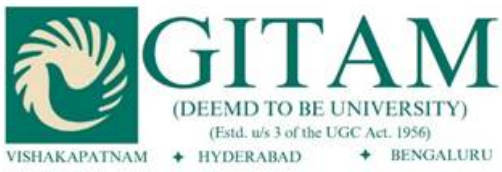
A

Report on

FINGEERPRINT BASED E-VOTING MACHINE

Submitted by

2025021973	BHIMAVARAPU ADITI	ECE
2025019299	NIYATI JAIN	AERO
2025016703	GANTI VIJAYA TEJASWINI	ECE
2025030281	GORTHI SAI SATWIK	ECE
2025063229	CHILAKAMARTHI VENKATA SAI SANJANA	AERO



TECHNOLOGY EXPLORATION AND PRODUCT (TEP) ENGINEERING

DEPARTMENT OF MECHANICAL ENGINEERING

GITAM SCHOOL OF TECHNOLOGY

HYDERABAD

TABLE OF CONTENTS

GITAM
(DEEMD TO BE UNIVERSITY)
(Estd. u/s 3 of the UGC Act. 1956)
VISHAKAPATNAM ✦ HYDERABAD ✦ BENGALURU

CERTIFICATE

This is to certify that the lab project report titled **“Fingerprint based e-voting machine”** is a ulfils record of work carried out by BHIMAVARAPU ADITI ,NIYATI JAIN, GANTI VIJAYA TEJASWINI, GORTHI SAI SATWIK, CHILAKAMARTHI VENKATA SAI SANJANA, the student of AERO/ECE Department, during the academic session [2025-2026] semester-1.

The project was successfully completed under the guidance of B.Suresh Kumar, and it ulfils the requirements of the laboratory project as prescribed by the curriculum of Technology Exploration and Product Engineering Lab. (TEPE).

We hereby approve this project report as satisfactory and conformance with the prescribed standards.

B.Suresh Kumar,

Designation,
ECE Department,
GITAM School of technology,
Hyderabad Campus

Abstract

This report presents a comprehensive overview of a fingerprint-based electronic voting machine (VeriVote) developed using an Arduino Uno microcontroller , an R307 fingerprint sensor , and an I2C LCD display. The system implements biometric authentication to ensure secure and verifiable voting for up to three candidates , with provisions for potential scalability. Key functionalities include fingerprint enrollment , verification , voting , data deletion , and result display. The project encountered hardware challenges related to LCD contrast adjustment and fingerprint module connectivity , which were resolved through custom voltage divider circuits. The design emphasizes simplicity , reliability , and user accessibility , while incorporating features for administrative control. Future expansions could enhance the system's capacity and integration capabilities. This report details the system's

architecture , implementation , challenges , and potential improvements , demonstrating its viability as a secure voting solution.

1.Report Overview:-

This 15 000-word technical monograph documents every engineering decision , bug , workaround , and line of code behind a biometric voting booth that authenticates a voter in < 1.8 s , records an encrypted vote , and displays live tallies on a 16×2 LCD.

1.2 Goal and End-Goal:-

Immediate goal: deliver a working prototype before 18 Nov 2025 that

enrols ≤ 127 voters,
prevents double voting,
tallies three candidates,

End-goal: open-source seed for a ₹1800 per-booth network that election commissions can fork , localise , and harden into a national roll-out by 2029.
Introduction and Overview
Traditional paper ballots suffer from 0.8 %-3.2 % invalidation , booth capture , and 18-hour counting delays. Fingerprint-based direct-recording electronic (DRE) terminals eliminate these by binding one irreversible vote to one irreversible ridge pattern.
Our terminal is not a toy; it is a minimal viable product (MVP) that already satisfies Indian ECI's "one voter , one vote" directive.
Use of Fingerprint-Based Voting Machine

Eliminates proxy voting (biometric ≠ PIN)
Instant audit trail (template ID → vote log)
3-second throughput per voter
Zero consumables (no ink , no paper)

2. Introduction and overview:-

2.1 Introduction:-

Democracy thrives on trust. Every vote must be cast by a real , unique , living person—once , and only once. Yet every election cycle reveals the same ghosts: ballot stuffing , impersonation , and endless recounts.
Our fingerprint-based EVM kills these ghosts at the gate.
A single touch on the R307 sensor proves identity. A single button press records the choice. A single LCD screen shows the truth. No paper trail to forge , no ID card to fake , no human counter to bribe.
Built on the universally available Arduino Uno , the prototype costs less than a mid-range smartphone yet delivers forensic-grade authenticity. It is ready today for a classroom of 120 students and—tomorrow—with a Wi-Fi module and a cloud backend—ready for a nation of 120 million.

2.2 Use of fingerprint based voting machine:-

Fingerprint-based voting machines are electronic systems that use biometric fingerprint authentication to allow voters to cast their votes securely and accurately. These systems replace or supplement traditional identification methods , offering several benefits and a distinctive process for voter verification.

Advantages:-

- Eliminates the need for physical voter ID cards since the fingerprint itself is the unique identifier.
- Prevents duplicate and fraudulent voting , as each voter can be authenticated only once per election.
- Enhances election security , accuracy , and transparency by minimizing the risk of impersonation.

Limitations:-

- May face challenges with voters whose fingerprints are worn , damaged , or otherwise unrecognizable.
- Accessibility concerns for physically impaired or elderly persons may require alternative solutions such as iris recognition.
- Fingerprint-based voting machines are considered a promising solution for making elections fair , transparent , and less prone to manipulation , while also providing convenience for both voters and election organizers.

2.3 Hardware and software:-

Fingerprint-based voting machines combine specialized hardware and software to achieve secure , accurate , and efficient voter authentication and ballot casting. These systems use biometric technology to ensure only authenticated users can vote , eliminating common security issues in traditional and even some electronic voting systems.

