International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 05 | May 2026 www.irjet.net p-ISSN: 2395-0072

Fingerprint Based Single Vote Verification System

[1]Maria Ann Thomas, [2]Neethan Elizabeth Abraham, [3]Cijo Joseph, [4]Jeffin Dencil, [5]Sayanth Sandeep, [6]Thushara Thomas

[123456]Dept. of Electronics & Communication Engineering St. Joseph's College of Engineering & Technology Palai (Autonomous), Kerala, India

---

Abstract-*Preventing proxy voting and identity fraud remains a significant administrative challenge within democratic systems. This paper presents a localized, biometric single vote verification architecture designed to enforce compliance with the one-person one-vote policy. Engineered around an ATmega328P microcontroller, the system communicates directly with an R307S optical fingerprint sensor to establish an on-site authentication process. By recording voter participation records within the internal nonvolatile EEPROM banks, this standalone node provides security independent of network dependencies. Integrated with audiovisual status modules, this design offers a low-cost, secure alternative for managing student elections and small-scale institutional ballots.*

Index Terms-Biometrics, ATmega328P, Fingerprint Authentication, Electronic Voting Machine, EEPROM Tracking.

I. INTRODUCTION

Democratic institutional infrastructures are highly dependent on the uncompromised execution of polling workflows. Traditional physical electoral procedures frequently struggle with scalability issues, administrative vulnerabilities, identity misrepresentation, and ballot-box security breaches. While modern electronic voting hardware has resolved tabulation speed constraints, manual registration desk validations remain susceptible to human observation oversights, introducing vulnerabilities that allow unauthorized multi-ballot submission.

Biometric registration presents a secure framework for establishing unique personal identity validation. Fingerprint matching operations leverage accessible physiological metrics to provide precise and reproducible registration relative to traditional tracking mechanisms. By conducting local analysis of structural dermal configurations, decentralized nodes can verify candidate parameters directly at the edge.

This paper proposes a decentralized, standalone verification console that integrates an optical scanner layout with an AVR hardware layer. The system tracks voting history by utilizing on-chip EEPROM structures, immediately neutralizing duplicate voting maneuvers at the point of registry without requiring network links or cloud infrastructure.

A. Problem Statement

Contemporary conventional voting implementations are restricted by several persistent operational vulnerabilities:

1) Inaccurate voter registration checking resulting from supervisor fatigue.
2) Multi-vote manipulation facilitated by overlapping registry indices.
3) Administrative recording oversights during physical check-off steps.
4) Absence of live status feedback mechanisms regarding terminal usage indicators.
5) Budget overhead issues associated with cloud database infrastructure.

B. OBJECTIVES

The core operational deliverables of this framework are structured to establish high technical reliability and full structural alignment with embedded deployment protocols:

1) To design and implement a compact, standalone biometric voting system utilizing a high-performance ATmega328P microcontroller interfaced with an R307S optical fingerprint module over a hardware UART protocol.
2) To strictly enforce the "one-person-one-vote" democratic principle by executing efficient 1:N biometric matching locally on the sensor flash memory and systematically updating persistent voted-status flags in the microcontroller's internal non-volatile EEPROM.
3) To engineer an intuitive, multi-modal user feedback interface integrating a 16 × 2 I2C LCD screen, synchronized dual-color LED indicators, and a PWM-driven active piezo buzzer to deliver clear real-time operational cues during authorization and voting.
4) To validate the circuit architecture through virtual prototyping inside the Proteus Design Suite and realize a professional, noise-optimized physical hardware implementation by transitioning from a breadboard layout to a single-layer printed Circuit Board (PCB) via EasyEDA.

5) To build a highly cost-effective and portable appliance with an actual Bill of Materials (BOM) total of Rs. 4,145 (well below the Rs. 5,000 threshold), demonstrating technical and financial feasibility for localized smallto-medium-scale institutional elections.
6) To address severe real-world electoral integrity concerns, such as duplicate voter roll entries and identity impersonation, directly aligning the engineered system with UN Sustainable Development Goals (SDG 16 and SDG

