Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 5, May : 2023

BIOMETRIC BASED ELECTRONIC VOTING MACHINE (EVM)

Priyanshi Jhalani, Student, Dept. Of Electronics and Communication Engineering, ABES Engineering College, D.R. A.P.J Abdul Kalam Technical University.
Muskan Bharadwaj, Student, Dept. Of Electronics and Communication Engineering, ABES Engineering College, D.R. A.P.J Abdul Kalam Technical University.
Pavni Sharma, Student, Dept. Of Electronics and Communication Engineering, ABES Engineering College, D.R. A.P.J Abdul Kalam Technical University.
Ms. Shilpa Srivastava, Assistant Professor, Dept. Of Electronics and Communication Engineering, ABES Engineering College, D.R. A.P.J Abdul Kalam Technical University.

Abstract
This paper presents the design of a biometric voting machine that uses a fingerprint scanner and an Arduino microcontroller. The system requires the individual to register their fingerprint with the machine, which is centrally stored in the Arduino's memory.When the voter wants to cast a vote, they place their finger on the fingerprint module. If the fingerprint matches the stored data, the voter can cast their vote and the LCD display confirms the selected candidate's name. The device has a simple hardware design, is easily transportable to polling centers reduces the need for polling staff, and provides easy and accurate vote counting.
Keywords: biometric, LCD, EVM, fingerprint, keys.

I. Introduction

We have developed a two-tier verification system to ensure that only authorized users can cast their vote. The first step involves verifying the user's identity using a government-issued identification card such as Aadhar or voter ID. To implement this step, we plan to create an identification card that utilizes an RFID tag. This tag can be verified using an RFID reader, ensuring that the user's identity is accurate.

The second step in our verification process involves the use of biometric data. Specifically, we will be using fingerprints to verify the identity of the user. Fingerprints have been used as a form of identification for centuries and are considered a reliable way of verifying a person's identity.

By combining these two verification steps, we can provide a robust authentication system that ensures only authorized users can cast their vote. This is critical to maintaining the integrity of the voting system and preventing fraud.

To ensure that our system is secure and reliable, we will be using state-of-the-art technology and working closely with experts in the field of cybersecurity. We believe that our two-tier verification system is a significant step towards ensuring the security and accuracy of the voting process. Our goal is to create a system that is accessible, reliable, and trustworthy, ensuring that every vote counts.

II. Objective

The objective of our system is to address the issue of fake voting that has been a major controversy during elections in India. This problem is mainly caused by the low polling percentage, which can lead to people casting fake votes. To overcome this problem, we have designed a two-tier security system for each vote.

Our system is designed to ensure that each voter is verified using a unique ID verification and biometric verification. This will ensure that only authorized voters can cast their votes. Our system will check whether the data from both verifications match. If they do not match, the system will turn on a buzzer to indicate that the user data does not match.

By implementing this two-tier security system, we aim to prevent fake voting and ensure that every vote is counted accurately. This will help to maintain the integrity of the electoral process and ensure

that the voice of every citizen is heard. We believe that our system will provide a reliable and secure way for citizens to exercise their right to vote without fear of fraud or manipulation.

III. Literature

In the literature survey, we found four papers related to electronic voting systems. The first paper introduced an Electronic Smart Voting System (ESVS) with secured data identification using cryptography in 2018. The authors, Sunita Patil, Amish Bansal, and Utkarsh Raina, described the function of ESVS, which used biometric authentication and OTP-based verification processes. The system utilized Aadhar numbers and voter identification for verification.

The second paper introduced a location-free voting system using IoT technology in 2018. The authors, Qasim Abbas, Tariq Ali, and Hussnain Abbas, highlighted the potential of IoT technology to enable voters to vote from any location worldwide, without restrictions, while maintaining privacy and security.

The third paper introduced an application for an online voting system using an Android device in 2018. The author, Himanshu Vinod Purandare, argued that elections are crucial for deciding the future of the country. The system was designed with high-level security, but the existing system had flaws, such as long wait times in queues for casting votes and weaker security measures.

The fourth paper, Design of Secured E-voting System, was introduced in 2013 by the author Hanady Hussien. The paper addressed the challenge of security in an E-voting system that can be spread widely. The system utilized RFID technology to store all conditions that complied with government rules for checking voter eligibility.