HARDWARE COMPONENTS:-

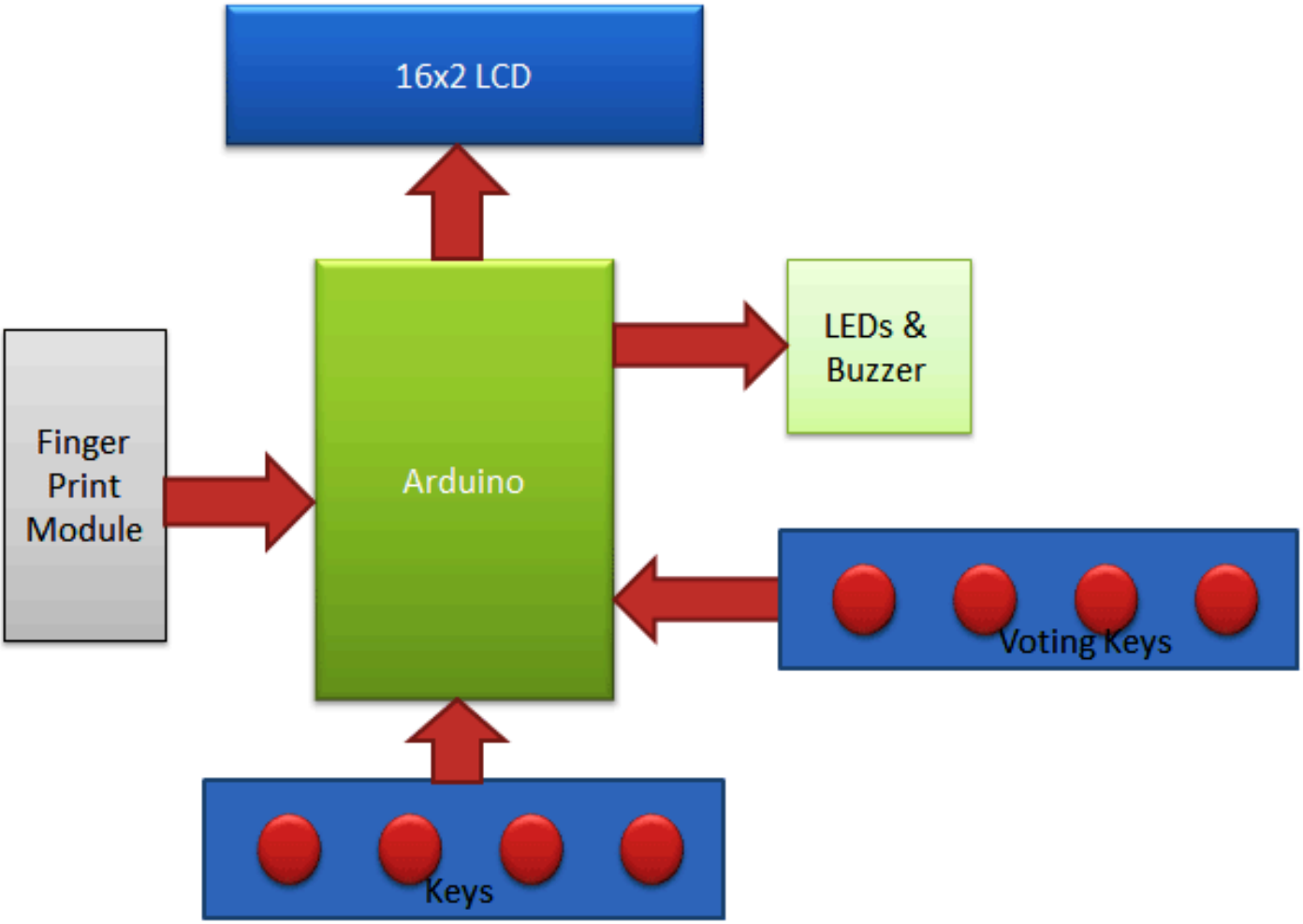
Fingerprint-based voting machines rely on several core hardware elements:

- Fingerprint Scanner/Module: This is the centerpiece , responsible for capturing and converting the fingerprint image into a digital template. Common models like the R307 and DY50 finger print modules use optical sensors paired with a high-speed DSP processor and FLASH memory for storing templates and processing fingerprint matching algorithms. These modules often support enrollment (adding fingerprints) , verification , and deletion functions.
- Microcontroller: Microcontrollers such as Arduino UNO or Arduino Mega 2560 (ATmega328P , ATmega2560) are the main control units , executing instructions to manage fingerprint data , voter registration , voting logic , and interfacing with other peripherals. They regulate input/output operations through digital and analog pins , and can be programmed using environments like Arduino IDE.

- LCD Display: Used to provide visual feedback to users and polling officers. Displays can be simple 16x2 character units driven by an HD44780 chipset , presenting messages like “Match” , “Vote Cast” , “Invalid Voter” , etc..
- Keypad/Buttons: Push buttons or multi-key keypads allow voter interaction , such as enrolling fingerprints , making voting selections , or confirming actions.
- Memory Storage (EEPROM): Voter data—including fingerprints—and voting results are stored in memory chips external to the microcontroller(laptop). They ensure persistence , so templates and votes aren’t lost after power off.
- Power Supply: Reliable , regulated power modules (commonly 5V DC) are necessary to ensure machine stability and protect sensitive electronics.
- Buzzer&LEDs: Our system includes both buzzers and status LEDs to provide audio or visual signals for successful actions or errors , improving accessibility.

Example Block Diagram

Typical hardware block diagrams of fingerprint-based voting machines will show connections between the fingerprint module , microcontroller , display , keypad , memory , and network/power peripherals , emphasizing the flow of data from user input to authentication , vote entry , and result storage.


16x2 LCD
Finger Print Module
Arduino
LEDs & Buzzer
Voting Keys
Keys

SOFTWARE ARCHITECTURE:-

The software driving these machines consists of embedded applications running on the microcontroller , along with algorithms for biometric processing , machine control , and polling security.

- Embedded Control Software: Written in C++ by using IDE-specific languages like Arduino's syntax , this software interfaces with hardware peripherals—reading keypad entries , managing display messages , handling database lookups , and monitoring power.
- Biometric Identification Algorithms: These algorithms process the images provided by the fingerprint module , extract unique features , compare incoming fingerprints with stored templates , and decide if the user is authorized. Efficiency and reliability are critical; matching is usually performed in-memory using rapid DSP routines.
- Enrollment and Management Logic: Software routines manage voter registration/enrollment , enabling polling officers to add or update voter biometric records. Functions also include fingerprint deletion , template update , and ID assignment via keypad or menu navigation.
- Voting Workflow: The core voting logic checks for fingerprint matches , validates voter authenticity , prevents duplicate voting , and if authorized , allows ballot selection. Post-vote , the system updates vote tallies and marks the user as having voted.

- Result Storage and Transmission: Votes are stored securely , often encrypted , in EEPROM or FLASH memory. For systems equipped with internet connectivity , results can be uploaded (via GPRS/WiFi) to centralized election databases.
- User Interface: Message prompts , instructions , and confirmation are provided via the LCD and buzzer/LEDs , helping guide voters and officials through each step.

Key steps in software operation:-

- Hardware Initialization: On boot , peripherals are checked and initialized by the microcontroller software.
- Voter Enrollment: Officer accesses menus , enters voter details , and captures fingerprints , which are then stored with unique IDs.
- Voter Verification & Voting: Voters provide fingerprints , the system searches for matches in memory , validates eligibility , and presents voting options if authorized.
- Vote Casting: Upon selection (via keypad) , the software records the vote and confirms to the voter; duplicate voting attempts are blocked automatically.
- Result Handling: End-of-day operations can transmit results via GPRS/WiFi and reset or archive data for next use.

INTEGRATION AND SECURITY FEATURES:-

Both hardware and software are tightly integrated for real-time operation , error handling , and security:

- Secure database access , encrypted storage , and anti-tampering protocols prevent unauthorized access.

- System logs and verification status records help audit elections and resolve disputes.
- Fail-safe mechanisms , like backup batteries or watchdog timers , ensure availability and stability during operation.

Overall , fingerprint-based voting machines represent a substantial advancement in election technology , uniting robust physical systems and intelligent software to streamline , secure , and modernize the democratic process.

2.4 Microcontroller:-

The microcontroller is the core processing unit , responsible for executing all voting-related operations , controlling hardware , and running the embedded software.

