International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 14, Issue 11, November 2025)

Biometric EVM System

Aman Kumar[1], Aryan Raj[2], Shubh Dwivedi[3], Abhishek Baghel[4], Dr. Mayur Shukla[5]

[1, 2, 3, 4]*Students,* [5]*Associate Professor, Department of Electronics and Communication Engineering, Lakshmi Narain College of Technology Excellence, Bhopal (M.P.), India*

***Abstract*--The Biometric Electronic Voting Machine (EVM) is a secure, technology-driven system designed to ensure accurate voter authentication and fair election processes. The system replaces traditional manual identification with biometric verification such as fingerprint or facial recognition, ensuring that only eligible voters can cast their votes and that each voter votes only once.**

The system consists of three major components: voter authentication module, ballot casting unit, and vote storage/counting module. When a voter arrives, their biometric data is scanned and matched with pre-registered voter records stored securely in a database. If the biometric match is successful, the voting panel is activated, allowing the voter to select their preferred candidate. Once a vote is cast, it is encrypted and stored in the system to prevent tampering. The system also updates the status of the voter to prevent re-voting.

This biometric EVM enhances security, eliminates identity fraud, reduces human intervention, and ensures transparency in the voting process. It provides faster authentication, accurate vote counting, and reliable results, making it suitable for modern election management.

***Keywords*--EVM, Arduino and Image Processing.**

I. INTRODUCTION

Elections are a crucial part of any democratic system, and ensuring the integrity, security, and accuracy of the voting process is essential for fair governance. Traditional voting systems, whether paper-based ballots or standard Electronic Voting Machines (EVMs), often face challenges such as voter impersonation, multiple voting, human error, and delays in result processing. To overcome these issues, modern technologies like biometrics are being integrated into election systems to enhance reliability and transparency.

A Biometric Electronic Voting Machine (EVM) is an advanced voting system that uses biometric authentication—such as fingerprints or facial recognition—to verify the identity of voters before allowing them to cast their votes. By linking each voter's biometric data with a secure database, the system ensures that only valid and registered voters participate, and each individual can vote only once.

This paper focuses on designing and implementing a biometric-enabled EVM that simplifies the election process, minimizes fraud, reduces manual intervention, and provides quick and accurate vote counting.

By combining biometric technology with digital vote recording, the system improves the overall efficiency and trustworthiness of elections, making it a promising solution for future voting systems.

II. LITERATURE SURVEY

1. DA Kumar, TUS Begum:- In this study, the authors are interested in designing and analysing the Electronic Voting System based on the fingerprint minutiae which is the core in current modern approach for fingerprint analysis. The new design is analysed by conducting pilot election among a class of students for selecting their representative. Various analysis predicted shows that the proposed electronic voting system resolves many issues of the current system with the help of biometric technology.

2. BB Bederson, B Lee :- These systems offer the promise of faster and more accurate voting, but the current usability and systemic problems. This paper surveys issues relating to usability of electronic voting.

3.Md. Asfaqul Alam,Md. Maminul Islam, Md. Nazmul Hassan, Md. Sharif Uddin Azad:- Electronic voting machine has already been developed and widely used in many developed countries. But most of them use Radio Frequency ID. In developing countries RFID for each person does not exist. And using RFID is still a costly solution. Some of the developing countries use image processing technique to detect citizens. But only image processing is not enough. Keeping these problems in mind this paper a raspberry pi will be used as host. The Raspberry Pi is a credit card sized single computer or SoC uses ARM1176JZF-S core

4. M. Venkateswarluand Y. V. V. Kumar:- Biometric system based electronic voting machine with security algorithm and password protection on ARM micro controller and GSM.

5. Sivaganesan, D.:- Utilization of smart applications in various domains is facilitated pervasively by sensor nodes (SN) that are connected in a wireless manner and a number of smart things. Hazards due to internal and external attacks exist along with the advantages of the smart things and its applications. Security measures are influenced by three main factors namely scalability, latency and network lifespan, without which mitigation of internal attacks is a challenge.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 14, Issue 11, November 2025)

The deployment of SN based Internet of things (IoT) is decentralized in nature. However, centralized solutions and security measures are provided by most researchers. A data driven trust mechanism based on blockchain is presented in this paper as a decentralized and energy efficient solution for detection of internal attacks in IoT powered SNs. In grey and black hole attack settings, the message overhead is improved using the proposed model when compared to the existing solutions. In both grey and black hole attacks, the time taken for detection of malicious nodes is also reduced considerably. The network lifetime is improved significantly due to the enhancement of these factors.

