© 2026 ADYPJIET, Volume 1(1), Online ISSN: 3049-1517, June 2026, pp. 24-37

Ajeenkya DY Patil Journal of Innovation in Engineering & Technology

Journal Homepage: https://www.adypsoe.in/adypjiet

BioVote: A Secure Electronic Voting System Using Fingerprint Authentication

[1]Dr. Saniya Ansari,
[2]Dhanashree Chede,
[3]Samarth Burkul,
[4]Tanmay Deore,

[1]Associate Professor, E & TC Dept, Ajeenkya D Y Patil School of Engineering, INDIA
[2-4] UG students, Ajeenkya D Y Patil School of Engineering, Pune, INDIA

Article History:
Received: 04/05/2026
Revised: 20/06/2026
Accepted: 25/06/2026

Abstract:
Free and fair elections are a prerequisite for any democratic country. The customary voting procedure using ballot papers or ordinary electronic voting machines is vulnerable to impersonation, double voting and lack of transparency. In this paper, we design and develop a biometric voting system BioVote based on fingerprint authentication on the Arduino platform. In this system, the fingerprints of each voter are collected and stored at a safe and secure place, and they are used for electronic voting. The fingerprint is subsequently used to authenticate the voter during the voting process, so that voters cannot vote more than once. It is used mainly by businesses, educational institutions, and in small elections where the need for security and accuracy is paramount. The LCD display is user-friendly, displaying information and a message acknowledging the candidate chosen. Administrative options allow the adding and deletion of fingerprint IDs, providing a level of flexibility and control in the process. The hardware system is cost-effective and simple to use. Tests show the system is more reliable, faster, and more immune to fraud than other systems.

Keywords: Biometric Authentication, Arduino, Fingerprint Recognition, Module, ID, Keys, Embedded System

1.0 Introduction

The proposed system has two main parts: electronic voting and vote counting. In the electronic voting process, voters cast their votes using fingerprint authentication instead of paper ballots. Each

voter is identified by the unique pattern of their fingerprint, making the voting process secure and reliable. A fingerprint sensor is connected to the system to capture and verify the fingerprint before allowing the voter to cast their vote. The sensor communicates with the microcontroller to process the fingerprint data. The fingerprint module scans the voter's finger and converts it into a digital fingerprint record, which is stored in its memory. During voting, the system scans the fingerprint again and compares it with the stored record to confirm the voter's identity. The Arduino controls the entire process, including fingerprint verification, vote casting, and data handling. The votes are counted automatically by the electronic system, and the final results are shown on an LCD display. This removes the need for manual vote counting and helps reduce errors. Since every person has a unique fingerprint, the system ensures that each voter can vote only once. This system is particularly useful in organizations, educational institutions, and cooperative societies, where voting is used to select leaders or committee members. In This fingerprint-based voting system is useful for organizations, educational institutions, and cooperative societies where elections are held to choose leaders or committee members. In traditional voting systems, counting votes manually can sometimes lead to mistakes, such as counting the same vote twice, missing votes, or even deliberate manipulation. These problems can reduce the fairness of the election and make people lose confidence in the voting process.

The proposed system offers a secure and reliable solution by using fingerprint authentication to verify each voter before they cast their vote. It also counts the votes automatically, which reduces human errors and saves time. As each person's fingerprint is unique, the system prevents duplicate voting and helps ensure that every eligible voter can vote only once. This improves the accuracy, security, and transparency of the entire voting process.

2.0 Objective of Research

The main objective of this research is to develop a secure and reliable biometric voting system using fingerprint authentication and an Arduino-based platform. Before voting, each user must register their fingerprint, which is stored in the system for future verification. During the election, the user places their finger on the fingerprint sensor, and the system compares the scanned fingerprint with the stored record to confirm the user's identity. Only after successful verification is the user allowed to cast their vote, ensuring that only authorized voters can participate in the election. The proposed system uses a fingerprint sensor to capture the user's fingerprint and compare it with the fingerprint records stored in the database. If the fingerprint matches a registered record, the user is allowed to cast a vote. If no match is found, the system denies access and displays a security message. This process helps ensure that only registered and authorized users can participate in the voting process, making the system more secure and reliable. The proposed system verifies each user's identity by scanning their fingerprint with a biometric sensor. The scanned fingerprint is then compared with the fingerprint records already stored in the system. If a matching record is found, the user is allowed to vote. If the fingerprint does not match any registered record, the system blocks access and displays a security message. This simple verification process ensures that only registered and authorized users can cast their votes, helping to prevent unauthorized access and making the voting system more secure, accurate, and trustworthy. In addition, the system is simple to use, affordable to implement, and easy to maintain. It is well suited for organizations,

educational institutions, and small-scale elections where a secure, accurate, and efficient voting process is important. By providing reliable voter authentication and automatic vote counting, the system offers a practical solution for conducting fair and transparent elections.

