

# A Secure Biometric Voting System Using Fingerprint Authentication and Face Recognition

Ms. Ishika Mehta<sup>1</sup>, Ms. Jaya Yadav<sup>2</sup>, Ms. Alina Shaikh<sup>3</sup>, Mr. Sheikh Kashif<sup>4</sup>

<sup>1,2,3</sup> Student, Department of Computer Engineering, Thakur Shyamnarayan Engineering College, Maharashtra, India

<sup>4</sup>Assistant Professor, Department of Computer Engineering, Thakur Shyamnarayan Engineering College, Maharashtra, India

\*\*\*

**Abstract** - Traditional voting systems are often vulnerable to identity fraud, ballot manipulation, and delays in result compilation. By leveraging fingerprint biometrics, the system ensures that each voter can only cast one vote, thereby eliminating the possibility of voter fraud and multiple voting. The system [1] operates as follows: each voter is required to authenticate their identity through fingerprint scanning before accessing the voting platform. The fingerprint data is matched with a pre-existing voter database to verify eligibility.

Once authenticated, the voter is granted access to the digital ballot system, where they can securely cast their vote. The IOT component connects the voting terminals to a centralized server over a secure network, ensuring real-time data transmission and immediate updates to the voting status.

In this system, each voter is first registered using a biometric fingerprint sensor. The fingerprint data is stored securely in the system database. During voting, the voter's fingerprint is scanned again and matched with the stored data to verify their identity. In addition to fingerprint authentication, face recognition is also used as an extra layer of security to ensure that only the correct person is allowed to vote. Once the voter is successfully verified, they are allowed to cast their vote by selecting their preferred candidate using a set of buttons provided on the voting machine. The system ensures that each voter can vote only once, thereby preventing duplicate voting. The IOT [1] component connects the voting terminals to a centralized server over a secure network, ensuring real-time data transmission and immediate updates to the voting status.

Overall, this project demonstrates how combining biometric authentication with electronic voting can enhance security, improve efficiency, and build trust in the electoral process, especially for small-scale applications such as college elections or controlled environments.

**Key Words:** IOT, Fingerprint Authentication, Voting system, Biometric security, LCD, Real-time data processing, Smart Voting System, Biometric Authentication, Fingerprint Recognition, Face Recognition, Secure Voting, Embedded System

## 1. INTRODUCTION

Democracy is the law in India. Voting [3] is an important way for citizens to exercise their constitutional right to vote in a democracy like India. Voters commonly cast their ballots in a polling place. As technology develops, electronic voting machines continue to be used to cast votes. The Election Commission of India, in partnership with Bharat Electronics Limited (BEL) and Electronics Corporation of India Limited, developed the Indian electronic voting machine (EVM) in 1989. (ECIL). Since 2004, all national and state legislature elections in India have been performed with electronic voting machines. Only 31 of the 120 democratic countries rely on voting by electronic machines, either regionally or nationwide. Other countries continue to utilize ballots made of paper as they don't trust electronic voting machines.

Elections form the basis of any democratic nation, whereby its people get to decide over their leaders and the future course of their country. Traditional voting systems have often been plagued by fake voting, ballot tampering, and delays in result processing, ultimately diminishing public trust in election results. In various countries, manual or electronic systems of voting require the use of identity cards or paper-based verification; such a process is prone to human error and manipulation. In fact, studies have pointed out that even minor mismatching in the voter authentication process can create large-scale disputes and controversies in the credibility of the results of elections. Therefore, there is an increasing requirement for a safe, automated, and transparent system of voting that can guarantee one-person-one-vote authenticity. [2]

To address these issues, there is a growing need for more secure and advanced voting systems. Integrating biometric authentication methods such as fingerprint and face recognition can help ensure that only authorized voters are allowed to vote. This project focuses on developing a smart voting system that combines biometric verification with electronic voting to enhance security, accuracy, and trust in the electoral process.

