International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.010 ISSN: 2581-4621

Biometric-Based Secure Voting System to Reduce Vote Rigging

Mrs D. Anusha[1], P. Sai Kiran[2], S. Rupak[3], V. Ram Charan[4], Ch. Manideepak[5]
Dept. of AI & DS, Vidya Jyothi Institute of Technology, Hyderabad, India

***Abstract*—**The **Biometric Secured Voting System to Reduce Vote Rigging** is designed to enhance the security, transparency, and reliability of the electoral process by integrating biometric authentication with modern database technologies. Traditional voting systems often face challenges such as impersonation, duplicate voting, and lack of strong identity verification, which can compromise the integrity of elections. This project addresses these issues by implementing a secure voting mechanism based on unique biometric identification.
In this system, each voter is registered with a unique fingerprint ID, which is used for authentication during the voting process.
The system ensures that only authorized voters can cast their vote and strictly enforces the principle of "one person–one vote" by preventing multiple voting attempts through a vote-lock mechanism. The backend of the system is implemented using **Python**, while MongoDB is used as the database to store voter information, candidate details, and voting records efficiently.
The system is divided into modules such as voter registration, authentication, vote casting, and result generation. Once a vote is cast, it is securely stored in the database, and the vote count is automaticallyupdated using efficient database operations. The results are generated instantly, reducing manual effort and minimizing errors.
The proposed system demonstrates a simple yet effective approach to reducing vote rigging and improving trust in the voting process. Although biometric authentication is simulated in this project, it provides a strong foundation for real- world implementation with actual biometric devices. With further enhancements such as multi-factor authentication and blockchain integration, the system can be extended to support large-scale, highly secure election environments

***Keywords*—** Biometric Authentication , Secure Voting System, Electronic Voting (E-Voting),Vote Rigging Prevention, Fingerprint Identification, One Person One Vote, Voter Verification, Database Management, MongoDB, Python, NoSQL Database, Data Security, Authentication System, Digital Voting, Election Integrity

I. INTRODUCTION

In a democratic society, the integrity and transparency of the electoral process are fundamental to ensuring fair governance and public trust. Traditional voting systems, including paper-based ballots and early electronic voting machines, have been widely used for decades; however, they often suffer from critical challenges such as impersonation, multiple voting, vote rigging, and lack of robust identity verification mechanisms. These vulnerabilities can significantly affect the credibility of election results and undermine democratic principles.
With the rapid advancement of technology, there is a growing need for a more secure, efficient, and reliable voting system that can address these issues effectively. One promising approach is the integration of biometric authentication techniques into the voting process. Biometric systems use unique physiological or behavioral characteristics, such as fingerprints, iris patterns, or facial features, to verify the identity of individuals. Among these, fingerprint recognition is one of the most widely adopted methods due to its accuracy, reliability, and ease of implementation.
The proposed **Biometric Secured Voting System to Reduce Vote Rigging** leverages biometric authentication to ensure that only eligible voters can participate in the election process. In this system, each voter is assigned a unique fingerprint ID during registration, which is used for authentication at the time of voting. This mechanism enforces the principle of "one person–one vote" by preventing unauthorized access and eliminating duplicate voting attempts.
The system is implemented using **Python** for backend logic and MongoDB for data storage and

DOI:10.46647/ijetms.2026.v10i03.010 ISSN: 2581-4621

management. MongoDB provides a flexible and scalable NoSQL architecture, enabling efficient handling of voter data, candidate information, and voting records. The system is designed with modular components, including voter registration, authentication, vote casting, and result generation, ensuring ease of development, maintenance, and scalability.

Furthermore, the proposed system enhances the speed and accuracy of election results by automating vote counting and minimizing human intervention. Although the current implementation uses a simulated biometric approach, it establishes a strong foundation for future integration with real biometric devices and advanced security mechanisms such as encryption and blockchain technology.

