iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.80339

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Secure Voting System Using Blockchain

Sohail Shaikh[1], Anas Chougle[2], Sidhantha Padhi[3], Piyush Gharat[4], Prof. Kirti Pawar[5]
Department of Information Technology, Saraswati College of Engineering, Kharghar, India

Abstract: ***This paper presents a secure web-based voting system using blockchain technology to ensure transparency, integrity, and reliability in digital elections. The system is developed using the React.js, Node.js, Firebase, and Ethereum blockchain integrated through MetaMask and deployed on a test network using the Hardhat. Users authenticate via Gmail-based OTP verification and are allowed to cast votes through a user-friendly interface. To enhance security, the system captures the user's facial image during vote submission and stores data securely on Firebase, while hashed records are maintained on the blockchain to ensure immutability. The system enforces a strict one-user-one-vote policy, preventing duplicate voting. An admin panel allows candidate management without revealing vote counts during the election process. Result is displayed graphically after voting concludes, and encrypted data can be exported for analysis. Additionally, a voice-assisted feature in Hindi improves accessibility for illiterate users, making it inclusive and efficient.***

Keywords: Blockchain, Secure Voting System, Ethereum, MetaMask, Firebase, OTP Authentication, Face Recognition, E-voting, Decentralized Applications (DApps), Hardhat, Web Security.

I. INTRODUCTION

In recent years, the adoption of digital technologies in governance has significantly increased, leading to the development of electronic voting (e-voting) systems. However, traditional e-voting system often faces critical challenges such as lack of transparency, vulnerability to cyber-attack, data tampering, and limited accessibility for diverse user group. These issues raise concern about the reliability and integrity of election processes. Blockchain technology has emerged as a promising solution to address these challenges due to its decentralized, immutable, and transparent nature. By storing voting data in a distribute ledger, blockchain ensures that once a vote is recorded, it cannot be altered or deleted. This property makes it highly suitable for secure voting applications. This paper proposes a Secure Voting System using Blockchain, developed as a web-based application utilizing modern technologies such as React.js, Node.js, Firebase, and Ethereum blockchain. The system integrated MetaMask for secure transactions and used a hardhat test network for deployment and testing. The proposed solution enhances security through Gmail-based OTP authentication and real-time facial image during vote casting to prevent impersonation and fraud. Additionally, the system enforces strict one-user-one-vote policy and ensure that administrative authorities cannot access live voting result, there by maintaining fairness. The inclusion of voice-assisted functionality in Hindi further improves accessibility for illiterate users, making the system inclusive and user-friendly. The objective of this research is to design and implement a secure, transparent, and scalable voting system that leverages blockchain technology to overcome the limitations of traditional e-voting systems while ensuring usability for all users.

A. Problem Statement

Traditional voting system, including paper-based and existing electronic voting (e-voting) systems, suffer from several critical challenges such as lack of transparency, risk of data tampering, voter impersonation, and limited accessibility. Manual voting process are time-consuming, prone to human errors, and require significant administrative effort, while many digital voting systems rely on centralized architecture that are vulnerable to cyber-attack unauthorized manipulation. Furthermore, ensuring the authenticity of voters remains a major concern, as conventional system often lack robust identity verification mechanisms. Issues such as duplicate voting, vote manipulation, and lack of trust in the system reduce public confidence in election outcomes. Additionally, existing system do not adequately support illiterate users or individuals with limited digital literacy, making the voting process less inclusive.

II. LITERATURE SURVEY

Electronic voting has attracted significant research attention because traditional voting methods and many centralized e-voting platforms face problem such as vote tampering, identity fraud, lack of transparency, and limited voter trust. Recent review studies show that blockchain is widely considered a strong foundation for e-voting because it offers decentralization, immutability, auditability, and improved integrity of election records. At the same time, the literature also shows that privacy, voter authentication, scalability, and usability remain major open challenges in practical deployment.

