Arduino Nano-powered Fingerprint Voting Machine For Secure and Accessible Elections

***Pinjari Vajid, *Kakhandki Anis, *Vhandale Mahesh, **Halcherikar Ramesh, **Joshi Aashish**

**E&TC Students **Assistant Professor at KIT Shelve.*
Department of Electronics and Telecommunication Engineering,
Babasaheb Ambedkar Technological University Lonere, Maharashtra, India.

[1]*Received: 30 March 2024; Accepted: 28 April 2024; Published: 14 May 2024*

ABSTRACT

An abstract is a concise summary of a paper, providing essential information for readers to understand the study. In this study, our innovative system aims to address the key challenges of traditional voting methods, including security vulnerabilities, logistical complexities, and accessibility barriers. By harnessing the power of biometric authentication through fingerprint recognition, our voting machine ensures the integrity and confidentiality of each vote cast.

The core of our system is built upon the Arduino Nano platform, renowned for its versatility, affordability, and ease of integration. Coupled with state-of-the-art fingerprint sensors, this solution offers a seamless and robust method for voter verification, eliminating the risk of fraudulent or duplicate voting.

Keywords: *Fingerprint; Arduino-nano; secure; Secure Voting.*

INTRODUCTION

- In the landscape of democratic governance, the sanctity of the voting process stands as the cornerstone of legitimacy. However, traditional voting methodologies often grapple with challenges such as identity verification, ballot tampering, and inclusivity. In response to these pressing concerns, we present an innovative solution poised to redefine the electoral paradigm: a fingerprint-based voting machine ingeniously engineered around Arduino Nano microcontrollers and cutting-edge fingerprint sensor technology.

- With each election cycle, the specter of voter fraud looms large, casting doubt on the credibility of electoral outcomes. Existing mechanisms for verifying voter identity, such as photo identification or signature matching, are susceptible to manipulation and exploitation. In contrast, biometric authentication offers a paradigm shift towards a more robust and foolproof verification process. By leveraging the unique physiological characteristics of fingerprints, our voting machine ensures the indisputable identification of voters, mitigating the risk of fraudulent or duplicate voting.

- Central to the efficacy of our solution is the utilization of Arduino Nano, a miniature yet powerful microcontroller renowned for its versatility and scalability. Combined with advanced fingerprint sensors, this compact computing platform forms the backbone of a sophisticated yet accessible voting system. The Arduino Nano's low cost, open-source nature, and extensive community support render it an ideal candidate for democratizing electoral technology, transcending the barriers of resource constraints and technical expertise.

- Moreover, our innovative approach champions inclusivity, striving to extend the franchise to all eligible voters regardless of their physical abilities or technological proficiency. By designing intuitive user interfaces and ergonomic hardware, we aim to dismantle the barriers that impede voter participation,

[1] *How to cite the article:* Vajid P., Anis K., Mahesh V., Ramesh H., Aashish J. (May, 2024); Arduino Nano-powered Fingerprint Voting Machine For Secure and Accessible Elections; *International Journal of Advances in Engineering Research*, May 2024, Vol 27, Issue 5, 16-21

fostering a more equitable and representative democracy.

- As we embark on this transformative journey towards electoral integrity and accessibility, our vision is clear: to forge a path towards fairer, more transparent, and more inclusive elections. By harnessing the synergistic potential of Arduino Nano and fingerprint authentication, we endeavor to safeguard the sanctity of the ballot box and fortify the foundations of democracy for generations to come. We have engineered a groundbreaking fingerprint-based voting machine that eliminates the necessity for voters to carry identification documents. At the polling station, individuals only need to place their finger on the device, enabling instant acquisition of their fingerprint for identification purposes. Our sophisticated fingerprint reader seamlessly extracts data from the fingerprint, which is then transmitted to the control unit for verification.