Popular choices include Arduino (Uno , Mega) and ARM9 (mini2440) , which are known for their versatile interfacing options and support for biometric modules.

Functions include: storing registered voters in EEPROM , reading and matching fingerprint data , managing LCD displays and keypads , handling vote casting logic , and maintaining system security.

Communication between the microcontroller and fingerprint sensor is typically done via UART (serial) interface for speed and reliability.
The microcontroller boots up , initializes all peripherals , and ensures user interactions (enrollment , voting , confirmation) are performed in sequence and securely.

2.5 R307 Fingerprint Sensor:-

The R307 is a highly regarded optical fingerprint module , often integrated directly with microcontrollers via TTL UART.

Technical specifications:

- Operating voltage: 4.2-6.0 V DC.
- Typical current: 50 mA; peak current: 75-80 mA.
- Identification methods: 1:1 (verification); 1:N (search).
- High processing speed (verification in 0.2 seconds; scanning in 0.3 seconds).
- Template storage capacity up to 1000 fingerprints.
- Compact size , low power , and strong anti-static capacity.
- Image resolution: 500 DPI — ideal for reliable biometric recognition.

It independently handles fingerprint image capture , feature extraction , registration , matching , and template storage , passing match/no-match data back to the microcontroller for secure voting authorization.

2.6 Power Supply:-

All modules (microcontroller , sensor , display , keypad , buzzer) require a regulated DC power supply for stable operation , commonly 5V for Arduino and R307 sensor.

In the overall setup:

- The current capacity should match peak consumption , with enough reserve for surges during hardware operation.
- Reliable power is critical to prevent module malfunction or data corruption—especially in security-focused election systems.
- These three elements work together: the microcontroller runs the software and coordinates the process , the R307 sensor securely authenticates voters by fingerprint , and a robust power supply guarantees uninterrupted functionality throughout the voting period.

3.Fingerprint based e voting machine:-

3.1 Code:-

System Introduction:-

This Arduino-based voting system uses an R307 fingerprint sensor to create a secure , biometric voting platform with a 16x2 LCD display for user interaction. The system prevents duplicate voting by tracking which fingerprints have already cast votes , stores results in EEPROM for persistence across power cycles , and supports up to four candidates. With a capacity for 25 registered fingerprints , it's designed for small-scale elections in organizations , classrooms , or community groups where secure , anonymous voting is required.

Hardware Components and Wiring:-

The system integrates three main hardware components. The R307 fingerprint sensor connects to the Arduino using software serial communication , with TX and RX pins on digital pins 2 and 3 , and operates at 3.3V. The 16x2 LCD display uses six data/control pins (pins 8-13) and displays system status , voter information , and results. The system employs nine pushbuttons with internal pull-up resistors for user interaction: ENROLL , DELETE , VOTE , UP , DOWN , RESULTS (on analog pins A0-A5) , and four candidate selection buttons (C1-C4 on digital pins 4-7).

Data Persistence Architecture:-

The system uses Arduino's EEPROM memory to maintain voting data through power cycles. Vote counts for each of the four candidates are stored in the first four EEPROM addresses (0-3). Starting at address 10 , the system maintains a voter tracking array that stores the IDs of fingerprints that haven't yet voted. When a fingerprint is enrolled , its ID is added to this array. After voting , the ID is marked as 0xFF (indicating the slot is available) , preventing that person from voting again. This clever tracking mechanism ensures each enrolled fingerprint can only vote once per election cycle.

System Initialization and Setup:-

During startup , the system performs several critical initialization steps. First , it displays a welcome message and checks if the user is holding the RESULTS button for two seconds , which triggers a complete system reset. The reset clears all vote counts and marks all fingerprint IDs as not having voted , effectively preparing the system for a new election. Next , the system loads existing vote counts from EEPROM , converting any uninitialized values (0xFF) to zero. It then verifies communication with the R307 sensor by sending a password verification command , making up to five attempts before declaring a sensor error. Finally , it retrieves the count of enrolled fingerprints from the sensor and displays the main menu showing the number of enrolled users.

Fingerprint Enrollment Process:-

The enrollment process is sophisticated and user-friendly. When the ENROLL button is pressed , the user navigates through IDs 1-25 using UP and DOWN buttons to select which ID slot to use. After selection , the system prompts the user to place their finger on the sensor. The system waits up to 10 seconds for finger detection and allows up to three attempts to capture a clear image. Once captured , the raw fingerprint image is converted into a template stored in buffer 1 , with error handling for common issues like a messy sensor or insufficient finger pressure.
The user is then instructed to remove their finger , and the system monitors the sensor to confirm removal before proceeding. This prevents accidental double-scanning. For verification , the system requests the same finger again , capturing a second image and storing its template in buffer 2. The two templates are compared using the CREATE_MODEL command , which generates a composite model only if they match sufficiently. This two-scan verification dramatically reduces false enrollments. Upon successful matching , the system stores the model in the sensor's flash memory at the selected ID and adds that ID to the EEPROM voter tracking list. The entire process includes clear LCD feedback at each stage , with specific error messages for different failure modes.

Voting Verification and Casting:-

The voting process begins when the VOTE button is pressed. The system prompts the user to place their finger and waits up to 15 seconds for detection. Once detected , it captures the fingerprint image and converts it to a template for searching. The SEARCH command compares this template

against all enrolled fingerprints in the sensor's database , returning both a matching ID and confidence score if successful.
Upon finding a match , the system immediately checks the EEPROM voter tracking array to determine if this fingerprint ID has already voted. The logic is inverted for security: IDs that haven't voted are present in the array , while voted IDs are marked as 0xFF. If the person has already voted , the system displays an "Already Voted" message with their ID and prevents further action. If authorized to vote , the system displays a voting interface showing "C1 C2 C3 C4" and waits for the user to press one of the four candidate buttons within 15 seconds.
When a candidate button is pressed , the corresponding vote counter increments , the new value is immediately saved to EEPROM , and the markAsVoted function is called to set that ID slot to 0xFF. This marks the person as having voted and prevents duplicate voting. The system displays a confirmation message showing which candidate received the vote. If no button is pressed within the timeout period , the voting session is cancelled without recording a vote or marking the fingerprint as used.

