IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 6, June 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306248|

Fingerprint Based Voting System

Balakarthik M, Dr. A R Jayasudha Ph.D

II MCA Student, Department of Master of Computer Applications, Hindusthan College of Engineering and Technology, Coimbatore, India.

HOD, Department of Master of Computer Applications, Hindusthan College of Engineering and Technology, Coimbatore, India

ABSTRACT: The goal of the project fingerprint-based voting system provides a strong answer for safe and transparent elections by addressing major issues including voter impersonation and multiple votes cast by the same person. By using biometric authentication, the voting process is made more credible by guaranteeing that every vote is associated with a specific voter. The Tkinter toolkit for Python is used to create an intuitive user interface that makes the system accessible and simple to use for administrators and voters alike. All things considered, this project shows how biometric technologies and contemporary software development techniques may be combined to build a safe, effective, and user-friendly voting system.

I.INTRODUCTION

The system's principal goal is to establish Voting systems that are secure and effective are becoming more and more important in recent years. Whether paper-based or digital, traditional voting procedures frequently encounter difficulties such voter fraud, impersonation, and the laborious manual vote-counting procedure. These difficulties emphasise the necessity for an increasingly dependable and secure election administration system. By giving voters a way to be individually identified, biometric technology specifically, fingerprint recognition offers a potentially viable solution to these problems and ensures the integrity of the voting process. This project shows a fingerprint-based voting system that combines the R307 fingerprint sensor for biometric verification, the Tkinter library for Python for the graphical user interface (GUI), and a serial interface for communication between the sensor and the application.

1.1 ELECTRONICAL GADGET:

A variety of electronic devices are included in the Fingerprint-Based Voting System to guarantee a safe and effective voting procedure. Fingerprint scanners, which record and confirm voters' identities, and voting terminals with interactive touchscreens, where ballots are cast, are at the heart of the system. Through the use of IoT communication modules, these devices are connected, allowing for the real-time transfer of data to a central server that is outfitted with blockchain technology and cutting-edge encryption for safe and transparent data management. Election officials may monitor and report on the system in real time, and backup power supply guarantee uninterrupted functioning. Voter registration units serve as a means of collecting biometric data initially and updating it on a regular basis. A strong network architecture ensures seamless connectivity and data security for the duration of the electoral process.

1.2 REVIEW:

A safe and effective option for today's elections is a fingerprint-based voting system with software and Internet of Things integration. Voters are authenticated using biometric technology in this method, guaranteeing that each person can only cast one vote. Fingerprint scanners and other Internet of Things devices collect and send biometric data to a central server for validation. The voter's identification is then instantly verified by software algorithms that compare the fingerprints to a pre-registered database. This approach expedites the voting process, lowers the possibility of fraud, and does away with the requirement for hard copy voter ID checks. Furthermore, the technology can boost accessibility, give prompt feedback on voter eligibility, and improve the general integrity of the election process.

1.3 PROBLEM DESCRIPTION:

Critical issues with traditional voting systems, including voter fraud, identity theft, and inefficient administrative procedures, are addressed with the Fingerprint-Based Voting System. These issues frequently erode public confidence in democratic institutions and taint election results. This solution seeks to address these problems by combining

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306248|

biometric authentication with IoT technology to provide safe voter verification, real-time data transfer, and increased transparency, opening the door for more equitable, dependable, and trustworthy elections.

1.4 GOAL:

Enhancing election security, expediting the voting process, and guaranteeing voter identity are the main objectives of a fingerprint-based voting system that integrates IoT and software. The technology uses biometric verification to ensure that each voter can only cast one ballot, hence preventing voter fraud and duplication. It also aims to make voting more accessible and efficient by cutting down on wait times and making voting easier for voters. The incorporation of Internet of Things devices guarantees instantaneous data transmission and validation, furnishing prompt feedback about voter eligibility and augmenting the general integrity and lucidity of the voting procedure. This system's dependability and user-friendly layout are intended to increase public confidence in elections.

