

Fingerprint Sensor Based Controlling and Operation of Power Supply with GSM

Saawan Hiwale¹, Priyanka Haramkar¹, Pranjal Patil¹, Dipak Mhaske¹, Vishvajitsingh Rajput¹, Manmohan Sharma²

¹Student, Department of Electrical Engineering, Sant Gadge Baba Amravati University, Amravati, India.

²Professor, Department of Electrical Engineering, Sant Gadge Baba Amravati University, Amravati, India.

Pankaj Ladhhad Institute of Technology and Management Studies, Buldana, Maharashtra, India.

Corresponding Author: sawanhiwale8797@gmail.com

Abstract: - The use of fingerprint for identity has been used in regulation enforcement for approximately a century. Fingerprint-based identification is one of the most crucial biometric technologies that have drawn a great quantity of attention recently. The electronic lock the usage of fingerprint recognition includes a method of verifying the user's identification by means of the usage of fingerprint recognition as a key to electronic lock. The work highlights the development of fingerprint reputation device the usage of Arduino Uno. Verification is finished by using evaluating the record of authorized fingerprint image with incoming fingerprint photograph. The incoming fingerprint photograph will first undergo the extraction and filtering processes. Then the fact of incoming fingerprint picture will go through the comparison system to evaluate it with legal fingerprint picture. If the picture matched with legal fingerprint photo then gadget will turn on the principle deliver and display the data on LCD. It may also tell the legal person by means of sending SMS with the use of GSM module. One of much broader utility of fingerprint is offering safety for sensible labs in collages. In this context, we are supplying fingerprint access manipulate for Power Supply in lab. So most effective legal character is chargeable for use of device.

Key Words - Fingerprints, GSM Module, LCD.

I. INTRODUCTION

The subject of biometrics, or the identification of people based on physiological or behavioural characteristics, has recently received an extensive quantity of interest in current studies as a result of its applicability within the fields of information technology and security. With the accelerated utilization of PIN numbers and passwords in regular life, the vulnerabilities of those technologies have become more apparent (e.g. password-cracking). Biometric authorization's strengths are that it calls for the person to be present and that it eliminates the hassles of passwords and PIN's (or may be utilized in parallel with those for added security). Specifically, online identity verification, ATM machines, and constructing front authorization, are all region where it is very useful to implement an automatic identification. Some of the technology which have been investigated are fingerprinting, iris scanning, facial scanning, voice detection, and palm scanning. Of these, fingerprinting has been in improvement for the longest, and even as the other technologies have attracted more current interest in journals and research groups, we are focusing on the potential to conduct robust fingerprint verification with minimal overhead. The FBI can

effortlessly afford the fanciest new technology, however at the patron and civilian level, charge is a super limiting factor, which is why virtual video technologies for biometrics haven't begun to make whole lot headway within the marketplace. The cause of our task was to layout a fingerprint verification machine that might reliably confirm the identification of a person through matching the scanned fingerprint to a database (that contains images of all of the people in the device). The aim of the task was to operate the Power Supply using this device.

II. MOTIVATION AND OBJECTIVE

A. Motivation

Maintaining the proper record of Power Supply is very important for every organization whether it be an educational institution or business organization. Designing a Fingerprint sensor based power supply system for improving practical lab security. So that only authorized person can use the system was an important key behind motivating this project. This would improve accuracy of a consumption of load records because it will

not allow unauthorized person to access the system. I try to make an application with this technology

B. Objective

- The devices will be controlled by manual operation.
- Low power consumption, low cost, small size, excellent performance.
- To maximize accuracy.
- Power Consumption is low.
- A fingerprint recognition system can be used for both verification and identification.
- Using GSM module warn the authorized user in case of forgery use.

III. BLOCK DIAGRAM AND WORKING

A. Component used

- ARDUINO UNO
- GSM MODULE
- RELAY MODULE
- FINGERPRINT MODULE
- LCD DISPLAY
- LOAD
- POWER SUPPLY

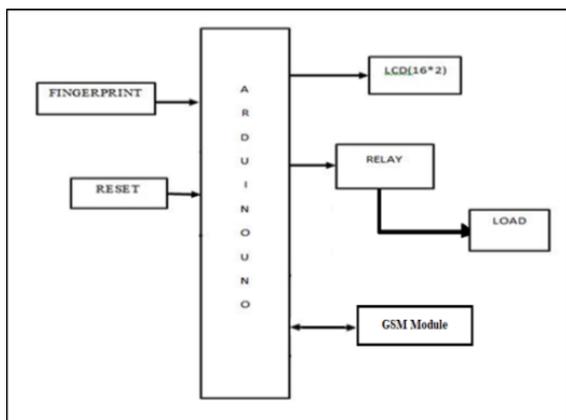


Fig.1. Block Diagram

1) Arduino Uno:

The Arduino Uno is a microcontroller board based on the ATmega328 (datasheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an

ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started. The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter.

