Biometric Voting Machine Using Fingerprint Sensor

More Rushikesh Ravsaheb [1], Jadhav Rohit Rajendra [2], Bhalerao Anushka Rajendra [3]

[1] *Final year students, Department of chemical Engineering, Pravara Rural Engineering College, Maharashtra, India*
[2] *Final year students, Department of chemical Engineering, Pravara Rural Engineering College, Maharashtra, India*
[3] *Final year students, Department of chemical Engineering, Pravara Rural Engineering College, Maharashtra, India*

Mr. V. K. Jadhav
Assistant Professor, Department of Instrumentation and Control Engineering,
Pravara Rural Engineering College, Loni, Tal-Rahata, Dist.-Ahmednagar. (Maharashtra)

Prof. C. B. Kadu
Professor, Department of Instrumentation and Control Engineering,
Pravara Rural Engineering College, Loni, Tal-Rahata, Dist.-Ahmednagar. (Maharashtra)

ABSTRACT

This research paper explores the design, implementation, and effects of integrating biometric voting machines into the electoral process. These machines enhance security and efficiency by combining biometric technology with traditional voting methods. Key components include biometric sensors, data encryption, and voter authentication protocols. The benefits are improved security, reduced fraud, and better accessibility for disabled voters. Challenges such as privacy concerns, technological limitations, and costs are also discussed. The paper highlights the need for collaboration among policymakers, technologists, and stakeholders to address these issues responsibly. Ultimately, this research contributes to the discussion on electoral reform, aiming to make elections more secure, efficient, and inclusive. This study lays the groundwork for future research on modernizing electoral processes worldwide.

.**KEYWORD**- *Advanced voting system, Hybrid EVM solution, Fingerprint recognition*

1. INTRODUCTION

Secure and reliable elections are essential for a democratic society. Biometric voting machines enhance the security and reliability of the electoral process. A key advancement is integrating the RS307 communication protocol with the Arduino Uno microcontroller, ensuring robust communication with biometric scanners for seamless authentication. The Arduino Uno also enables real-time data processing, improving voter registration efficiency. This research examines the technical implementation and effectiveness of a biometric voting machine using the RS307 protocol and Arduino Uno. The RS307 ensures accurate and secure biometric data transmission, while the Arduino Uno manages real-time data processing for swift voter authentication and registration. The study aims to assess the design, functionality, and performance of this biometric voting machine to advance electoral integrity and accessibility. By exploring design methodology, implementation specifics, and experimental outcomes, this research highlights how biometric voting machines can enhance transparency and inclusivity in elections. It provides insights into the future of electoral technology and its potential to improve democratic practices globally.

2. METHODOLOGY

2.1 DESIGN FRAMEWORK:

- **Identify Essential Components :**

Biometric Sensors : Devices capable of capturing unique biological characteristics of voters. The choice of sensor impacts the accuracy and reliability of the system.

Microcontrollers : The core processing units that manage data flow and control various operations within the voting machine. The Arduino Uno microcontroller was chosen for its versatility and ease of use.

Communication Systems : Protocols and interfaces that enable communication between different components, ensuring seamless data transmission. The RS307 protocol was selected for its robust performance in handling biometric data.

Display Screens : Interfaces that provide visual feedback to users, aiding in navigation and ensuring user-friendly interactions during the voting process.

- **Select Biometric Techniques :**

Fingerprint Scanning: This method involves recording the unique patterns of ridges and valleys found on a person's finger. It is widely used due to its high accuracy and ease of use.

Iris Scanning: This technique captures the unique patterns within the colored ring around the pupil of the eye. Known for its high accuracy and ability to resist false matches, iris scanning requires more advanced technology.

- **Assess Communication Systems :**

RS307 : This communication protocol was chosen for its strong performance in securely transmitting biometric data. It offers high reliability and efficiency, making it well-suited for integration with biometric sensors.

RS232 : An alternative communication method known for its simplicity and wide usage. However, it was deemed less suitable due to its lower data transmission rates and potential for interference compared to RS307.