1.5 PERSPECTIVE:

Election procedures have advanced significantly with the introduction of a fingerprint-based voting system that integrates IoT and software, both technologically and socially. Important problems including voter fraud, identity theft, and inefficiencies in conventional voting procedures are addressed by this innovation. The method increases trust in election integrity by guaranteeing safe and precise voter authentication. Additionally, the ability of IoT devices to handle data in real-time streamlines processes, improving voter accessibility and efficiency. This strategy not only updates the voting apparatus but also shows that using cutting edge technology to support democratic values and improve civic participation is a priority.

II. SYSTEM SPECIFICATION

2.1 HARDWARE REQUIREMENTS:

- Pentium-IV(Processor).
- 256 MB Ram
- 512 KB Cache Memory
- Hard disk 10 GB
- Microsoft Compatible 101 or more Key Board

2.2 SOFTWARE REQUIRMENTS:

- **Operating System** :Windows / Linux any one
- **Programming language:** Python
- **Web-Technology** : Open Source
- **Front-End** : Python
- **Back-End** : Sql
- **Web Server** : Apache

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306248|

III. PROJECT DESCRIPTION

3.1 BLOCK DIAGRAM:

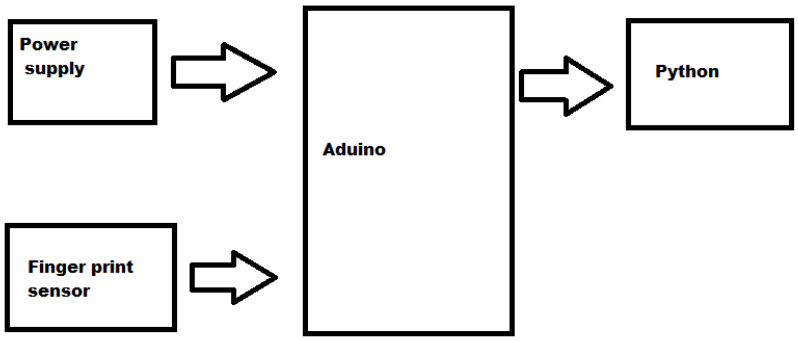

Figure 3.1-Block diagram

3.2 BLOCK EXPLANATION:

3.2.1 ARDUINO:

An open-source microcontroller platform called an Arduino board is used to create interactive projects. It is made up of a development environment for writing software for the microcontroller and a programmable circuit board. Digital and analogue input/output (I/O) pins on Arduino boards are available for connecting to a variety of sensors and actuators. They are employed in many different contexts, ranging from straightforward hobby projects to intricate automation systems. The Arduino Integrated Development Environment (IDE) is easy enough for novices to use and robust enough for more experienced users due to its community support and ease of use. An Arduino board is essential for do-it-yourself electronics and robotics projects because to its versatility in controlling lights, motors, sensors, and other devices.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306248|