Jafar et al. (2022) presented a systematic literature review and meta-analysis of scalable blockchain-based e-voting systems. Their study examined 76 article and concluded that blockchain can reduce data tampering and strengthen election integrity. However, the review emphasized that privacy protection, transaction speed, and large-scale scalability are still unresolved issues in many existing proposals. This study is important because it identifies the major technical barriers that later blockchain voting systems continue to address.

A 2024 review published by Wiley analysed the significance, strategies, and challenges of blockchain-based electronic voting systems and highlighted the need for secure voter registration, reliable authentication, encrypted vote casting, and transparent result handling. Similarly, the 2025 Springer survey on architectures, trends, solutions, and challenges explained that a trustworthy e-voting system must include secure registration, accessible voter interfaces, protected vote casting, encryption, verification, and fair result announcement. These surveys show that security alone is not sufficient; usability and accessibility are also necessary for real-world acceptance.

Chafiq et al. (2024) proposed a blockchain-based electronic voting case study for Morocco using Solana. Their work focused on auditability, permanent vote recording, transparency, and accessibility for users with different levels of technical knowledge. The study demonstrates that blockchain-based systems can be designed to be both secure and user-friendly, which is highly relevant to modern public voting applications.

Sujatha et al. (2024) proposed a blockchain-powered e-voting model that emphasized secure voter authentication, smart-contract-based election automation, and the use of biometric and facial recognition techniques. Their work is particularly relevant because it moves beyond simple blockchain vote storage and adds stronger identity verification methods to reduce impersonation and fraudulent participation. This directly supports the idea that modern e-voting systems should combine blockchain with authentication mechanisms rather than relying on blockchain alone

III.PROPOSED SYSTEM / METHODOLOGY

The proposed system is a secure web-based voting platform using blockchain technology designed to ensure transparency, data integrity, and voter authentication. The system integrates modern web technology such as React.js for the frontend and Nodes.js for backend processing, along with Firebase for secure data storage. The Ethereum blockchain is used to record votes in a decentralized and immutable manner, with MetaMask acting as the interface for blockchain transactions. The system is deployed and tested using a Hardhat test network.

The proposed solution addresses key limitation of traditional voting system, such as vote tampering, duplicate voting, and lack of transparency. It incorporates advanced security mechanism including Gmail-based OTP authentication and real-time face capture during vote casting to verify voter identity. Additionally, then system ensures fairness by restricting administrators from viewing live vote counts during the election process. The overall workflow of the system is illustrated in Fig. 4.1 (Flowchart of Voting Process), and the structure design of the system is shown in Fig 4.2 (System Architecture Diagram).

