Volume 11, Issue 4, April – 2026 International Journal of Innovative Science and Research Technology
ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26apr1534

E-Voting System in India and its Challenges

Soumyadip Mukherjee[1]; Soumen Bhowmik[2]

[1]Research Scholar M. Tech, CSE, Bengal Institute of Technology and Management Santiniketan, Birbhum, India
[2]Assistant Professor, Department of CSE, Bengal Institute of Technology and Management Santiniketan, Birbhum, India

Publication Date: 2026/05/08

Abstract: This research paper is studies a secure web-based e-voting system for India and also focusing on proper authentication and data protection. The system uses biometric checking and encryption to ensure only valid voters can cast their own votes, and that results remain confidential. Compared with traditional voting systems, the web-based approach offers better security, efficiency, and accessibility. While current testing relies on simulated data, future work will integrate real election datasets and advanced cryptographic methods. The study shows that secure online voting can strengthen the trust and participation in India's democratic process.

Keywords: *Electronic Voting Machines, Cryptographic Techniques, CAPTCHA, Cyber-Attacks, ERP.*

How to Cite: Soumyadip Mukherjee; Soumen Bhowmik (2026) E-Voting System in India and its Challenges. *International Journal of Innovative Science and Research Technology*, 11(4), 3609-3611. https://doi.org/10.38124/ijisrt/26apr1534

I. INTRODUCTION

The conduct of elections in India has evolved significantly over the decades. Initially, paper ballots were employed, but this method was plagued by inefficiencies such as delayed result processing, ballot tampering, and high operational costs. To overcome these challenges, the Election Commission of India introduced Electronic Voting Machines (EVMs), which streamlined the process and improved transparency. However, EVMs still require voters to physically visit polling stations, limiting accessibility and convenience in a digital era.

To address these limitations, researchers have proposed various electronic voting systems leveraging modern technologies. Cloud-based voting systems have been explored for managing large-scale elections and securely handling voter data [1]. Cryptographic techniques have been emphasized to ensure vote secrecy and system integrity [2]. Secure online voting systems incorporating authentication mechanisms such as OTP and CAPTCHA have also been proposed [3]. More recently, virtual voting systems have enabled remote participation while maintaining security through digital verification technologies [4].

Despite these advancements, the challenge of ensuring both security and authenticity in remote voting remains paramount. Several studies highlight the importance of encryption algorithms, secure communication protocols, and robust authentication mechanisms [6, 7]. Against this backdrop, the present study focuses on a comparative analysis of web-based secure e-voting systems with proper authentication.

This research emphasizes the development of a secure e-voting application using .NET framework and SQL Server database, integrating biometric authentication mechanisms such as fingerprint and face recognition. By combining web-based accessibility with advanced biometric verification, the proposed system aims to enhance transparency, efficiency, and trust in the electoral process, while ensuring that only legitimate voters can participate.

II. LITERATURE REVIEW

Modern e-voting systems employ encryption [3] to secure ballots and voter data. However, many implementations still face challenges in achieving complete end-to-end security, particularly against sophisticated cyber-attacks and insider threats. Stronger cryptographic frameworks are required to ensure confidentiality, integrity, and non-repudiation throughout the voting process.

A critical weakness in existing systems is the lack of robust, real-time authentication [2]. Conventional methods such as passwords, OTPs, or CAPTCHAs provide only limited assurance of voter identity. These approaches are vulnerable to phishing, credential theft, and replay attacks, which compromise the reliability of the voting process.

Most current e-voting solutions operate as standalone applications without integration into enterprise-level ERP architectures [1]. This absence of ERP-based design reduces scalability, hampers centralized data management, and limits the ability to streamline workflows in large-scale elections.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26apr1534

While G. Kumar et al [4] shows that some systems incorporate basic authentication but due to that some comprehensive multi-factor authentication (MFA) is often missing. The absence of layered verification mechanisms weakens voter identity assurance and increases the risk of unauthorized access.