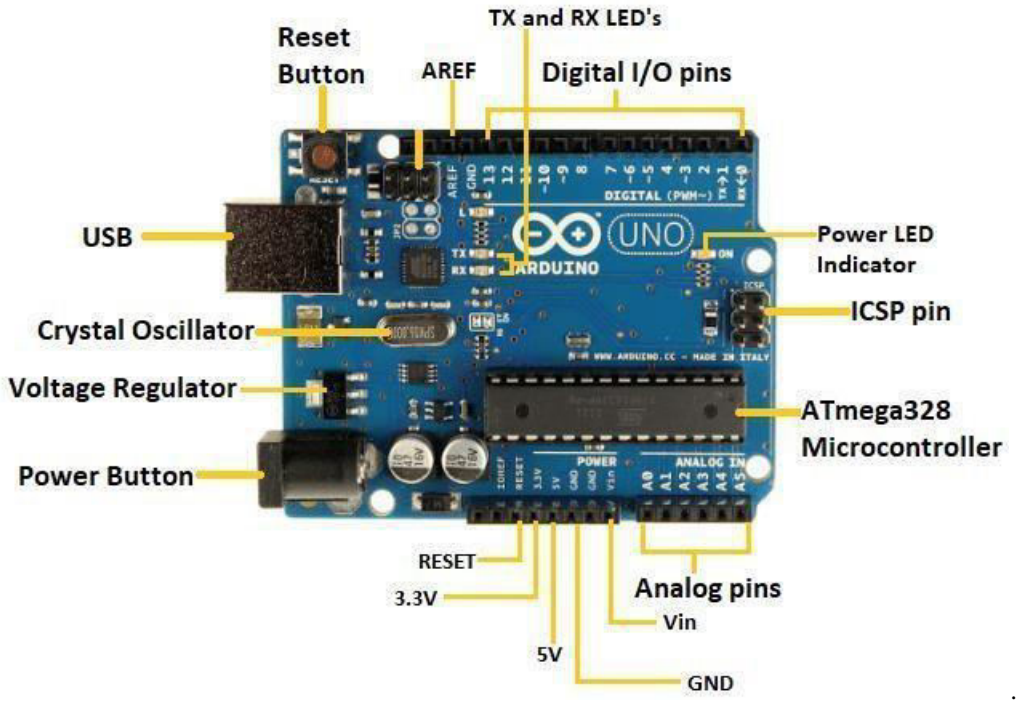

Figure 3.2.1-ARDUINO BOARD

3.2.2 BOARD ARCHITECTURE:

An Arduino board's architecture centres on a microcontroller, usually an ATmega328 seen on the Arduino Uno, or another member of the Atmel AVR series. The microprocessor, power supply pins, digital and analogue input/output (I/O) pins, and communication interfaces are important parts. The board has a voltage regulator, a crystal oscillator to provide precise timing, and a USB connector for programming and power. For authoring and uploading code, it also has an integrated development environment (IDE). Because the I/O ports enable communication with a range of sensors and actuators, Arduino is a flexible platform for developing and constructing interactive electronics projects. Because of its simple architecture and strong community support, Arduino is usable by both novice and expert users.

3.2.3 CPU ARCHITECTURE:

Dual-core Xtensa LX6 microprocessors, which are 32-bit RISC processors.Clock frequency can go up to 240 MHz.The dual-core design allows for better multitasking and performance.

3.2.4 MEMORY:

An Arduino board typically includes several types of memory to support its functions: flash memory, SRAM, and EEPROM. Flash memory stores the program code and is non-volatile, meaning it retains information even when the board is powered off. For example, the Arduino Uno has 32 KB of flash memory, with 0.5 KB used by the bootloader. SRAM (Static Random-Access Memory) is used for creating and manipulating variables while the program is running; the Uno has 2 KB of SRAM. EEPROM (Electrically Erasable Programmable Read-Only Memory) allows data to be saved between sessions, useful for storing settings or calibration values, and the Uno includes 1 KB of EEPROM. This combination of memory types allows the Arduino board to efficiently manage both temporary and permanent data storage, making it versatile for various applications

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306248|

3.3 FINGER PRINT SENSOR:

A fingerprint sensor module is a small electronic device used for a variety of purposes, including identity verification, access control, security, and fingerprint pattern analysis. These modules offer a trustworthy and safe method of confirming a person's identity by using biometric technology to identify distinctive patterns in each fingerprint.

3.3.1 FINGER PRINT SENSOR PIN DESCRIPTION:

1. VCC (Power Supply): The operational voltage for the fingerprint sensor module is supplied by this pin. Attach the device to the positive supply voltage, which in this instance is 3.3V.
2. GND (Ground): To finish the circuit, attach this pin to the power supply's ground.
3. TX (Transmit Data): Data from the fingerprint sensor module is sent to a host device using this pin. It is frequently utilised in UART-style communication interfaces.
4. RX (Receive Data): Data from the host device is received via this pin. It is used in communication interfaces such as UART to supplement the TX pin.