III. METHODOLOGY

The Biometric Electronic Voting Machine (EVM) is designed to ensure secure, transparent, and tamper-proof voting by verifying the identity of each voter using biometric authentication. The system combines fingerprint recognition technology with a microcontroller-based voting mechanism to prevent fake voting and multiple votes by the same person.

1. Voter Registration Phase

Before the election, every voter's fingerprint and details (such as name, voter ID, etc.) are stored in the system database.This registration ensures accurate identification during the voting process.

2. Authentication Phase

When a voter approaches the EVM:

Step 1: Fingerprint Scanning

The voter places their finger on the fingerprint sensor.

The sensor captures the fingerprint image and converts it into a digital template.

Step 2: Fingerprint Matching

The fingerprint module compares the captured print with the pre-stored templates.

If the fingerprint matches, the voter is authenticated.

If not, the system denies access and displays an "Authentication Failed" message.

3. Voting Phase

Once the voter is successfully authenticated:

Step 1: Display of Candidates

The list of candidates appears on the LCD or LED display.

Each candidate is assigned a unique button or option number.

Step 2: Casting the Vote

The voter presses the button corresponding to their chosen candidate.

The micro-controller registers the vote securely in its memory.

Step 3: Vote Confirmation

The system shows a confirmation message on the display such as "Vote Successfully Registered".

A buzzer can beep to indicate successful vote recording.

4. Anti-Double Voting Mechanism

The system marks the voter's fingerprint as "voted" in the database.

If the same voter tries to vote again:

The sensor identifies the fingerprint.

The system rejects the attempt with a message like "Already Voted".

This prevents duplicate or fraudulent votes.

5. Secure Storage of Votes

All votes are stored in the microcontroller memory (EEPROM or SD card).

Each candidate has a separate counter.

Votes are stored in a tamper-proof manner and cannot be altered by users.

6. Result Calculation Phase

Once the voting session ends:

Step 1: Result Command

The admin enters a secure password.

The micro-controller displays the total votes received by each candidate.

Step 2: Display of Final Results.

Table 1
Component Detail

S.No	Component Name	Quantity
1	Arduino Nano	1
2	Push button	8
3	Variable resistance	1
4	Burzzer	1
5	16*2 LCD Display	1
6	R-307 fingerprint sensor	1
7	Power supply 5v	1
8	Zero PCB	1

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 14, Issue 11, November 2025)

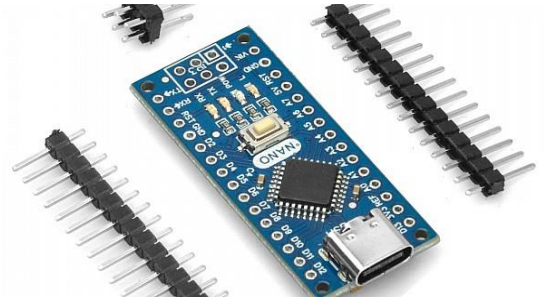

Fig. 1- Arduino Nano

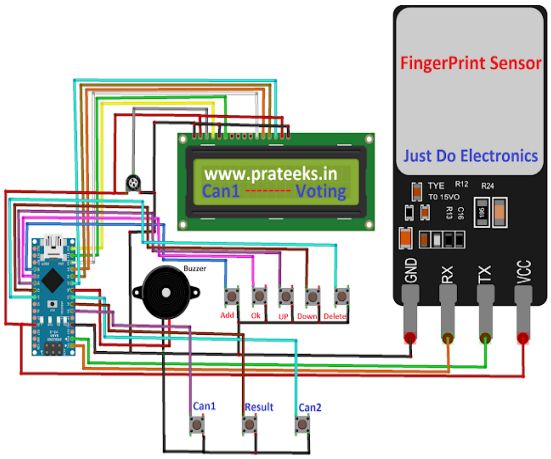

Fig. 2- Circuit Diagram

IV. Working Principle

System Overview: The system uses an Arduino board as the main controller along with a fingerprint sensor module, an LCD display, push buttons, LEDs, and a buzzer. The Arduino communicates with the fingerprint sensor module to verify the identity of the voters.

Enrollment Process: Before the voting process begins, voters need to enrol their fingerprints. The Fingerprints are to be stored in the EEPROM memory.

Voting Process: Once the enrollment is complete, the voting process can begin. Voters place their fingers on the fingerprint sensor, and the system verifies their identity by matching the captured fingerprint with the stored fingerprints in the EEPROM.

Security and Authentication: The fingerprint sensor provides a high level of security and authentication, as each person's fingerprint is unique.

