Bio-Ballot: Fingerprint-Secured Voting with Real-Time Transparency

Hemashree[1], Jayaprakash B S[2], Jishnu T[3], Nikesh B[4], Prof. Gourish S Hegde[5]
[1,2,3,4]*Department of Electronics and Communication Engineering, Srinivas Institute of Technology, Mangaluru – 574 143, Karnataka, India*
[5]*Assistant Professor, Department of Electronics and Communication Engineering, Srinivas Institute of Technology, Mangaluru – 574 143, Karnataka, India*
doi.org/10.64643/IJIRTV12I12-206811-459

***Abstract*—This paper presents the design and implementation of Bio-Ballot, a fingerprint-secured electronic voting system with real-time transparency. The system leverages biometric authentication using the R307 optical fingerprint sensor interfaced with an Arduino UNO microcontroller to ensure that each registered voter casts exactly one vote, strictly upholding the principle of one person, one vote. Votes are securely stored in the Arduino's internal EEPROM, ensuring data persistence even during sudden power failures. A 16×2 LCD provides live statistics including total votes, gender-based participation counts, and candidate-wise results. The system features a hybrid architecture, combining complete offline functionality for areas with limited connectivity and optional online monitoring through an ESP Wi-Fi module and Flask-based backend server. Testing confirmed a 0% False Accept Rate (FAR), 100% enrollment success rate, and seamless data synchronization between offline EEPROM storage and the online database. Bio-Ballot demonstrates a practical, cost-effective, and tamper-resistant solution for secure and transparent elections applicable to both local and large-scale deployments.**

***Index Terms*—Arduino UNO, biometric authentication, EEPROM storage, fingerprint sensor, R307, electronic voting, ESP8266, Flask server, real-time monitoring, embedded systems.**

I. INTRODUCTION

Conventional voting systems face persistent challenges including voter impersonation, duplicate voting, and lack of real-time transparency. These vulnerabilities erode public trust in electoral processes, particularly in regions with limited infrastructure. Bio-Ballot – Fingerprint-Secured Voting with Real-Time Transparency is developed to directly address these challenges by integrating biometric authentication into an embedded voting platform.

At the core of the system lies the Arduino UNO microcontroller, which coordinates the R307 fingerprint sensor, 16×2 I2C LCD display, EEPROM memory, push buttons, LED indicators, and a buzzer. Every vote is securely stored in EEPROM, ensuring data integrity even during sudden power failures. The LCD enhances transparency by displaying live statistics total votes cast and gender-based participation keeping operators and participants informed in real time.

A unique feature of Bio-Ballot is its hybrid architecture combining offline reliability with optional online scalability. In offline mode, it functions as a fully self-contained unit ideal for rural or remote areas. With the integration of an ESP Wi-Fi module and a Flask-based server, the system supports centralized monitoring and long-term digital record-keeping, making it adaptable to large-scale deployments.

II. LITERATURE SURVEY

Kumar et al. [1] explored minutiae-based fingerprint matching algorithms to reduce False Acceptance Rate (FAR) and False Rejection Rate (FRR) in secure voting systems, demonstrating that biometric verification significantly improves voter authentication accuracy while preventing duplicate voting. However, challenges persist for rural users with worn or dry fingerprints.

Alzubaidi and Kalita [2] conducted a broad review of offline IoT-based voting mechanisms, emphasizing the integration of real-time LCD feedback for transparency and Arduino-based voter gender classification. They acknowledged the limited scalability of such systems for larger electoral applications.

Gupta and Reddy [3] proposed an Arduino and fingerprint sensor-based e-voting system emphasizing ease of use and low-cost offline implementation using button-based inputs. While limited to four candidates, it established a practical framework for standalone, localized voting machines.

III. SYSTEM REQUIREMENTS

A. Hardware Components

The Arduino UNO (ATmega328P) serves as the main controller, operating at 16 MHz with 14 digital I/O pins, 6 analog inputs, and 1 KB internal EEPROM. It handles fingerprint authentication, vote recording, live statistics display, and peripheral device management.

