



## **BIOMETRIC CONFIRMATION AND ALERT SYSTEM**

P.Jayashree<sup>1</sup>, A.Athimoolam<sup>2</sup>, G.Baskaran<sup>3</sup>, K.Kaaviya<sup>4</sup>

**Abstract-**The major concern for the households and the office environment today is security, and for this concern various approaches are in place to address the problem. Additionally, terrorism and unauthorized access to places have become a major issue now-a-days, and there is a need for a secure system to prevent unauthorized access especially in shared access environment. With this consideration, a design and prototype of a biometric fingerprint based alert and confirmation system has been developed. Humans have used their fingerprints for personal identification for many centuries and the matching accuracy using fingerprints has been very high. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip which is unique for every person. The proposed system is reliable and very secure for ease lifestyle. In this, fingerprints of the authorized users are enrolled and verified to provide access to a facility that is used by multiple users which can be used for the working faculties in schools, colleges etc. This is an Arduino uno based flexible working device which provides physical security using the fingerprint sensor technology. NodeMCU (Node Microcontroller Unit) is used to send notification to the personnel to alert the user some time before they keep their finger print and to send an confirmation message once after they have registered their finger print in the biometric system.

**Keywords:** Biometric, fingerprint, matching, confirmation, alert, notification

### **1. INTRODUCTION OF BIOMETRIC SYSTEM**

Fingerprint is a form of biometric identification which is unique as well as does not change in one's entire lifetime. Fingerprints are matched with the stored fingerprints by using the scanner. With technology affecting every aspect of modern living and our world becoming increasingly digitized, protection of confidential information becomes more difficult. This has put the focus on biometric security which is the effective way to prove an individual's identity. Biometric systems are used to recognize individuals and regulate access to physical spaces, information, services, and to other rights or benefits. It includes improving the convenience and efficiency of routine access transactions, reducing fraud, and enhancing public safety and national security. Arduino is connected with finger print sensor and nodeMCU. NodeMCU Development board is featured with analog pins, digital pins, wifi capability, and serial communication protocols. The nodeMCU is an open source software and hardware development environment that is built around a very inexpensive System-on-a-Chip (SoC) called the ESP8266. This project aims to give an alert and confirmation message once the individual has kept the fingerprint on the biometric system concerning improved security for the individual because the finger print can be captured by the scanner and stored to use later, without the person being present.

### **2. LITERATURE REVIEW**

#### *2.1 Existing Methodology*

Various aspects of everyday life are slowly becoming digitized as our life experiences and creative efforts are accumulated in personal computers, digital media devices, and mobile devices. The use of passwords and other authentication methods protected these collections of personal and potentially confidential information. Traditional confidentiality and authentication methods (e.g., personal passwords) are not secure nowadays. In addition it also requires the user to remember a variety of passwords, which can result in user error, passwords can be stolen and pure password authentication is vulnerable to unintentional information disclosure.

#### *2.2 Disadvantages of Existing Method*

It only alerts the user when the fingerprint is kept and there is no confirmation message. Forgetting passwords may lead to higher risk. Physical attributes are much harder to fake than identity cards and does not provide strong identity check (only based on password).

### **3. HARDWARE REQUIREMENT**

- Finger print sensor
- Arduino Controller
- NodeMCU

<sup>1</sup> Assistant Professor, Department of EIE, Kongu Engineering College, Perundurai, Tamilnadu, India

<sup>2,3,4</sup> Final Year Student, Department of EIE, Kongu Engineering College, Perundurai, Tamilnadu, India

#### 4. TECHNICAL DESCRIPTION

Working of Finger Print Sensor: The basic concept of a finger print sensor is an optical scanner which is a Charge Coupled Device (CCD), the same light sensor system used in digital cameras and camcorders. An optical scanner uses visible light (photons) to create multiple fingerprint patterns (minutiae).

A CCD is simply an array of light sensitive diodes called photosites, which generates an electrical signal in response to the light photons. Each photosite records a pixel, a tiny dot representing the light hitting that spot.