Henry O. Ohize [5] designed a blockchain-based e-voting framework to modernize electoral processes and strengthen voter trust. By leveraging distributed ledger technology, the system ensures immutability, transparency, and auditability of votes, while advanced cryptographic techniques safeguard privacy and integrity. Emphasis is placed on scalability and performance, enabling reliable deployment in large-scale elections. The framework addresses key challenges such as cybersecurity risks and infrastructure demands, while pointing to future research in optimizing blockchain algorithms and integrating stronger cryptographic methods. Ultimately, it offers a pathway toward secure, transparent, and inclusive democratic systems.

III. RESEARCH APPROACH AND SYSTEM METHODOLOGY

➢ *Overview*

A secure e-voting system consist multiple modules designed to ensure proper voter authentication, secure vote storage, and accurate result processing. The system architecture also ensures transparency, accessibility, and data integrity through encryption and multi-factor authentication mechanisms.

➢ *System Flow*

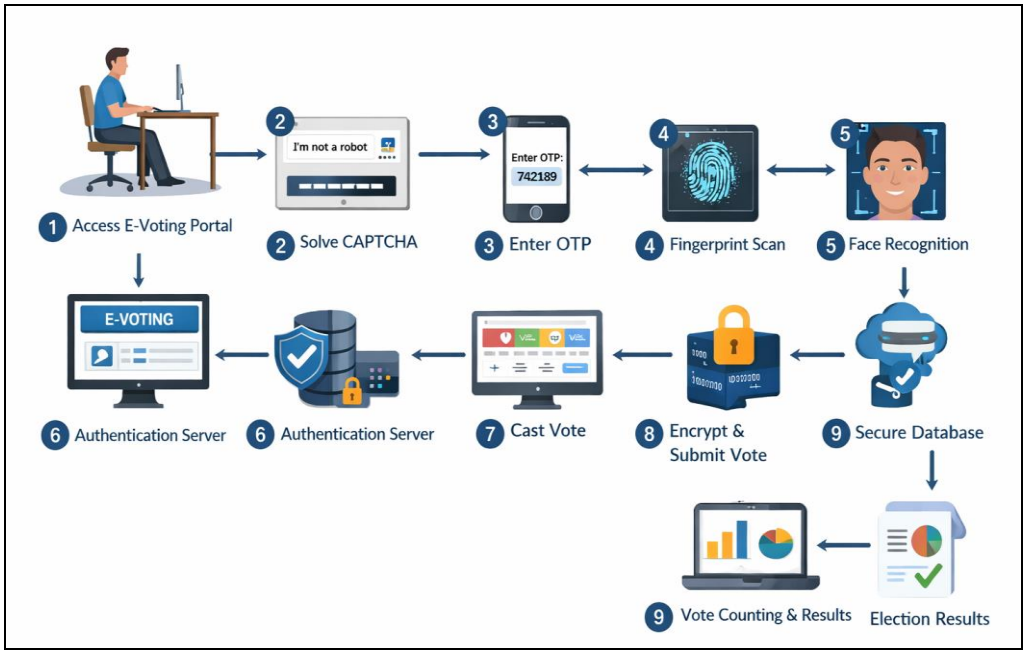

Fig 1 Flow Diagram of the System

In the above figure the secure e-voting process begins with the voter accessing the e-voting portal and logging in using their user ID, password, and voter ID details. For added security, CAPTCHA and OTP verification are required. The authentication server then validates the voter through biometric methods such as fingerprint or face recognition.

➢ *System Modules*

- *Voter Registration Module:*

This module securely stores voter details in the database in the form of a unique identification number linked to biometric data (fingerprint and facial features) of each voter is assigned before the election. The registration process ensures that only legitimate voters are enrolled.

- *Authentication Module:*

The authentication process involves CAPTCHA verification, OTP validation, and biometric authentication (fingerprint and face recognition). These layers collectively prevent unauthorized access and impersonation.

- *Voting Module:*

Once authenticated, the voter accesses the web-based voting interface developed using ASP.NET. The voter selects a candidate by the symbol assigned to the candidate by the election commission, and the vote is encrypted using AES-256 before submission.