The R307 optical fingerprint sensor operates at 3.3–6V via UART, supporting image acquisition, feature extraction, template storage, and matching. Each voter's fingerprint is matched to a stored template, and the matched ID is linked to gender data for demographic vote classification.

A 16×2 I2C LCD displays system messages (e.g., "Place Finger," "Vote Casted," "Access Denied") and real-time statistics. Five tactile push buttons enable candidate selection. An internal piezoelectric buzzer and candidate-specific LEDs provide audio-visual feedback.

The ESP8266/ESP32 Wi-Fi module enables optional online mode, transmitting encrypted vote activity to the Flask server for real-time transparency. A custom 3D-printed PLA enclosure houses all components for portability and protection.

B. Software Components

The Arduino IDE with embedded C/C++ is used for firmware development. Key libraries include the Adafruit Fingerprint Sensor Library (enrollment, matching, deletion), the Liquid Crystal library (LCD control), and the EEPROM library (non-volatile vote storage). The Flask framework provides a lightweight backend API for vote logging and real-time monitoring.

Table I: Pin Configuration

Sl.	Component	Pin
1	Fingerprint Sensor TX	Pin 2
2	Fingerprint Sensor RX	Pin 3
3	LCD SDA (I2C)	A4
4	LCD SCL (I2C)	A5
5–9	Buttons (Candidates 1–5)	Pins 4–7, 10
10–14	LEDs (Candidates 1–5)	Pins 11–13, A0, A1
15	Buzzer	Pin 8
16	Admin Button	Pin 9

IV. METHODOLOGY

The development followed a six-phase structured methodology to ensure accuracy, security, and reliability.

Phase 1 – Requirement Analysis: Key challenges in traditional voting impersonation, duplicate voting, lack of transparency was identified. Functional requirements including fingerprint authentication, duplicate prevention, live statistics, and optional online monitoring were finalized.

Phase 2 – Workflow Planning: A complete operational sequence was defined: (1) voter places finger, (2) fingerprint is matched, (3) system checks EEPROM for prior votes, (4) voter selects candidate via push button, (5) vote is stored in EEPROM, (6) LCD updates live statistics, and (7) data is optionally transmitted via ESP module.

Phase 3 – Hardware Planning: Component interfacing was mapped, including UART-based R307 integration, 4-bit LCD operation, button debouncing, buzzer/LED feedback, and ESP module wiring.

Phase 4 – Software Development: Modular code was developed for biometric authentication, duplicate vote prevention (EEPROM-based voter status), vote casting logic, gender-based counter increments, LCD display updates, and encrypted online synchronization via HTTP to the Flask server.

Phase 5 – System Integration: All hardware and software modules were combined and verified for inter-module communication and functionality.

Phase 6 – Testing and Validation: Module-level and system-level testing was conducted, including fingerprint accuracy tests, EEPROM stability tests, full voting cycle simulations, and online synchronization validation.

V. DESIGN AND IMPLEMENTATION

A. System Architecture

The Bio-Ballot architecture comprises six functional units: (1) Fingerprint Authentication Unit (R307 sensor), (2) Control Unit (Arduino UNO), (3) Voting Interface Unit (push buttons + LCD), (4) Data Storage Unit (EEPROM), (5) Feedback Unit (LEDs + buzzer), and (6) Online Extension Unit (ESP8266/ESP32 + Flask server). The operational flow is:

Voter → Fingerprint Sensor → Arduino → Voting Logic → EEPROM → LCD Display → (Optional) Server.

B. Algorithm

The system follows an event-driven algorithm: (1) Initialize all peripherals and load EEPROM data. (2) Display "Place Finger to Vote" in standby. (3) Capture and match fingerprint; deny access if unmatched. (4) Check EEPROM for prior votes; block if already voted. (5) Display candidates and await button press. (6) Record vote in EEPROM, update gender counters, trigger buzzer/LED. (7) Monitor admin button combination; allow result viewing or secure reset on successful admin fingerprint authentication.