## 1.1 Problem Identification

The current voting systems face challenges such as voter impersonation, fraud, errors, and limited accessibility, undermining the integrity and trust in elections. Traditional methods are also time-consuming and prone to mistakes, while real-time monitoring and transparent auditing are often lacking. This project aims to address these issues by developing a "Fingerprint Based Voting System Using IoT," [6] which combines biometric authentication with IoT technology to create a secure, efficient, and accessible voting process. The system will enhance voter identification, prevent fraud, improve transparency, and offer remote voting capabilities, ensuring a more reliable and trusted electoral process.

One major issue with this system is the lack of strong identity verification. There is a possibility of duplicate voting or impersonation, where individuals may attempt to vote more than once or on behalf of others. Additionally, manual handling of ballots increases the risk of tampering or manipulation, which can affect the fairness and transparency of the election process.

Due to these limitations, traditional voting systems are not fully secure or efficient. They require large manpower, careful monitoring, and still may not guarantee accuracy. Therefore, there is a need for a more reliable system that can ensure secure voter verification, prevent fraud, and provide accurate results, leading to the development of a smart voting system using biometric authentication.

## 1.2 Objectives of the Project

The Fingerprint Voting System[3] Using IOT offers a revolutionary way to streamline and secure the voting process by integrating biometric authentication with IOT technology. This system ensures voter identity verification[6] using fingerprint recognition, allowing only authorized individuals to cast their votes. The IOT infrastructure connects voting terminals to central the user-friendly interface makes the voting process smooth and accessible for all voters, while the elimination of paper ballots and manual processes helps reduce the cost and complexity of elections.

### Primary Objective

The main objective of the VoteSure system is to design and develop a secure and reliable smart voting machine that uses biometric fingerprint authentication to verify voter identity before allowing vote casting. The system aims to prevent multiple voting, impersonation, and electoral fraud while ensuring accurate and fast vote counting. By integrating biometric verification with digital storage, the project enhances transparency, efficiency, and reliability in the voting process. The system also aims to demonstrate how

modern technologies like IoT and encryption can improve traditional voting mechanisms.

### Secondary Objectives

- To authenticate voters using fingerprint recognition.
- To prevent duplicate or fake voting.
- To store votes securely in digital format.
- To enable quick and accurate vote counting.
- To improve transparency and reduce manual errors.

The Fingerprint Voting System[3] Using IOT offers a revolutionary way to streamline and secure the voting process by integrating biometric authentication with IOT technology. This system ensures voter identity verification[6] using fingerprint

recognition, allowing only authorized individuals to cast their votes. The IOT infrastructure connects voting terminals to central the user-friendly interface makes the voting process smooth and accessible for all voters, while the elimination of paper ballots and manual processes helps reduce the cost and complexity of elections.

The Fingerprint Voting System[3] Using IOT offers a revolutionary way to streamline and secure the voting process by integrating biometric authentication with IOT technology. This system ensures voter identity verification[6] using fingerprint recognition, allowing only authorized individuals to cast their votes. The IOT infrastructure connects voting terminals to central the user-friendly interface makes the voting process smooth and accessible for all voters, while the elimination of paper ballots and manual processes helps reduce the cost and complexity of elections.

The Fingerprint Voting System[3] Using IOT offers a revolutionary way to streamline and secure the voting process by integrating biometric authentication with IOT technology. This system ensures voter identity verification[6] using fingerprint recognition, allowing only authorized individuals to cast their votes. The IOT infrastructure connects voting terminals to central the user-friendly interface makes the voting process smooth and accessible for all voters, while the elimination of paper ballots and manual processes helps reduce the cost and complexity of elections.

The Fingerprint Voting System[3] Using IOT offers a revolutionary way to streamline and secure the voting process by integrating biometric authentication with IOT technology. This system ensures voter identity verification[6] using fingerprint recognition, allowing only authorized individuals to cast their votes. The IOT infrastructure connects voting terminals to central the user-friendly interface makes the voting process smooth and

accessible for all voters, while the elimination of paper ballots and manual processes helps reduce the cost and complexity of elections.