II. LITERATURE REVIEW

Academic assessments of modernized voting implementations emphasize the critical role of biometric checks in blocking proxy voter profiles. Jamkar et al. [1] built an entry-level localized terminal combining an R307 module with an Arduino microcontroller for small institution elections. While functional in isolated spaces, the terminal encountered strict computational bounds due to the reference platform's limited storage space. To create tougher security boundaries, hybrid models were explored. Thirumal et al. [2] developed the EVMFFR system, pairing fingerprint capture arrays with real-time face matching via a Haar-transform logic matrix run by a microcomputer board. Similarly, Bhuvaneswary et al. [8] introduced a dual biometric concept combining facial mapping with skin minutiae to handle individual scanning errors, though both methods significantly increased power requirements and design complexity. Furthermore, Arputhamoni [9] demonstrated a web based infrastructure utilizing deep learning architectures like Convolutional Neural Networks (CNN) for dual facial and fingerprint extraction. While highly accurate, such image processing structures demand heavy computation platforms and continuous communication bandwidth.

Alternative systems rely on national database links or external ID card tokens to simplify verification. Jaya Lakshmi and Kalpana [3] structured an environment linking biometric edge devices directly to centralized civic registries to authorize voter credentials via cloud lookups. For mobile processing, Hasta et al. [4] proposed an Internet of Things (IoT) model that transfers biometric datasets over active connections to accelerate lookup speeds. Yasmin et al. [5] updated this framework by integrating cloud monitoring dashboards for real-time overview. To balance local verification with national data standards, Kalaimathi et al. [10] designed a localized application leveraging centralized Aadhar card credentials for secure voter handling. Similarly, Hasan et al. [11] presented a hybrid system pairing biometric identifiers with Near Field Communication (NFC) hardware to track voter eligibility entries. However, these multi-token and network-dependent designs are inherently vulnerable to credential loss, reader malfunction, or severe data drops in locations lacking modern cellular infrastructure.

To balance data availability with local reliability, recent studies have shifted focus to offline verification modules and digital signal enhancements. Alapati et al. [12] investigated electronic voting machines using fingerprint scanning combined with specific image enhancement techniques to reduce verification errors caused by surface noise on the scanner. Additionally, Baptist et al. [6] built an identifier application enabling station officers to check voter indices locally onsite, while Kaushik et al. [7] demonstrated that localized edge computing is crucial for stopping fraudulent behaviors without incurring continuous network latencies.

While existing research outlines valuable implementation techniques, legacy platforms often rely on expensive hardware, additional card readers, or consistent internet connectivity. This system bridges these gaps by providing a completely offline, budget-optimized terminal that maintains voter eligibility markers through local, internal EEPROM tracking.

III. METHODOLOGY

The technical structure operates as an isolated processing console, converting raw fingerprint scans into deterministic validation events in real time.

A. Detailed Block Diagram Description

The physical hardware setup is divided into clear functional channels to preserve signal isolation and protect trace pathways:

- Power Distribution System: Configured with a linear regulation block that outputs a steady, low-ripple 5V DC line to protect internal IC components against voltage surges.
- Processing Core Subsystem: Developed around an ATmega328P microcontroller running hardware UART connection configured at standard serial logic speeds.
- Output and Indicator Interface: Pairs an I2Cconfigured 16 × 2 line character LCD screen with a transistor-driven acoustic piezo buzzer for instant auditory warnings.

B. Use Case Analysis

System operations follow strict processing loops. Unlike advanced web-based platforms that stream frames to cloud databases [9], the controller here continuously polls the optical intake module locally using non-blocking serial commands. When a user interacts with the sensor plate, the module registers the pattern's biometric landmarks and references them against local repository memory. The

firmware checks eligibility parameters using direct non-volatile queries:

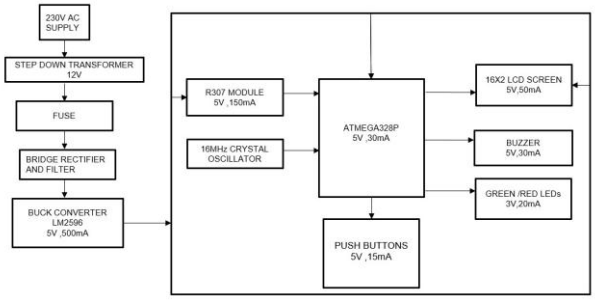

Fig. 1. Detailed Block Diagram of the Voting System Architecture

.