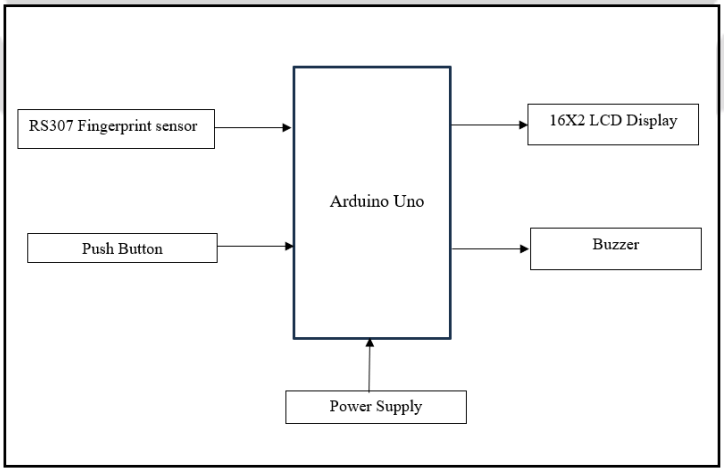

Figure 2.1 System Architecture of Voting Machine

2.2 TECHNICAL IMPLEMENTATION:

- **Select Hardware :**

Arduino Uno Microcontroller : Chosen for its sufficient processing power, versatility, and ease of programming. The Arduino Uno serves as the central processing unit, managing data flow and control operations within the system.

16x2 LCD Display : Selected for user interaction, providing clear and concise visual feedback to voters during the authentication and voting process. The display is user-friendly and integrates well with the Arduino Uno.

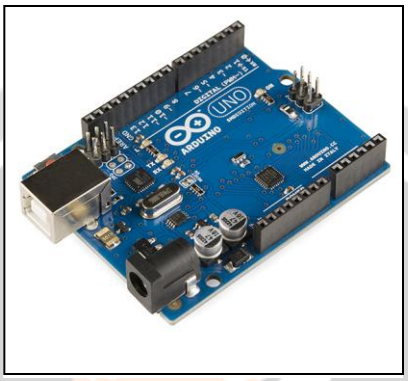

Figure 2.3 Arduino Uno

- **Component Integration :**

Biometric Sensors and Arduino Uno : The biometric sensors, specifically fingerprint scanners, were connected to the Arduino Uno microcontroller. This integration was achieved through careful wiring and coding to enable accurate data capture and processing.

Arduino Uno and LCD Display : The 16x2 LCD display was connected to the Arduino Uno, allowing it to display real-time information to the user. This setup ensured that the system could provide feedback on voter authentication status and guide the user through the voting process.

Figure 2.4 R307 Fingerprint Sensor

- **Establish Communication Links :**

Developing Communication Links : The RS307 protocol was implemented to facilitate robust and secure data transfer between the biometric sensors and the Arduino Uno microcontroller. This protocol was chosen for its high reliability and efficiency in handling biometric data.

Ensuring Reliable Data Transfer : Extensive testing and calibration were performed to ensure that the communication links were stable and could handle the required data transfer rates. This step was crucial in maintaining the integrity and reliability of the biometric voting machine.

2.3 SOFTWARE DEVELOPMENT:

- **Microcontroller Programming :**

Biometric Data Processing : Capturing and processing biometric data from fingerprint sensors. The microcontroller reads and interprets the biometric inputs accurately for reliable voter authentication.

Voter Authentication : Implementing algorithms to compare captured biometric data against stored records for swift and accurate voter verification.

Overall Operation Management : Managing the sequence of operations from voter interaction to vote casting, ensuring a smooth user experience.

- **Design User Interface**

User Interface Design : Creating a clear interface to guide voters step-by-step with instructions and feedback at each stage, from biometric scanning to vote confirmation.

Interactive Elements : Implementing prompts, status updates, and confirmation messages to ensure voters are well-informed and confident during the process.

2.4 EXPERIMENTAL SETUP:

- **Build and Test Prototype :**

Prototype Construction : Assembling biometric sensors, the Arduino Uno microcontroller, a 16x2 LCD display, and other components into a cohesive unit.