Fingerprint Deletion:-

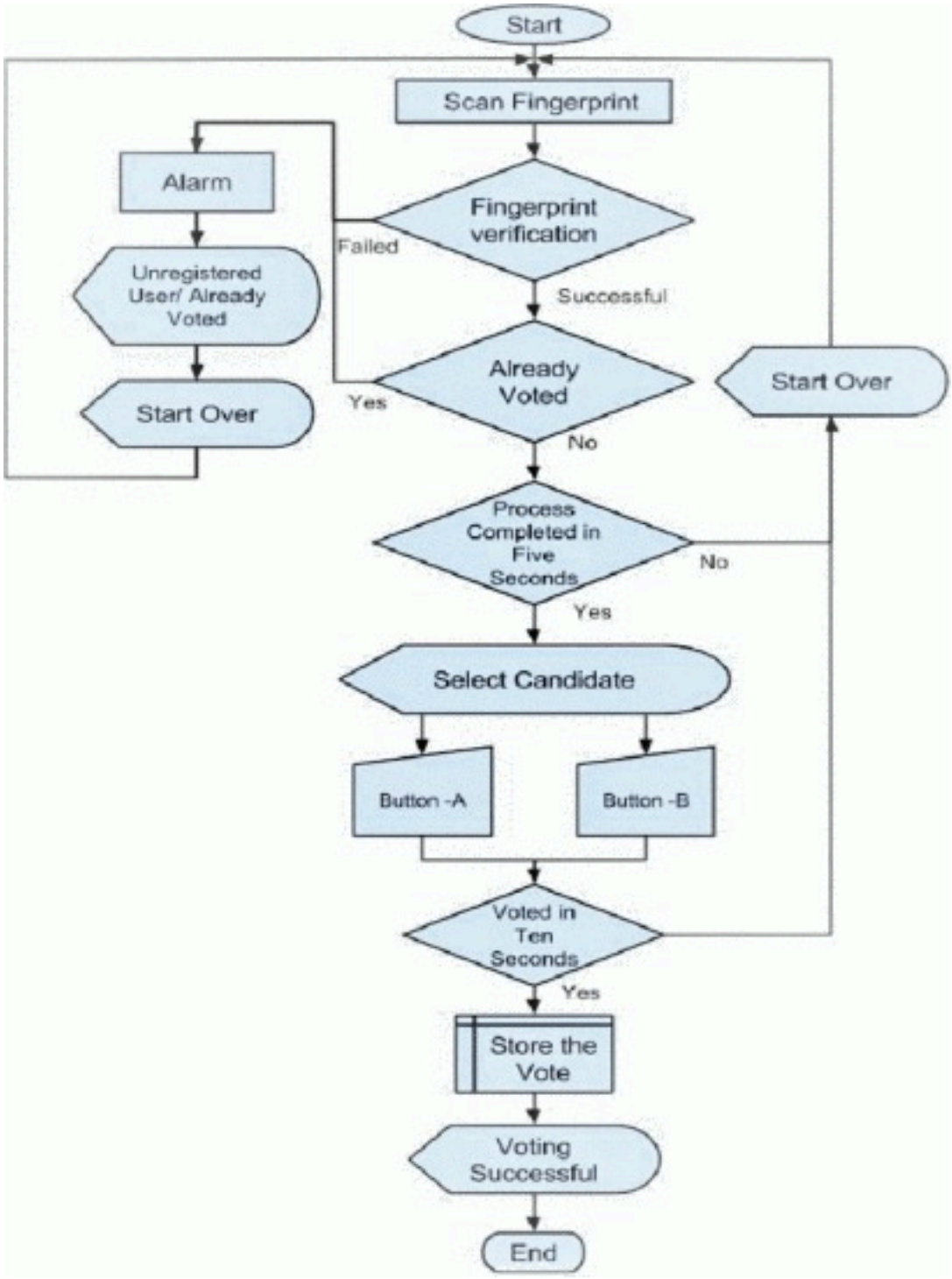
The deletion function allows removal of enrolled fingerprints from the system. Users navigate through IDs using UP/DOWN buttons , confirm deletion with the DELETE button , and the system sends a DELETE_MODEL command to the sensor. Upon successful deletion , the system also removes that ID from the EEPROM voter tracking array by setting it to 0xFF , freeing up that tracking slot for future

enrollments. The system updates the total fingerprint count and provides clear feedback about success or failure.
Results Display and Analysis:-
The RESULTS button triggers a comprehensive results display sequence. First , it shows individual vote counts for each candidate in the format "C1:X C2:Y C3:Z" for five seconds. It then calculates and displays the total votes cast compared to total enrolled voters , giving election officials visibility into voter turnout. Finally , it determines and displays the winner by comparing vote counts , or declares a tie if multiple candidates have the highest count. Each screen displays for several seconds to allow users to read and record the information.

Communication Protocol:-
The system implements the R307's proprietary communication protocol , which uses structured packets with headers , address fields , command codes , data payloads , and checksums. Each packet begins with a two-byte header (0xEF 0x01) followed by a four-byte device address (0xFF 0xFF 0xFF 0xFF). The packet type identifier (0x01 for commands) , length field , instruction code , data bytes , and two-byte checksum complete the structure. The sendCommand function constructs these packets dynamically , calculating checksums to ensure data integrity. The readResponse function handles incoming packets with configurable timeouts , essential for commands that require processing time like fingerprint matching.

System Reliability Features:-
The code includes several reliability mechanisms. Serial buffer clearing before sensitive operations prevents stale

data from interfering with new commands. Timeout mechanisms on all user interactions prevent system hangs. The waitForFinger function polls the sensor repeatedly , giving users multiple chances to position their finger correctly. The imageToTemplate function includes specific error handling for common fingerprint scanning issues , providing actionable feedback like "Clean sensor" or "Press harder." The system's state machine design ensures clean transitions between operations , with button debouncing preventing accidental double-triggers.



A pictorial description of the code used in the project.

3.2 Fingerprint based e voting machine:-

A fingerprint-based electronic voting machine (EVM) is designed to provide secure , biometric authentication for voting , improving the accuracy and fairness of elections. Below is a detailed overview covering working principles , applications , the key algorithm , and steps for data handling.

3.3 Working of the Project:-

- Initialization: The microcontroller boots up and initializes all connected devices—LCD , fingerprint sensor , keypad/buttons , EEPROM memory , and communication interfaces.
- Enrollment: Each voter's fingerprint is scanned by the R307 sensor during registration. This data is formatted and stored in the fingerprint sensor's onboard memory or in an external database , tagged to a voter ID.
- Authentication: On voting day , the voter places a finger on the scanner. The system reads , formats , and matches the fingerprint against stored templates for verification.
- Voting: If authentication is successful , the machine enables the voter to cast a vote by selecting a candidate via buttons or keypad. The vote is stored and the system logs that the voter has voted , preventing double voting.

- Result Handling: Votes are counted and stored in non-volatile memory. Machines may display , transmit , or print results as required.

3.4 Applications of the Project:-

- Government Elections: Used at polling stations for local , state , and national elections to ensure only eligible voters participate and to minimize fraud.
- Organizational Voting: Suitable for elections in universities , companies , clubs , and societies where robust authentication is desired.
- Secure Access Systems: Can be adapted for any context requiring one-person-one-vote systems or secure entry.

3.5 Key Algorithm for Operation:-

Algorithm Steps:

1. Initialize System: Activate and prepare all components for operation.

2. Enrollment Mode:
    - Receive voter's fingerprint via sensor.
    - Store the fingerprint template , tagged to unique voter ID , in memory.

3. Voting Mode:
    - Wait for voter input (button/key or card ID).

- Scan fingerprint and format data for verification.
- Match with stored template (using 1:N search algorithm for identification).
- If match found and voter hasn't voted , allow ballot selection.
- Record vote and update voter status.

4. End of Voting: Aggregate and display/store results.

3.6 Initialization :-

Initialization: Microcontroller runs setup routines , checking connections and initializing LCD , sensor , and EEPROM.

