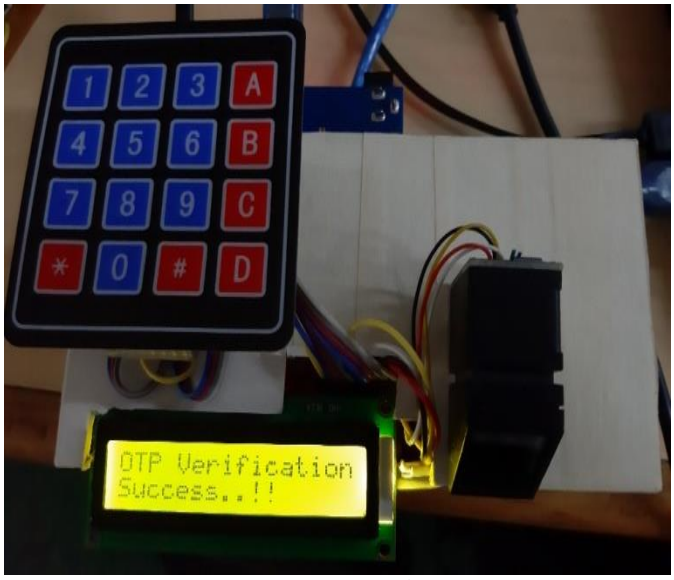

Figure 3: Person's Identity Verification Module

7. RESULTS

The Serial Monitor is showing the established connection of NodeMCU with the mobile hotspot to access internet.

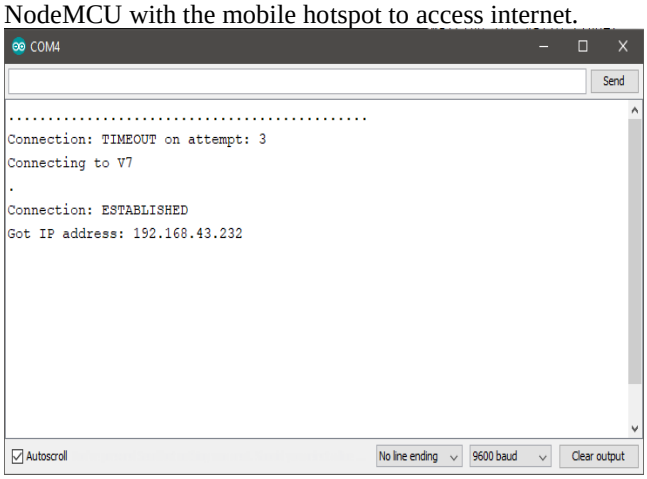

Figure 4: NodeMCU Connection with Internet

Fingerprint Sensor is connected to Arduino UNO R3 and is waiting for a valid finger.

Figure 5:Fingerprint Detected on Arduino

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 07, July-2019

After the Successful Fingerprint Verification, NodeMCU sends an OTP to the stored E-mail Id.

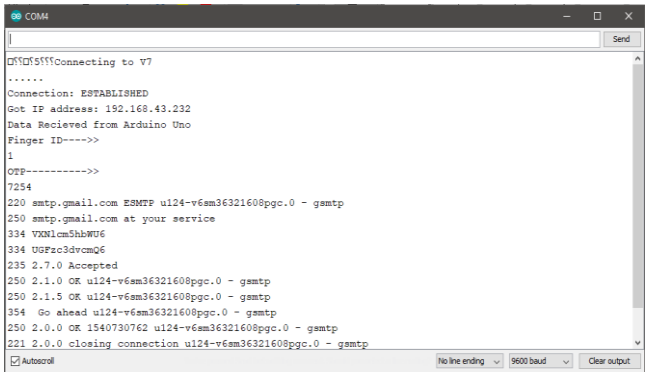

Figure 6: Sending Email using Gmail SMTP Server

The OTP is Received on the registered E-Mail.

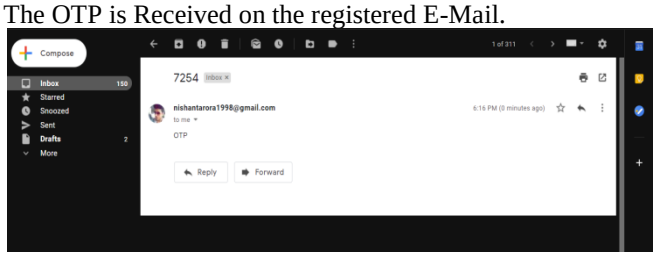

Figure 7: OTP Received on Gmail

After the received OTP is entered through the 4x4 Matrix Keypad, the OTP is being verified.