3.0 Literature survey

Biometric systems, especially fingerprint recognition, are widely used for secure user authentication because every person's fingerprint is unique and remains unchanged over time [1-3]. Many studies have shown that fingerprint matching provides accurate and reliable identification, making it suitable for security-related applications [4], [6]. In voting systems, fingerprint authentication helps prevent problems such as fake voting, voter impersonation, and multiple voting by the same person [7], [8]. Although advanced technologies such as encryption and blockchain can provide additional security, they also make the system more complex and expensive to implement [5], [9]. Therefore, there is a need for a simple, affordable, and reliable fingerprint-based voting system like BioVote, especially for organizations, educational institutions, and other small-scale elections.

4.0 Working Principal

The fingerprint-based biometric voting system works in two main stages: voter enrollment and voting. During the enrollment stage, each user must first register their fingerprint in the system. To begin the registration process, the user presses the ENROLL button on the keypad. The LCD screen then asks the user to choose a unique ID where the fingerprint will be stored. The user can select the ID using the UP and DOWN buttons and confirm the selection by pressing the OK button.

After the ID is confirmed, the fingerprint sensor scans the user's fingerprint. To ensure accurate registration, the system may ask the user to place and remove the same finger more than once. The captured fingerprint is processed and converted into a digital fingerprint template, which is securely stored in the fingerprint module under the selected ID. Once the fingerprint is successfully saved, the registration process is complete, and the user is eligible to participate in the voting process.

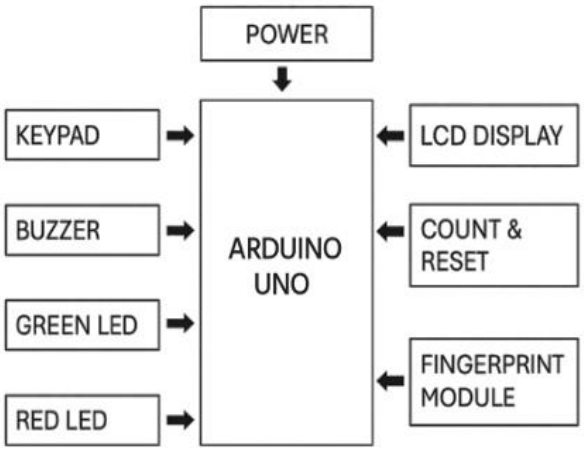

Fig. 1: Block Diagram

4.1 Voting Process

In the voting phase, the registered user places their finger on the sensor for authentication. The system scans and compares the fingerprint with the stored database. If a valid match is found, the system checks whether the user has already voted. If the user is verified and has not voted before, access is granted to cast the vote using input buttons. The selected candidate is displayed on the LCD, and the vote is recorded in the system. If the fingerprint does not match or the user has already voted, the system denies access and displays a warning message. This prevents unauthorized access and duplicate voting. Additionally, the system provides an option to delete registered users by pressing the DEL key, selecting the corresponding ID, and confirming the deletion. The LCD displays a confirmation message once the ID is successfully removed.

All operations are managed by the Arduino microcontroller, ensuring smooth coordination between input, processing, and output devices. The system is designed as a standalone unit, where all data is stored locally without any network connection. This isolation enhances security by minimizing the risk of external attacks or hacking.