- *Vote Storage Module:*

Encrypted votes are stored in a SQL Server cloud database. The system maintains audit logs and ensures data confidentiality through encryption and secure communication protocols (SSL/TLS).

- *Result Processing Module:*

The stored votes are decrypted and tallied securely. The system validates the integrity of each vote before generating the final election results.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26apr1534

Once authentication is successful, the voter is directed to the voting interface, where they can view candidates and cast their vote. The submitted vote is encrypted and stored securely in the database server. Finally, the result processing system decrypts and counts the votes, producing the official election results. This flow ensures end-to-end security, starting from voter authentication to the publication of verified results.

IV. COMPARATIVE ANALYSIS AND DISCUSSION

Table 1 Comparative Analysis of Voting Systems

Voting System	Advantages	Limitations	Authentication Mechanism	Security Level
Paper Ballot System	Simple, transparent, easy to understand	Slow counting, human errors, risk of ballot tampering	Manual verification (ID cards, voter lists)	Low
Electronic Voting Machine	Faster counting, reduced invalid votes, easy result tabulation	Requires physical presence, limited auditability	Basic authentication (voter ID, polling officer check)	Medium
Online Voting System	Remote voting, high accessibility, convenient for users	Vulnerable to cyber-attacks, privacy concerns	Username/password, OTP	Medium to High
Cloud-Based E-Voting	Scalable, centralized management, real-time monitoring	Requires strong security, dependent on network and cloud infrastructure	Multi-factor authentication, biometric verification	High (if properly secured)

The traditional paper ballot system ensured transparency but suffered from slow result processing and high operational costs. The introduction of Electronic Voting Machines (EVMs) improved efficiency and reduced invalid votes but still required voters to be physically present at polling stations. To overcome these limitations, online voting systems have been proposed to enable remote participation, enhancing accessibility. However, these systems face challenges related to cyber security and data protection. The proposed cloud-based e-voting system integrates encryption, biometric authentication, and secure database management to address these issues, ensuring both scalability and security.

The comparative analysis demonstrates that while each voting system has its own advantages and limitations, a cloud-based web e-voting system with multi-factor biometric authentication provides a more scalable, accessible, and secure approach. Although challenges such as cyber security threats and privacy concerns remain, continuous advancements in authentication technologies and security protocols can effectively address these issues.

V. CONCLUTION

The electronic voting system represents a significant advancement in modern electoral processes, particularly in a populous country like India where managing millions of voters poses considerable logistical and security challenges. Presently uses voting methods, including paper ballots and Electronic Voting Machines (EVMs), have contributed to improving efficiency; however, they still face limitations in terms of accessibility, transparency, and security.

This study highlights that web-based secure e-voting systems, when integrated with proper authentication mechanisms, offer a promising solution to these challenges. Technologies such as fingerprint recognition and facial recognition enhance voter verification by ensuring that only authorized individuals can cast their votes, thereby reducing the risk of fraud and impersonation. Additionally, the use of encryption techniques and secure cloud infrastructure strengthens data integrity, confidentiality, and system reliability.

In conclusion, the adoption of a web-based secure e-voting system with fingerprint and facial recognition has the potential to revolutionize the electoral process by making it more transparent, efficient, and trustworthy. Future developments should focus on enhancing security frameworks, ensuring user privacy, and increasing public trust in digital voting systems.

REFERENCES

[1]. P. K. Malviya, “E-Voting System Using Cloud in Indian Scenario,” International Journal of Engineering Science & Advanced Technology.
[2]. G. Ofori- Dwumfuo and E. Paatey, “The Design of an Electronic Voting System,” Research Journal of Information Technology, 2011.
[3]. A. Nadaph, R. Bondre, A. Katiyar, D. Goswami, and T. Naidu, “Secure Online Voting System,” International Journal of Engineering Research and General Science, 2015.
[4]. G. Kumar et al., “Virtual Voting System,” International Journal of Informatics Information System and Computer Engineering, 2021”.
[5]. Henry O. Ohize, “Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges”.
[6]. Masood Ahmad, “Security, usability, and biometric authentication scheme for electronic voting using multiple keys”.
[7]. Dr. David Jefferson, “Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)”.