iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

FINGERPRINT BASED BIOMETRIC VOTING MACHINE USING ARDUINO

Mrs. Shobha Hugar,
Associate Professor, Department of Electronics & Communication Engineering,
Sapthagiri College of Engineering, Bengaluru, Karnataka, India

Abhishek S K,
Ashrith M L, B S Nandan Kishore,
Students, Department of Artificial Intelligence and Machine Learning,
Sapthagiri College of Engineering, Bengaluru, Karnataka, India

[1] shobhahugar@sapthagiri.edu.in [2] abhisheksk5656@gmail.com [3] ashrithmlsapthagiricollege@gmail.com
[4] bsnandankishore@gmail.com

ABSTRACT
The implementation of a fingerprint-based biometric voting machine utilizing Arduino enhances the security and reliability of electoral processes. By integrating a fingerprint sensor with an Arduino microcontroller, the system provides an effective mechanism for voter authentication. In the Traditional voting methods, we often face challenges such as identity fraud and multiple voting, whereas this biometric approach will ensure that only registered individuals can cast their votes. This system captures and stores the biometric data of authorized voters in a secure database. During the voting process, individuals authenticate themselves by placing their fingers on the sensor, which compares their fingerprints with stored templates. If a match is confirmed, access to the voting interface is granted; otherwise, the user is denied entry, preventing fraudulent voting attempts. The Arduino unit facilitates fingerprint recognition, data handling, and interaction with a display that presents voting options. The voting results are stored securely and can be retrieved for verification, ensuring transparency and accuracy. This system significantly enhances security, minimizes human errors, and bolsters confidence in the democratic process. By integrating fingerprint recognition technology, this voting system offers a dependable, efficient, and cost-effective solution for secure elections.

1. INTRODUCTION

A fingerprint-based biometric voting machine presents a modernized approach to election security and efficiency. Traditional voting mechanisms are susceptible to identity fraud, multiple voting attempts, and human error. Implementing biometric verification through fingerprint recognition eliminates these vulnerabilities by ensuring that each vote is associated with a unique and authenticated individual. This system is built around an Arduino microcontroller, which serves as a flexible and cost-effective platform for the project. The fingerprint sensor captures biometric data, verifies voter identity, and authorizes voting access only to registered individuals. Since fingerprints are unique to each person, the system ensures an accurate and tamper-resistant voting process. The primary components of the system include a fingerprint sensor, Arduino board, and a display unit (LCD or LED). The fingerprint sensor extracts and converts fingerprint patterns into a digital template. These templates are matched with stored data to verify voter identity before granting access to cast a vote. This biometric approach eliminates the need for paper-based ballots, reduces errors, and accelerates the voting process. By preventing fraudulent voting, improving authentication, and streamlining electoral procedures, this system represents a substantial advancement in electoral technology. The future may see broader adoption of such biometric systems to further enhance election security and efficiency.

2. LITERATURE SURVEY

To replace traditional voting methods such as ballot papers, Electronic Voting Machines (EVMs) were introduced in India in 1998 [4]. These machines consist of a control unit and a balloting unit, making them more

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

secure but also increasing complexity. Various improvements and advancements have been made over the years [9] to enhance their efficiency and security.

• **Ballot Voting:** This voting method involves the use of paper ballots, where voters manually write the name of their chosen candidate. These ballots are then placed into a designated ballot box for collection. However, this process can be time-consuming and prone to human errors in counting.

• **VVPAT (Voter Verifiable Paper Audit Trail):** VVPAT serves as an independent verification system designed to ensure election transparency as it will allow voters to ensure that the votes has been accurately recorded. This technology has been implemented alongside electronic voting machines, particularly during the 2019 elections in India.

• **Electronic Voting Machine (EVM):** Electronic voting was introduced in India between 1998 and 2001 to replace the traditional paper ballot system. Prior to its adoption, elections relied on paper ballots, which were vulnerable to fraudulent activities. The introduction of EVMs improved the security and efficiency of the voting process by reducing manual errors and streamlining vote counting.

• **Remote Internet Voting:** This voting method enables individuals to cast their votes via the internet from any location with online access. By leveraging internet-based technology, remote voting increases voter participation and convenience. However, its effectiveness depends on reliable internet connectivity and cybersecurity measures to prevent unauthorized access [5].

3.METHODOLOGY

The fingerprint-based biometric voting system operates in two main phases: voter registration and the actual voting process. During the registration phase, each user must enroll their fingerprint in the system. Block diagram can be observed in. This is initiated by pressing the ENROLL key, after which the LCD screen prompts the user to input a location ID where the fingerprint will get stored in the Arduino's memory. Navigation through the IDs is done using the UP/DOWN buttons, and the selection is confirmed with the OK button. Once the ID is selected, the fingerprint sensor requests the user to place the finger on the sensor. To ensure accurate identification, the system asks the user to remove and put their finger again. During this process, the fingerprint sensor captures an image of the fingerprint, processes it into a recognizable format, and saves it under the assigned ID in the memory. After successful registration, the voter is authenticated and eligible to cast a vote. This process must be completed for all users before they can participate in the voting process.