Initial Testing : Performing tests in a controlled environment to verify the functionality of the prototype, ensuring accurate data capture, proper algorithm execution, and correct user feedback display**.**

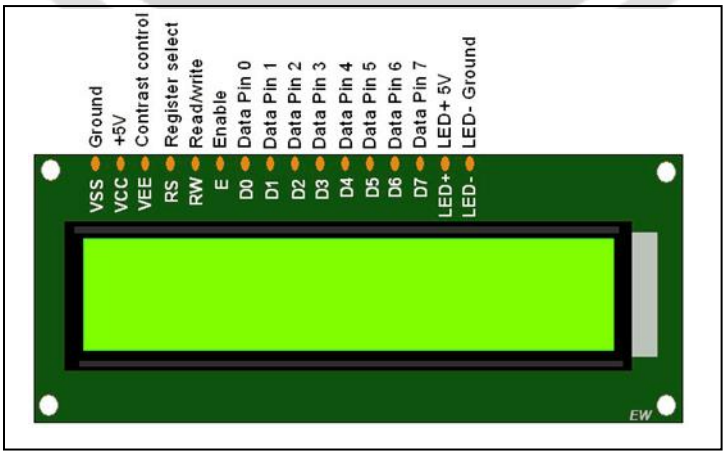

Figure 2.5 16 X 2 LCD Display

- **Simulate Voting Conditions :**

Voting Scenarios : Creating scenarios with diverse voter demographics (ages, genders, biometric characteristics) and environmental conditions (lighting, noise levels) to test robustness.

Performance Evaluation : Observing how the machine handled different inputs and conditions to assess reliability and accuracy.

- **Gather Data :**

System Performance Metrics : Measuring response times, error rates, and the accuracy of biometric authentication to gauge efficiency and reliability.

User Satisfaction : Gathering user feedback on ease of use, clarity of instructions, and overall experience.

Identify Areas for Improvement : Analyzing data to optimize response times, reduce error rates, and enhance user satisfaction.

2.5 PERFORMANCE EVALUATION:

- **Quantitative Analysis :**

Authentication Speed : Measuring the time taken by the system to authenticate a voter using their biometric data. We aimed to ensure that the process was swift enough to maintain a smooth voting flow without causing delays.

Accuracy : Assessing the accuracy of the biometric sensors in correctly identifying and authenticating voters. This included calculating the false acceptance rate (FAR) and false rejection rate (FRR) to ensure high precision and reliability.

Reliability : Evaluating the system's reliability over multiple voting sessions and various conditions. We tested the machine's consistency in performance to confirm its robustness and dependability in different scenarios.

- **Qualitative Assessment :**

User Feedback: Gathering thorough feedback from individuals who interacted with the machine, focusing on their experiences regarding ease of use, clarity of instructions, and overall satisfaction with the voting process.

Expert Reviews: Soliciting assessments from specialists in biometric technology and electoral systems. Their evaluations aided in identifying potential enhancements in design and functionality to elevate user experience and system performance.

Usability Testing: Carrying out tests to assess the ease with which voters could navigate the system. This entailed observing their interactions, pinpointing any challenges they faced, and implementing required adjustments to enhance accessibility and user-friendliness.

2.6 ETHICAL CONSIDERATIONS:

- **Ensure Privacy :**

Strong Encryption : Applied advanced encryption techniques to protect biometric data during transmission and storage, ensuring confidentiality and security.

Legal and Ethical Compliance : Adhered to legal and ethical guidelines, such as GDPR or local data protection laws, to handle voter data responsibly.

Data Anonymization : Where possible, anonymized biometric data to protect individual identities by removing personal identifiers.

- **Obtain Ethical Clearance :**

Ethical Approval : Obtained approval from relevant authorities, such as institutional review boards (IRBs) or ethics committees, ensuring our research methods were ethically sound.

Informed Consent : Informed all participants about the study's nature, their role, and their rights, and obtained their consent, ensuring voluntary participation.

Participant Rights : Protected participants' rights, allowing them to withdraw at any time and ensuring their data was used only for the study's purposes.

2.7 LIMITATIONS AND FUTURE DIRECTIONS:

- **Identify Challenges**

Technological Limitations : Current biometric technologies face limitations in accuracy, speed, and environmental adaptability. Issues like worn or scarred fingerprints and varying lighting conditions can affect performance.

Cost Implications : Implementing biometric voting machines on a large scale involves significant costs, including initial investment, maintenance, updates, and support, which can be a barrier for regions with limited budgets.

Regulatory Issues : Navigating legal and regulatory requirements, such as data protection laws and privacy concerns, is complex and time-consuming, impacting the deployment of biometric systems in voting processes.