In summary, the literature survey revealed various electronic voting systems that have been proposed in recent years, each with unique features and challenges. Our two-tier security system builds upon these existing systems to provide a reliable and secure way for citizens to exercise their right to vote without fear of fraud or manipulation.

IV. Proposed System

We have implemented a two-tier verification system for user authentication. The first step involves verifying the user's government-issued identity card, such as Aadhar or voter ID, using an RFID tag that is read by an RFID reader. The second step involves verifying the user's biometric information, specifically their fingerprints, which have been used for identification purposes for centuries. By combining these two steps, we have developed an authentication system that ensures only verified users are allowed to cast their votes.

V. Working Principle

The two-tier verification system comprises of two processes- RFID verification and fingerprint verification. In the first process, a unique RFID tag containing the user's data is assigned to each individual, which can be verified only by an RFID reader. The reader compares the data on the tag with the information provided by the user to the officer. In the second process, the user's fingerprint data is stored in the system or fingerprint sensor R305. The fingerprint data can be accessed from Aadhar data by the Government of India. The IOT verifies the RFID data with the fingerprint data, and if they match, the appropriate user is allowed to proceed. If not, the buzzer turns on to indicate a

mismatch. This entire process takes only 2-3 minutes, making it a quick and efficient two-tier verification system.

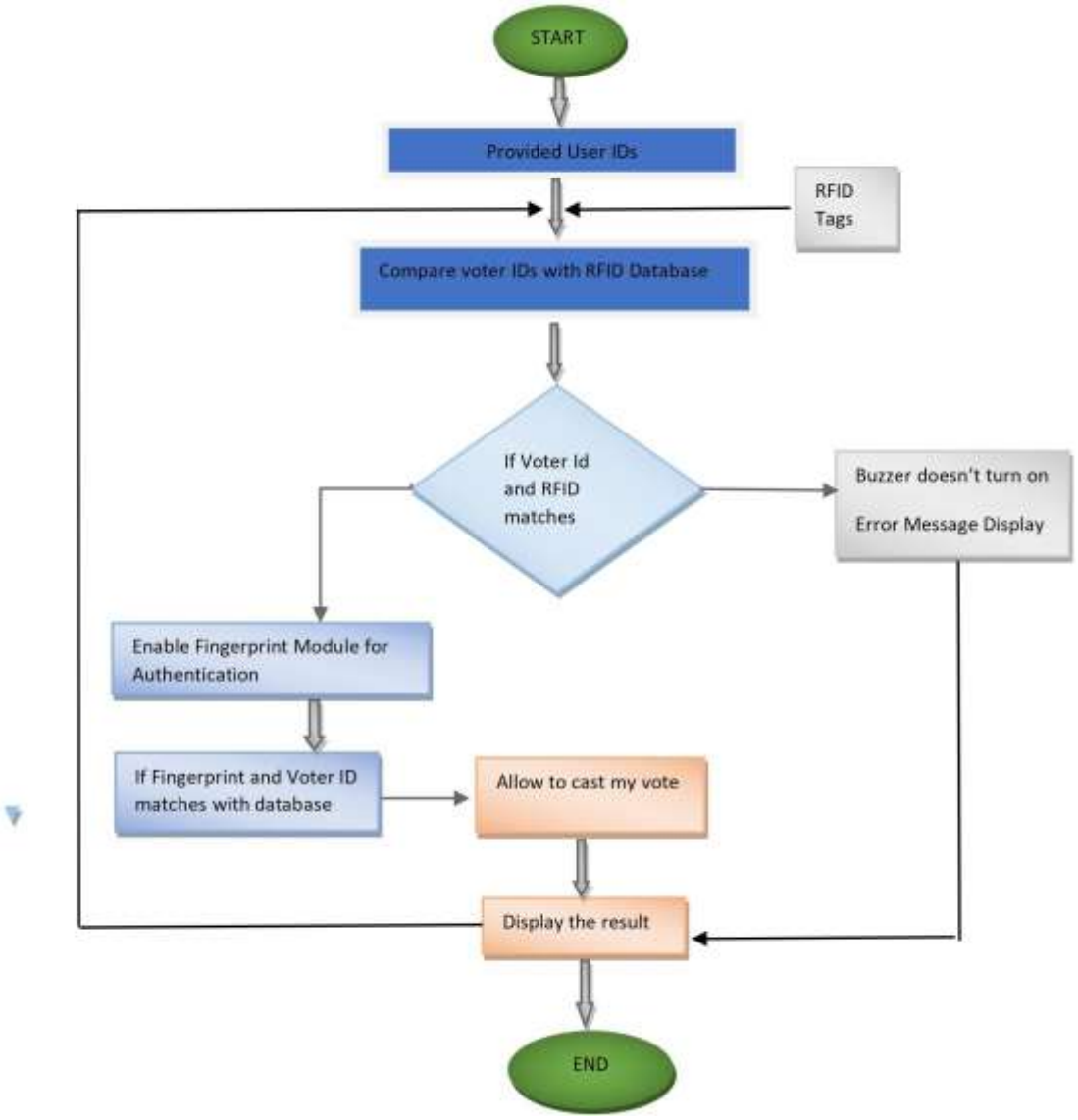

Figure 1: Flowchart

5.1 Algorithm

1. Begin
2. Collect voter information using RFID tag
3. Scan the RFID tag using RFID reader
4. Place finger on fingerprint sensor (R305)
5. Verify fingerprint data with Aadhar data
6. Display result on 16*2 LCD display
7. Upload program code to Arduino Uno
8. If fingerprint matches, authenticate user to vote
9. If fingerprint does not match, turn ON buzzer and deny voting
10. Use IOT to monitor authentication status and count votes
11. Display unauthenticated user on LCD display

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 5, May : 2023