In conclusion, this research aims to develop a secure and efficient voting system that reduces vote rigging and enhances trust in the electoral process. By combining biometric authentication with modern database technologies, the system offers a practical solution for improving election security and reliability in both small-scale and large-scale voting environments.

B. Theoretical Background

The development of a **Biometric Secured Voting System to Reduce Vote Rigging** is grounded in several key theoretical concepts, including biometric authentication, electronic voting systems, database management, and data security principles. These concepts collectively form the foundation for designing a secure, reliable, and efficient voting system.

1. Biometric Authentication

Biometric authentication is based on the identification and verification of individuals using unique biological characteristics such as fingerprints, iris patterns, or facial features. Among these, fingerprint recognition is one of the most widely used techniques due to its high accuracy and low cost. The theoretical basis of biometric systems lies in the uniqueness and permanence of biological traits, which ensures that each individual can be uniquely identified.

In the proposed system, a fingerprint ID (simulated) is used to represent the biometric identity of a voter. The authentication process involves matching the provided fingerprint ID with the stored data in the database. This ensures that only authorized individuals can participate in the voting process and eliminates the risk of impersonation.

2. Electronic Voting Systems (E- Voting)

Electronic voting systems aim to replace traditional paper-based voting methods with digital platforms that improve efficiency, accuracy, and speed. The theoretical principles of e-voting include:

- **Authentication** – verifying the identity of voters
- **Authorization** – allowing only eligible voters to vote
- **Integrity** – ensuring that votes are not altered
- **Confidentiality** – protecting voter privacy
- **Non-repudiation** – preventing denial of voting activity

The proposed system satisfies these principles by integrating biometric authentication and implementing a vote- lock mechanism to enforce the “one person–one vote” rule.

3. Database Management Systems

A database management system (DBMS) is essential for storing, managing, and retrieving data efficiently. The system uses MongoDB, a NoSQL database that stores data in the form of JSON-like documents. Unlike traditional relational databases, MongoDB provides flexibility, scalability, and high performance.

The theoretical advantage of NoSQL databases lies in their schema-less structure, which allows dynamic storage of voter and voting data. Collections such as voters, candidates, and votes are used to organize the data logically and efficiently.

4. Data Security and Integrity

Security is a critical aspect of any voting system. The theoretical framework for data security includes:

- **Authentication mechanisms** to verify user identity

- **Access control** to restrict unauthorized actions
- **Data integrity** to ensure accurate and unaltered information
- **Encryption techniques** to protect sensitive data

In the proposed system, security is achieved through biometric verification and database-level safeguards. The use of a has_voted flag ensures that each voter can cast a vote only once, thereby maintaining data integrity.

5. One Person–One Vote Principle

A fundamental concept in democratic systems is the principle of "one person– one vote," which ensures equality in the voting process. The proposed system enforces this principle through a vote-lock mechanism. Once a voter casts a vote, their status is updated in the database, preventing any further voting attempts.

6. System Modeling Concepts

The system follows a modular design approach, where different functionalities such as registration, authentication, voting, and result generation are implemented as separate modules. This modular structure improves maintainability, scalability, and ease of implementation.

II. LITERATURE SURVEY

The development of secure electronic voting systems has been widely explored by researchers, with a strong focus on improving authentication, security, and transparency. Early studies by A. K. Jain et al. highlighted the effectiveness of biometric authentication, particularly fingerprint recognition, due to its uniqueness and reliability in identifying individuals. Building on this, several researchers proposed biometric-based voting systems to eliminate impersonation and ensure that only authorized voters can participate. Studies such as those by D. Ashok Kumar and T. Ummal Sariba Begum demonstrated that fingerprint- based voting systems significantly reduce fraudulent activities and enhance voter verification. Additionally, research on electronic voting security by R. Mercuri and S. Wolchok et al. identified vulnerabilities in traditional and electronic voting machines, emphasizing the need for stronger authentication mechanisms and secure system design. Cryptographic approaches introduced by D. Chaum further contributed to secure voting by ensuring vote confidentiality and integrity, although their complexity limits practical implementation. With advancements in data management, modern systems have started adopting NoSQL databases such as MongoDB for efficient and scalable data storage. Despite these advancements, existing systems still face challenges such as duplicate voting, limited scalability, and security risks. The proposed system addresses these issues by integrating biometric authentication with a secure
vote-lock mechanism and efficient database management, thereby providing a reliable and scalable solution to reduce vote rigging.