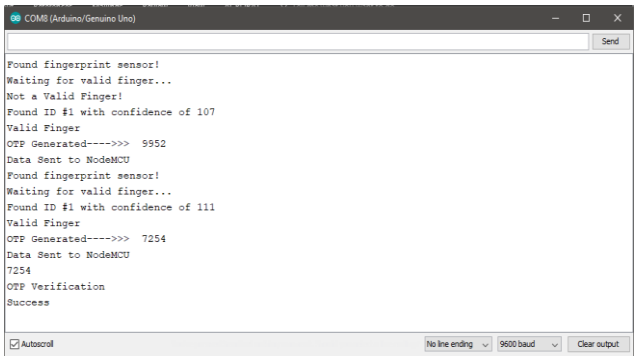

Figure 8: OTP Verified

8. FUTURE SCOPE AND CONCLUSION

Internet has become an important part of human's social life and educational life without which they are just helpless. The Internet of things (IOT) devices not only controls but also monitors the electronic, electrical and various mechanical systems which are used in various types of infrastructures. The Home Security System which exist in the market are mostly based on Camera and sensors like IR, Ultrasonic, Motion etc. There major focus is only for the intruder alert. This project is a unique and new idea which is implementing IOT so there is a lot of scope of improvement and modification in the future versions. In future, instead of creating a database, AADHAAR database can be linked to the backend server which will reduce cut the cost by huge margins. The cost of maintaining database is large as there has to be proper backups and efficiency. Camera can be added to the module which will increase the security. The camera will capture the image of any person who tries to imitate someone. If the verification is unsuccessful, it may capture the image. Other Modifications can be done like adding notifications to the household owners if there is some unusual activity recorded. As we are moving towards Digital India and there are many smart city projects going on, the model can be used for security in smart homes.

9. REFERENCES

[1] Kevin Ashton, That 'Internet of Things' Thing, RFID Journal, June, 2009.

[2] R Piyare, M .Tazil,Bluetooth Based Home automation system using cellphone,Article in IEEE 15th International Symposium on Consumer Electronics,2011.

[3] Sonali Sen, Shamik Chakrabarty, Raghav Toshniwal, Ankita Bhaumik, Design of an Intelligent Voice Controlled Home Automation System, *International Journal of Computer Applications (0975 – 8887), Volume 121 – No.15, July 2015.*

[4] 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*

[5] Divil Jain 1, Dr. P.S. Ramkumar2, Dr.K.V.S.S.S.S Sairam, IoT based Biometric Access Control System, International Journal of Innovative Research in Science, Engineering and Technology,Vol.5,Special Issue 9, May 2016.

[6] Sudha Kousalya, G. Reddi Priya, R. Vasanthi,B Venkatesh,IOT Based Smart Security and Smart Home Automation, International Journal of Engineering Research & Technology (IJERT),Vol. 7 Issue 04, April-2018, http://www.ijert.org, ISSN: 2278-0181

[7] "The working principle of an Arduino - IEEE Conference Publication", *Ieeexplore.ieee.org*, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/6997578/. (Accessed: 06-Aug- 2018).

[8] Electronics for You. (2018). *Arduino Based GSM Home Security System*. [online] Available at: https://electronicsforu.com/electronics-projects/arduino-gsm-home-security-system [Accessed 28 Oct. 2018].

[9] AADHAR BASED ELECTRONIC VOTING SYSTEM USING BIOMETRIC AUTHENTICATION AND IOT. (2017). *International Journal of Recent Trends in Engineering and Research*, 3(3), pp.203-208.

[10] Author: M. (2018). *Arduino Uno, Gmail*. [online] Instructables.com. Available at: https://www.instructables.com/id/Arduino-Uno-Gmail/ [Accessed 28 Oct. 2018].

[11] HOME AUTOMATION USING ARDUINO. (2018). *International Journal of Recent Trends in Engineering and Research*, pp.195-199.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)