## 2. LITERATURE SURVEY

The integration of IoT technology into fingerprint-based voting systems has emerged as a promising solution for improving both the security and efficiency of electoral processes. By incorporating biometric authentication alongside real-time data handling, these systems aim to ensure voter legitimacy and significantly reduce the chances of electoral malpractice [3], [4], [5]. Research highlights the effectiveness of fingerprint recognition in accurately identifying eligible voters, while IoT enables continuous monitoring and centralized control of voting operations. Despite these advantages, several concerns persist, particularly in areas such as data privacy, system dependability, and user trust. Addressing these challenges requires further investigation, including the development of stronger security mechanisms and the exploration of advanced technologies like blockchain to enhance transparency and protect the integrity of the voting system.

### 2.1 Limitations of Existing Systems

There are many drawbacks in using the paper ballot like more man power and time taking process for casting a vote and for announcing the result. Every year the population is increasing so it is hard to use the paper ballot systems and technology is growing so in 1977 the chief election commissioner mooted the idea of EVM. [7]. Despite the improvements introduced by electronic and biometric-based voting systems, several important concerns still remain. One major issue is data privacy, as sensitive information such as biometric data must be stored securely. If this data is not properly protected, it can lead to misuse or unauthorized access, raising serious privacy concerns for users.

Another limitation is related to system dependability and reliability. Electronic systems may face technical problems such as hardware failure, software errors, or network issues, which can disrupt the voting process. In some cases, system failures can lead to delays or incorrect results, reducing confidence in the system. Additionally, many systems depend on a single method of authentication, which may not be sufficient to prevent all types of fraud.

There is also a challenge in terms of user trust and transparency. Voters may feel uncertain about whether their votes are being recorded and counted correctly, especially when the process is not visible. To overcome these limitations, there is a need for stronger security measures, better system design, and the use of advanced technologies. Techniques such as multi-level authentication and secure data handling can improve reliability, while emerging

technologies like blockchain can be explored to increase transparency and ensure the integrity of the voting system.

## 2.2 Summary of Research Papers

The reviewed papers collectively focus on enhancing the security, efficiency, and transparency of voting systems through the integration of biometric technologies and modern computing approaches. Most of the proposed systems rely on fingerprint-based authentication, often combined with additional methods such as facial recognition, RFID, or Aadhaar verification, to ensure that only eligible voters can cast their votes and only once. The use of IoT enables real-time data transmission and centralized monitoring, while technologies like cloud computing, artificial intelligence, and blockchain further strengthen data security and system reliability. These systems significantly reduce issues present in traditional voting methods, such as voter impersonation, ballot tampering, and delays in vote counting, while also improving accuracy and public trust in the electoral process [1], [7], [8], [9].

Despite these advantages, several challenges and limitations are consistently identified across the studies. Key concerns include data privacy risks associated with storing sensitive biometric information, high implementation and maintenance costs, and scalability issues when applied at a national level. Additionally, system reliability depends heavily on network connectivity and hardware performance, and biometric recognition may face difficulties under real-world conditions. Public acceptance and trust also remain critical factors for successful adoption. Overall, while biometric and IoT-based voting systems present a promising future for secure and efficient elections, further research and development are necessary to address these challenges and ensure practical, large-scale implementation [2], [3], [4], [5].

## 3. METHODOLOGY

This project introduces a secure and efficient biometric based voting and authentication system that integrates the R307 fingerprint module with an ESP32/Arduino microcontroller. The primary objective of the system is to ensure a reliable and tamper-resistant voting process by utilizing biometric identification techniques. The R307 fingerprint sensor plays a central role in capturing and verifying users' fingerprints, thereby preventing duplicate entries and eliminating the possibility of unauthorized voting.

To manage the system effectively, four control buttons are incorporated, namely enroll, increment, decrement, and delete. These buttons allow administrators to register new users, navigate stored fingerprint records, and remove data when necessary. In addition, three dedicated buttons are assigned for candidate selection, enabling voters to cast their votes in a simple and user-friendly manner. This structured

interface ensures that both administrative operations and voting procedures are carried out smoothly.