III. METHODOLOGY

The proposed **Biometric Secured Voting System to Reduce Vote Rigging** is developed using a modular and systematic approach that integrates biometric authentication with efficient database management. Initially, voters are registered in the system by storing their personal details along with a unique fingerprint ID (simulated) in the database, with an initial voting status set to false.
During the voting phase, the system performs biometric authentication by verifying the entered fingerprint ID against the stored records, ensuring that only authorized users can access the system.
Once authenticated, the voter is presented with a list of candidates and allowed to cast a vote, which is recorded in the database. Simultaneously, the vote count of the selected candidate is updated, and the voter's status is changed to indicate that they have already voted, thereby enforcing the "one person–one vote" principle and preventing duplicate voting. The system utilizes MongoDB to store voter information, candidate details, and voting records in a flexible and scalable manner. Finally, the system generates results automatically by aggregating the votes stored in the database, providing accurate and real-time output without manual intervention. This methodology ensures a secure, efficient, and reliable voting process.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.010 ISSN: 2581-4621

IV. SYSTEM DESIGN

The **Biometric Secured Voting System to Reduce Vote Rigging** is designed using a modular and layered architecture to ensure security, scalability, and efficient operation. The system integrates biometric authentication, database management, and application logic to provide a secure and reliable voting process. The overall design focuses on ensuring accurate voter identification, preventing duplicate voting, and enabling real-time result generation.

1. Architecture Overview

The system follows a **three-layer architecture**:

- **Presentation Layer** – Provides the user interface for voter interaction, including registration, authentication, and voting operations.
- **Application Layer** – Implements the core logic of the system such as authentication, vote validation, and vote processing.
- **Database Layer** – Stores and manages all data related to voters, candidates, and votes.

The interaction between these layers ensures smooth data flow and system functionality.

2. Module Design

The system is divided into the following modules:

a. Voter Registration Module

This module collects voter details and assigns a unique fingerprint ID. The information is stored in the database with a default voting status to indicate that the voter has not yet voted.

b. Authentication Module

This module verifies the identity of the voter using the fingerprint ID. It compares the input with stored records to ensure only valid voters are allowed to proceed.

c. Voting Module

After authentication, the voter is presented with a list of candidates. The selected vote is recorded in the database, and the candidate's vote count is updated.

d. Vote Lock Mechanism

This module ensures that each voter can vote only once. After casting a vote, the system updates the voter's status, preventing any further voting attempts.

e. Result Generation Module

This module calculates the total votes for each candidate and displays the results instantly using database aggregation.

3. Database Design

The system uses MongoDB, which organizes data into collections instead of tables. The main collections include:

- **voters** – stores voter details and voting status
- **candidates** – stores candidate information and vote count
- **votes** – stores individual vote records

MongoDB's flexible schema allows efficient storage and scalability, making it suitable for large-scale applications.

3. Data Flow Design

The system follows a structured data flow:

Input (voter details/fingerprint) → Authentication → Vote Selection → Database Update → Result Output

This flow ensures that each step is validated and securely processed.

5. Security Design

Security is a critical aspect of the system design. The system ensures:

- Unique identification through biometric authentication
- Prevention of duplicate voting using the vote-lock mechanism

DOI:10.46647/ijetms.2026.v10i03.010 ISSN: 2581-4621

- Data integrity through controlled database operations
- Restricted access to authorized users only

6. System Workflow

The complete workflow of the system is as follows:

Voter Registration → Biometric Authentication → Vote Casting → Vote Lock → Result Generation

This workflow ensures a secure, efficient, and transparent voting process.