3.4CIRCUIT DIAGRAM:

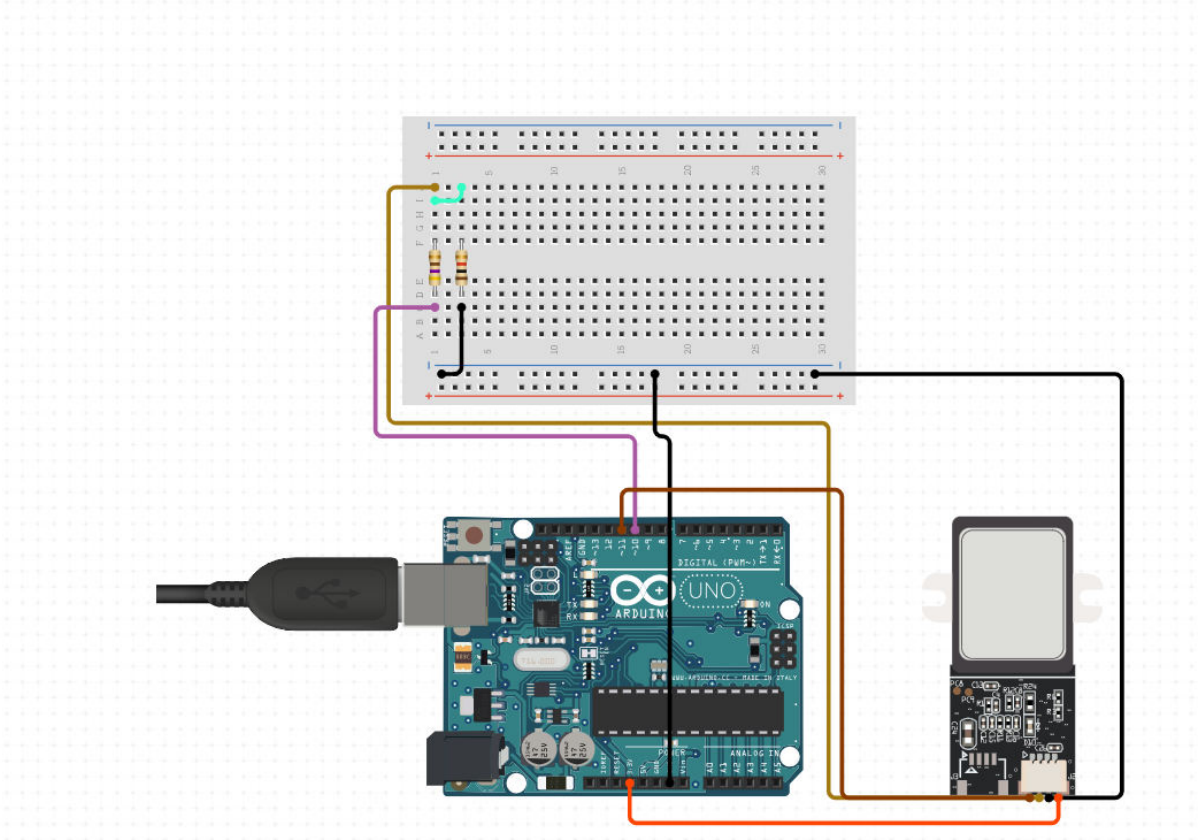

Figure 3.4-Circuit Diagram

IV. IMPLEMENTATION AND RESULT ANALYSIS

4.1. RESULT ANALYSIS:

The goal of result analysis for a fingerprint-based voting system that integrates software and IoT is to assess how accurate, efficient, and effective the system is in an electoral setting. The decrease in instances of voter fraud, the quickness and accuracy of voter identification, and the general level of voter satisfaction are important indicators. Data

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306248|

including the quantity of voters who were successfully validated, the number of authentication failures, and system outages would all be analysed. It would also evaluate how the system affects accessibility and voter turnout, especially for people with impairments or those living in rural areas. The analysis attempts to illustrate the system's benefits in terms of security, ease of use, and scalability by contrasting these results with conventional voting techniques. This will offer valuable information for future advancements and wider use.

V. FUTURE ENHANCEMENT

Future developments for the Fingerprint-Based Voting System may concentrate on strengthening user interface, expanding scalability, and bolstering security protocols. Integrating biometric recognition technology with cutting-edge tools like artificial intelligence (AI) and machine learning could improve accuracy and quickly identify fraudulent activity. Furthermore, the implementation of blockchain-powered decentralised identity systems may enhance privacy protection and guarantee the accuracy of voter data. Additionally, the creation of remote voting choices and mobile voting applications may boost accessibility and voter turnout, and ongoing improvements to IoT infrastructure may make it possible for people to connect and communicate easily in a variety of election contexts. All things considered, continued investigation and creativity in these domains may further advance the Fingerprint-Based Voting System towards even higher dependability, openness, and inclusivity in subsequent elections.