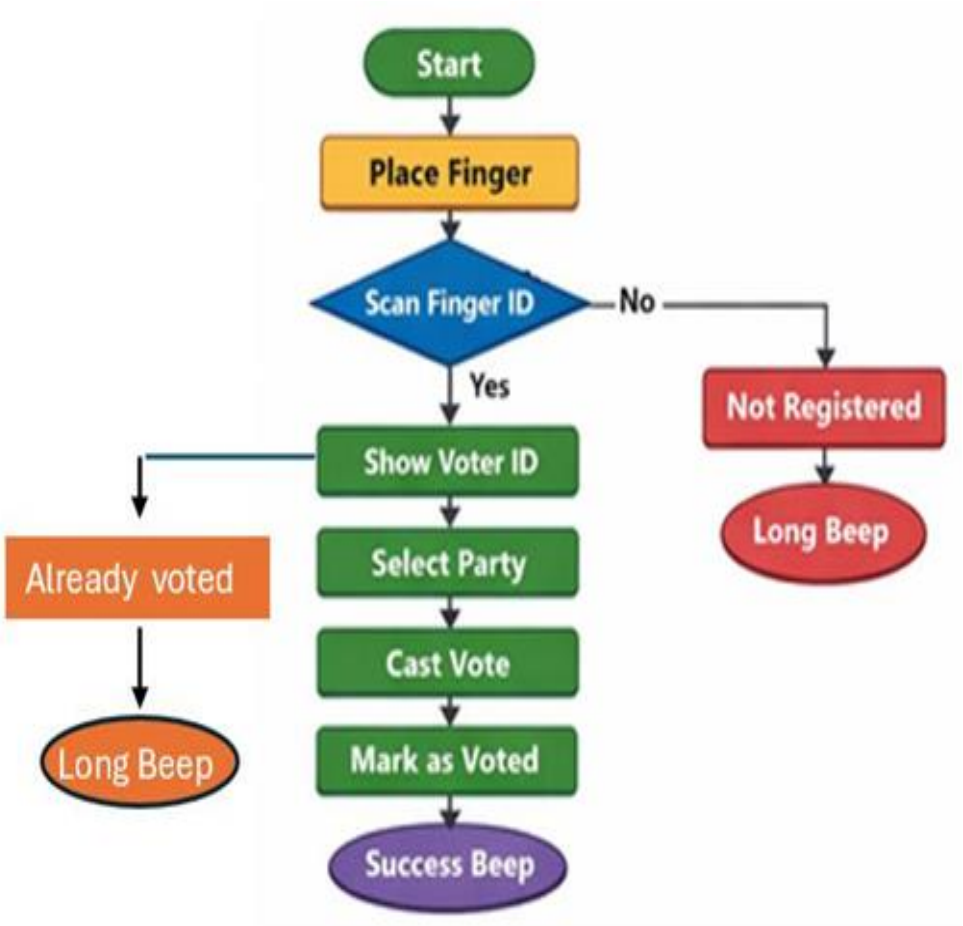

Fig. 2: Flowchart of the Fingerprint Voting System

4.2 Hardware Description:

Requirement: This system is based on the concept of biometric identification of users which requires the following components which are shown in Fig. 2.

1. Fingerprint sensor R305 - For biometric identification
2. Arduino Uno - To store data
3. 16x2 LCD - For displaying results
4. Buzzer - For vote confirmation
5. LED - For voter confirmation
6. Connecting wires - For connections
7. Keypad - For selecting the party

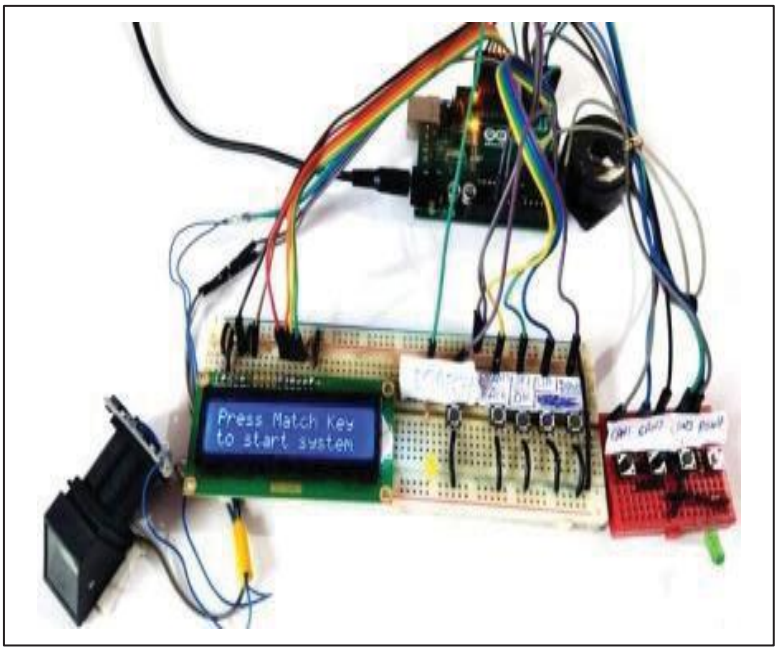

Fig. 3: Circuit Connections

A. Arduino

The Arduino Uno, based on the ATmega328 microcontroller, acts as the central control unit of the proposed system. It consists of 14 digital input/output pins and 6 analog input pins, along with a 16 MHz crystal oscillator, USB interface, power jack, and reset circuitry. The Arduino coordinates all system operations, including fingerprint authentication, vote processing, and result display.

Overall, the hardware components work together smoothly to provide an efficient and user-friendly voting system. The fingerprint sensor, keypad, Arduino, and LCD display communicate effectively to ensure accurate operation, making the system reliable, easy to use, and suitable for secure voting applications.