Working of Arduino Controller: Arduino is an open-source platform used for building electronics projects. Arduino consists of both a physical programmable circuit board (often referred to as a microcontroller) and a piece of software, or IDE (Integrated Development Environment) that runs on Windows, Macintosh OSX, and Linux operating systems, used to write and upload computer code to the physical board.

Working of NodeMCU: NodeMCU Development board is featured with wifi capability, analog pin, digital pins and serial communication protocols. ESP8266 module is programmed directly using the Arduino IDE.

#### 5. BLOCK DIAGRAM OF PROPOSED METHOD

The block diagram of proposed methodology is shown in the Figure 1. Integrated Development Environment (IDE) software is used for coding which is to be dumped into arduino to receive the signal from finger print sensor.

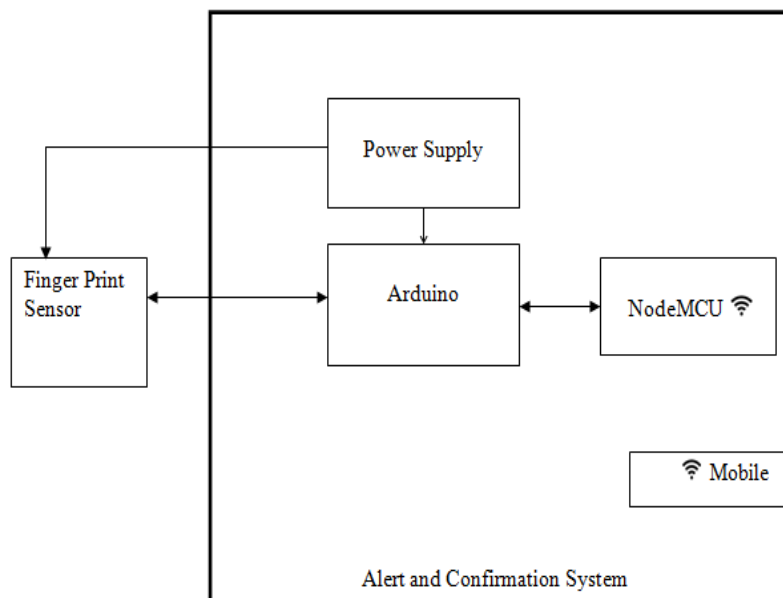


Figure 1. Block Diagram of the Process

#### 6. PROCESS FLOW CHART

Adafruit fingerprint sensor library is uploaded into arduino IDE and the program is compiled. The Figure 2 explains in detail about the flow of programming in the proposed method. If the authorized user does not keep the finger print within the time interval of 10 minutes, alert notification is sent to user's mobile. If the authorized user keeps the finger print within the time interval, the user ID is read by the arduino and checks whether the given ID of the user has been registered or not. When a person keeps the finger on the scan, and if the finger print of the person is registered, the output will go HIGH and a confirmation message will be sent to the user's mobile. If the finger print of the person is not registered, the output will go LOW and there will be no output from arduino.