V. RESULTS

The proposed **Biometric Secured Voting System to Reduce Vote Rigging** was successfully implemented and evaluated to assess its performance, accuracy, and reliability. The system was tested under various scenarios, including voter registration, biometric authentication, vote casting, duplicate voting attempts, and result generation. The outcomes demonstrate that the system effectively meets its objective of providing a secure and transparent voting process.

During testing, multiple voters were registered with unique fingerprint IDs, and the system successfully stored all voter information in the database without duplication. The authentication module accurately verified voter identities by matching the provided fingerprint ID with the stored records. Valid users were granted access to vote, while invalid or unregistered users were denied access, ensuring secure authentication.

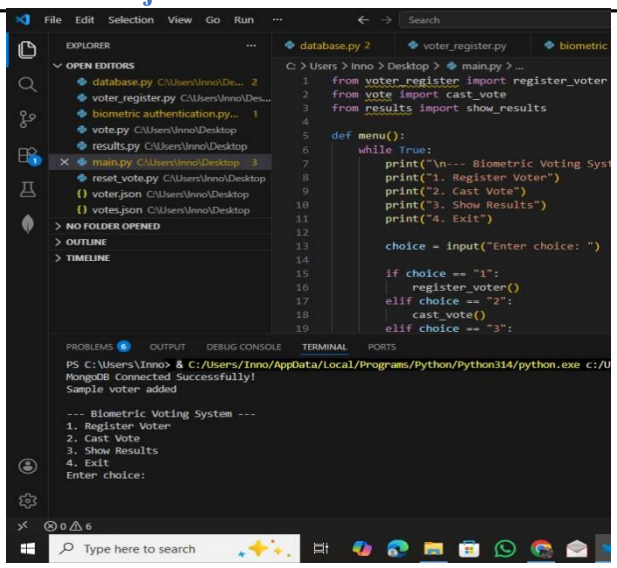
The voting module functioned efficiently by allowing authenticated voters to select their preferred candidate and cast their vote. Each vote was recorded in the database, and the corresponding candidate's vote count was updated in real time. The vote-lock mechanism was tested by attempting multiple votes from the same voter, and the system correctly prevented duplicate voting by displaying an appropriate message indicating that the voter had already voted. This confirms the successful enforcement of the "one person–one vote" principle.

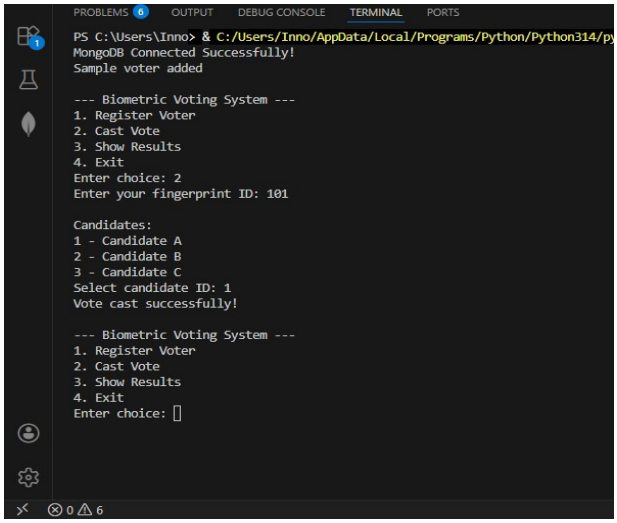
The system utilized MongoDB for data storage, which provided fast and reliable data handling. The database efficiently managed voter details, candidate information, and voting records, ensuring consistency and scalability. The result generation module automatically calculated the total votes for each candidate and displayed accurate results instantly, eliminating the need for manual counting and reducing human errors.