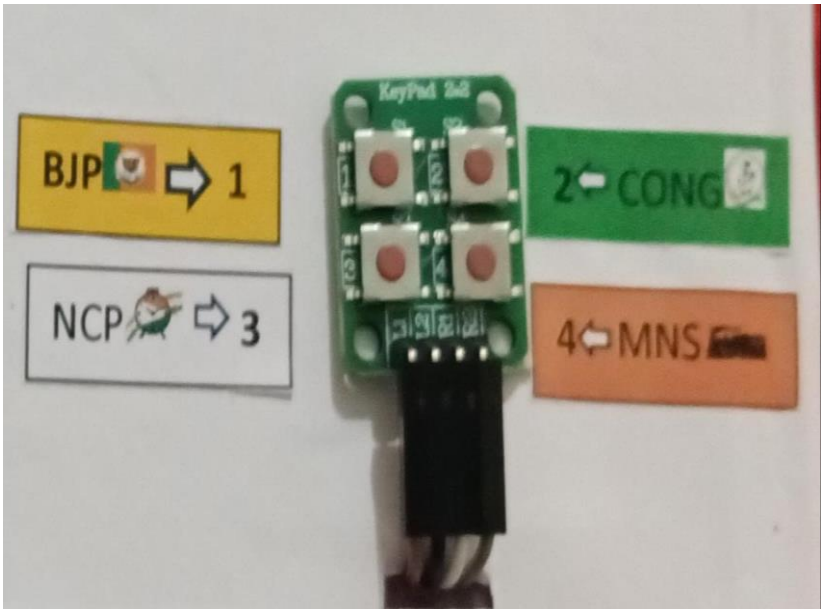

Fig. 4: Voting Keys

B. Fingerprint Module

The R305 fingerprint module is the main biometric sensor used in the proposed BioVote system. It captures, processes, and stores users' fingerprint data for identity verification. The module is widely used because it provides reliable performance, responds quickly, and can be easily connected to Arduino and other microcontrollers, making it a suitable choice for secure biometric voting applications. The module works by scanning the fingerprint image and converting it into a digital template using internal processing algorithms. This template is then stored in the module's memory at a specific ID location. During authentication, the sensor compares the input fingerprint with stored templates to verify the user's identity.

The R305 module supports both enrollment and matching operations internally, which reduces the processing load on the Arduino. It communicates with the microcontroller through serial communication (UART), making integration simple and efficient. Due to its high accuracy and compact design, the R305 fingerprint sensor is suitable for secure applications such as biometric voting systems, access control, and authentication systems.

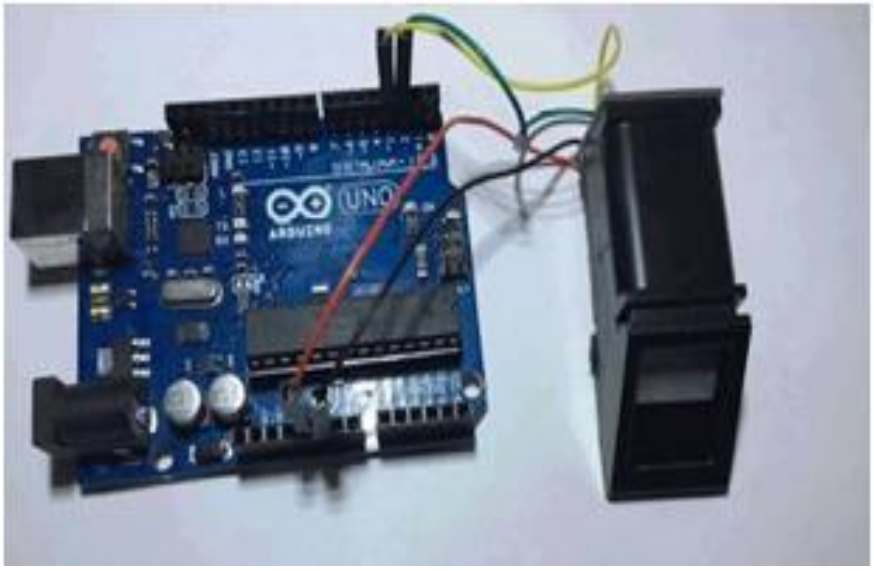

Fig. 5: Fingerprint Scanner

C. LCD Display

The system uses a 16×2 LCD display with an LED backlight to provide a user-friendly interface. The display is capable of showing two rows with up to 16 characters per row, making it suitable for displaying system messages and instructions clearly. In this project, the LCD is interfaced using an I2C module, which reduces the number of required connection pins and simplifies wiring with the Arduino. The LCD acts as a communication medium between the user and the system. It displays important messages during different stages of operation. Initially, a welcome message is shown when the system is powered on. During enrollment, it prompts the user with messages such as “Place your finger.” While verifying the fingerprint, the system displays messages like “Identifying [10].