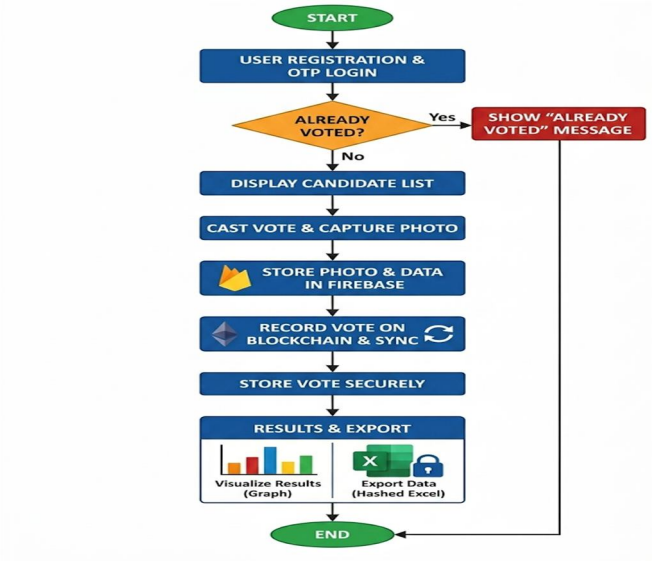


Fig. 4.1 Flowchart

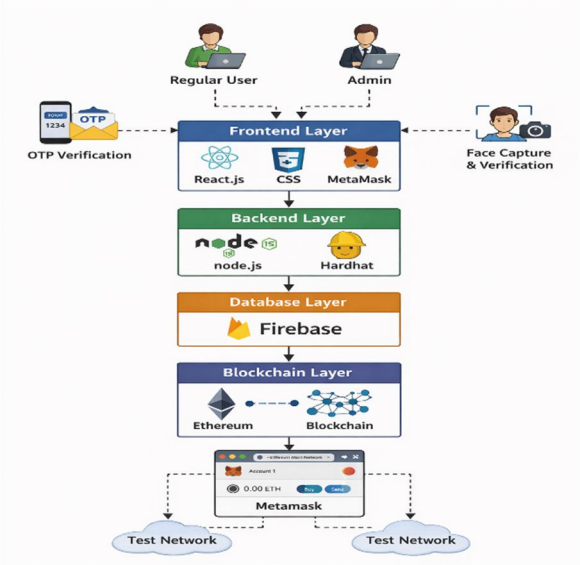


Fig. 4.2 Archtecture diagram

A. Methodology

1) *User Registration and Authentication:* The system begins with user registration using an email ID. During login, an OTP (One-Time Password) is sent to the registered email, which is valid for a limited time. Only after successful OTP verification, the user is authenticated and allowed to access the voting system.
2) *Duplicate Vote Verification:* After login, the system checks whether the user has already cast a vote. If the user has already voted, the system displays an "Already Voted" message and restricts further actions. If not, the system proceeds to the next step.
3) *Candidate Display and Vote Casting:* The system displays the list of candidates to the authenticated user. The user selects a candidate and clicks the vote button to cast their vote.
4) *Face Capture and Data Storage:* During vote submission, the system activates the camera and captures the user's photo for identity verification. The captured image and user details are securely stored in Firebase.
5) *Blockchain Integration:* The voting data is converted into a hashed format and recorded on the Ethereum blockchain using MetaMask. This ensures immutability, transparency, and protection against data tampering.
6) *Vote confirmation and Security:* After successful submission, the system confirms the vote and securely stores it. The system strictly enforces the one-user-one-vote policy.
7) *Result Visualization:* Once voting is completed, the results are displayed in graphical form, making them easy to understand and analyse.
8) *Data Export:* The administrator can download the voting data in Excel format. The data is stored in hashed (encrypted) form to maintain security and privacy.

IV. IMPLEMENTATION

The implementation of the proposed secure voting system was carried out as a web-based application by integrating frontend, backend, database, and blockchain technologies into a single platform. The frontend was developed using the React.js and CSS to create a responsive and user-friendly interface. Different pages such as Home, Register, Login, Vote, Admin, and Results were designed to provide smooth navigation for users and administrators. The registration module allows users to create an account using their email ID, while the login module verifies the user through an OTP-based authentication mechanism. The OTP is sent to the registered email address and remains valid for a limited time, which improves login security. The Secure user authentication is achieved through OTP-based login using a registered email ID. The system enforces a one-user-one-vote policy by verifying whether the user has already voted. Eligible users can view the candidate list and cast their vote, during which a real-time face capture feature is used for identity verification. User data and captured images are securely stored in Firebase Firestore, while the voting data is hashed and recorded on the Ethereum blockchain using smart contracts. MetaMask is integrated to handle blockchain transactions securely. The admin module allows candidate management but restricts admin from voting and viewing live vote counts. Finally, results are displayed in graphical format, and data can be exported in encrypted (hashed) Excel format to ensure privacy and security.

