ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(b) Jan – Feb 2026

Original Research Article

DIGITAL-BASED ANTI-BOGUS VOTING SYSTEM FOR ENHANCING SECURITY AND TRANSPARENCY IN INDIAN ELECTIONS

** Vighnesh Sushil Rane & ** Hemangi Rane*

** Student, MSC Computer Science part-2, Department of Computer Science & IT, B. K. Birla College, kalyan, ** Assistant Professor, Department of Computer Science & IT, B.K. Birla College, (Empowered Autonomous Status), Kalyan.*

Abstract:

India, as the world's largest democracy, relies on a constitutionally governed electoral system to ensure free and fair elections. While Electronic Voting Machines have improved efficiency, concerns regarding bogus voting, duplicate or repeated entries, impersonation, and unauthorized access continue to affect public perception of electoral transparency. Strengthening digital verification mechanisms has become essential to enhance voter trust and system integrity. This study examines a digital-based anti-bogus voting system aimed at improving security and transparency in Indian elections. The system emphasizes structured voter authentication, identity validation, and controlled vote-casting mechanisms to minimize fraudulent practices. By integrating secure digital verification processes within the existing electoral structure, the system supports sustainable electoral governance and reduces opportunities for malpractice. The study further analyses the public perception regarding digital authentication in elections which will highlight the potential of technology- driven solutions in reinforcing democratic trust and institutional credibility.

Keywords: *EVM, Blockchain technology, Digital Literacy, Biometric validation*

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0) which permits unrestricted use, distribution, and reproduction in any medium for non-commercial Use Provided the Original Author and Source Are Credited.

Introduction:

India, recognized as the world's largest democracy, conducts elections on a massive scale under a constitutionally structured electoral framework. The integrity of this system is fundamental to maintaining democratic stability, public trust, and institutional legitimacy. Over the years, the adoption of Electronic Voting Machines has significantly enhanced efficiency, speed, and logistical management of elections[1]. However, despite technological advancements, concerns related to bogus voting, impersonation, duplicate voter registration, and unauthorized voting attempts continue to influence public perception regarding electoral transparency and security. In an increasingly digital era, the demand for stronger verification mechanisms and tampering the systems has become more prominent. Citizens expect not only efficiency but also accountability, traceability, and transparency in electoral processes. Strengthening election infrastructure through advanced digital technologies is therefore essential to ensure sustainable democratic governance. One of the most transformative technologies capable of reinforcing electoral transparency is blockchain technology. Blockchain technology is a decentralized, distributed ledger mechanism where the transaction records are hold permanently across a network of computers[2, 3]. Due to its immutable and tamper-resistant nature, blockchain offers a

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(b) Jan – Feb 2026

Original Research Article

transparent audit trail that cannot be altered without network-wide consensus. In the context of elections, this feature becomes highly significant, as it enables secure vote recording, prevents unauthorized data modification, and enhances traceability without compromising voter anonymity[4] .

The integration of blockchain within a digital-based anti-bogus voting system introduces a dual layer of security. First, structured digital identity verification mechanisms—such as authenticated voter databases and controlled vote-casting access—help prevent duplicate and unauthorized voting. Second, blockchain ensures that once a vote is recorded, it remains immutable and verifiable, thereby minimizing risks of manipulation or post-election tampering. This combination strengthens both preventive and protective dimensions of electoral security[5].

Furthermore, digital authentication frameworks supported by cryptographic validation mechanisms can enhance public confidence in election outcomes. By reducing manual intervention and increasing automated verification processes, the electoral system becomes more transparent, accountable, and resilient. The incorporation of blockchain does not replace existing EVM infrastructure but complements it by adding a secure verification and audit layer.

In light of growing global discourse on digital democracy and election security, there is a pressing need to explore technology-driven models that enhance electoral governance without compromising inclusivity or constitutional principles. This study examines a digital-based anti-bogus voting system that integrates structured identity verification and blockchain-backed security mechanisms to strengthen transparency and prevent electoral malpractice in Indian elections.

By focusing on digital authentication, controlled vote validation, and blockchain-enabled transparency, the study aims to contribute to sustainable and secure electoral governance in India. The findings further assess public perception regarding digital election security measures, thereby bridging technological innovation with democratic accountability.