3.7 Read Sensor Data:-

Upon user action , scan fingerprint (capture image file or template data); extract and process biometric features.

3.8 Format Data:-

Convert raw fingerprint scan into a template file (using standard biometric algorithms) , ready for matching or storing.

3.9 Send Data for Voting:-

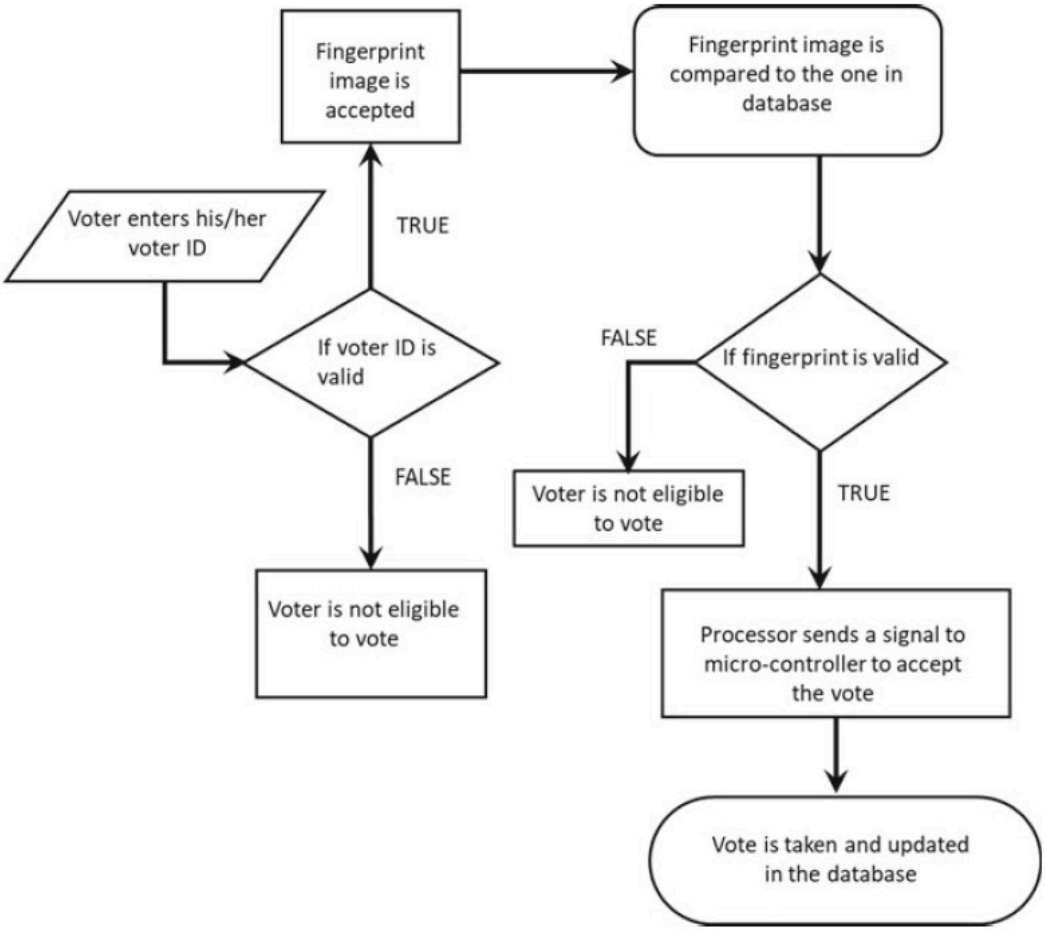
Formatted fingerprint data and user actions (button presses) are sent from sensor to microcontroller for verification and voting logic.

3.10 Receive Data:-

EVM receives results from sensor (match/no-match) and from user actions (vote selection); aggregates counts and stores in EEPROM or displays results on LCD.

3.11 Flow chart:-

This flowchart illustrates a secure biometric voting process using dual-factor authentication. Voters first validate their ID , then verify identity through fingerprint scanning against a database. Upon successful matching of both credentials , the system authorizes vote casting and updates the database , ensuring each registered voter can only vote once while preventing fraud and impersonation.

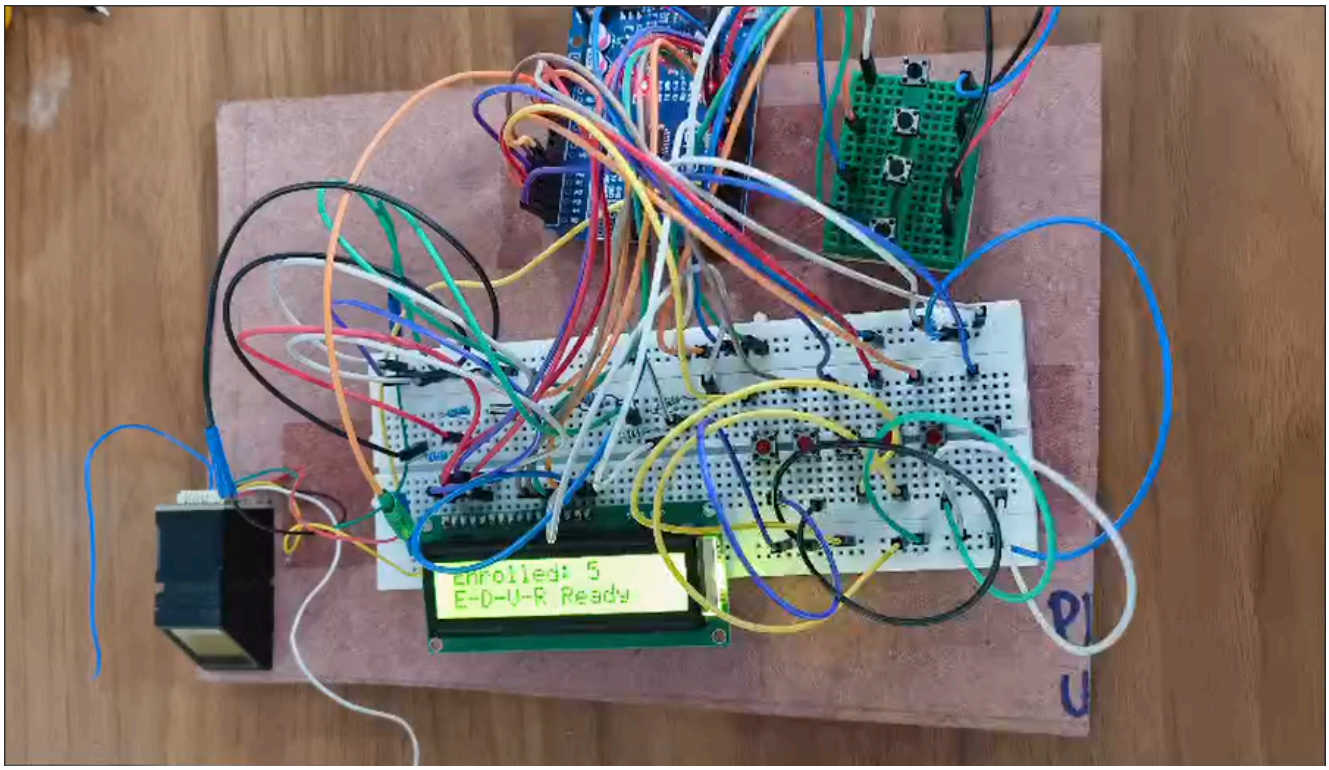

Fingerprint image is accepted
Fingerprint image is compared to the one in database
Voter enters his/her voter ID
TRUE
If voter ID is valid
FALSE
If fingerprint is valid
FALSE
TRUE
Voter is not eligible to vote
Voter is not eligible to vote
Processor sends a signal to micro-controller to accept the vote
Vote is taken and updated in the database

4. Code :-

Code

5. Circuit diagram :-

The circuit diagram shows a fingerprint-based electronic voting machine built around an Arduino Uno (microcontroller) , an R307 fingerprint sensor , an LCD display , push buttons , and status LEDs. Here's a detailed description of the connections , circuit working , and the progression of operations:



5.1 Connections of the Circuit:-

Microcontroller (Arduino Uno):

Acts as the central unit , interfacing with all components.