5.1. CONCLUSION:

To sum up, the Fingerprint-Based Voting System (Software + IoT) offers a safe, effective, and transparent way to update voting procedures, marking a substantial leap in electoral technology. The solution improves voter accessibility and efficiency while fortifying voting security and integrity through the integration of biometric authentication with IoT infrastructure. Voter information and election results are protected from illegal access and manipulation using cutting-edge encryption and blockchain technology, boosting public confidence in the democratic process. The Fingerprint-Based Voting System shows enormous potential to transform electoral procedures and guarantee free and democratic elections in the digital era, despite obstacles and complications.

VI. RESULTS

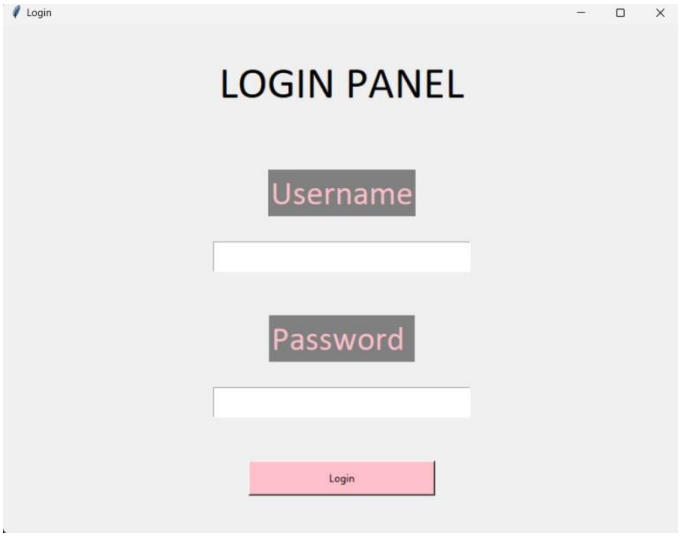

Figure 6.1 – USER LOGIN VOTING SYSTEM

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306248|

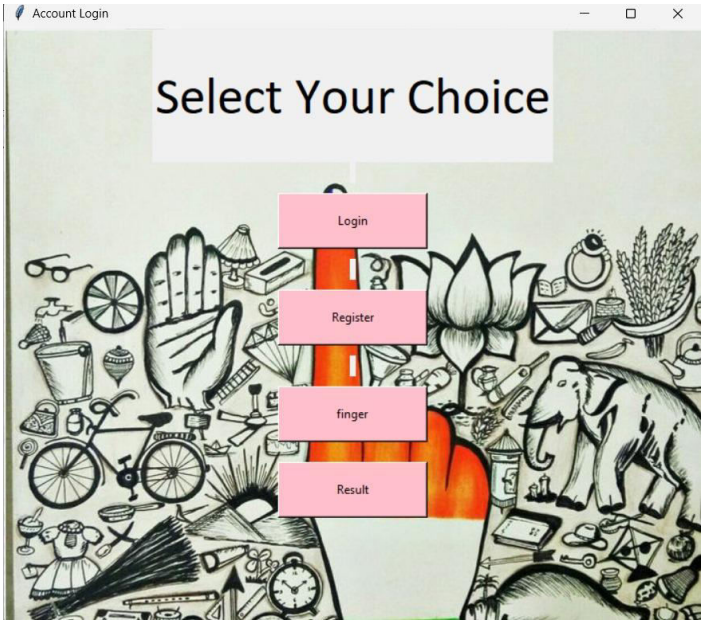

Figure 6.2 – INDEX OF THE FINGERPRINT BASED VOTING SYSTEM

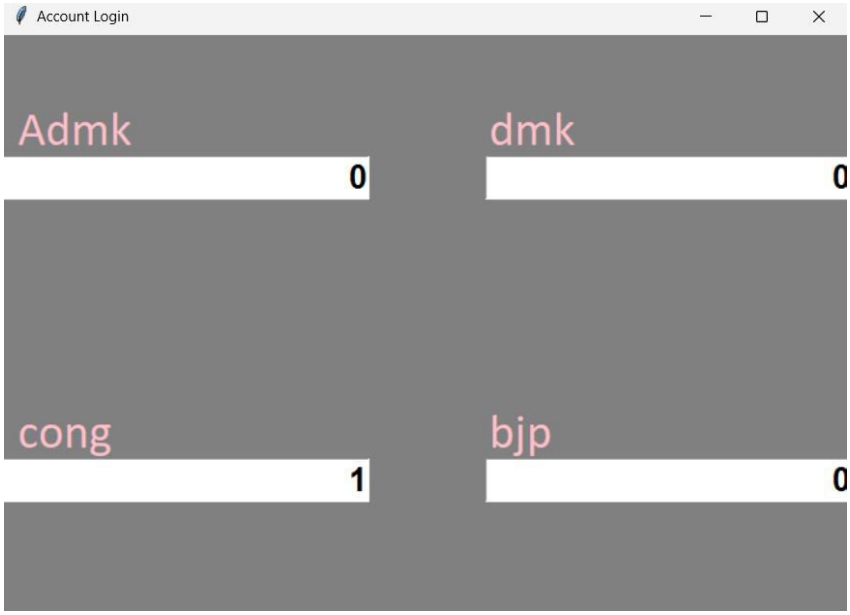