In the above algorithm, the first two steps involve collecting the voter information using an RFID tag. The third step involves scanning the RFID tag using the RFID reader. Then, the voter must place their finger on the fingerprint sensor, which is step four. In step five, the fingerprint data is verified with Aadhar data, and the result is displayed on a 16*2 LCD display in step six. The seventh step involves uploading the program code to Arduino Uno. If the fingerprint matches the Aadhar data, the user is authenticated to vote in step eight. If the fingerprint does not match, the buzzer is turned ON, and the user is denied voting in step nine. The system uses IOT to monitor authentication status and count votes, which is step ten. In step eleven, the LCD display shows the unauthenticated user. The process ends in step twelve.

VI. Hardware description

6.1 Fingerprint Sensor

The Fingerprint Sensor R305 is an optical fingerprint reader that can store up to 1000 sets of data. It is capable of processing enrolment and matching and has a scanning speed of 0.5 seconds and a verification speed of 0.3 seconds, with a safety level of 5.

6.2 Arduino Uno

The Arduino Uno board is a microcontroller based on the ATmega328P and can be programmed using the Arduino IDE through a USB cable. The software includes a serial screen that allows easy communication with the board.

6.3 16*2 LCD (Liquid Crystal Display)

It is a flat panel display that uses liquid crystals to operate. It has a wide range of use cases in devices such as smartphones, televisions, and computer monitors. LCD technology allows for displays that are thinner than CRT technology.

6.4 Power Supply

A power supply is required to convert AC signals to DC signals and reduce signal amplitude. A power supply unit (PSU) is a device that supplies electricity or other forms of energy to an output load.

6.5 Keyboard

A keypad is a set of buttons arranged in a block that typically includes digits and other symbols. It is found on devices such as calculators, combination locks, and phones that require numeric input. It is often part of a computer keyboard and includes a separate grid of numerical and functional keys for efficient data entry.

6.6 RFID

RFID Reader - It reads the data from the RFID tag and verifies it with user-provided data.
RFID Tag- It contains user data such as name and ID.

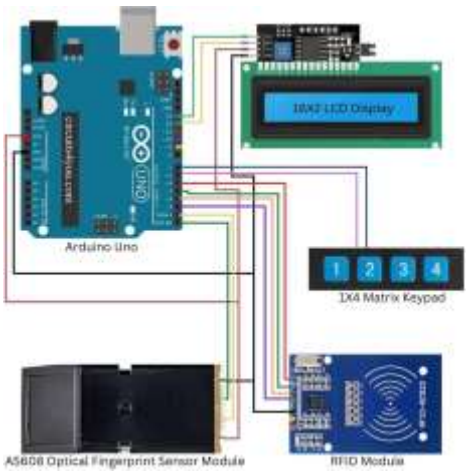

Figure 2: Circuit diagram

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 5, May : 2023

VII. Simulations and Experimental Results

Figure 3: Circuit

Figure 4: Container

Figure 5: “Scan Your Card” message on LCD

Figure 6: Scanning RFID card

Figure 7: Scanning and matching data

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 5, May : 2023

Figure 8: User scanning fingerprint

Figure 9: User verified

Figure 10: User data not found or mismatched

VII. Application and Advantages

This RFID Biometric EVM system has various applications, such as:

- It is mainly used for the verification process during elections to ensure that only authorized voters can cast their vote.
- The system is easy to operate, making it suitable for people of all ages and backgrounds.
- It is economical and feasible, making it accessible to all sections of society.
- The system requires less manpower, reducing the cost of deployment and increasing efficiency.

Only authenticated users can vote, eliminating the possibility of fraudulent practices and ensuring the accuracy of election results**.**

Conclusion

In conclusion, the proposed fingerprint-based voting machine provides a more secure and efficient voting process compared to traditional paper ballot machines. This system addresses many issues faced during the voting period, such as illegal voting, multiple votes by the same person, and eligibility verification. It also reduces the time required for voting, and the number of staff required to manage the voting process. The system provides an easy and accurate counting process without any issues, and allows for the implementation of voting preventive measures.

The effectiveness of this machine depends on its net interface and usability. With the implementation of this system, the voting process becomes more transparent and maintains the integrity of the voting process. It also provides the opportunity for anyone to vote from anywhere within the electoral limits, further increasing the convenience of the voting process.

Overall, the fingerprint-based voting machine provides a feasible and economical solution for implementing secure and efficient voting processes. This system can contribute to the healthy growth of a developing nation by ensuring a fair and reliable voting process.

References

[1] Electronic Voting Machine: https://eci.gov.in/evm/
[2] EVM and its history: https://en.wikipedia.org/wiki/Electronic_voting_in_India
[3] International Journal of Trend in Scientific Research and Development (IJTSRD) Conference | Issue | March 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470 Fostering | Innovation, Integration and Inclusion Through Interdisciplinary Practices in Management @ | IJTSRD | Unique Paper ID - IJTSRD23046 | Conference Issue | FIIITIPM - 2019 | March 2019 Page: 1 A Critical
[4] Study of Electronic Voting Machine (EVM) Utilization in Election Procedure Dr. A. V. Nikam1, Dr. P. C. Shetiye2, Dr. S. D. Bhoite3
[5] High Performance Electronic Voting Machine (EVM) Implementation Using ARM Cortex M3 | Date of Conference: 07-09 October 2020 | Date Added to IEEE Xplore: 10 November 2020 | INSPEC Accession
[6] Electronic voting machine — A review | Electronic ISBN:978-1-4673-1039-0 | Print ISBN:978-1-4673-1037-6 | CD:978-1-4673-1038-3 | Date of Conference: 21-23 March 2012 | Date Added to IEEE Xplore: 31 May 2012 | INSPEC Accession Number: 12770736 | DOI: 10.1109/ICPRIME.2012.6208285
[7] A.K. Agarwala, D. T. Shahani, and P. V. Indiresan. Report of the expert committee for evaluation of the upgraded electronic voting machine (EVM). Sept. 2006. http://www.scribd.com/doc/6794194
[8] R.. Anderson and M. Kuhn. Tamper resistance: A cautionary note. In Proc. Second USENIX Workshop on Electronic Commerce, Oakland, CA, 1996.
[9] A.W Appel. Certification of December 1, 2008. http://citp.princeton.edu/voting/advantage/seals/ appel-dec08-certif.pdf. [4] A. W. Appel, M. Ginsburg, H. Hursti, B. W. Kernighan, C. D. Richards, G. Tan, and P. Venetis. The New Jersey voting-machine lawsuit and the AVC Advantage DRE voting machine. In Proc. Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE), Montr´eal, Canada, Aug. 2009.
[10] A.Aviv, P. Cern´y, S. Clark, E. Cronin, G. Shah, M. Sherr, and M. Blaze. Security evaluation of ES&S voting machines and election management system. In Proc. USENIX/ACCURATE Electronic Voting Technology Workshop (EVT), San Jose, CA, July 2008.
[11] D. Bowen. “Top-to-Bottom” Review (TTBR) of voting machines certified for use in California. California Secretary of State, Aug. 2007.