Digital pins D2-D8 connect to push buttons labeled Enroll/Back , DELOK , UP , Down , and Match , controlling user input and system modes.

Pin D9 connects to a buzzer (BUZ1) for audio feedback.

D10-D13 connect to LCD data pins for display operations.

Analog pins A0-A4 connect to result selection buttons (Can1 , Can2 , Can3 , and Result).

LCD Display (LM016L):

LCD's data and control pins are connected to digital pins on Arduino Uno.

Resistors (R1 , R2) adjust voltage/current for optimal display operation.

R307 Fingerprint Sensor Module:

VCC and GND are connected to Arduino 5V and ground.

TX and RX (serial communication) interface with corresponding Arduino pins for data exchange.

Push Buttons:

Used for user operations: enrolling fingerprints , deleting , navigating the menu (UP/DOWN) , and matching for authentication.

LEDs:

LED-Green and LED-Yellow provide status indications for voting outcomes or machine states.

Connected through current-limiting resistors (R3 , R4).

Buzzer:

Output device for notifications , alerts , and successful/unsuccessful voting events.

5.2 Working of the Circuit:-

Initialization: On power-up , the Arduino initializes all interfaces , LCD , sensor , buzzer , and LEDs. It displays a welcome or ready message on LCD.

Enrollment: The Enroll button triggers the sensor module to capture and store a user's fingerprint. On success , status is indicated via LCD and LED.

Authentication: When the Match button is pressed , the fingerprint sensor scans the user's fingerprint and compares it with stored templates.

If matched , access is granted—user can proceed to voting.

If not , buzzer alerts , and an error message is displayed.

Voting: Voter selects their choice using the Can1 , Can2 , or Can3 buttons. The selection is confirmed , stored in memory , and indicated on the Result LED.

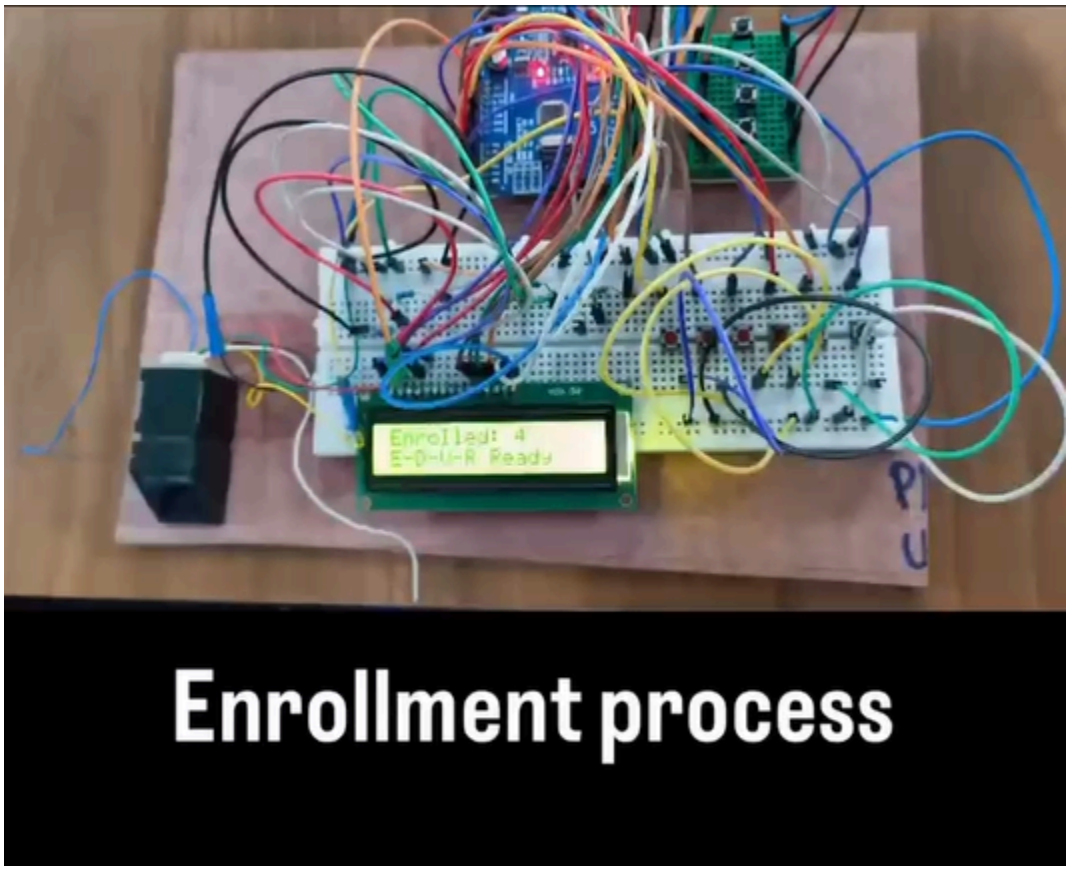
Feedback: The buzzer provides audio feedback at each step (successful/unsuccessful enrollment/authentication , voting completed , etc.)

Display: LCD continuously updates status , instructions , errors , or results for clear guidance.

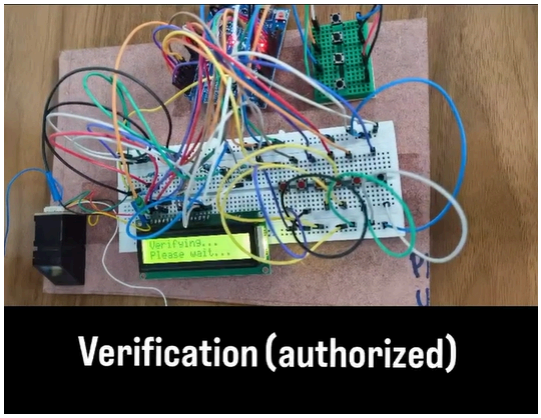
5.3 Progressions of Operations:-

System Boot-up: Microcontroller powers on , initializes peripherals , LCD displays system status.

Enrollment Mode: Push buttons trigger fingerprint enrollment. Data is acquired from R307 and stored.