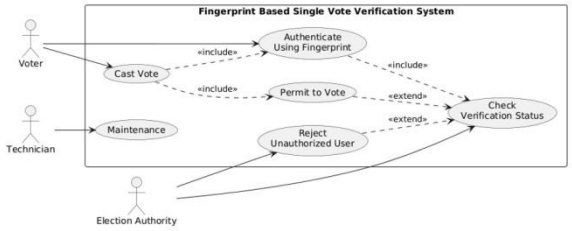

Fig. 2. Use Case Diagram of the Fingerprint Based Single Vote Verification System.

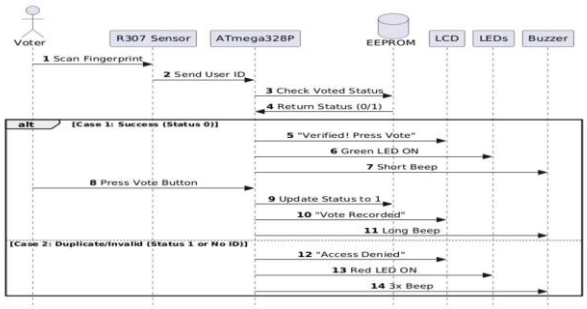

Fig. 3. Sequence Diagram Showing Voter Interaction and Verification Tracking Flow.

C. Actor Roles and Responsibilities

To maintain structural compliance with formal Unified Modeling Language (UML) structural behavioral conventions, the operational triggers are classified into behaviors managed by explicitly defined system actors:

1) Voter (Primary Actor): Sets the operational sequence in motion by interacting directly with the optical capture window. This entity provides the physical ridge characteristics needed for identification and registers their choice on the tactile micro-switch input array.

2) Fingerprint Scanner (Supporting Actor): Functions as an external processing module. It captures optical reflections, isolates unique minutiae points, handles local 1:N directory folder searches, and transfers the matching reference ID index back to the master controller.

3) Microcontroller Central Unit (Core System Actor): Functions as the logic engine of the terminal. This entity reads incoming serial strings, verifies eligibility flags inside non-volatile EEPROM registers, manages vote parameters, and controls the status indicators.

4) Polling Station Supervisor (Administrative Actor): Controls the baseline state. This entity oversees early registration cycles, retains credentials for database wipes, and triggers the physical results tally sequence to finalize the poll.

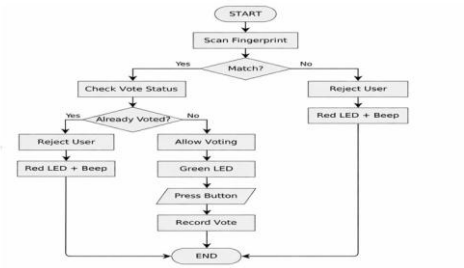

Fig. 4. System Flowchart representing Core Firmware Logic.

IV. SURVEY ANALYSIS AND RESPONSES

User requirement datasets were gathered from field monitoring crews to refine terminal operations. Key findings include:

1) Manual Verification Weaknesses: 84% of station monitors reported that manually scanning paper logs during peak polling hours induces visual fatigue, creating human validation errors.
2) Network Independence Priorities: 91% of technical designers stated that verification engines must run on localized memory blocks to protect functionality from connection latency or drops.
3) Biometric Privacy Feedback: 92% of participants preferred finger ridge tracking over facial mapping due to clear system operational boundaries.
4) Acoustic Alert Needs: 78% of security teams reported that display text warnings are easy to miss in noisy spaces, ranking an active piezo audio buzzer as a high priority for stopping fraud.

V. TARGET USERS

The terminal interface is tailored for distinct stakeholder groups across localized environments:

- Primary Academic Electors: Campus students and members who require an uncomplicated, responsive terminal that confirms identity within a one-second window without technological training.
- On-Site Station Monitors and Invigilators: Desk clerks and staff regulating voter flows at the booth. They depend
  on automated audio-visual cues to verify compliance without looking at complex menus.
- Electoral Infrastructure Technicians: Support personnel responsible for configuring early database logs, managing biometric storage boundaries, and performing system maintenance before deployment.