Vote Counting: The system keeps track of the votes by updating the vote count in the EEPROM. The LCD display shows the current vote counts for each candidate.

System Reset: The system includes a reset functionality that allows all stored fingerprints and vote counts to be cleared, providing a fresh start for a new voting session.

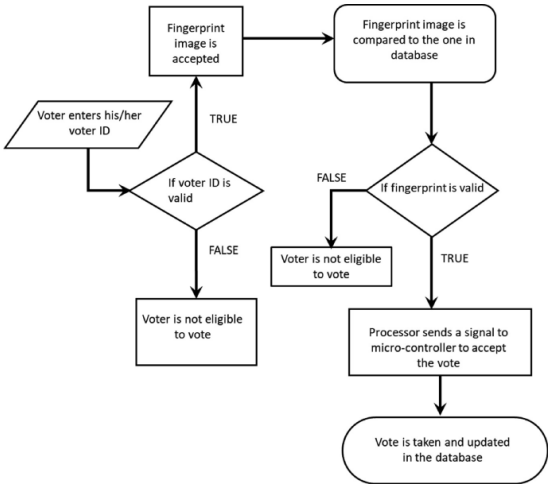

Fig.-3 Designed Model

V. Results

Improved security and fraud reduction: The project can demonstrate a significant reduction in voter impersonation and illegal multiple voting by using unique biometric identifiers.

Enhanced efficiency: Real-time biometric verification speeds up the voting process, reduces long queues, and automates vote counting for quicker, more accurate results.

Increased transparency and integrity: A secure, tamper-resistant system helps build public trust by ensuring that every vote is cast by an eligible, authenticated voter.

Experimental validation: Project results are often confirmed through testing, such as a proof-of-concept for an organization or university, verifying the system's effectiveness and accuracy.

VI. Conclusion

The Biometric Electronic Voting Machine (EVM) system demonstrates a modern, secure, and highly reliable approach to conducting elections. By integrating biometric authentication with traditional electronic voting, the project successfully eliminates risks like voter impersonation, bogus voting, and multiple voting attempts. The system ensures that only valid and verified voters can cast their vote, making the entire process more transparent and trustworthy.

This project not only enhances security but also improves speed, accuracy, and efficiency in vote recording and counting. By minimizing human intervention and automating identity verification, it significantly reduces operational errors. The prototype highlights how emerging technologies—such as fingerprint sensors, microcontrollers, and digital storage—can be leveraged to strengthen democratic systems.

Overall, the Biometric EVM system stands as a promising, future-ready solution that can pave the way for safer, smarter, and more credible elections.

REFERENCES

[1] Ashok Kumar D., Ummal Sariba Begum T., "A Novel design of Electronic Voting System Using Fingerprint ", *International Journal of Innovative Technology Creative Engineering* (ISSN: 2045-8711), Vol. 1, No. 1. pp: 12 - 19, January 2011.

[2] Benjamin B., Bederson, Bong shin Lee. Robert M. Sherman. Paul S., Herrnson, Richard G. Niemi. "Electronic Voting System Usability Issues ", In Proceedings of the SIGCHI conference on Human factors in computing systems, 2003.

[3] Md. Asfaqul Alam, Md. Maminul Islam, Md. Nazmul Hassan, Md. Sharif Uddin Azad (2014), "Raspberry Pi and image processing based Electronic Voting Machine (EVM) ", *International Journal of Scientific Engineering Research*, Vol. 5, Issue 1, pp. 1506 – 1510.

[4] M. Venkateswarluand Y. V. V. Kumar (2014), "Biometric System Based Electronic Voting Machine with security algorithm and password protection on ARM Micro-controller and GSM," *International Journal of Science Engineering and Advance Technology*, vol. 2, no. 7, pp. 197 - 200.

[5] Sivaganesan, D. "A Data Driven Trust Mechanism Based on Blockchain in IoT Sensor Networks for Detection and Mitigation of Attacks." *Journal of trends in Computer Science and Smart technology (TCSST)* 3, no. 01 (2021): 59 - 69.

[6] Smys, S., and Wang Haoxiang. "Data Elimination on Repetition using a Blockchain based Cyber Threat Intelligence." *IRO Journal on Sustainable Wireless Systems* 2, no. 4 (2021): 149 - 154.

[7] M. R. Prasad, P. Bojja and M. Nakirekanti (2016), "AADHAR based Electronic Voting Machine using Arduino," *International Journal of Computer Applications*, vol. 145, no. 12, pp. 39 - 42.