- The control unit retrieves the data from the reader and cross-references it with the voter information stored during registration. If the fingerprint data matches the pre-existing records, the voter is granted permission to cast their ballot. In the event of a mismatch, an alert message is displayed on the LCD screen, and the individual is prevented from voting. The actual voting process is conducted manually using push buttons, with the LCD providing real-time feedback, including messages, alerts, and voting outcomes.

- This innovative system streamlines the voting process, enhances security, and ensures the integrity of the electoral system, marking a significant leap forward in democratic practices.

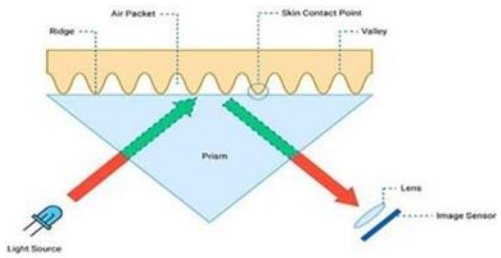

Fig. Optical Fingerprint Scanner Working Principle

BLOCK DIAGRAM

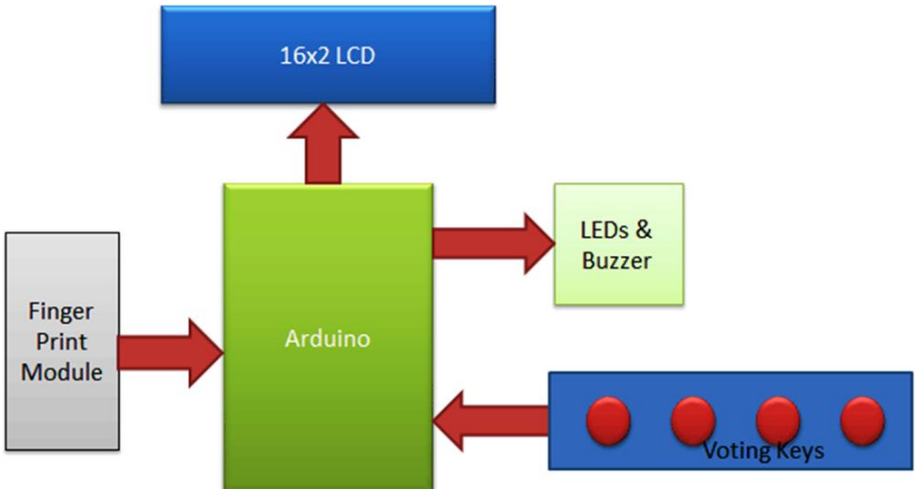

Figure 1. Block Diagram of System.

BLOCK DIAGRAM DESCRIPTION:

FINGERPRINT SENSOR INTERFACING WITH ARDUINO NANO FOR VOTING MACHINE.

1. **Input Module:**
   - Fingerprint Sensor: Captures and processes fingerprint data for voter identification. Interfaces with Arduino Nano

for data transmission and processing.

- **Push Buttons**: Serve as voting keys for manual selection of candidates. Each button corresponds to a specific candidate or voting option.

2. **Processing Unit**:

- **Arduino Nano**: Acts as the central processing unit (CPU) of the system. Receives input signals from the fingerprint sensor and push buttons.
- **Control Logic**: Executes decision-making algorithms for voter authentication and vote counting. Manages the flow of data between input modules and output devices.

3. **Memory Storage**:

- **Internal Memory (EEPROM)**: Stores pre-registered fingerprint data and voter information for comparison during the authentication process. Provides non-volatile storage for critical system data.

4. **Output Module:**

- **LCD Display:** Provides visual feedback to the voter and polling officials. Displays messages, warnings, and voting results in real time.
- **Indicator LEDs**: Illuminate to signify system status, such as successful voter authentication or error conditions.

5. **Power Supply:**

- **Power Source:** Supplies electrical power to all components of the system. May include batteries or external power adapters, depending on the deployment environment.

6. **Communication Interface**:

- **Serial Communication**: Facilitates data exchange between Arduino Nano and peripheral devices, including the fingerprint sensor and LCD. Ensures seamless integration and operation of system components.