C. Secure Admin Reset

The reset functionality is protected by multiple layers: admin must authenticate via fingerprint, then hold a designated button for 5 continuous seconds during which the LCD displays a countdown. Early release cancels the reset. On completion, all vote counters, gender counts, candidate tallies, and "already voted" EEPROM flags are cleared to zero.

VI. RESULTS AND DISCUSSION

A. Fingerprint Enrollment and Authentication

All test voters were enrolled with a 100% success rate using the R307 sensor. The system achieved a 0% False Accept Rate (FAR) across all trials. False Reject Rate (FRR) errors were attributed exclusively to improper finger placement (excessive dryness, partial impressions) and resolved immediately upon repositioning. Average fingerprint recognition time was approximately 1 second.

B. Vote Casting and Data Persistence

All five candidate buttons responded in under 100 milliseconds. Gender-based vote classification showed no mismatches across all test sessions. EEPROM storage demonstrated complete data persistence through repeated power cycles, with accurate vote totals recovered in all cases. No data corruption or memory loss was observed.

C. Online Synchronization

The ESP module established Wi-Fi connectivity within 2–4 seconds and maintained stable HTTP communication with the Flask server (HTTP 200 responses consistently received). The average delay between hardware voter registration and online dashboard update was under 1 second. The online voter management table accurately reflected each voter's "Voted/Not Voted" status, with zero synchronization mismatches observed.

D. Admin Interface

Admin login via fingerprint reliably blocked all unauthorized access attempts. The LCD admin dashboard displayed accurate, real-time candidate-wise and gender-wise statistics that matched EEPROM values throughout extended testing. The secure reset function operated reliably; accidental resets were prevented in all test cases by the 5-second hold requirement.

VII. CONCLUSION AND FUTURE SCOPE

Bio-Ballot successfully demonstrates a practical, low-cost, and tamper-resistant embedded voting system. Key results 0% FAR, 100% enrollment success, complete EEPROM data persistence, and sub-1-second online synchronization validate the system's suitability for small-to-medium scale elections.

The hybrid offline/online architecture makes it deployable in both rural areas with limited connectivity and urban environments requiring centralized monitoring.

Future enhancements include: (1) expansion of voter and candidate capacity using external EEPROM modules; (2) encryption of stored vote data; (3) OLED/TFT display upgrade for improved usability; (4) rechargeable battery integration for portability; (5) USB/SD card result export for auditing; and (6) AI-based liveness detection to further strengthen biometric security.

ACKNOWLEDGMENT

The authors thank the management of A Shama Rao Foundation, Principal Dr. Shrinivasa Mayya D, HOD Dr. Soorya Krishna K, project guide Prof. Gourish S Hegde, and project coordinator Prof. Deeksha of Srinivas Institute of Technology, Mangaluru, for their invaluable guidance and support throughout this project.

REFERENCES

[1] R. Kumar, A. Sharma, and V. Mehta, "Secure Biometric Voting System Using Fingerprint Recognition," *IEEE*, 2022.
[2] Alzubaidi and J. Kalita, "Authentication in IoT-Based Voting Systems: A Review," *IEEE*, 2022.
[3] P. Gupta and S. Reddy, "Offline E-Voting System Using Arduino and Biometric Sensor," *IEEE*, 2022.
[4] Hangzhou Grow Technology Co. Ltd., "R307 Optical Fingerprint Sensor Module Datasheet." [Online]. Available: https://www.electronicwings.com/public/uploads/user/fingerprint-module-r307.pdf
[5] Arduino.cc, "Arduino Uno Rev3 – Technical Documentation." [Online]. Available: https://store.arduino.cc/products/arduino-uno-rev3
[6] Hitachi Semiconductor, "HD44780U LCD Controller Datasheet." [Online]. Available: https://www.sparkfun.com/datasheets/LCD/HD44780.pdf
[7] Microchip Technology Inc., "24LC256 – I²C Serial EEPROM Datasheet." [Online]. Available: https://www.microchip.com/en-us/product/24LC256