Figure 6.3 – RESULT OF FINGERPRINT BASED VOTING SYSTEM

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306248|

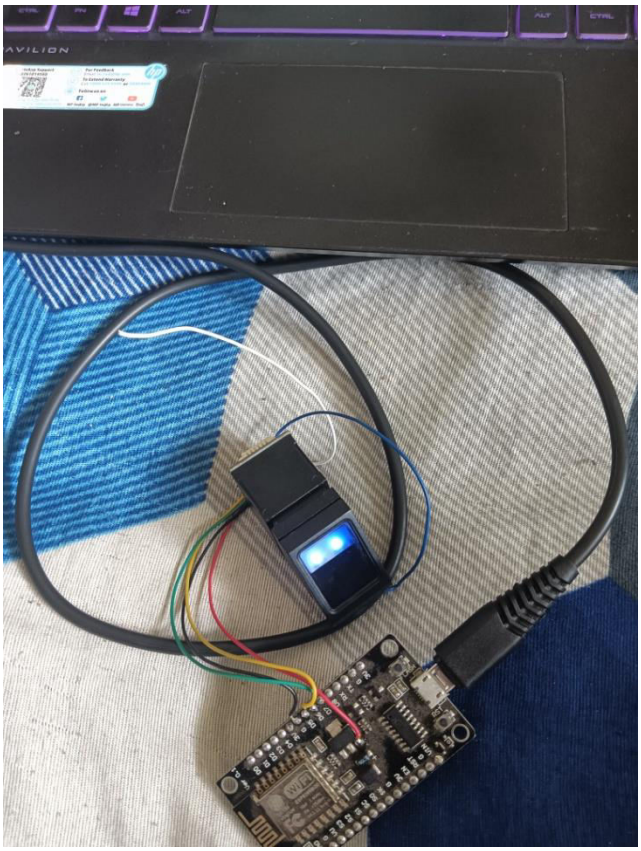

Figure 6.4 – CONNECTION OF FINGERPRINT SENSOR

REFERENCES

1. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20. DOI: 10.1109/TCSVT.2003.818349
2. Grinberg, M. (2018). Flask Web Development: Developing Web Applications with Python. O'Reilly Media, Inc.
3. Ramli, R., & Rehman, A. (2011). Biometric technology and applications to e-voting system. Proceedings of the International Conference on Computer Applications and Industrial Electronics (ICCAIE), 309-314. DOI: 10.1109/ICCAIE.2011.6162163
4. Liu, S., & Silverman, M. (2001). A practical guide to biometric security technology. IT Professional, 3(1), 27-32. DOI: 10.1109/6294.899930
5. Kumar, R., Sengupta, J., & Chatterjee, A. (2010). Biometric Authentication: A Study on Different Biometric Traits and Security Issues. International Journal of Advanced Research in Computer Science, 1(4), 146-153.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details