SCHEMATIC DIAGRAM

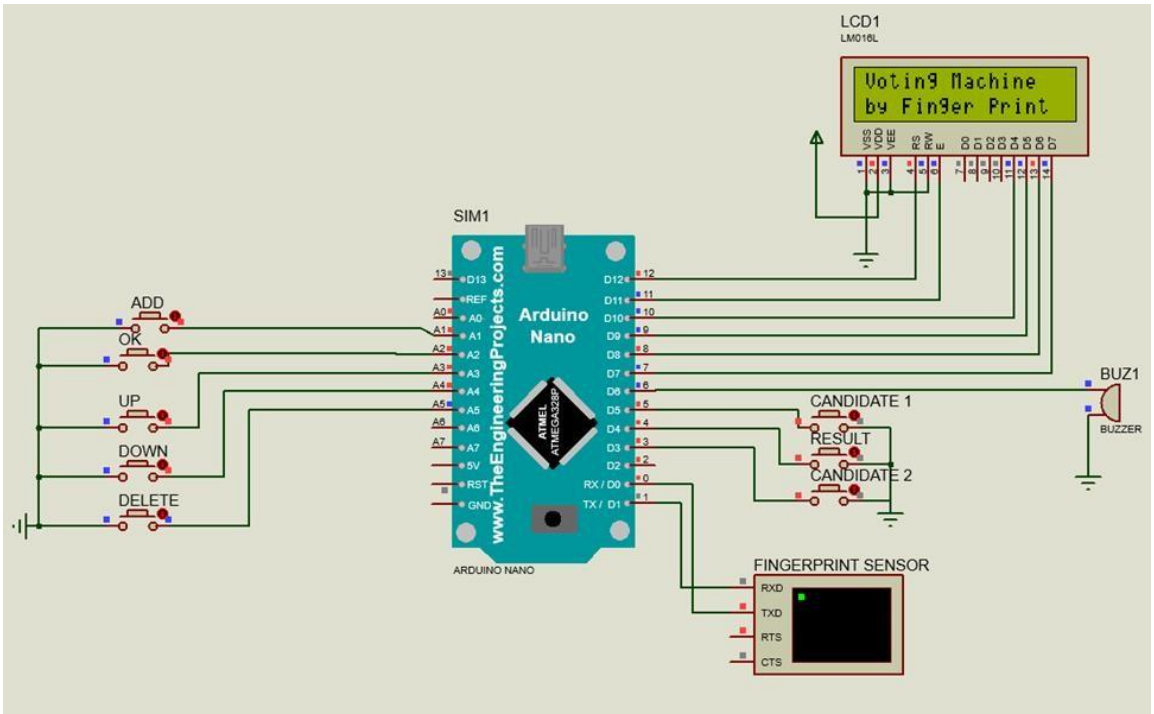

Figure 2. Schematic Diagram

OPERATION OF SCHEMATIC

In our simulated realm, we meticulously replicate the intricate workings of a fingerprint-based voting system using virtual components and advanced software emulation techniques. This simulation endeavor aims not only to unveil the inner workings of the system but also to offer a profound comprehension of its operational dynamics, module interactions, and real-world efficacy.

At the heart of our simulation lies the input module, where we harness the power of virtual fingerprint sensors to emulate the functionality of their physical counterparts. These simulated sensors ingeniously generate synthetic fingerprint data, which serves as the cornerstone of voter authentication. Complementing this, our virtual push buttons, with their seamless mimicry of physical keys, empower users to simulate voting actions with precision and ease, triggering a cascade of events within the system.

Steering our simulation forward is the processing unit, symbolized by an emulated Arduino Nano, a beacon of computational prowess. Here, intricate program logic unfolds, deftly handling inputs from our simulated modules. From fingerprint data processing for authentication to tallying votes triggered by virtual button presses, the Arduino Nano orchestrates a symphony of operations with finesse and accuracy.