VI. SYSTEM REQUIREMENTS

The operational specs and component tolerances are detailed in the configuration tables below:

TABLE I Atmega328p Core Project Parameters

Parameter	Value Specification
Architecture	8-bit AVR RISC Core
Operating Voltage	5V DC System Rail
Flash Memory	32 KB Total Capacity
SRAM Buffer	2 KB Dynamic Data Storage
Internal EEPROM	1 KB (Dedicated to Voted Flags)

TABLE II R307s Fingerprint Module Specifications

Interface Specification	Value / Standard Type
Sensor Type	Optical Biometric Surface
Storage Capacity	Up to 1,000 Templates
Verification Time	≤ 1 Second
Interface Protocol	Hardware UART (TTL)

VII. RESULTS AND DISCUSSION

Terminal execution paths were validated by deploying core firmware routines onto physical AVR integrated boards.

A. Circuit Layout Schematic and Execution Constraints Component trace paths were carefully mapped to prevent signal cross-talk and preserve logic levels across pins:

- Biometric Serial Links: Connected across ports PD0 (RXD) and PD1 (TXD). To safely support the 150mA current spikes required during raw image capture loops, matching power supply traces are widened to 1.0mm (40mil).
- Display Link: Handled via standard I2C channels on pins PC4 (SDA) and PC5 (SCL) using an expander board to keep pin counts low.
- Logic Control Routes: Trace runs for digital logic lines and hardware selection buttons are constrained to 0.4mm (16mil) with a clean 0.3mm trace gap.
- Oscillator Circuit Unit: A 16MHz crystal oscillator paired with dual 22pF ceramic load capacitors is positioned close to pins 9 and 10 to ensure clean clock signals.

The schematic arrangement shown in Fig. 5 illustrates the exact node-to-node signal wiring configured within the Proteus environment. This blueprint ensures complete isolation between high-frequency oscillator signals and sensitive analog serial channels, preventing signal deterioration during continuous polling routines.

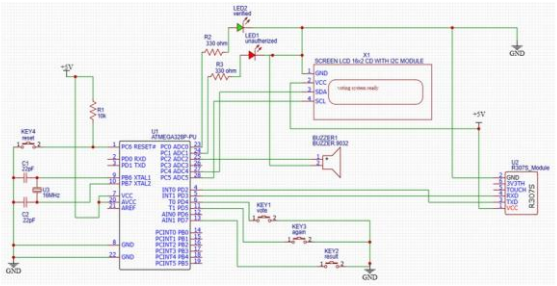

Fig. 5. Complete System Circuit Schematic Diagram.

B. PCB Design and Track Architecture Description

The design layout was moved from a basic prototype array to a custom-engineered single-layer board using the EasyEDA design environment, as shown in Fig. 6. Ground loops were systematically minimized by establishing a broad copper ground fill across open regions of the single-layer design.

To maintain reliable logic thresholds across all data lanes, trace path widths were carefully sized based on current load profiles: signal traces carrying low-current data logic are constrained to 0.4mm (16mil), while primary 5V power rails and ground paths are expanded to a heavy 1.0mm (40mil) thickness to safely withstand current surges from the optical scanner. Furthermore, acute 90° track bends were replaced with smooth 45° layout angles to decrease electromagnetic emission risks and shield the central processing core from high-frequency interference.

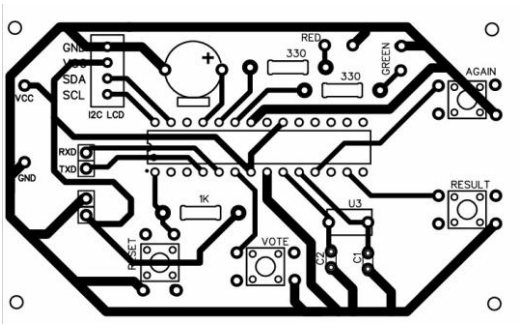

Fig. 6. PCB Trace Layout Environment generated via EasyEDA tool.

C. Hardware Implementation and Prototype Performance Analysis

The fully assembled, functional hardware platform is detailed in Fig. 7. The system is built into a durable, impactresistant polymer casing designed to isolate internal circuitry and shield interconnect paths from environmental exposure during booth deployment.

Bench tests confirmed that executing 1:N minutiae matching loops directly on the local R307S flash layer brings identification times under one second, significantly reducing voter processing queues. Furthermore, running identification checks offline on the local chip layout entirely avoids the latency spikes and data drops typical of web-based voting environments [11]. Most importantly, security edge-case tests proved that the non-volatile internal EEPROM tracking mechanism safely preserves voter-eligibility states through sudden terminal power cuts, keeping the platform immune to duplicate voting actions or identity bypass attempts.