All hardware components are interconnected using jumper wires, creating a compact and organized setup suitable for prototype and small-scale deployment. The microcontroller serves as the core processing unit, coordinating all operations such as user enrollment, identity verification, vote recording, and data management. Overall, this system improves transparency, accuracy, and efficiency in the voting process. Its design makes it particularly suitable for small scale electronic voting environments, as well as for secure access control applications where reliable user authentication is essential.

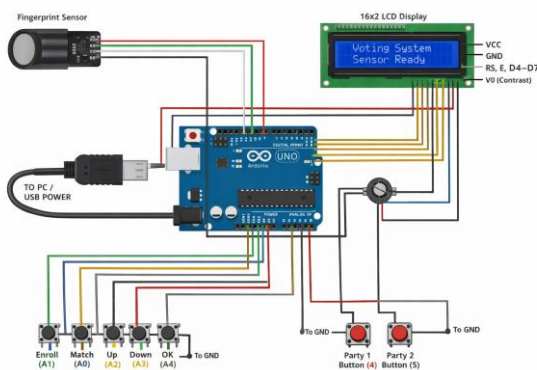


Fig 1- Circuit Diagram

### 3.1 Design Methodology

The project follows the Waterfall Model, a structured and sequential approach to system development. In the requirements phase, led by Team Leader Ishika, the system objectives were defined, including secure voting using fingerprint authentication (R307s) module and candidate selection through push buttons.

In the design phase, Designer created the system architecture, circuit diagrams, and workflow for enrolment, verification, and voting processes. The development phase, carried out by Developer, involved assembling hardware components such as Arduino uno R3, fingerprint module, push buttons using jumper wires, LCD to display the result along with programming the system functionalities.

During the testing phase, Tester evaluated each module individually and as a complete system to ensure accuracy, reliability, and prevention of duplicate voting. In the deployment phase, the system was implemented as a working prototype and demonstrated in real-time conditions.

Finally, in the maintenance phase, the entire team monitors system performance, fixes issues, and updates features to ensure long-term efficiency and scalability

### 3.2 Technology Used

**Embedded Systems:** The project is based on embedded system technology where the ESP32/Arduino microcontroller acts as the core unit, controlling all hardware components and executing programmed instructions in real time.

**Biometric Authentication:** Fingerprint recognition using the R307 module ensures secure user identification. This technology prevents unauthorized access and duplicate voting by verifying unique biometric data.

**Embedded C / Arduino Programming:** The system is programmed using Embedded C in the Arduino IDE, enabling interaction between hardware components and execution of system logic.

**Human-Machine Interaction (HMI):** Push buttons provide a simple interface for users to interact with the system, making operations like enrolment and voting easy and user-friendly.

## 4. HARDWARE REQUIREMENTS

### Arduino UNO R3

Acts as the main controller of the system. It processes inputs from sensors, buttons, and modules, and controls outputs accordingly. Based on the ATmega328P, it is simple, reliable, and easy to program, making it suitable for basic control tasks (unlike ESP32, it has no built-in Wi-Fi).



Fig 2- Arduino UNO R3

### R307 Fingerprint Module

A biometric sensor used for fingerprint enrollment and verification. It has inbuilt storage, fast recognition speed, and high accuracy, ensuring secure and duplicate-free authentication.



Fig 3- R307 Fingerprint Module

**Push Buttons (5 Control + 2 Candidate Selection)**

Used for user interaction. Control buttons manage operations like enroll, increment, decrement, and delete, while candidate buttons allow vote selection.



Fig 4- Push Buttons

**Jumper Wires**

Used for circuit connections and prototyping. They ensure flexible and easy assembly of components without soldering.



Fig 5- Jumper Wires

**Supporting Components**

- Power Supply
- Breadboard
- Buzzer
- Display Module (LCD or similar)

**5. SYSTEM ARCHITECTURE**

The proposed system is divided into multiple layers to ensure secure and smooth operation. Each layer in the system performs a specific function, and together they create a seamless workflow from voter authentication to vote recording.