Enveloping our system in a veil of digital memory is the virtual EEPROM, a bastion of non-volatile storage prowess. Within its digital confines, critical data, including pre-registered fingerprint templates and voter information, finds sanctuary, ensuring the seamless execution of authentication processes.

As our simulated journey unfolds, the output module comes to life, with a virtual LCD serving as the window to our system's soul. Here, users and officials are greeted with a tapestry of visual feedback, ranging from simulated messages and warnings to the unfolding drama of voting results, all meticulously generated by the processing unit's logic.

Guiding our simulation's narrative are virtual indicator LEDs, beacons of system status that illuminate the digital landscape with their nuanced glow, signaling every twist and turn in the electoral journey.

In this digital realm, a virtual power source fuels our endeavor, ensuring uninterrupted operation akin to its physical counterpart, whether through batteries or external power adapters.

Facilitating seamless communication among our simulated components is the virtual serial communication interface, a conduit of data exchange that mirrors real-world integration protocols, binding our system's diverse elements into a cohesive whole.

Through this immersive simulation, users embark on a voyage of discovery, unraveling the intricate dance of module interactions, validating system behavior across diverse scenarios, and ultimately, honing the efficacy and reliability of our fingerprint-based voting system. This simulation emerges not merely as a testing ground but as a crucible of innovation, refining our system's design and functionality, and paving the way for its seamless integration into the fabric of real-world electoral processes.