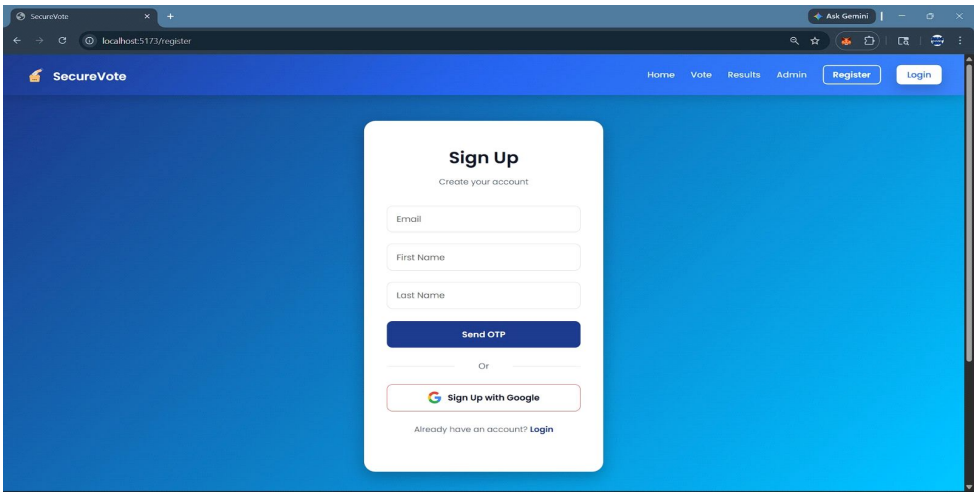


Fig. 5.1 User Registration Page

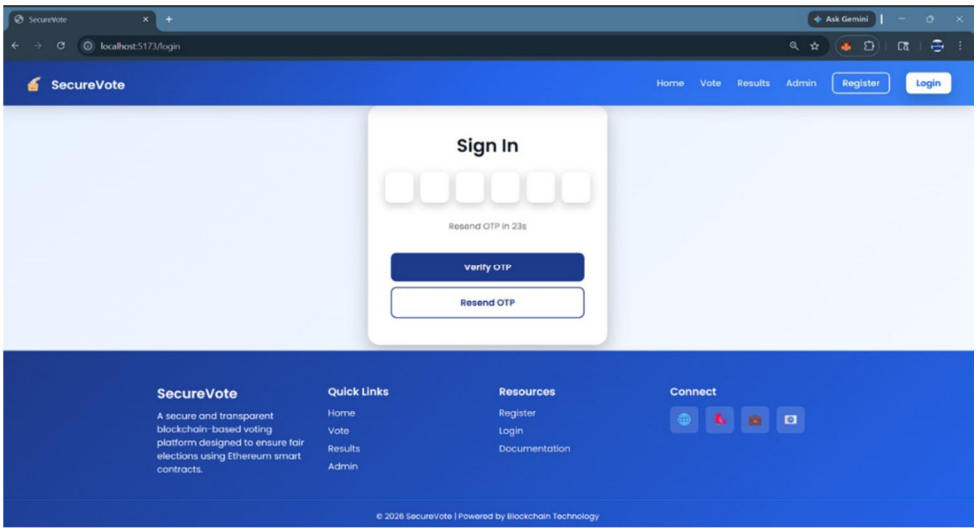


Fig. 5.2 OTP Login Verification Page

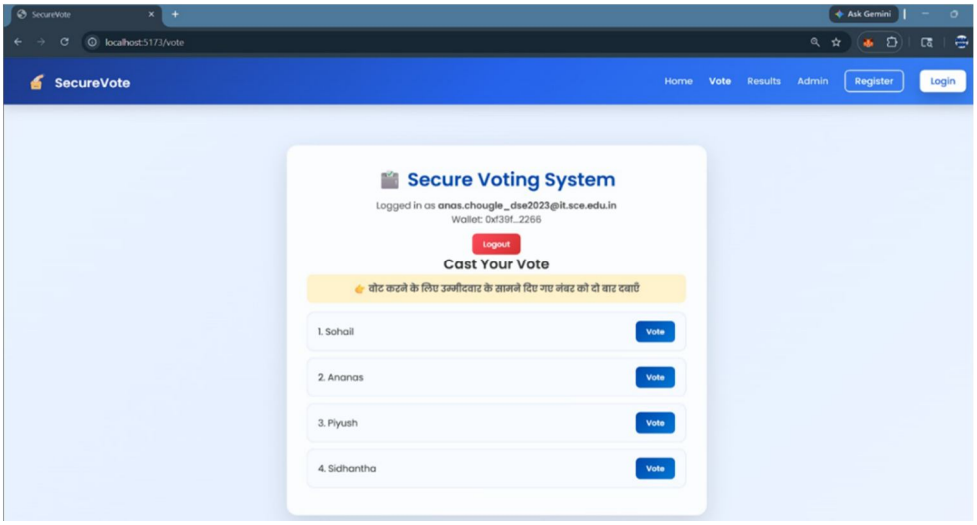


Fig. 5.3 Candidate List Page

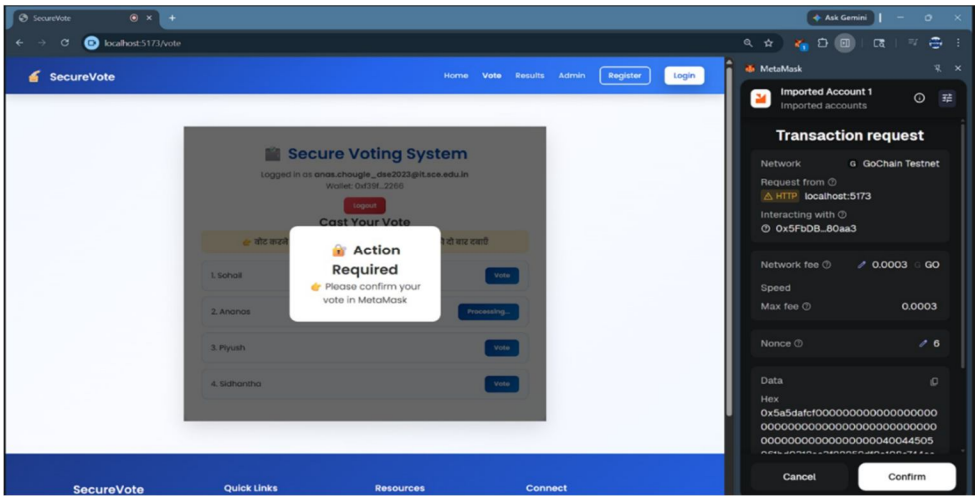


Fig. 5.4 Vote Casting + Face Capture

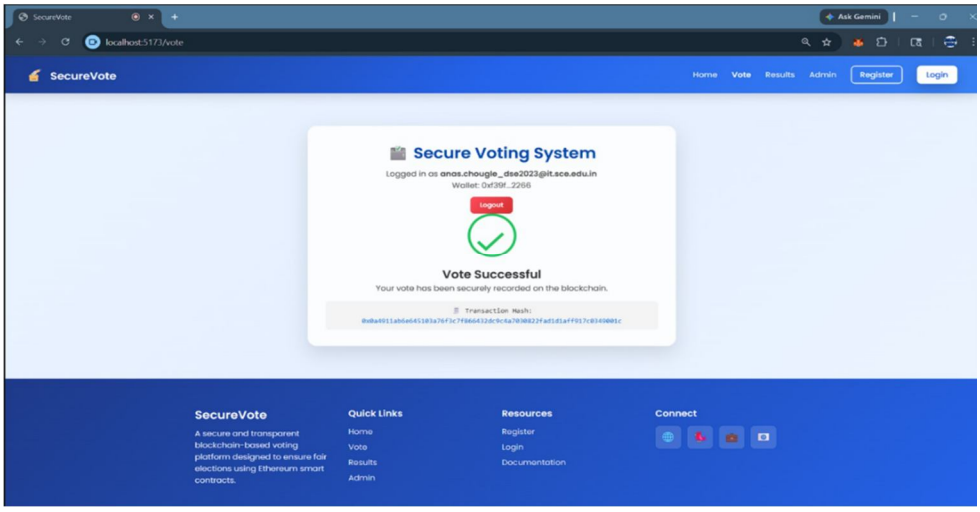


Fig. 5.5 “Already Voted” Message

V. RESULTS AND DISCUSSION

The proposed blockchain-based voting system was successfully implemented and tested, demonstrating improved security, transparency, and usability compared to traditional voting systems. The integration of OTP-based authentication ensured that only authorized users could access the system, while the one-user-one-vote mechanism effectively prevented duplicate voting attempts by displaying an “Already Voted” message for repeated access. The face capture feature during vote submission enhanced identity verification and reduced the chances of impersonation. User data and captured images were securely stored in Firebase, while voting data was hashed and recorded on the Ethereum blockchain, ensuring immutability and protection against data tampering. The use of MetaMask enabled secure transaction handling and provided a verifiable transaction record.