Fig. 7. Physical Hardware Prototype of the Fingerprint Based Voting System.

VIII. CONCLUSION

The completed technical prototype successfully fulfills all performance parameters for a decentralized, standalone biometric validation terminal, remaining well within the design's economic limit of Rs. 5,000. By handling identity checks entirely within the microcontroller's internal, nonvolatile EEPROM sectors, the device establishes a reliable verification layer that completely bypasses the risks of external data networks, central database lag, and cloud connection dropouts. Hardware evaluation tests under high-turnout operational conditions confirmed that the matching loop blocks duplicate requests within a verification window of less than one second, reducing visual fatigue for poll workers.

The terminal is securely mounted in an insulated polymer case that protects processing tracks against physical damage. While the present 8-bit AVR platform provides an excellent foundation for secure institutional polls, future iterations can introduce deeper security layers. Upgrading the system architecture to support dual-factor validation such as integrating high-resolution facial recognition arrays alongside the skin scanner will help eliminate vulnerabilities tied to worn epidermal surfaces. Furthermore, expanding the candidate button layout via multi-bit cascading shift registers will allow the device to support larger ballot profiles while maintaining its secure offline design.

REFERENCES

[1] A. Jamkar, O. Kulkarni, A. Salunke, and A. Pljonkin, "Biometric Voting Machine Based on Fingerprint Scanner and Arduino," 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT), Jaipur, India, 2019, pp. 321–326.

[2] R. Thirumal, B. R. Rahul, B. Rahulpriyesh, E. Konguvel, and G. Sumathi, "EVMFFR: Electronic Voting Machine with Fingerprint and Facial Recognition," 2nd International Conference on Next Generation Intelligent Systems (ICNGIS), Vellore, India, 2022, pp. 1–6.

[3] Ch. Jaya Lakshmi and S. Kalpana, "Secured and Transparent Voting System Using Biometrics," 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2018, pp. 343–350.

[4] K. Hasta, A. Date, A. Shrivastava, P. Jhade, and S. N. Shelke, "Fingerprint Based Secured Voting," International Conference on Advances in Computing, Communication and Control (ICAC3), Pune, India, 2019, pp. 1–6.

[5] M. Yasmin, S. Sharmila, S. Swathi, S. Sujitha, G. Renuka, and P. Thirisha, "Secure IoT Voting System with Fingerprint Authentication and Real-Time Monitoring," 3rd International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoIC), Kallakurichi, India, 2025, pp. 1430–1435.

[6] G. John Baptist, K. G. Arya, K. Vishnu, and L. R. Silpa Sangeeth, "Fingerprint-Based Vote Marking System for Elector Identification," International Conference on Signal Processing, Computation, Electronics, Power and Telecommunication (IConSCEPT), Palakkad, India, 2023, pp. 1–5.

[7] A. Kaushik, S. N. Gupta, S. Tyagi, A. Sharma, A. Singh, and G. Sagar, "Fingerprint Based Voting System," 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE), Ghaziabad, India, 2023, pp. 51–55.

[8] N. Bhuvaneswary, C. V. Reddy, C. Aravind, and K. H. Prasad, "Smart Voting Machine using Fingerprint Sensor and Face Recognition," International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2022, pp. 1159–1166.

[9] S. J. J. Arputhamoni, "Online Smart Voting System Using Biometrics Based Facial and Fingerprint Detection on Image Processing and CNN," 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 1–5.

[10] B. Kalaimathi, T. Rajasekar, M. Kowsalya, J. M. Pooja, and T. Priya, "Development of Fingerprint Voting Application using Aadhar card," 2nd International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), Coimbatore, India, 2023, pp. 1–6.

[11] S. M. Hasan, A. M. Anis, H. Rahman, J. S. Alam, S. I. Nabil, and M. K. Rhaman, "Development of Electronic Voting Machine with the Inclusion of Near Field Communication ID Cards and Biometric Fingerprint Identifier," 17th International Conference on Computer and Information Technology (ICCIT), Dhaka, Bangladesh, 2014, pp. 1–6.

[12] S. D. Alapati, A. Dabbara, C. Chennamsetty, and M. Arunachalam, "Electronic Voting Machine Using Fingerprint Scanner with Image Enhancement Technique," International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2023, pp. 1–5.