If the user is successfully authenticated, the display shows “Please vote,” allowing the user to proceed. If authentication fails, a “No access” message is displayed. After voting, the system can also display confirmation messages and, when required, the final results showing candidate names along with their respective vote counts.

Overall, the LCD display enhances usability by providing real-time feedback and guidance throughout the voting process.

Fig. 6: LCD Display

TABLE I: LCD Display to Arduino Connections

LCD DISPLAY	ARDUINO BOARD
VIN	5V PIN
GND	GND
SDA	A4
SCL	A5

TABLE II: Fingerprint Module to Arduino Connections

FINGERPRINT MODULE	ARDUINO BOARD
VCC	5V PIN
GND	GND
TX	RXD
RX	TXD

D. Algorithm:

The complete voting procedure is carried out in a sequence of steps, including fingerprint enrollment, authentication, and vote casting. The process is described as follows:

Step 1: Start the system

Step 2: Select enrollment mode

Step 3: Place finger to register the ID

Step 4: Place finger for verification

Step 5: The system authenticates the voter

Step 6: Enable voting options

Step 7: Select the candidate

Step 8: Vote recorded successfully

Step 9: Stop / Ready for the next voter

5.0 Results & Discussion:

First, enroll the voter's fingerprint and store it using the given ID.

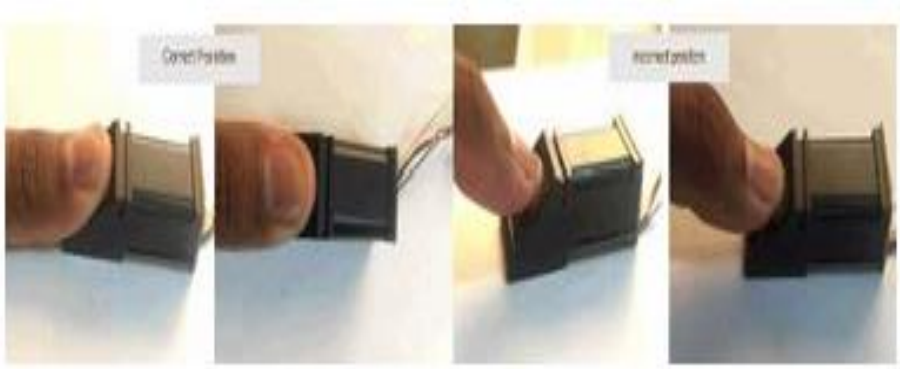

Fig. 7: Place the Finger on the Fingerprint Module

At this stage, the system prompts the user to select an ID to store their fingerprint. After selecting the ID, the voter places their finger on the fingerprint module for scanning. During enrollment, the user places their finger twice. The first scan captures and converts the image, while the second scan verifies it with the first. If both scans match, the fingerprint is stored under the selected ID. Otherwise, a "Fingerprint did not match" message displayed on LCD.

Then, the system checks whether the voter is valid for vote casting.