The admin module functioned efficiently by allowing candidate management without exposing live vote counts, thereby maintaining fairness during the election process. After completion of voting, the system generated results in graphical format, making them easy to interpret and analyze. Additionally, the exported data in hashed format ensured privacy and prevented unauthorized access.

Overall, the system performed reliably and demonstrated that combining blockchain technology with modern authentication methods and user-friendly features can provide a secure, transparent, and efficient digital voting solution suitable for real-world applications. The system also demonstrated good performance in terms of response time and user interaction, providing a smooth and efficient voting experience. Furthermore, the integration of accessibility features such as Hindi voice assistance improved usability, making the system more inclusive for a wider range of users.

VI. CONCLUSION

The proposed blockchain-based secure voting system successfully addresses the major limitations of traditional and electronic voting methods by ensuring transparency, security, and data integrity. The integration of OTP-based authentication, face capture verification, and blockchain technology effectively prevents unauthorized access, duplicate voting, and data tampering.

The system also maintains fairness by restricting admin access to live vote counts and provides clear result visualization through graphical representation. Additionally, features such as hashed data storage and Hindi voice assistance enhance privacy and accessibility. Overall, the system demonstrates a reliable, user-friendly, and scalable solution for secure digital voting, making it suitable for real-world applications.

VII. FUTURE SCOPE

The proposed system, while effective in a simulated environment, can be expanded and enhanced for large-scale, real-world elections. Future studies can focus on the following aspects.

1) Scalability and Performance Optimization: Future research can explore the use of advanced blockchain platforms or hybrid architectures to handle larger numbers of voters efficiently without compromising speed or security.

2) Governmental and Legal Framework Integration: To make the system suitable for official elections, future work can address legal, regulatory, and ethical considerations and ensure compliance with electoral laws.

3) Cross-Platform Accessibility: Extending the system to mobile and cloud-based platforms would enhance accessibility and allow voters to participate securely from remote locations.

REFERENCES

[1] U. Jafar, M. A. Zahid, and A. U. Rehman, "A systematic literature review and meta-analysis on scalable blockchain-based electronic voting systems," *IEEE Access*, vol. 10, pp. 123456–123470, 2022.

[2] H. O. Ohize, A. S. Alfa, and M. S. Ibrahim, "Blockchain for securing electronic voting systems: A survey of architectures, trends, and challenges," *Cluster Computing*, vol. 28, pp. 1123–1145, 2025.

[3] T. Chafiq, A. Touhafi, and M. Bouhorma, "Blockchain-based electronic voting system: A case study," *Journal of Information Security and Applications*, vol. 78, 2024.