- Microcontroller ATmega328
- Operating Voltage 5V.
- Input Voltage (recommended) 7-12V.
- Input Voltage (limits) 6-20V.
- Digital I/O Pins 14 (of which 6 provide PWM output).
- Analog Input Pins 6.
- DC Current per I/O Pin 40 mA.
- DC Current for 3.3V Pin 50 mA.
- Flash Memory 32 KB (ATmega328) of which 0.5 KB used by bootloaders.
- RAM 2 KB (ATmega328).
- Clock Speed 16 MHz

2) Relay module:

An easy electromagnetic relay includes a coil of cord wrapped round a soft iron core, an iron yoke which presents a low reluctance course for magnetic flux, a movable iron armature, and one or more sets of contacts. The armature is hinged to the yoke and routinely linked to one or extra unit of moving contacts. It is held in place by way of a spring so that after the relay is de-energized there's an air gap inside the magnetic circuit. In this condition, one of the two units of contacts within the relay pictured is closed, and the alternative set is open. Other relays may additionally have extra or fewer units of contacts depending on their function. The relay in the photo also has a twine connecting the armature to the yoke. This guarantees continuity of the circuit between the moving contacts at the armature, and the circuit track on the revealed circuit board (PCB) through the yoke, that's soldered to the PCB.



Fig.2. Relay Module

3) Fingerprint Module R307:

R307 Fingerprint Module includes optical fingerprint sensor, high-velocity DSP processor, high-overall performance fingerprint alignment algorithm, high-capability FLASH chips and different hardware and software program composition, solid overall performance, easy structure, with fingerprint entry, picture processing, fingerprint matching, seek and template storage and different functions.

- Supply voltage: DC 4.2 ~ 6.0V.
- Supply current: 50mA (typical)
- Peak current: 80mA.
- Fingerprint photograph input time: <0.3 seconds

4) GSM Module:

A GSM Module is basically a GSM Modem (like SIM 900A) connected to a PCB with different types of output taken from the board – say TTL Output (for Arduino, 8051 and other microcontrollers) and RS232 Output to interface directly with a PC (private computer). The board may even have pins or provisions to connect mic and speaker, to take out +5V or other values of power and ground connections. These kinds of provisions range with one of kind modules.



Fig.3. GSM Module

IV. WORKING

- Switch on power supply of Arduino uno.
- Here Fingerprint Database will be created.
- User will provide his Fingerprint Data through fingerprint module.
- Controller compares the data with stored database.
- If the match score exceeds the threshold, the result is a match and controller sends the signal to relay to turn on main supply. Information is displayed on

LCD screen that power supply is ON and same information and same is sent to user through SMS using GSM module.

- When a person whose fingerprint data is not stored in system when try to access the system then in that case system will not respond to him and deny his access. Thus system remains unaffected and warns the authorized user by sending SMS that someone is trying to access the system.
- The authorized person can turn OFF the main supply by using his enrolled fingerprint. In this case controller sends the signal to relay to turn OFF main supply and information is displayed on LCD that power supply is OFF. Same information is sent to user using GSM module.

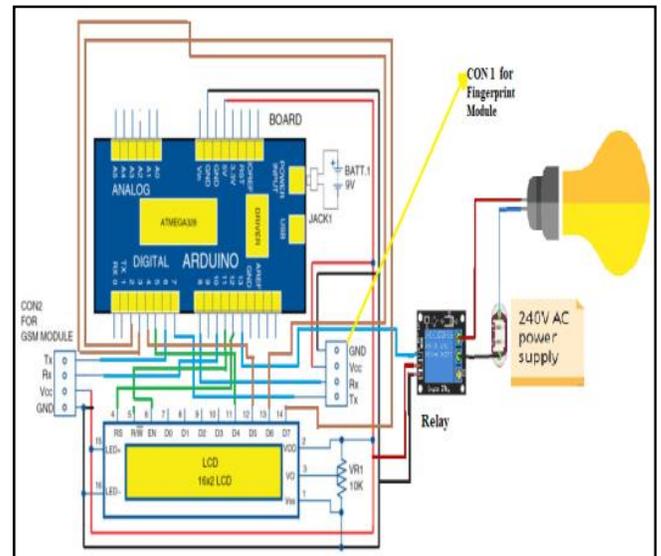


Fig.4. Circuit Diagram

V. RESULTS AND DISCUSSION

When a person provides Fingerprint data it is compared with user's enrolled fingerprint template. If the match score exceeds the threshold, the result is a match and controller sends the signal to relay to turn on main supply. Information is displayed on LCD screen that power supply is ON and same information and same is sent to user through SMS using GSM module. Thus the user can monitor the use of power supply.