A stored ID can be removed by selecting it and pressing the DEL key. Once deleted, the LCD screen will confirm the deletion by displaying the corresponding ID number. Each system operates independently, meaning that the data is stored locally within a single unit. There is no interconnection between multiple systems, ensuring that each operates in isolation. This design enhances security by preventing unauthorized access and reducing the risk of hacking.

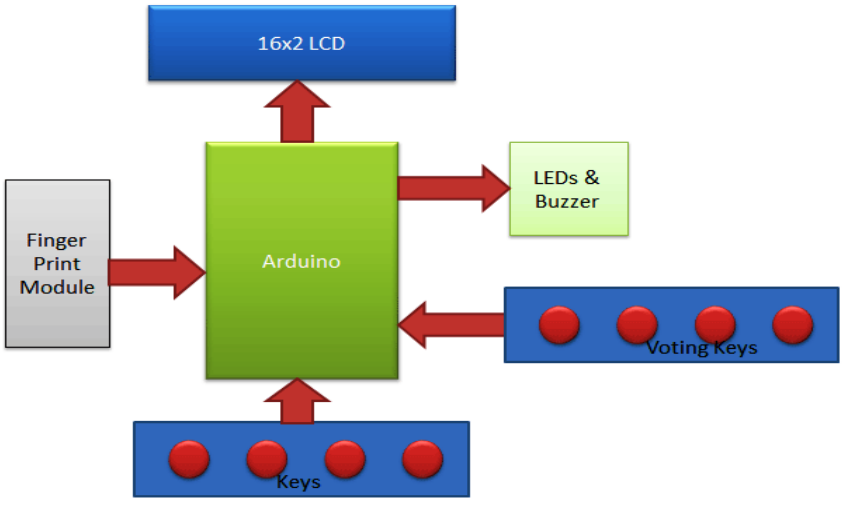

Figure 3.1 Block Diagram

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

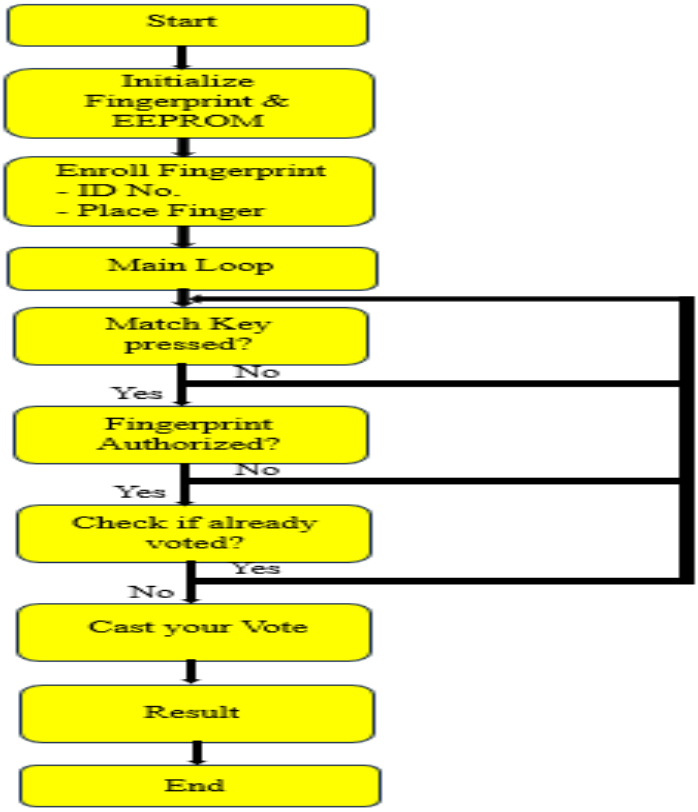

Figure 3.2 Flowchart

Step 1: Start
• This is the beginning point of the process. It signifies that the system is ready to begin the fingerprint-based voting process.

Step 2: Initialize Fingerprint & EEPROM
• Fingerprint Sensor Initialization: The fingerprint sensor is activated and prepared to scan fingerprints. EEPROM Initialization: EEPROM (Electrically Erasable Programmable Read-Only Memory) is initialized to store and retrieve fingerprint data and voting records.

Step 3: Enroll Fingerprint
• Assign ID Number: Each user is assigned a unique ID number to differentiate their fingerprints.
• Fingerprint Scanning: The user places their finger on the sensor to enroll their fingerprint. The system captures the fingerprint data and stores it in the EEPROM with the associated ID number.

Step 4: Main Loop
• The system enters the main operational loop, where it continuously checks for user inputs and processes them accordingly.

Step 5: Match Key Pressed
• Yes: If the match key is pressed, the system proceeds to the next step to verify the fingerprint.
• No: If the match key is not pressed, the system remains in the main loop, waiting for the user to press the key.

Step 6: Fingerprint Authorized
• Yes: If the fingerprint is authorized (matched with the enrolled fingerprints), the system proceeds to check if the user has already voted.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

• No: If the fingerprint is not authorized, the system returns to the main loop, waiting for a valid fingerprint.