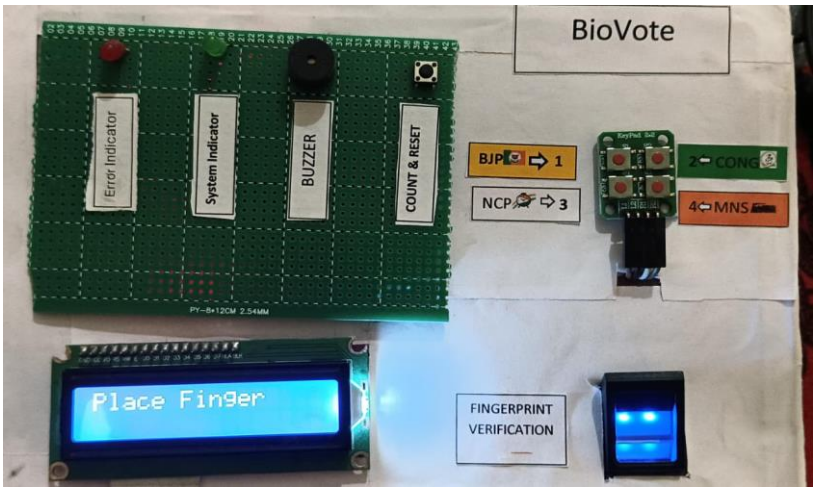

Fig. 8: Fingerprint Scan

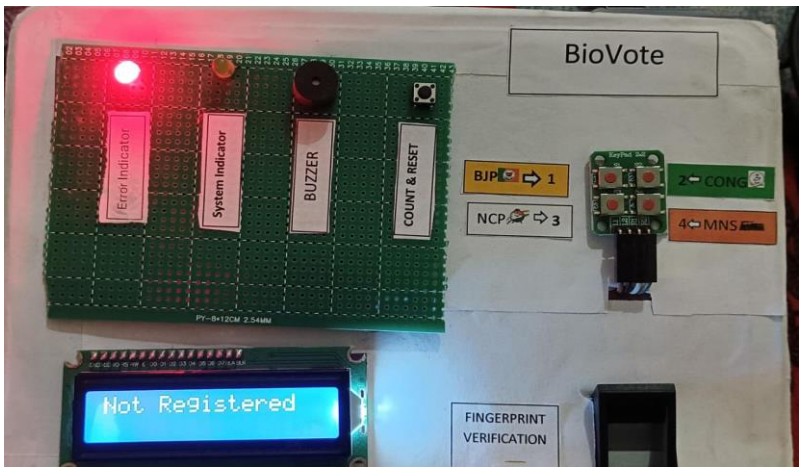

Fig. 9: Finger Not Registered

In this step, the voter places their finger on the fingerprint sensor for authentication. The system scans the fingerprint and compares it with the stored database. If a match is found, the LCD displays messages such as “Match Found” along with the corresponding ID of the registered user. If no match is detected, the system displays a “Not Registered” message, indicating that the voter is not authorized.

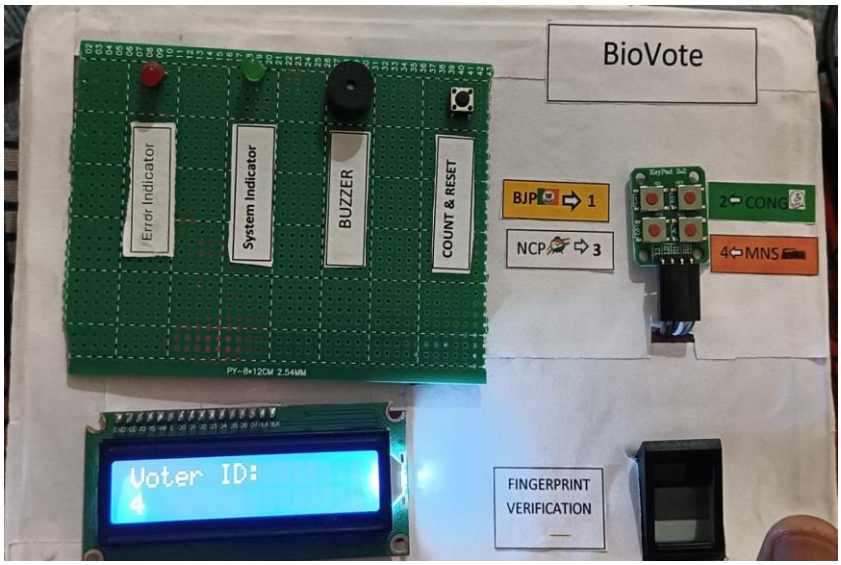

Fig. 10: Result of Finger Scanning

Then, voters cast their votes.

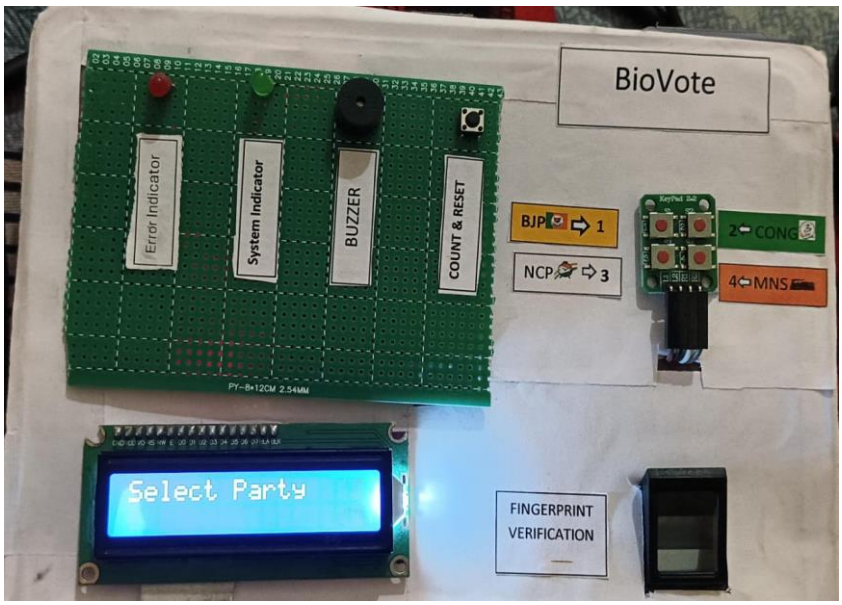

Fig. 11: Vote Casting - Ready to Select the Party

In this step, voters select a party based on their preference from the party list. Once a party is selected, it cannot be change to another party.