Problem Statement:

Free and fair elections form the foundation of democratic governance in India. Although the electoral process has evolved through the adoption of Electronic Voting Machines (EVMs), concerns related to electoral integrity continue to influence public perception. Issues such as bogus voting, duplicate voter registration, impersonation, unauthorized voting attempts, and alleged data manipulation raise questions regarding the robustness of verification and monitoring mechanisms within the electoral system.

While EVMs enhance operational efficiency and reduce manual counting errors, they primarily focus on vote recording rather than comprehensive digital authentication and tamper-proof audit validation. The absence of an integrated digital verification layer capable of ensuring real-time identity validation and immutable record storage creates perceived vulnerabilities. In large-scale elections involving millions of voters, even minor gaps in verification processes can impact public trust and institutional credibility.

Another critical challenge lies in balancing transparency with security. Electoral systems must protect voter anonymity while simultaneously ensuring that each eligible citizen casts only one valid vote. Achieving this balance requires advanced technological mechanisms that can authenticate voters, prevent duplicate entries, and

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(b) Jan – Feb 2026

Original Research Article

securely record voting activity without exposing personal data.

Moreover, in the context of increasing digital transformation across governance sectors, citizens expect higher standards of accountability and traceability. Traditional verification processes, when not digitally reinforced, may struggle to meet these evolving expectations. The absence of cryptographically secured immutable audit trails further limits the ability to provide transparent verification without relying heavily on centralized control mechanisms.

Blockchain technology presents potential advantages in addressing these concerns due to its decentralized architecture, cryptographic validation, and tamper-resistant record-keeping capabilities[6]. However, its structured integration within the electoral framework remains limited in practical application. There is a need to examine how digital-based authentication mechanisms combined with blockchain-backed security can strengthen electoral transparency while maintaining constitutional integrity[7]. Therefore, the core problem addressed in this study is the lack of a comprehensive digital-based anti-bogus voting system that integrates secure identity verification and blockchain-enabled audit mechanisms to enhance electoral security, prevent fraudulent practices, and improve public trust in Indian elections.

Significance of the Study:

The integrity of electoral systems directly influences democratic stability, institutional credibility, and citizen trust. In a country like India, where elections are conducted at an unprecedented scale, ensuring transparency and security within the voting process is of paramount importance. This study holds significance as it addresses growing concerns related to bogus voting, impersonation, duplicate registrations, and unauthorized voting attempts through a structured digital-based solution.

From a governance perspective, the research contributes to the evolving field of digital electoral administration by emphasizing the importance of secure identity authentication and transparent verification mechanisms. By examining the integration of digital validation processes with blockchain-backed record systems, the study highlights how modern technological tools can strengthen accountability without compromising voter anonymity.

Technologically, the study underscores the relevance of blockchain as a tamper-resistant and decentralized audit layer within electoral systems. Blockchain's immutable ledger structure enhances traceability, reduces the possibility of data manipulation, and builds confidence in the finality of recorded votes[8]. The research demonstrates how combining digital authentication with blockchain infrastructure can provide multi-layered security to electoral processes. This study is significant because public trust is a critical component of democratic participation. Perceived vulnerabilities in election systems can reduce voter confidence and participation levels [9]. By exploring a secure digital-based anti-bogus voting system, the research aims to contribute toward improving transparency and reinforcing citizen trust in electoral outcomes.

Academically, this study contributes to interdisciplinary research at the intersection of digital governance, cybersecurity, blockchain technology, and democratic systems. It provides a structured framework that can serve as a foundation for further empirical research, policy evaluation, and technology-driven electoral reforms.

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(b) Jan – Feb 2026

Original Research Article

Furthermore, the study aligns with the broader objective of sustainable governance by promoting systems that reduce manual intervention, enhance automation, and establish long-term institutional resilience. As nations increasingly adopt digital governance mechanisms, developing secure, transparent, and scalable election systems becomes essential for future democratic sustainability.

Objectives of the Study:

The main objective of this study is to examine how a digital-based anti-bogus voting system can improve security and transparency in Indian elections using blockchain technology. The study focuses on understanding existing challenges in the electoral process and exploring how structured digital verification and blockchain technology can help reduce fraudulent practices.