FLOWCHART OF SYSTEM

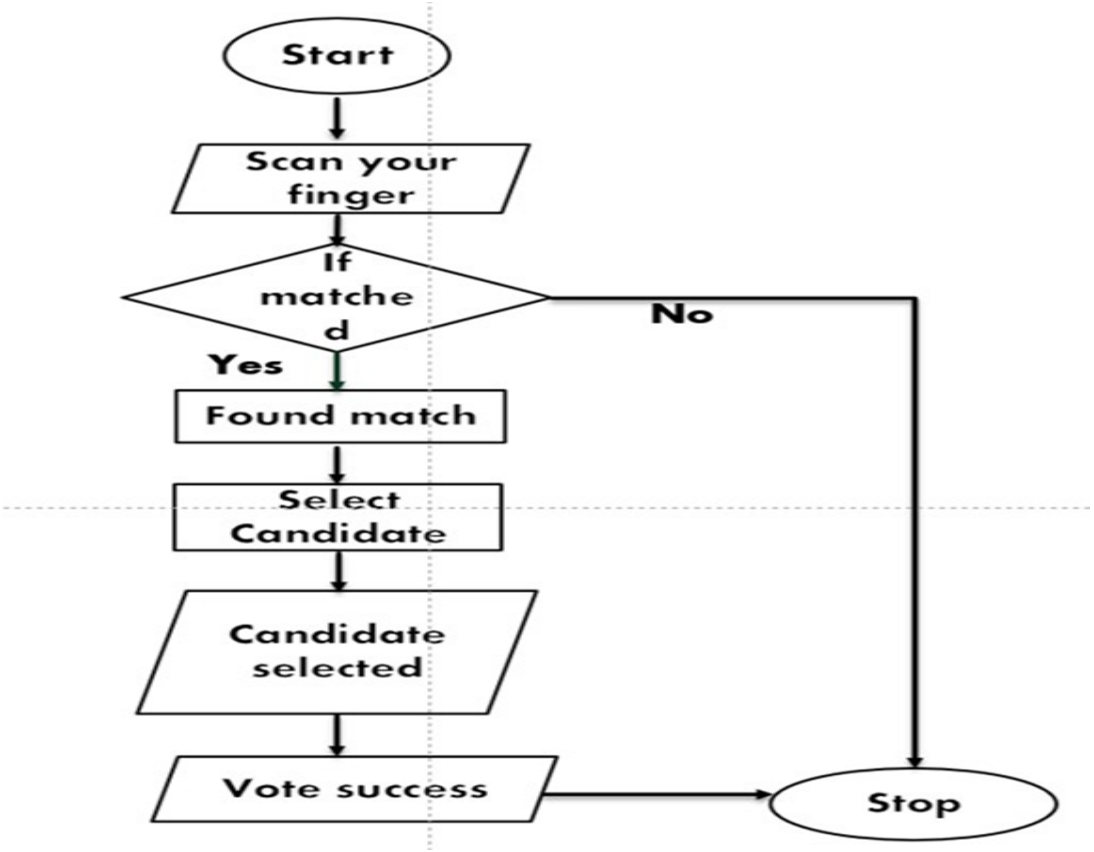

Figure 3. Flowchart of System

Flowchart: Voter Identity Verification Process

1. **Start**: The verification process begins when a voter approaches the voting machine.

2. **Capture Fingerprint**: The voter places their finger on the fingerprint sensor, initiating the capture of their fingerprint data.

3. **Process Fingerprint**: The system processes the captured fingerprint data to extract unique biometric features.

4. **Retrieve Voter Data**: Next, the system retrieves the voter's data from the internal memory storage, including their pre-registered fingerprint template and voter information.

5. **Compare Fingerprint Data:** The system compares the processed fingerprint data with the pre-registered fingerprint template stored in the memory.

6. **Verification Decision:** If the processed fingerprint data matches the pre-registered template, the voter's identity is verified, and the process proceeds to the next step. If there's no match, the voter's identity cannot be verified, and an error message is displayed.

7. **Display Verification Result:** The system displays the verification result on the LCD. If the voter's identity is successfully verified, a message indicating "Identity Verified" is shown. If verification fails, a message indicating "Identity Not Verified" is displayed.

8. **Proceed to Voting**: If the voter's identity is successfully verified, they are allowed to proceed to the voting stage. If verification fails, the voter is not permitted to cast their vote, and further action may be taken as per the electoral procedures.

9. **End:** The verification process ends, and the voter either proceeds to cast their vote or exits the voting process

based on the verification result.
This flowchart outlines the sequential steps involved in verifying a voter's identity using their fingerprint in the voting system. It ensures a systematic and transparent process, contributing to the integrity and efficiency of the electoral process.

ACKNOWLEDGMENT

We extend our heartfelt appreciation to all individuals who contributed to the realization of this fingerprint-based voting system project. Our gratitude goes out to the dedicated team members who tirelessly collaborated on various aspects of system design, development, and testing. Special thanks to our project advisors for their invaluable guidance, insightful feedback, and unwavering support throughout the journey. Additionally, we express our gratitude to the academic institutions and research facilities that provided resources and facilities essential for the project's success. Lastly, we extend our sincere appreciation to the participants and volunteers who generously shared their time, expertise, and feedback, contributing to the refinement and validation of our system. This project owes its success to the dedication and collaboration of all involved parties, and for that, we are deeply thankful.

REFERENCES

1. Amir Nur Iman Bin Mohd Zaid2, Mohammed Hazim Alkawaz3 1,2,3Faculty of Information Sciences and Engineering, Management & Science University, Malaysia. 1School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON, K1N 6N5, Canada. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 15, Number 1, 2020 (Special Issue) © Research India Publications. http://www.ripublication.com
2. SHILPA C VENUGOPAL1 , RESMI K. RAJAN, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 IJERTV4IS050948 www.ijert.org (This work is licensed under a Creative Commons Attribution 4.0 International License.) Vol. 4 Issue 05, May-2015.
3. SHILPA C VENUGOPAL1 , RESMI K. RAJAN, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 15, Number 1, 2020 (Special Issue) © Research India Publications. http://www.ripublication.com
4. National Conference on Information, Communication and Energy Systems and Technologies - 2019 © 2019 IJSRSET | Volume 5 | Issue 7 | Print ISSN: 2395-1990 |Online ISSN: 2394-4099