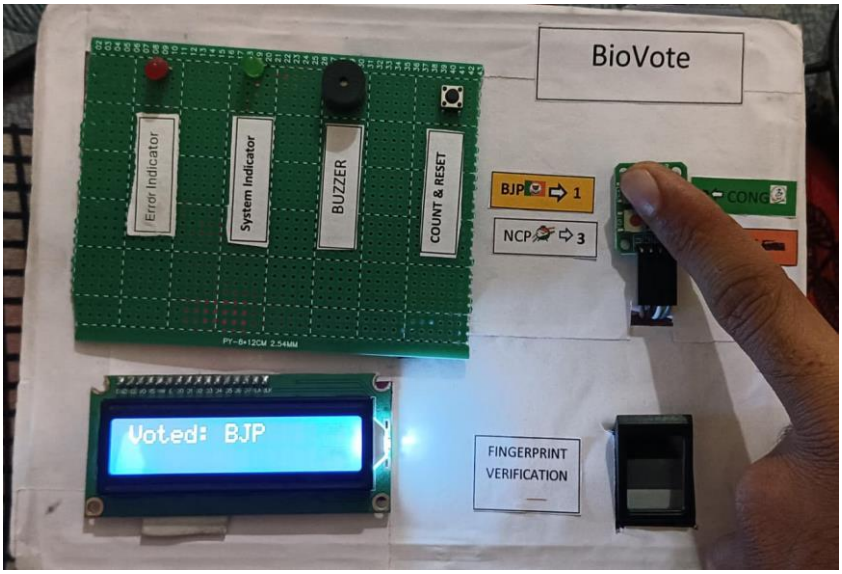

Fig. 12: Vote Casting with Party Selection

After the voter selects their preferred party or candidate, the vote is recorded by the system. Once the voting process is complete, the COUNT button is pressed to calculate the total number of votes received by each party. The results are then displayed on the LCD screen, and the party or candidate with the highest number of votes is declared the winner.