The specific objectives of the study are:

1. To identify major concerns related to bogus voting, duplicate voter registration, impersonation, and unauthorized voting in elections.
2. To analyse the need for stronger digital authentication mechanisms within the existing electoral framework.
3. To examine the role of blockchain technology in enhancing transparency, data security, and tamper- resistant vote recording.
4. To evaluate public perception regarding the use of digital verification systems in elections.
5. To study whether integrating secure digital-based mechanisms can increase voter trust and confidence in the electoral process.
6. To assess how digital security measures can contribute to sustainable and transparent electoral governance.
7. To explore practical measures that can strengthen election monitoring while maintaining voter privacy and constitutional integrity.

These objectives guide the research in analysing both the technological and governance aspects of election security. The study aims to connect digital innovation with democratic responsibility, ensuring that technological solutions are aligned with public trust and institutional stability.

Hypothesis of the Study:

To analyze the relationship between digital security mechanisms and electoral transparency, the following hypotheses are formulated:

Hypothesis 1

$H0_1$: Digital-based authentication mechanisms do not significantly influence public trust in the electoral process.

$H1_1$: Digital-based authentication mechanisms significantly influence public trust in the electoral process.

Hypothesis 2

$H0_2$: The integration of blockchain technology does not significantly enhance transparency in elections.

$H1_2$: The integration of blockchain technology significantly enhances electoral transparency.

These hypotheses will be tested using primary data collected through a structured survey questionnaire. The data will be analyzed to evaluate the effectiveness of digital security mechanisms in improving electoral transparency and minimizing fraudulent voting practices.

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(b) Jan – Feb 2026

Original Research Article

Review of Literature:

Rajeev D. V. et al. (2026) proposed a digital voting system that used face recognition for biometric voter authentication. Their study demonstrated that verifying voter identity before vote casting helped reduce impersonation and duplicate voting, while also improving transparency, efficiency, and reliability in the electoral process [10]. Abdul Feroz et al. proposed a secure electronic voting system that combined blockchain technology with machine learning to improve election security and transparency. The study used a permissioned blockchain for secure vote storage and smart contracts for vote verification, while machine learning techniques were applied to detect fraudulent patterns and suspicious voting activities. The proposed system demonstrated improved auditability, privacy protection, and resistance to common attacks in electronic voting systems [8].Mohammad Hajian Berenjestanaki et al. conducted a comprehensive review of blockchain- based electronic voting systems and analyzed their potential to improve transparency, security, and integrity in digital elections. Their study examined numerous research works and highlighted key benefits such as decentralization, auditability, and trustworthiness, while also identifying challenges related to privacy, usability, and scalability in implementing blockchain-based voting systems.[11]

Adewale Olumide S. et al. reviewed various electronic voting systems to identify the challenges and limitations associated with existing voting methods. Their study highlighted issues such as election fraud, impersonation, and vote rigging, and emphasized the need for more secure voting technologies. The authors also suggested the development of a secure e-voting system using fingerprint authentication and visual cryptographic techniques to improve election integrity [12]. Aishwarya Indapwar et al. proposed an e-voting system based on blockchain technology to address security issues associated with centralized electronic voting systems. Their study highlighted that blockchain enables decentralized data storage, which reduces the risk of hacking and data tampering. The proposed system demonstrated how blockchain can improve transparency, reliability, and accuracy in the vote counting process.[13]

Research Methodology:

This study adopts a descriptive and exploratory research design to examine the role of digital based security mechanisms in enhancing transparency and preventing bogus voting in Indian elections. The research focuses on understanding public perception regarding digital authentication systems and blockchain technology in the electoral process.

a. **Research Design :** The study is based on both primary and secondary data sources. Secondary data was collected from research articles, journals, and published studies related to online voting systems, blockchain technology, and digital election security. These sources helped in understanding global trends and technological developments in electoral systems. Primary data was collected through a structured questionnaire designed to assess public opinion regarding digital-based voting security mechanisms.
b. **Data Collection Method:** A survey method was used to gather responses from participants. The survey was distributed online to ensure easy accessibility and broader participation. The questionnaire

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(b)

