International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Biometric Based Secure Voting System

Prashant Yemle[1], Sakshi Chavan[2], Pranav Akhade[2], Nandini Gaikwad[3], Ms. P. Y. Jadhav[4]

[1,2,3,4]Electronics And Telecommunication JSPM Polytechnic College Hadapsar, Pune, India

ABSTRACT

A Biometric Based Secure Voting System is designed to enhance the security, transparency, and reliability of the election process. Traditional voting methods are prone to issues such as duplicate voting, impersonation, and manual counting errors. This system uses fingerprint biometric authentication to verify voter identity before allowing vote casting. The system is implemented using a microcontroller/Raspberry Pi integrated with a fingerprint sensor, database server, and display unit. Each voter can vote only once, and the vote is securely stored in the database. The proposed system reduces election fraud, ensures fast vote counting, and improves overall election efficiency.

1. INTRODUCTION

Voting is a fundamental right in democratic countries. Traditional voting systems such as ballot papers and Electronic Voting Machines (EVMs) have limitations like:

- Fake voting
- Booth capturing
- Multiple voting
- Identity fraud
- Time-consuming counting process

To overcome these problems, biometric authentication technology is introduced. Fingerprint recognition is unique for every individual, making it a reliable method for voter verification.

The proposed system ensures:

- One person – one vote
- Secure voter identification
- Automatic vote counting
- Reduced human intervention

1. SYSTEM OVERVIEW

The Biometric Based Secure Voting System is an advanced electronic voting platform designed to enhance the security, accuracy, and transparency of the election process through biometric authentication. The system replaces or improves traditional voting methods by integrating fingerprint recognition technology with an automated vote recording and counting mechanism.

The primary objective of the system is to ensure that only eligible voters are allowed to cast their votes and that each voter can vote only once. This is achieved by using a fingerprint sensor to authenticate voters based on their unique biometric identity. Since fingerprints are unique for every individual, the system effectively eliminates impersonation and duplicate voting.

The overall system is composed of both hardware and software modules. The hardware unit includes a fingerprint sensor for biometric verification, a microcontroller or Raspberry Pi for processing, an LCD display for user interaction, voting buttons or a keypad for vote casting, and a power supply unit. The software module manages fingerprint recognition, voter database handling, vote storage, and result computation.

The operation of the system begins with voter enrollment, where voter details and fingerprint templates are securely stored in the database. During the voting process, the voter places their finger on the biometric sensor. The system compares the scanned fingerprint with stored records. If a valid match is found and the voter has not previously voted, the voting interface is activated. The voter can then select their preferred candidate. Once the vote is cast, it is securely stored, and the system updates the voter status to prevent multiple voting attempts.

Additionally, the system supports automated vote counting and instant result generation, significantly reducing the time and manpower required in traditional elections. Security features such as biometric verification, secure databases, and controlled access mechanisms ensure the reliability and integrity of the voting process.

Thus, the Biometric Based Secure Voting System provides a robust, fraud-resistant, and efficient solution for modern electoral systems suitable for governmental, institutional, and organizational voting applications.

2. METHODOLOGY

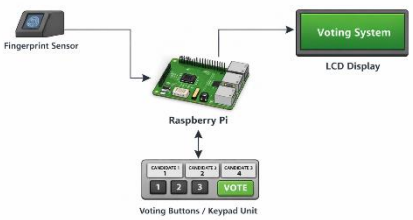
The proposed Biometric Based Secure Voting System follows a structured methodology to ensure secure voter authentication and accurate vote recording. The process begins with voter enrollment, where eligible voters' details and fingerprint templates are captured and stored in a secure database.

During voting, the voter places their finger on the biometric sensor for authentication. The system compares the scanned fingerprint with stored records. If the fingerprint matches and the voter has not voted before, access to the voting interface is granted; otherwise, voting is denied.

After successful verification, the voter selects their preferred candidate using the voting unit interface. The cast vote is securely stored in the database, and the voter's status is updated to prevent duplicate voting.

Finally, the system performs automatic vote counting and generates results instantly. This methodology ensures a secure, transparent, and efficient voting process by eliminating impersonation and multiple voting.

3. BLOCK DIAGRAM WITH EXPLAINATION



Biometric Based Secure Voting System

The block diagram of the proposed Biometric Based Secure Voting System illustrates the functional relationship between the fingerprint authentication unit, processing unit, and voting interface. The system

is designed to ensure secure voter verification and accurate vote recording through integrated hardware modules.

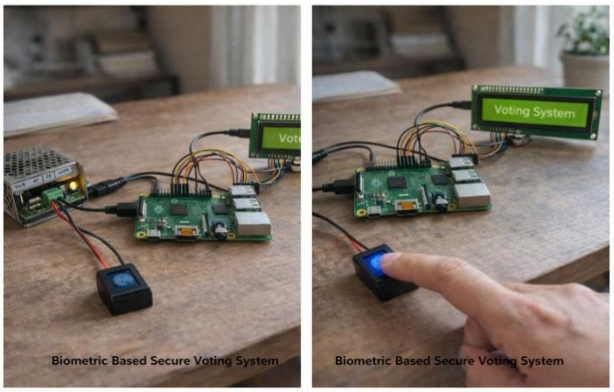
The fingerprint sensor serves as the primary input device of the system. It captures the voter's fingerprint and converts it into a digital template. This biometric data is transmitted to the Raspberry Pi, which acts as the central processing unit. The Raspberry Pi processes the received fingerprint data and compares it with the pre-stored voter database to authenticate the voter's identity.

If the fingerprint is successfully matched and the voter has not voted previously, the system grants authorization to proceed with voting. The LCD display provides real-time instructions and status messages to the voter, such as authentication results and voting prompts, thereby acting as the user interface of the system.

Following successful authentication, the voter uses the keyboard or keypad unit to cast their vote by selecting the desired candidate. The selected input is received by the Raspberry Pi, which records the vote securely and updates the voter's status in the database to prevent multiple voting.

Thus, the integration of the fingerprint sensor, Raspberry Pi, LCD display, and keyboard forms a secure and efficient biometric voting framework that ensures authorized access, eliminates duplicate voting, and enhances the transparency and reliability of the electoral process.

4. CIRCUIT DIAGRAM



6. ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to all those who supported and guided them in the successful completion of this research paper on the **Biometric Based Secure Voting System**.

We are highly thankful to our project guide and faculty members for their continuous encouragement, valuable suggestions, and technical guidance throughout the development of this work. Their expertise and motivation played a vital role in shaping this research.

We also extend our appreciation to the department and institution for providing the necessary facilities, resources, and laboratory support required for the implementation of the system.

Finally, we would like to thank our friends and family members for their constant support and cooperation, which helped us accomplish this work successfully.

7. REFERENCES

1. R. Ramya and S. Divya, "Biometric Based Electronic Voting System Using Fingerprint Recognition," *International Journal of Engineering Research & Technology (IJERT)*, vol. 4, no. 3, pp. 102–105,

2015.
2. S. A. Madankar and K. R. Ramteke, "Secure Electronic Voting System Using Biometrics," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 5, no. 4, pp. 1203–1207, 2016.
3. P. S. Patil and V. M. Wadhai, "Fingerprint Based Voting System," *International Journal of Scientific & Engineering Research (IJSER)*, vol. 7, no. 5, pp. 451–455, 2016.
4. A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.
5. N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing Security and Privacy in Biometrics-Based Authentication Systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.