Step 7: Check if Already Voted
• Yes: If the user has already voted, the system returns to the main loop and prevents duplicate voting.
• No: If the user has not voted, the system allows the user to proceed to cast their vote.

Step 8: Cast Your Vote
• The user is prompted to cast their vote. This may involve selecting a candidate or option on a voting interface.

Step 9: Result
• The system processes the vote and updates the voting records. The result of the voting process is displayed to the user, confirming that their vote has been successfully recorded.

Step 10: End
• This signifies the end and the final step of the voting process for the user. The system is ready to process the next user in the main loop.

4. APPLICATIONS

The Electronic Voting Machine (EVM) with Fingerprint Authentication has a wide range of applications, particularly in enhancing the integrity and efficiency of the electoral process. The primary application of this system lies in government elections at the national, state, or local levels. By integrating fingerprint authentication, the machine ensures that only registered voters can cast their vote. This minimizes the chances of impersonation, multiple voting, and bogus entries, which are common issues in traditional voting systems. In educational institutions, such as schools and universities, this system can be used for student council elections. It offers a secure and efficient method for conducting fair polls without the need for manual counting or supervision, thereby reducing human errors and saving time. The EVM can also be adopted by corporate organizations, societies, and unions for internal decision-making processes or board member elections. Its use eliminates the need for paper ballots, thus reducing administrative costs and environmental impact. Another key application is in community-level voting, such as housing societies, clubs, and local associations, where trust and transparency are crucial. Since the system is easy to operate and compact, it can be deployed in remote and rural areas where traditional electoral infrastructure might be lacking. Furthermore, the fingerprint-based EVM can be used for surveys and polls where authentic participation is important, such as opinion polls, policy feedback from registered members, or even in talent competitions where fairness is a priority. Overall, the fingerprint-enabled EVM boosts electoral credibility, ensures voter authentication, promotes eco-friendliness by avoiding paper usage, and enhances voting accessibility for people of all ages, including the illiterate population, since no written input is required.

5.CONCLUSION

The hardware implementation of the Electronic Voting Machine (EVM) effectively integrates a fingerprint sensor and an Arduino microcontroller to ensure secure and reliable voting. The LCD display presents real-time vote counts, enhancing transparency in the process. This system introduces an innovative and secure approach to electronic voting, reducing the risk of fraudulent activities.
Designed primarily for small-scale applications such as institutions and organizations, this biometric voting machine demonstrates the effectiveness of fingerprint authentication in electoral systems. The successful implementation highlights the potential of biometric technology in ensuring secure and efficient voting processes.

REFERENCES

1) V. Kiruthika Priya, V. Vimaladevi, B. Pandimeenal, T. Dhivya, “Arduino based smart electronic voting machine”, 2017 International Conference on Trends in Electronics and Informatics (ICEI) Year: 2017, conference Paper, Publisher: IEEE.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

2) Rahil Rezwan, Huzaifa Ahmed, M. R. N. Biplo, S. M. Shuvo, Md. Abdur Rahman, "Biometrically secured electronic voting machine", 2017 IEEE Region 10 Humanitarian Technology Conference (R10- HTC).
3) Prof. Sunita Patil, Amish Bansal, Utkarsha Raina, Vaibhavi Pujari, Raushan Kumar, "E-Smart Voting Machine with Secure Data Identification Using Cryptography", 2018 Publisher: IEEE
4) Annalisa Franco, "Fingerprint: Technologies and Algorithms for Biometrics Applications", Year: 2011, Course, Publisher: IEEE.
5) A. Piratheepan, S. Sasikaran, P. Thanushkanth, S. Tharsika, M. Nathiya, C. Sivakaran, N. Thiruchchelvan and K. Thiruthanigesan, "Fingerprint Voting System Using Arduino", College of Technology Jaffna, Sri Lanka University College of Anuradhapura, University of Vocational Technology, Sri Lanka
6) Rohan Patel, Vaibhav Ghorpade, Vinay Jain and Mansi Kambli, "Fingerprint Based e-Voting System using Aadhar Database", 2015.
7) S Wolchok, E Wustrow, JA Halderman. "Security analysis of India's electronic voting machines" 2010.
8) Qijun Zhao, Lei Zhang, David Zhang, and Nan Luo, "Adaptive Pore Model for Fingerprint Pore Extraction", IEEE, 978-1-4244-2175 - 6/08.
9) Md. Mahboob Karim, Nabila Shahnaz Khan, Ashratuz Zavin, Shusmoy Kundu, Asibul Islam, Brazab Nayak, "A proposed framework for biometric electronic voting system", IEEE International conference on 2017
10) Soumyajit Chakraborty, Siddhartha Mukherjee, Bhaswati Sadhukhan, Kazi Tanvi Yasmin,"Biometric Voting System using Adhar Card in India" 2016
11) https://www.arduino.cc/en/main/software.
12) https://learn.adafruit.com/adafruit-all-about-arduino-libraries-install- use/arduino-libraries.