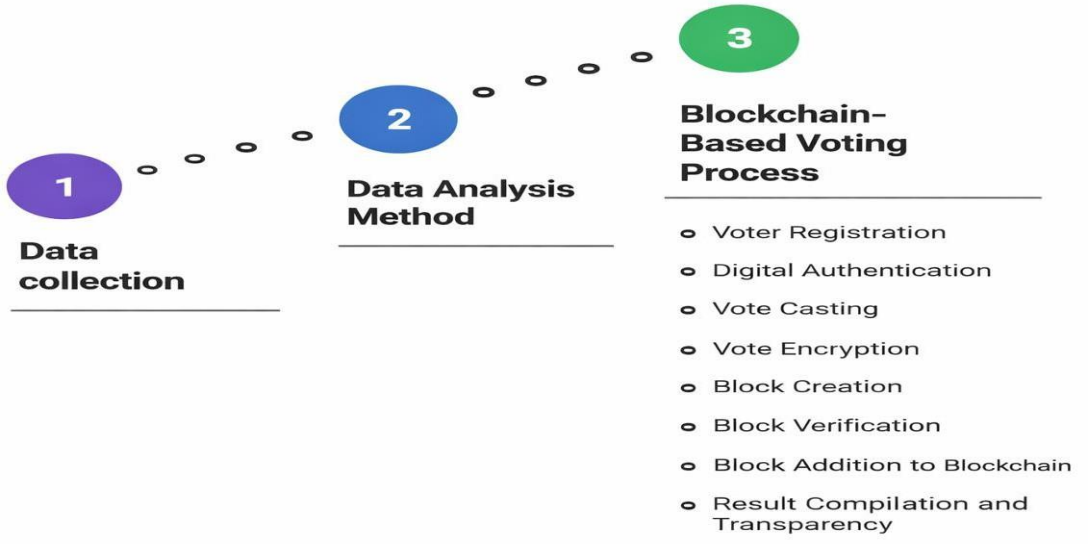
Jan – Feb 2026

Original Research Article

included multiple-choice and Likert-scale questions to measure perceptions related to: Trust in current voting systems , Concerns about bogus or duplicate voting, Support for digital identity verification, Perception of blockchain technology in elections, Opinion on transparency improvements .

c. **Data Analysis Method**: The collected data will be analysed using percentage analysis and descriptive statistics. Responses will be presented in the form of pie charts and tables to interpret public perception clearly. The hypotheses formulated in the study will be examined based on the majority of responses and observed trends.

d. **Use Blockchain Technology :** The proposed digital anti-bogus voting system integrates blockchain technology to enhance transparency, security, and reliability in the electoral process. Blockchain provides a decentralized and tamper-resistant ledger where voting records can be securely stored and verified.



This methodology enables the study to combine theoretical understanding with practical perception-based analysis, ensuring that the research findings are both academically structured and socially relevant.

Data Analysis and Interpretation:

A total of 22 respondents participated in the survey. The objective of the analysis was to understand public perception regarding digital-based electoral security mechanisms and the need for a secure digital voting framework[14]. The responses were analysed using percentage distribution and graphical representation.

1. **Trust the current Electronic Voting Machine (EVM) system:** Out of 22 respondents, 36.4% disagreed and 22.7% strongly disagreed with trusting the current EVM system. Around 27.3% remained neutral. Only 9.1% greed and 4.5% strongly agreed with the system.

   Interpretation: The findings indicate that a significant majority of respondents (approximately 59.1%) express low confidence in the current EVM system. This reflects existing concerns regarding transparency and verification processes. The result supports the need for enhanced digital safeguards and improved authentication mechanisms to strengthen public trust in elections.

ISSN: P-2455-0515
E- 2394-8450

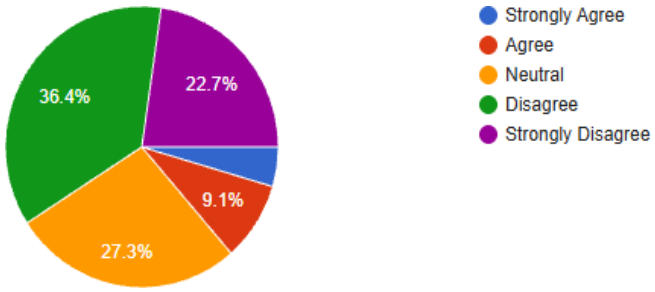
Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(b)