- **Propose Future Research :**

Advancements in Biometric Technology: The focus should be on improving sensor accuracy and performance across different conditions, alongside exploring alternative biometric methods like facial recognition or vein pattern recognition.

Enhancements in Data Security: Stronger encryption methods, secure communication protocols, and robust data storage solutions are vital to protect sensitive voter information and ensure system integrity.

Development of User-Friendly Interfaces: Creating intuitive interfaces that guide voters seamlessly through the process, considering the needs of individuals with disabilities and varying levels of technological proficiency, will enhance accessibility.

Cost-Effective Solutions: Research into affordable hardware options, leveraging open-source software, and implementing efficient maintenance strategies can lower costs without sacrificing functionality or security, enabling broader adoption.

.2.8 Flowchart of System :

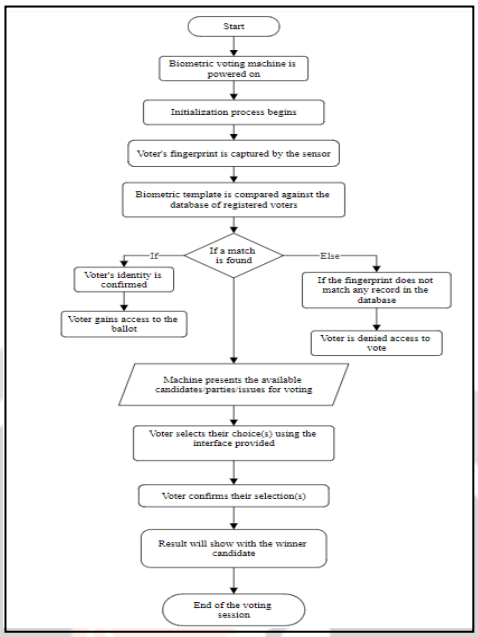

Figure 2.6 Flowchart of System

Figure 2.7 Working Model of Biometric Voting Machine

3. CONCLUSION

Biometric voting machines offer a promising solution to the limitations of traditional voting systems, providing improved security, fraud prevention, and accessibility. Although challenges like privacy concerns and technological limitations exist, the advantages of using biometric voting machines to modernize electoral processes are considerable. Collaboration among policymakers, technologists, and stakeholders is essential to ensure responsible implementation and protect voter rights. Biometric voting machines represent a significant advancement in promoting democratic principles and ensuring the integrity of electoral outcomes.

REFERENCES

[1] M. Singh, P. M. Benson, T. J. Titus, and V. S. S. Devi, "A secured biometric voting system using RFID linked with the Aadhar database," *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, 2020, pp. 1-6.

[2] J. Deepika, et al., "Smart electronic voting system based on biometric identification- survey," *2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM)*, Chennai, India, 2017, pp. 1-4.

[3] S. M. Hasan, et al., "Development of electronic voting machine with the inclusion of Near Field Communication ID cards and biometric fingerprint identifier," *2014 17th International Conference on Computer and Information Technology (ICCIT)*, Dhaka, Bangladesh, 2014, pp. 1-4.

[4] N. S. Pal, A. Singh, D. Malik, P. Kumar, H. Singh, and D. Verma, "RFID-based biometric electronic voting machine," *International Journal of Scientific Research and Management Studies (IJSRMS)*, vol. 2, no. 12, pp. 452-458, 2016.

[5] B. M. M. Reddy and D. Srihari, "RFID-based biometric voting machine linked to Adhaar for safe and secure voting," *International Journal of Science, Engineering and Technology Research (IJSETR)*, vol. 4, no. 4, pp. 995-1001, 2015

[6] A. M. Anis, et al., *Development of electronic voting machines with the inclusion of near-field communication ID cards, biometric fingerprint sensors, and POS printers*, M.S. thesis, BRAC University, Dhaka, Bangladesh, 2014.

[7] A. Kadbe, S. B. Gujar, and S. Chimote, "Biometric and RFID secured centralized voting system," *International Journal of Computer Science and Information Technologies*, vol. 4, no. 2, pp. 255-258, 2013.

[8] P. Ranjan, A. A. Badoni, S. B. Khandi, and N. Saini, "Design of RFID-based electronic voting machine," *International Journal on Human and Smart Device Interaction*, vol. 2, no. 1, pp. 1-6, 2015.