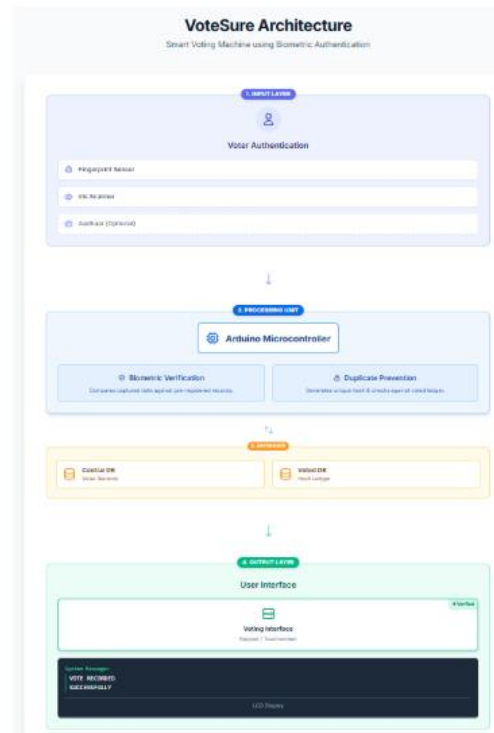


Fig -6: System Architecture

At the input layer, the system focuses on authenticating the voter using advanced biometric techniques such as fingerprint recognition and face detection. These methods provide a high level of security because biometric traits are unique to each individual and difficult to replicate. When a voter attempts to access the system, their fingerprint is scanned using a sensor module, and their facial features are captured through a camera. This data is then compared with the pre-stored biometric information in the system. Only if both (or either, depending on system design) match successfully, the voter is considered valid. This layer acts as the first line of defense against unauthorized access and ensures that only eligible voters can proceed further.

Once authentication is completed, the data moves to the processing layer, which serves as the brain of the system. This layer is controlled by a microcontroller such as Arduino or ESP32. It processes the incoming biometric data, performs validation checks, and manages decision-making operations. One of its critical responsibilities is to verify whether the authenticated voter has already cast their vote. This is done by checking unique voter IDs against stored records. If a duplicate attempt is detected, the system immediately blocks access and displays an appropriate message. The processing unit also coordinates communication between different components, ensuring smooth data flow across the system.

The next stage is the database layer, which plays a vital role in storing and managing data securely. This layer consists of two main parts: the voter database and the voting database. The voter database contains essential details such as voter

ID, biometric data (fingerprint templates and facial features), and eligibility status. On the other hand, the voting database records the votes cast by each voter in a secure and encrypted format. Proper database management ensures data integrity, prevents tampering, and allows efficient retrieval of information when needed. In some implementations, this layer can be connected to a centralized server or cloud storage to enhance scalability and accessibility.

Finally, the output layer provides the interface through which the voter interacts with the system. After successful authentication, the voter is presented with voting options using push buttons or a digital interface. The system ensures that the voting process is simple and user-friendly. Once a vote is cast, the system records it in the database and confirms the action. An LCD display is used to provide real-time feedback, such as "Authentication Successful," "Vote Recorded Successfully," or "Already Voted." This layer enhances user experience while maintaining transparency in the voting process.

Overall, this layered architecture improves the system's efficiency by clearly separating responsibilities across different stages. It enhances security through biometric verification, prevents fraudulent activities like duplicate voting, and ensures accurate data handling through structured storage and processing. By integrating hardware components with intelligent software control, the system achieves a robust and scalable solution for modern electronic voting applications.

## 6. RESULTS

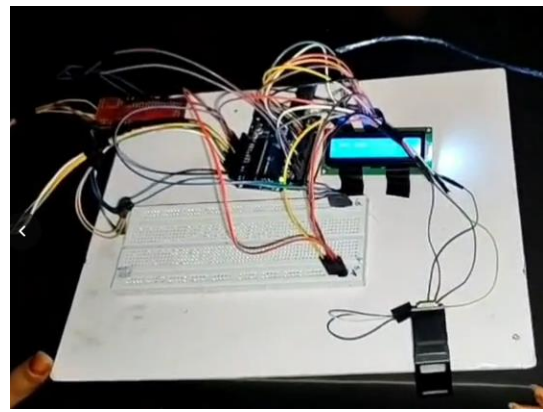
The developed smart voting system was successfully implemented and tested using the ESP32/Arduino microcontroller along with the R307 fingerprint module and camera module. The system was able to accurately register users and verify their identity using fingerprint authentication. During testing, the system correctly allowed each verified user to cast their vote using the candidate selection buttons.