Jan – Feb 2026

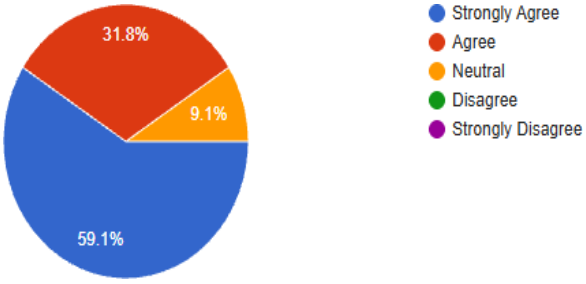
Original Research Article



2. ***Need for Stronger Digital Verification System***

More than 80% of respondents either Strongly Agree or Agree that stronger digital verification systems are required in elections. Very few respondents expressed neutrality or disagreement.

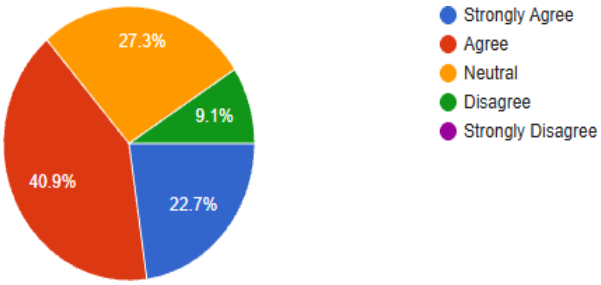
Interpretation: There is strong public support for the introduction of advanced digital verification methods in the electoral process.



3. ***OTP-Based Voter Authentication***

A majority of respondents (around 68%) agreed or strongly agreed that OTP-based voter authentication would increase trust in elections. Some respondents remained neutral, while very few disagreed.

Interpretation: This indicates that simple digital authentication methods like OTP verification are widely accepted and may enhance voter confidence.



4. ***A secure digital-based voting framework would improve transparency in elections***

Out of 22 respondents, 40.9% strongly agreed and 31.8% agreed that a secure digital-based voting framework would improve transparency in elections. Around 18.2% remained neutral, while 9.1% disagreed. No respondents selected strongly disagree.

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

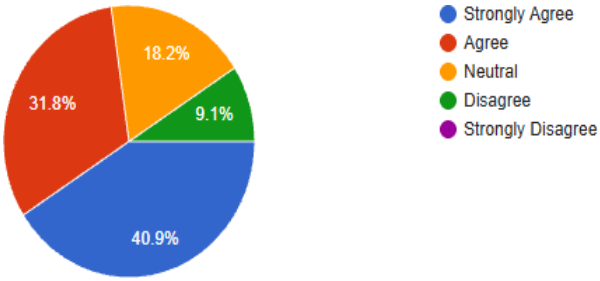
OPEN ACCESS

Volume–XIII, Special Issues–I(b)

Jan – Feb 2026

Original Research Article

Interpretation: The findings show that a strong majority (72.7%) support the idea that a secure digital-based framework can enhance transparency in elections. This reflects positive public perception toward digital transformation in the electoral system and strongly supports the study's hypothesis regarding improved trust and accountability through technological integration.



Challenges:

This study provides valuable insights into public perception regarding digital-based electoral security mechanisms, certain challenges and limitations were observed during the research process.

i. **Limited Sample Size :** The study was conducted with a total of 22 respondents. Although the responses provide meaningful insights, the sample size is relatively small. A larger sample across different regions of India could provide more diverse and statistically strong conclusions.

ii. **Awareness Gap About Blockchain Technology :** Some respondents may not have complete knowledge about blockchain technology or advanced digital voting mechanisms. Their responses might be influenced by limited technical understanding.

iii. **Digital Infrastructure Concerns :** Implementation of a secure digital-based voting framework would require strong digital infrastructure, secure servers, reliable internet connectivity, and nationwide digital literacy. In rural or remote areas, infrastructure limitations may create implementation challenges.

iv. **Policy and Regulatory Barriers :** Adoption of a digital-based voting framework would require approval and implementation by the Election Commission of India and other government authorities. Legal, constitutional, and administrative procedures may slow down the adoption process.

Conclusion:

This study aimed to examine public perception regarding the integration of secure digital verification mechanisms within the electoral system to enhance transparency and reduce bogus voting. Based on the survey conducted with 22 respondents, the findings reveal significant concerns about unauthorized voting and moderate trust in the existing system.