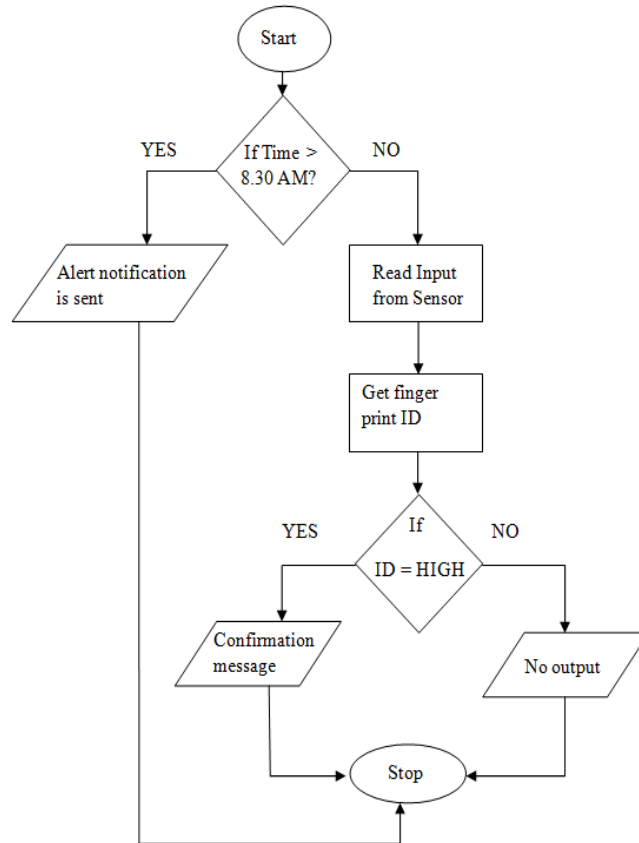


Figure 2.Flow Chart of Proposed Method

## 7. CIRCUIT DIAGRAM OF PROPOSED METHOD

The Figure 3 shows the circuit diagram for the proposed method which consists of an arduinouno, an optical finger print sensor and a nodeMCU. The receiver (RX) and transmitter (TX) pins of the finger print sensor are connected to the receiver (3) and transmitter (2) pins of arduino. The digital pin of nodeMCU (D4) is connected with the digital pin (11) of arduino. The ground and the power supply pins of nodeMCU are connected with the ground and power supply pins of arduino respectively.

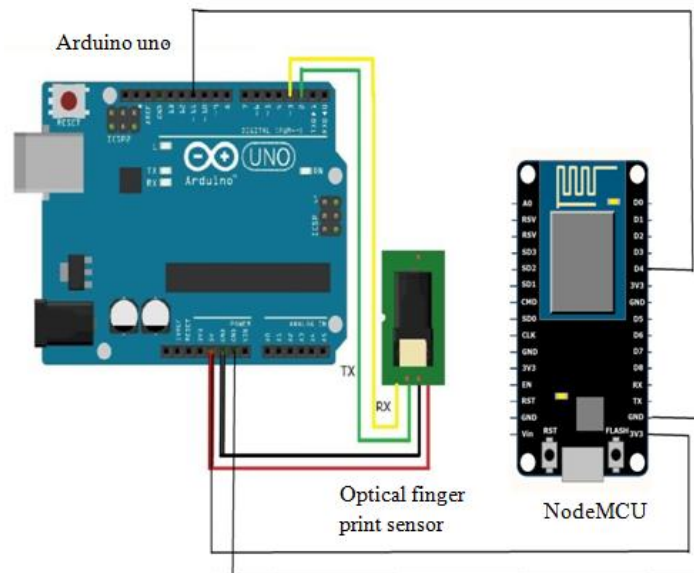


Figure 3.Circuit Diagram of Proposed Method

## 8. RESULT AND DISCUSSION

The behaviour of the system is discussed in this section. Various tests are devised to see if the individual functions are performing accordingly. After implementation of the tests, the results are collected to verify the functionalities of the individual components and the system was tested fully for any error. After saving the fingerprint, accuracy was tested and the finger was tried placing partially, inverted, in wet conditions etc. and checked whether the sensor was able to match the prints. When the finger is extremely dirty or oily, it did fail. But the sensor seems to get the reading right when the finger is less dirty or oily. The sensor claims to have 99% rate of accuracy and it seems to be living up to its promise.

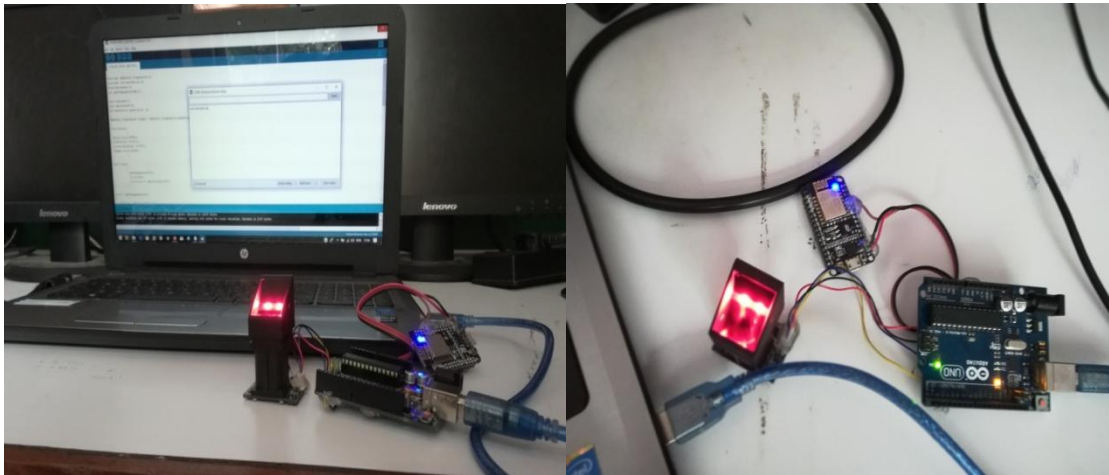
Finger print of a person is sensed by optical finger print sensor and an alert message is sent using nodeMCU and once the finger print is matched, confirmation message is sent to the person's mobile phone.