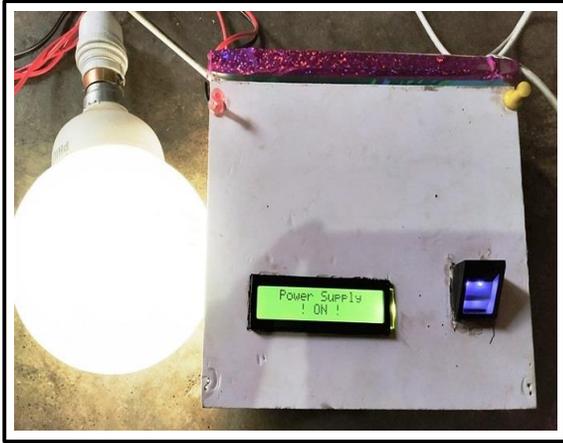


Fig.5. System Turn ON Main Supply

When a person whose fingerprint data is not stored in system try to access the system then in that case system will not respond to him and deny his access. Thus system remains unaffected and warns the authorized user by sending SMS that someone is trying to access the system.

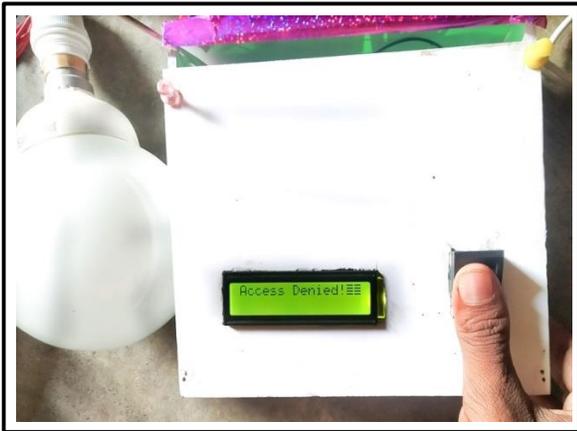


Fig.6. System Deny Access to Unauthorized Person

VI. CONCLUSION

The above implementation was sincerely an attempt to understand how the Fingerprint Recognition is used in controlling of power supply. From minutiae extraction to trivialities matching all level are covered in this implementation which generates a healthy score. The project was implemented and tested to ensure proper operation under said instruction.

REFERENCES

- [1]. A. Aditya Shankar, P. R. K. Sastry, A. L. Vishnu ram, A. Vamsidhar, International Journal of Engineering and Computer Science (IJECS) “Finger Print Based Door Locking System” vol.4, issue03, december2015.
- [2]. Manish Aggarwal, Department of Electronics and Communication Engineering, Elins International Journal of Science Engineering and Management” Secure Electronic Lock Based on Bluetooth Based OTP System” vol.2, Issue1, January 2017.
- [3]. Pavithra. B. C, Myna. B. C, kavyashree. M. Fingerprint Based Bank Locker System Using Microcontroller Proceeding of IRF International Conference, 5 April - 2014, Pondicherry, India, ISBN: 978-93-82702-71-9.
- [4]. Akanksha singh, arijit pal, bijay rai, “GSM Based Home Automation, Safety and Security Using Android Mobile Phone”, International Journal of Engineering Research & Technology (IJERT), vol.4, Issue 5, May 2015.
- [5]. Raqibull Hasan, Mohammad Monirujjaman Khan, Asaduzzaman Ashek, Isarat Jahan Rumpa, “Microcontroller Based Home Security System with GSM Technology” open Journal of Safety Science and Technology, 2015, 5, 55-62 Published online June 2015 in sciRes.
- [6]. Vini Madan, S.R.N Reddy, “GSM-Bluetooth based remote monitoring and control system with automatic light controller”, International Journal of Computer Applications, vol 46-No.1, may 2012.
- [7]. Prof.Benazir.H.M Dept. of ECE, Nisha S. Kalpathri, Chandralekha Sunagar, Shaikh Collage of Engineering and Technology, Belagavi, India “Fingerprint Authentication Smart Locking System Using OTP”, International Journal of Advance Research in Engineering, Science & Technology, vol 4, Issue 6, June-2017.
- [8]. Mr.Patil Bhushan S, Mr.Mahajan Vishal A, Mr. Suryawanshi Sagar A, Mr. Pawar Mayur B, Prof. Mr. U. R. Patole, “ Automatic Door Lock System using PIN on Android Phone”, International Research Journal of Engineering and Technology, vol 05, Issue 11, November 2018.