The analysis indicates that a majority of respondents believe bogus or duplicate voting remains a concern. Furthermore, strong support was observed for the implementation of stronger digital verification systems, including OTP-based authentication and secure digital identity verification before voting[15]. Most participants also agreed that a secure digital-based voting framework could improve transparency and public trust in

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(b) Jan – Feb 2026

Original Research Article

elections. The results suggest that citizens, particularly young and educated voters, are open to technological advancements in the electoral process. The findings support the hypothesis that integrating advanced digital security mechanisms can strengthen electoral integrity and enhance transparency.

However, successful implementation would require robust cybersecurity infrastructure, policylevel approval, digital literacy initiatives, and careful phased deployment. While digital transformation in elections presents challenges, it also offers significant opportunities to build a more transparent, secure, and trustworthy democratic system.

In conclusion, the study highlights that a secure digital-based voting framework, supported by multi-level authentication and blockchain-enabled transparency, has the potential to address existing concerns and improve confidence in the electoral process.

References:

1. *Khan, K., et al., Electronic Voting Machines Around The World and The Need Of Evms In Pakistan: A Comparative Analysis. International Journal of Social Sciences Bulletin, 2024.* ***2****(4): p. 2279-2294.*
2. *Dong, S., et al., Blockchain technology and application: an overview. PeerJ Computer Science, 2023.* ***9****: p. e1705.*
3. *Komalavalli, C., D. Saxena, and C. Laroiya, Overview of blockchain technology concepts, in*
4. *Handbook of research on blockchain technology. 2020, Elsevier. p. 349-371.*
5. *Hossain Faruk, M.J., et al., Transforming online voting: a novel system utilizing blockchain and biometric verification for enhanced security, privacy, and transparency. Cluster Computing, 2024.* ***27****(4): p. 4015-4034.*
6. *Okechukwu, O.F., et al., Blockchain-Based Secure and Transparent Electoral Systems: A Technical Framework for Developing Democracies.*
7. *Ahmed, S., Enhancing data security and transparency: The role of blockchain in decentralized systems. International Journal of Advanced Engineering, Management and Science, 2025.* ***11****(1): p. 593258.*
8. *Subrahmanyam, S., Blockchain Technology for Enhancing Data Integrity and Security, in Complexities and Challenges for Securing Digital Assets and Infrastructure. 2025, IGI Global Scientific Publishing. p. 29-46.*
9. *Feroz, A., et al., Blockchain and machine learning combined secured voting system. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 2026.* ***9****(1): p. 119-124.*
10. *Alvarez, R.M., J. Cao, and Y. Li, Voting experiences, perceptions of fraud, and voter confidence.*
11. *Social Science Quarterly, 2021.* ***102****(4): p. 1225-1238.*
12. *Rajeev, D. and T. Hayath, Digital Voting System with Face Recognition. International Journal of Scientific Research and Technology, 2026.*
13. *Jafar, U., M.J.A. Aziz, and Z. Shukur, Blockchain for electronic voting system—review and open research challenges. Sensors, 2021.* ***21****(17): p. 5874.*

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(b) Jan – Feb 2026

Original Research Article

14. *Adekunle, S.E., A Review of Electronic Voting Systems: Strategy for a Novel. International Journal of Information Engineering & Electronic Business, 2020.* ***12****(1).*
15. *Indapwar, A., M. Chandak, and A. Jain, E-voting system using blockchain technology. Int. J. of Advanced Trends in Computer Science and Engineering, 2020.* ***9****(3).*
16. *Offor, A.S., et al., Securing Us Elections: Threats, Vulnerabilities, Mitigations, And Opportunities For Technology. 2025.*
17. *Kumar, P.U., L. JoelJashwa, and B.U. Maheswari. Blockchain-Enabled Voting with Multi-Factor Authentication: Face Id, Aadhar & OTP. in 2026 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE). 2026. IEEE.*

Cite This Article:

Rane V.S. & Rane H. (2026) *Digital-Based Anti-Bogus Voting System for Enhancing Security and Transparency in Indian Elections.* **In Educreator Research Journal: Vol. XIII (Issue I),** pp. 190–199.

Doi: https://doi.org/10.5281/zenodo.20205345