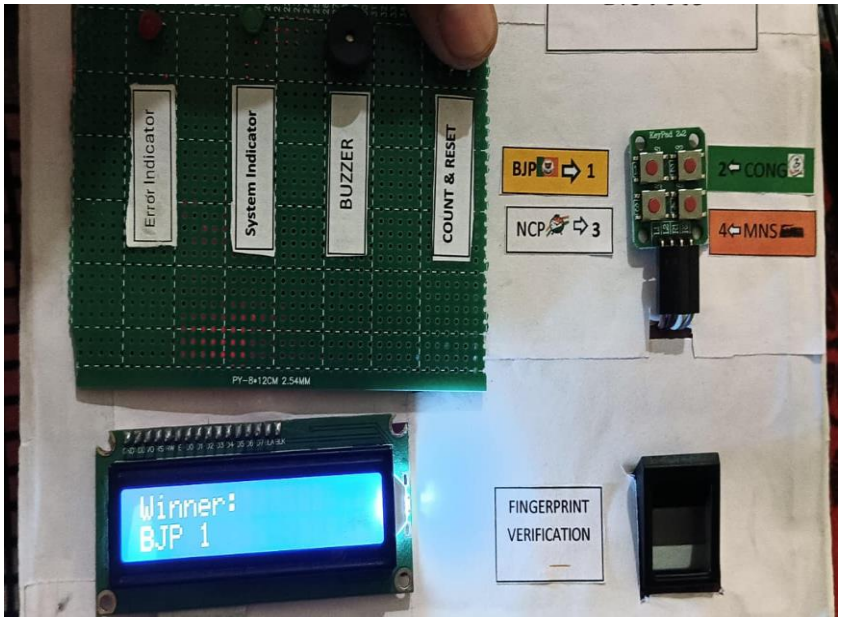

Fig. 13: Result Display

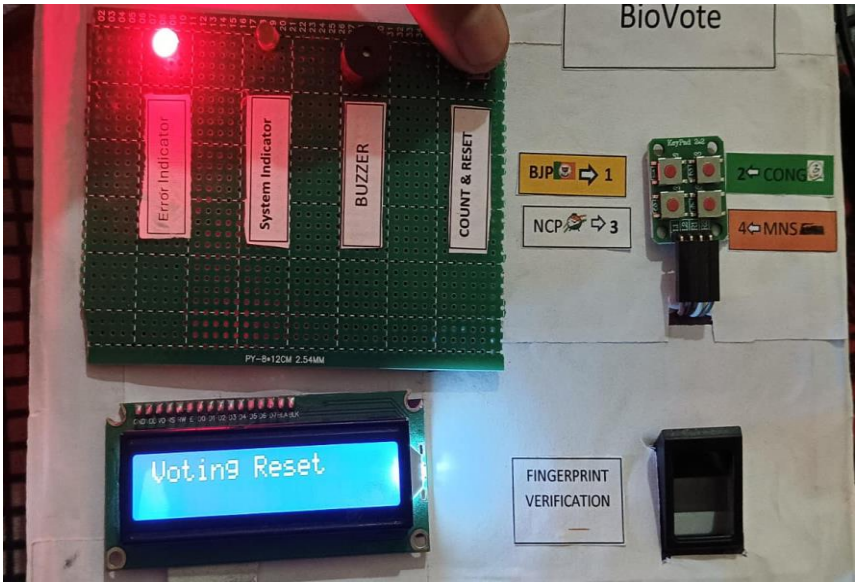

Fig. 14: Voting Reset Process

After displaying the final results, the system resets the vote count and returns to the initial state, making it ready for the next voting session.

A. Advantages:

1. Provides strong security by verifying each voter using their unique fingerprint.
2. Prevents duplicate voting and stops unauthorized users from casting votes.
3. Automatically records and counts votes, reducing the chances of human error.
4. Offers a simple and user-friendly interface, with clear instructions displayed on the LCD screen.
5. Consumes very little power, as the system operates using a +5V DC power supply.

B. Disadvantages:

1. The fingerprint sensor may occasionally fail to recognize a fingerprint because of poor finger placement, dirt, or variations in fingerprint quality.
2. Every user must register their fingerprint before they can participate in the voting process.
3. The system can support only a limited number of users and candidates because of the memory and hardware limitations of the device.

6.0 Conclusion

The hardware setup of the proposed system successfully implements an electronic voting machine using a fingerprint sensor and Arduino. The system operates effectively by verifying the user through fingerprint authentication and displaying the voting results on the LCD. It provides a secure and simple method for voting and helps prevent duplicate or unauthorized voting. This

project is suitable for small-scale applications such as institutions and organizations. Overall, the use of fingerprint technology makes the voting process more reliable and efficient.

References:

1. M. Odden, Biometric Cris: Legal Challenges to Biometric Identification Iinitiatives, 39(2) Challenges to Biometric Identification Initiatives.

2. M. Smith and S. Miller, The ethical application of biometric facial recognition technology, AI Soc, 37(1), 167–175, 2022, doi: 10.1007/s00146-021-01199-9.

3. L. H. Adamu and M. G. Taura, Embryogenesis and Applications of Fingerprints- a review, International Journal of Human Anatomy, 1(1),1–8, 2017.

4. W. Zafar, T. Ahmad, and M. Hassan, Minutiae based fingerprint matching techniques, 17th IEEE International Multi Topic Conference, 411–416, 2014.

5. A. C. S. Sheela and G. F. Ramya, E-voting system using homomorphic encryption technique, Journal of Physics: Conference Series, IOP Publishing Ltd, 2021.

6. V. Baraskar, finger Print Based Biometric Authetification System for ATM System, Asian Journal For Convergence In Technology (AJCT) ISSN: 2350-1146, 4(I) 2018.

7. J. Liu, T. Han, M. Tan, B. Tang, W. Hu, and Y. Yu, A Publicly Verifiable E-Voting System Based on Biometrics, Cryptography, 7(4), 2023.

8. N. B. Kintu, A Secure E-Voting System Using Biometric Fingerprint and Crypt Watermarks Methodology, ASCENT International Conference Proceedings – Information Systems and Engineering, 14 November 2018.

9. M. Hajian Berenjestanaki, H. R. Barzegar, N. El Ioini, and C. Pahl, “Blockchain-Based E-Voting Systems: A Technology Review,” Electronics (Basel), 13(1), 2023.

10. R. V. Adiraju, K. K. Masanipalli, T. D. Reddy, R. Pedapalli, S. Chundru, and A. K. Panigrahy, An extensive survey on finger and palm vein recognition system, Mater Today Proc, 45, 1804–1808, 2021.