Table 7.1 shows that if the authorized user registers their fingerprint a confirmation message will be sent to the user, or if the authorized user doesn't register their finger print then an alert message will be sent to the user. If any unauthorized user keeps the finger on the scan there will be no output from nodeMCU.

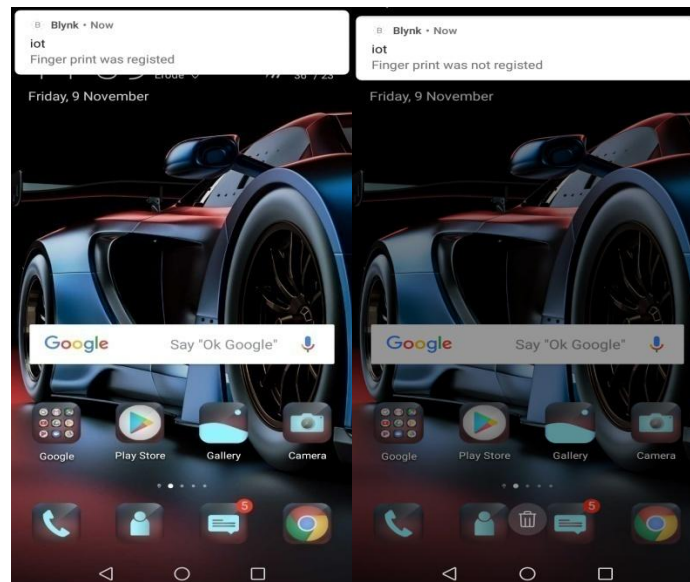
Table 8.1 Result of Biometric System at 8.30 AM

S.No	Print ID	Finger Bearer	Status	Message
1	86	Authorized user	Confirmation	Finger print was registered
2	87	Authorized user	Alert	Finger print was not registered
3	X	Unauthorized user	No output	No message will be sent

### Experimental Setup



### Project Output



## 9. FUTURE SCOPE

As the technologies and applications in biometrics evolve, the drawing up of comprehensive and adaptable standards to govern the sector will be a challenge, for the future. On smart phones and tablets, fingerprints are by far the most common form of biometric identification. This technology can be extended to more number of users which can be used in big organisations. Biometric technologies will significantly change the world and it depends upon the usage whether for good or bad purposes.

## 10. REFERENCES

- [1] Akinduyite CO, Adetunmbi AO, Olabode OO, Ibadunmoye EO (2013) "Fingerprint-Based Attendance Management System" Journal of Computer Sciences and Applications 1(5), pp 100-105.
- [2] Chintalapati S, Raghunadh MV (2013) "Automated attendance management system based on face recognition algorithms" IEEE International Conference on Computational Intelligence and Computing Research, Enathi.
- [3] Khatun AK, Haque MF, Ahmed S, Rahman MM (2015) "Design and implementation of iris recognition based attendance management system" International Conference on Electrical Engineering and Information Communication Technology (ICEEICT), Dhaka.
- [4] Lim TS, Sim SC and Mansor MM (2009) "RFID based attendance system" IEEE Symposium on Industrial Electronics & Applications Kuala Lumpur, pp 778-782.
- [5] Ujan, Ismaili IA (2011) "Biometric attendance system" IEEE/ICME International Conference on Complex Medical Engineering, Harbin Heilongjiang, pp 499-501.