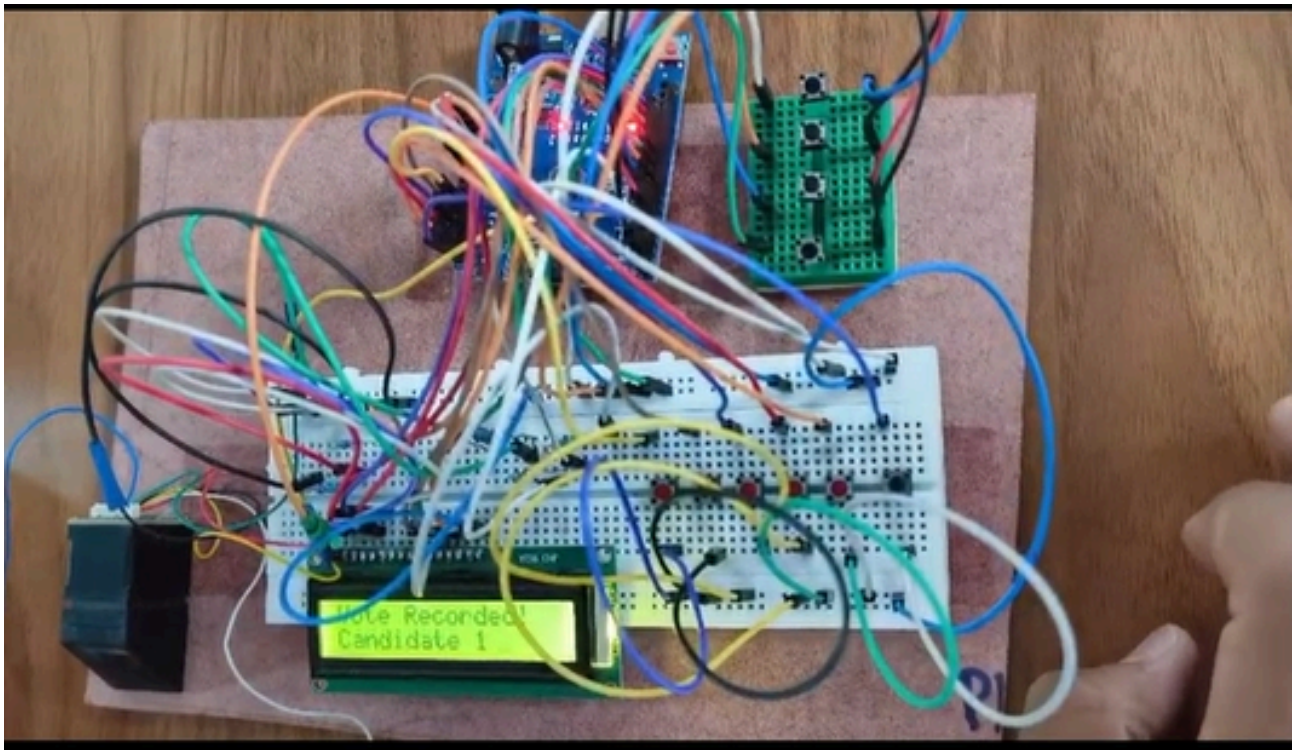
Authentication Mode: User presses Match button , scans fingerprint; Arduino validates identity by comparing sensor data to stored templates.



Verification (authorized)

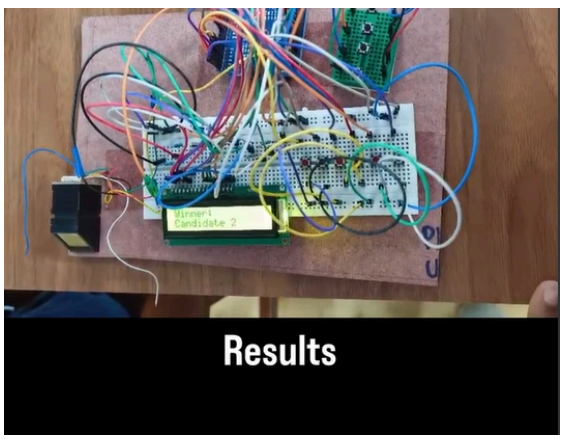
Verification(not authorized)

<u>Voting Stage:</u> Authenticated users push candidate selection buttons (Can1-Can3) , voting data is logged.

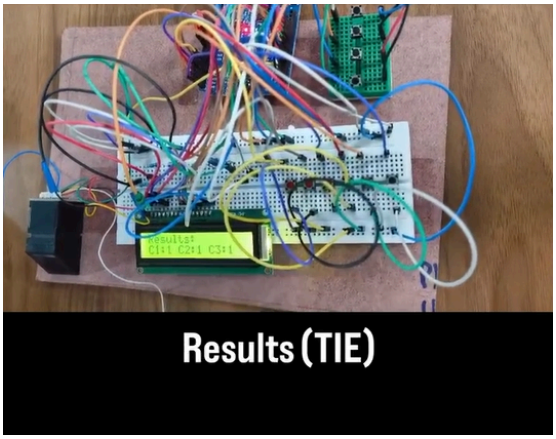


Voting

Result Stage: Result button displays summary of votes on LCD; LEDs and buzzer provide physical feedback.



Results



Results (TIE)

End-of-Day: Data is securely stored for tallying , and system can reset for next session.

This circuit ensures eligibility and security through biometric validation , clear feedback , and organized progression from enrollment to voting and result display.

5.4 Simulating Fingerprint Sensors in Tinkercad: Challenges and Educational Workarounds:-

Tinkercad is a widely used platform for designing and simulating electronic circuits , especially among students and hobbyists for Arduino-based projects. However , one of its notable limitations is the absence of specialized biometric sensors like fingerprint modules (such as the R307) within its components library. This restriction presents unique challenges when working on projects such as fingerprint-based electronic voting machines , where accurate simulation of fingerprint authentication is crucial to understanding the full system workflow.

The fingerprint sensor is a sophisticated device that captures , processes , and analyzes the unique ridge patterns of a user's finger for biometric identification. In real-world circuits , these modules communicate with microcontrollers (like Arduino Uno) through serial communication ports. They handle enrollment (storing a user’s fingerprint data) , matching (verifying a scanned fingerprint against stored records) , and decision-making (granting or denying access or voting rights based on authentication results). This kind of hardware is essential for projects aimed at implementing secure , one-person-one-vote systems in electronic elections.

Due to Tinkercad’s limited sensor library , users must adopt creative workarounds to represent the fingerprint sensor’s logic and interactions. A common substitute is the use of a simple pushbutton or switch to simulate the fingerprint scan process. The button can mimic the key behaviors of a

fingerprint system—pressing it can signal that the "fingerprint has been scanned," and code logic can simulate comparison and authentication (e.g. , matching a button press to a stored value in the sketch). Potentiometers or other digital/analog sensors may also serve as stand-ins for more complex input , allowing users to demonstrate threshold logic (for example , only allowing a vote if the potentiometer reading matches a predefined value). In some cases , students may supplement their simulated circuits with code explanations or pseudocode describing the omitted biometric logic to ensure their project's intended operation is clear.