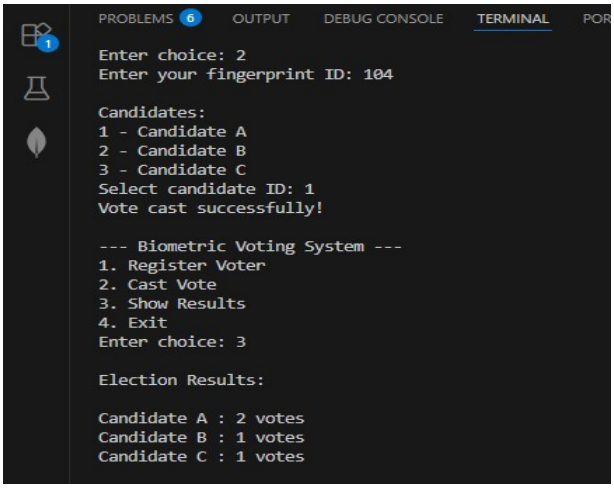
Performance analysis indicates that the system provides quick authentication, efficient vote processing, and real-time result generation. The accuracy of voter identification and vote counting was observed to be high, and the system successfully prevented fraudulent activities such as impersonation and duplicate voting. However, it is noted that the current implementation uses a simulated biometric approach, and real-world deployment would require integration with actual biometric devices.

In conclusion, the results confirm that the proposed system is effective in enhancing election security, improving transparency, and reducing vote rigging. The system demonstrates reliability, scalability, and efficiency, making it a suitable solution for modern electronic voting applications.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.010 ISSN: 2581-4621







VI. CONCLUSION

The **Biometric Secured Voting System to Reduce Vote Rigging** successfully demonstrates how modern technologies can be utilized to enhance the security, transparency, and reliability of the electoral process. The primary objective of this project was to address the critical issues present in traditional and electronic voting systems, such as **impersonation, duplicate voting, and lack of strong authentication mechanisms**.

By integrating **biometric authentication**, specifically fingerprint-based verification, the system

DOI:10.46647/ijetms.2026.v10i03.010 ISSN: 2581-4621

ensures that each voter is uniquely identified. This approach effectively enforces the principle of **"one person–one vote"**, thereby eliminating the possibility of multiple voting and reducing fraudulent activities. The use of **MongoDB**, a NoSQL database, provides efficient and scalable data storage, enabling the system to handle large volumes of voter information and voting records with high performance and reliability.

The implementation using **Python and PyMongo** demonstrates that the system is not only secure but also simple and efficient to develop. The modular design of the system, including registration, authentication, voting, and result generation modules, ensures smooth operation and easy maintainability.

Additionally, the automatic vote counting mechanism reduces human intervention, minimizes errors, and provides quick and accurate results.

The results obtained from the system confirm that the proposed solution effectively prevents duplicate voting, ensures secure authentication, and improves the overall efficiency of the voting process. Although the current implementation uses a simulated biometric approach, it clearly establishes a strong foundation for real-world deployment with actual fingerprint devices.

In conclusion, the proposed system provides a **robust, scalable, and secure voting solution** that significantly reduces vote rigging and enhances trust in the electoral process. With further improvements and integration of advanced technologies, this system has the potential to be implemented in real-time election environments, contributing to a more transparent and trustworthy democratic system.

REFERENCES

[1] **D. Ashok Kumar and T. Ummal Sariba Begum**, "A Novel Design of Electronic Voting System Using Fingerprint," *International Journal of Advanced Research in Computer Engineering & Technology*, 2013.

[2] **K. Prasad, K. Ramakrishna, and S. S. Babu**, "Biometric Based Electronic Voting System Using Fingerprint Recognition," *International Journal of Scientific and Engineering Research*, 2014.

[3] **A. Jain, A. Ross, and S. Prabhakar**, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, 2004.

[4] **NIST (National Institute of Standards and Technology)**, "Biometric Data Security Guidelines,"Available: https://www.nist.gov/

[5] **S. Nakamoto**, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. (Referenced for blockchain-based future voting systems)

[6] **OWASP Foundation**,"Web Application Security Guidelines," Available: https://owasp.org/

[7] D. Chaum "Secret-Ballot Receipts: True Voter-Verifiable Elections," *IEEE Security & Privacy*, 2004.