It was observed that once a user had voted, the system successfully prevented duplicate voting by restricting further access. The LCD display provided clear messages such as authentication success, voting status, and errors, which improved user interaction and understanding of the system.

The overall performance of the system was found to be reliable for small-scale applications. The response time was quick, and the system operated smoothly without major issues. The results demonstrate that the proposed system is effective in improving voting security, reducing manual errors, and ensuring transparency. However, minor improvements can be made in terms of speed and accuracy

of face recognition for better performance in real-world conditions.

After testing the biometric voting system, it showed clear improvements over traditional voting methods. The system was able to correctly identify registered voters using fingerprints and facial recognition almost every time. No fake or duplicate votes were allowed, which shows the system is very reliable. Voting and counting were much faster than paper-based methods. Votes were stored securely in the system and counted automatically, so there were no delays or mistakes. Overall, the system worked efficiently while keeping voter information safe and private [2].



**Fig 7- Final Demonstration**

## 7. CONCLUSIONS

The project successfully demonstrates a secure and efficient biometric-based voting system using fingerprint and face recognition. By integrating the R307 fingerprint module with an ESP32/Arduino microcontroller, the system is able to accurately verify users and prevent unauthorized access. The inclusion of simple push buttons for voting makes the system easy to use and suitable for practical implementation in small-scale environments.

The system effectively fulfills its main objectives, such as ensuring secure voter authentication, preventing duplicate voting, and providing a smooth and reliable voting process. The combination of biometric verification and electronic voting improves transparency and reduces the chances of fraud or manual errors. The system also shows how hardware and software can work together to create a dependable solution.

Overall, the project provides a strong foundation for developing secure voting systems. It highlights the importance of using modern technologies like biometrics to enhance the accuracy and trustworthiness of elections. The solution is practical, cost-effective, and can be used in controlled environments such as colleges or small organizations.

## 8. FUTURE DIRECTION

In the future, the system can be further improved by integrating cloud-based storage, which will allow centralized data management and easier access to voting records. Advanced face recognition techniques using AI can also be implemented to improve accuracy and make the system more reliable. Adding a display unit or developing a mobile application can enhance user interaction and make the system more user-friendly.

The system can also be expanded for larger-scale applications by improving its performance and scalability. Integration with IoT technologies can enable remote monitoring and real-time data updates. Additionally, implementing stronger security features such as encryption can further protect sensitive data and ensure safer communication between components.

Further enhancements can include the use of more advanced microcontrollers and improved biometric methods such as iris recognition. These upgrades can make the system more robust, accurate, and suitable for real-world applications. With continuous improvements, the system has the potential to be used in larger and more critical voting environments.

## REFERENCES

- [1] Anushka Fase "Fingerprint Based Voting System Using IOT"
- [2] Prof. Bina R. Rewatkar "Advance Voting System Using Biometric Verification and Artificial Intelligence"
- [3] Dr. Shalini Shravan "BIOMETRIC IDENTITY AND IOT-BASED ELECTRONIC VOTING MACHINE"
- [4] Prasad Ramchandra Mavarkar "Biometric Voting System"
- [5] CH Srilatha "Fingerprint-based biometric smart electronic voting machine using IoT and advanced interdisciplinary approaches"
- [6] R.Akila Mukesh, Muraree Lal Meena, G. Sasirekha, A. Selvameena, Tamilselvi Tt, Finger Print Based Voting System
- [7] MR.M JANARTHANAN "AADHAR BASED ELECTRONIC VOTING MACHINE"
- [8] Dr.V.LATHA "AADHAR BASED ELECTRONIC VOTING SYSTEM AND PROVIDING AUTHENTICATION ON INTERNET OF THINGS"
- [9] Chetan Adhikar "Development of Online Voting System Using Aadhar Authentication"