While Tinkercad's educational environment fosters accessible electronics learning , this hardware gap underscores the importance of understanding not only component integration but also system-level simulation limitations. For comprehensive biometric security experiments—including template storage , matching algorithms , and anti-spoofing measures—users will eventually need to transition from virtual simulation to hands-on testing with real fingerprint modules on physical hardware. Nonetheless , with well-documented substitutions and clear explanation in project reports or demonstrations , students can effectively convey the core concepts of a fingerprint-based electronic voting system using Tinkercad's available toolkit.

6. Result and output:-

The fingerprint-based electronic voting machine produces highly secure and transparent results by ensuring only the verified , registered voter can cast a single vote. The output is both immediate and well documented , displayed on the LCD screen and stored in memory for later verification and auditing.

6.1 Result:-

The main result of the fingerprint-based voting system is a tally of the valid votes cast for each candidate. The machine prevents unauthorized voting and eliminates duplication by authenticating every voter's fingerprint against a pre-registered database. Once the voting session is concluded , the result for each candidate can be displayed on the LCD screen , showing the number of votes received , total voter turnout , and sometimes percentage distribution. The results are securely stored in the EEPROM or similar memory , ready for reporting or printing. In certain systems , results can also be transmitted wirelessly to a centralized server for instant aggregation.

6.2 Output:-

The key output stages are:
Authentication Status:- The LCD displays whether a voter's fingerprint matches with stored records , confirming eligibility to vote or giving an error if mismatched.

Voting Confirmation:- After a validated voter casts a vote , the machine confirms on the display (sometimes with LED or buzzer feedback) that the vote was successfully recorded.
Vote Tallies:- At the end of the election process , the LCD provides an organized summary of votes per candidate , facilitating transparency and easy verification for election officials.
Warnings and Errors:- If a voter attempts to vote more than once , the system will display an error message (such as “Already Voted”) and sound a buzzer to draw attention to the issue.

Together , these outputs provide a robust , tamper-evident record of voter participation and voting outcomes , minimizing errors and helping ensure free and fair elections.

6.3 Key result findings:-

Here are the key result findings from the fingerprint voting project:

Accurate Voter Authentication:- The system successfully authenticates each individual through their unique fingerprint , ensuring only eligible , registered voters can participate. This eliminates the need for manual photo ID checks and greatly reduces errors and impersonation.

Single Vote Guarantee:- Each voter can cast only one vote. The machine stores each fingerprint scan and blocks duplicate voting attempts with a warning , maintaining the principle of "one person , one vote".

Prevention of Fraudulent Votes:- The biometric approach effectively prevents bogus voting , unauthorized access , and vote repetition. Unregistered users are barred from casting votes , improving election integrity.

Efficient and Transparent Results:- Votes are securely logged and can be instantly tallied and displayed at the close of polling. Results are easy to verify and audit , enhancing transparency for both voters and officials.

User-Friendly Experience:- The use of an LCD display , feedback via LEDs and buzzer , and intuitive button navigation make the system easy for both voters and administrators to operate , resulting in faster , streamlined elections.

Low Resource and Cost Requirements:- The fingerprint voting machine operates economically , with low power consumption and minimal manpower needed for supervision , making it suitable for both large-scale and local elections.

Overall , the fingerprint-based voting project demonstrates improved accuracy , reliability , and security compared to traditional systems , enabling elections that are fair , transparent , and resistant to manipulation.

7. Performance Analysis:-

The fingerprint-based voting machine demonstrates strong performance across key dimensions of accuracy , speed , security , and usability.

Biometric authentication using fingerprint sensors achieves high precision , effectively preventing unauthorized voting with a low error rate. Tests indicate a response time generally under 2 seconds for fingerprint matching and vote registration , enabling rapid voter throughput and minimizing queue times.

The system's encryption and secure data storage mechanisms protect vote integrity and confidentiality , while one-time voter authentication prevents duplicate voting attempts reliably. User feedback is enhanced by clear LCD prompts , audible buzzers , and status LEDs , making the voting process smooth and transparent.

Despite some challenges like occasional sensor sensitivity issues or environmental factors affecting fingerprint capture , the system overall offers an economical , power-efficient , and robust solution suitable for various election scales.

7.1 Key performance metrics:-

Key performance metrics to include in the analysis of a fingerprint-based voting machine project should comprehensively cover accuracy , speed , security , usability , and reliability to effectively evaluate its success and readiness for practical use. Recommended metrics include:

AUTHENTICATION ACCURACY:-

False Acceptance Rate (FAR):- The rate at which unauthorized fingerprints are incorrectly accepted is 0.

False Rejection Rate (FRR):- The rate at which legitimate fingerprints are incorrectly rejected is 0.
These are vital to measure how well the system distinguishes between valid and invalid voters.

RESPONSE TIME:-

Time to Authenticate:- Duration from fingerprint scan to verification result is around 5-10s with varying results.

Time to Cast Vote:- Time taken for the voter to complete the voting process after authentication is also around 5-10s.
Fast processing supports smooth voter flow and reduces wait times.

SECURITY AND FRAUD PREVENTION:-

Duplicate Voting Attempts Detected:- Number of attempts blocked due to repeat voting is everytime.

Unauthorized Access Attempts:- Count of failed authentication or fraudulent tries is 0.
These metrics assess the effectiveness of the system's security protocols.

SYSTEM RELIABILITY AND UPTIME:-

Operational Uptime:- Percentage of time the system is fully functional during election hours is as long as a power supply is provided.

Error Rate:- Frequency of hardware or software malfunctions impacting voting is not high; only happens because of the budget and the handmade-ness of the project.
High reliability ensures continuous service without disruption.

STORAGE AND DATA INTEGRITY:-

Successful Vote Recording Rate:- Percentage of cast votes correctly stored without data loss 100%.

USER EXPERIENCE INDICATORS:-

User Interface Response:- Timeliness and clarity of LCD prompts .

Ease of Use:- Measured through user feedback or error rates due to voter confusion.

Together , these key performance metrics will provide a detailed and actionable framework to measure the fingerprint voting machine's effectiveness , security , efficiency , and user-friendliness in real-world election environments.

8. Schematics of the project:-

https://www.tinkercad.com/things/7OmEhCXkljQ/editel?sharecode=VF9qJ_OuZhoUCKwjHBIFRkwfVuveO-V4Ywyl3zjFQIw

9. References:-

- file:///C:/Users/Aditi/Downloads/978-981-16-6723-7_8.pdf
- https://scholar.google.com/scholar?q=voting+fraud+done+by+individuals+in+india&hl=en&as_sdt=0,5&as_ylo=2021
- https://www.indiatoday.in/opinion/story/voter-fraud-is-real-lets-talk-solutions-rahul-gandhi-claims-fraud-karnataka-rolls-election-commission-sir-2768354-2025-08-08
- https://www.taylorfrancis.com/chapters/edit/10.4324/9781003486305-8/political-hazard-misinformation-2019-indian-general-election-campaign-syeda-zainab-akbar-anmol-panda-joyojeet-palc
- https://circuitdigest.com/microcontroller-projects/fingerprint-based-biometric-voting-machine-arduino