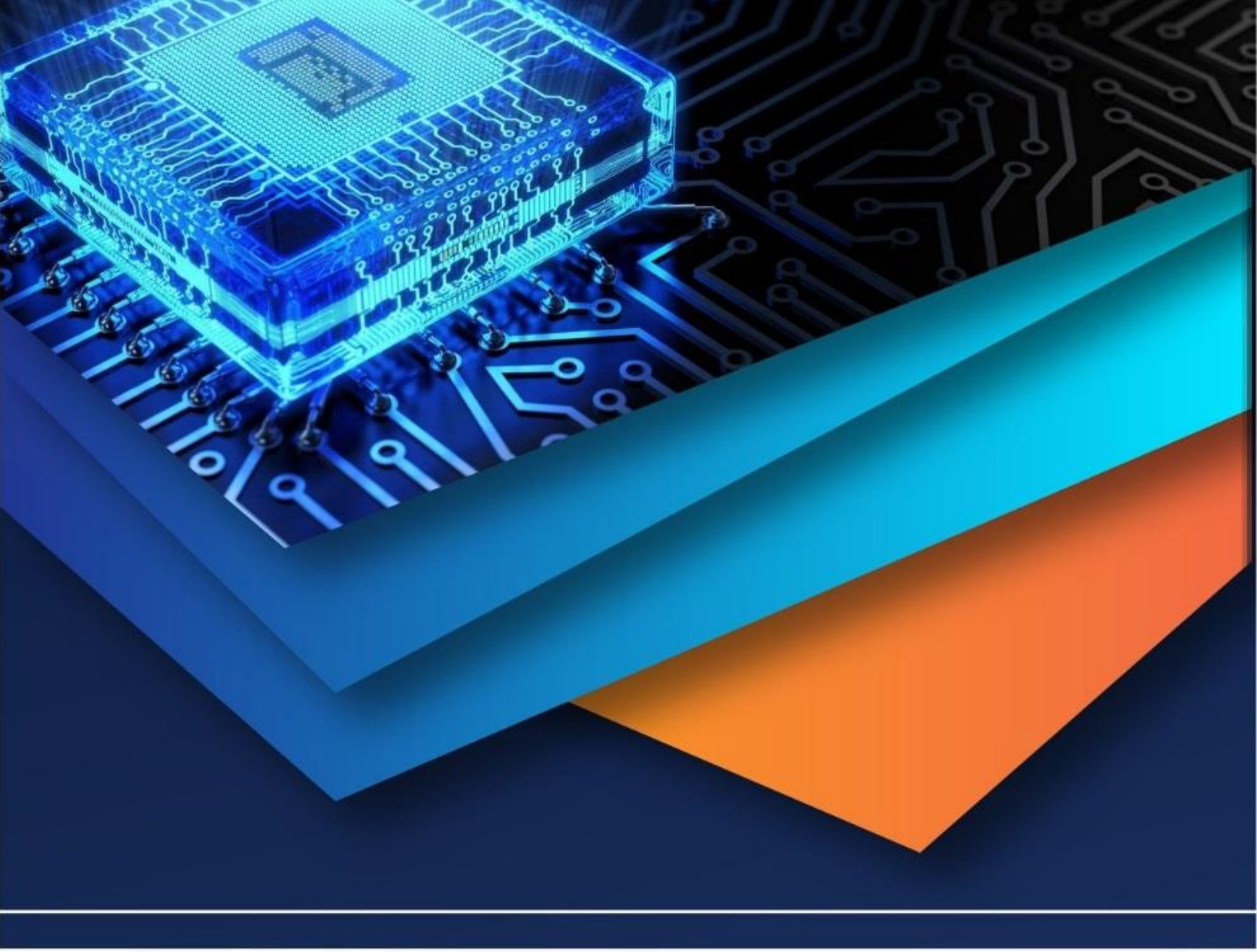
[4] B. Sujatha, R. Kumar, and P. Sharma, "Blockchain-powered e-voting: A novel approach to secure voter authentication and election automation," *Indian Journal of Science and Technology*, vol. 17, no. 5, pp. 210–218, 2024.

[5] M. J. H. Faruk, S. Rahman, and N. Islam, "A blockchain-based secure voting system with biometric verification," *Cluster Computing*, 2024.

[6] S. A. Joni, M. Rahman, and K. Ahmed, "Hybrid blockchain-based electronic voting system using deepface and post-quantum techniques," *MDPI Electronics*, vol. 13, no. 4, 2024

[7] A. Razaque, K. Rizvi, and S. Khan, "Blockchain-enabled smart contracts for secure and scalable electronic voting systems," *Journal of King Saud University – Computer and Information Sciences*, 2025.

[8] A. Singh and P. Verma, "A comprehensive analysis of blockchain-based voting systems," ACM Computing Surveys, 2025.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY