iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.68378

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 13 Issue IV Apr 2025- Available at www.ijraset.com

FaceChain Ballot

Bhavani M[1], Sathvika J[2], Yashaswini J[3], Sanjana S[4]
[1]*Assistant Professor,* [2,3,4]*Student, Department of Information Technology, G. Narayanamma Institute of Technology and Sciences, Hyderabad, India*

Abstract: ***blockchain-enabled electronic voting system aimed at mitigating the trust, security, and traceability issues that plague conventional electronic voting systems. Despite the recent proliferation in popularity of computerized (electronic) voting, concerns about manipulation and privacy remain. Because of its fundamental immutability and decentralization, blockchain technology offers a possible answer. This platform ensures that voting proceeds smoothly and autonomously without external interference by fully integrating blockchain technology to manage all voting processes. The solution guarantees full transparency during the entirety of the voting process and safeguards voters' identities using homomorphic encryption algorithms. The system's major novelty is the full de-centralisation of e-voting administration which improves e-voting process security and vote privacy. According to the proposed method, there is a more evident, more secure, and more private variant of the currently used electronic voting systems, and it could be deployed in a broader spectrum of voting scenarios.***
Keywords: homomorphic encryption, blockchain, security, transparency, decentralisation, privacy protection, electronic voting systems, and immutability.

I. INTRODUCTION

The validity and trustworthiness of electoral systems are threatened by several issues of the traditional election process, such as paper ballots or electronic voting machines (EVMs). The accuracy of vote tabulation results can be compromised by fragility of the conventional approach to human error, such as bad polling station management or bad vote count. Moreover, such systems are susceptible to fraud due to the following problems, such as ballot stuffing, EVM cheating and impersonation. Especially in large elections, the staffing needed to handle the printing, shipping, and secure storage of ballots increases the expense and inefficiency significantly. Reach to the physical locations of polling stations, where some groups, such as residents of remote localities, foreigners or people with disabilities, are concerned as far as the limited reach of voting systems, may also affect the low turnout of voters. The technology used in voting machines has attracted attention as a means of overcoming such limitations; facial recognition technology has been suggested as a potential answer to the lack of confidence in voter authentication. Such systems utilize the biometric information to ensure the efficiency of the voting process and the prevention of illegal duplication. They are also, however, subject to certain limitations, including both accuracy and demographic, susceptibility to spoofing and privacy issues with the gathering and storage of private biometric information. Furthermore, the scalability of such systems are constrained by the computational demands in particular during peak number of votes.

As a promising avenue for circumventing the restrictions of conventional and biometric based voting systems, blockchain-based voting systems may offer desirable routes to secure, auditable and citizens' vote oriented elections in the networked world, but such deployment seriously demands huge investments towards both infrastructure and voter participation.

II. LITERATURE REVIEW

There have been significant contributions to the literature review on new trends in FaceChain Ballot. This section covers publications from the literature survey on FaceChain Ballot.

The authors of [1] describe shortcomings of the usual voting schemes and allude to the issues regarding paper-based voting and hand-marking of every ballot. The study reveals several inefficiencies, such as ballot irregularities, human errors and prolonged vote counting. According to the specialists, digital voting system should be used to solve the problems, efficient the election process.

In the paper [2] the use of electronic voting machines (EVMs) in contemporary elections and the problems that come with it are presented and discussed. Although electronic ballot machines have decreased the dependence on paper ballots, they still are susceptible to the physical coercion and hacking. The paper states which attack paths are available through which it is possible to threaten the integrity of the election and which approaches are possible for securing the election, in particular, the establishment of voter authentication procedures or cryptographic procedures.

The paper[3]blockchain technology is proposed for election security issues. The authors describe a blockchain-based voting model that assures the vote immutability, decentralization, and transparency. Using smart contracts and distributed ledger technology, the system reduces its vulnerability to vote manipulation and unauthorized access. The thesis shows how blockchain mitigates single points of failure and allows to establish a tamper-proof voting system.

In paper[4] the combination of biometric authentication and electronic voting systems is addressed. The authors write about the application of technology for facial recognition to achieve a stronger voter identification and preventing identity theft. However, the article does not address the issues that are relevant for facial recognition, e.g., spurious and spoofable data. The paper proposes the application of multi-factor authentication to reinforce the security of biometric voting systems.

This paper[5] To strengthen the election security, a hybrid model that integrates blockchain with biometric verification The system of the investigators is based on facial recognition technology for voter authentication and votes on a distributed ledger. As indicated by the research, the synergy with the use of both technologies, is identified as a significant increase in the level of trust in the purchase, at the same time decreasing the level of fraud and the level of error. In order to deal with the problem in the storage of biometric information, the authors stress the importance of robust data encryption and privacy-preserving techniques.

Finally, the study in [6] looks at how scalable voting systems based on blockchain can be. The impact of different consensus mechanisms on transaction efficiency and pace, with regard to large elections, is explored by the authors. Results show that although blockchain offers a high level of security, it is still difficult to make maximum use of blockchain technology for turnout maximization. To increase the scalability of the system, the authors propose the implementation of the off-chain voting solution and thin cryptographic protocols" model.

III. PROPOSED SYSTEM AND METHODOLOGY

A. *Proposed System*

FaceChain Ballot is a blockchain-based electronic voting platform that incorporates facial recognition technology to improve the efficiency, security, and transparency of election procedures. Using the immutability and decentralization of blockchain technology together with robust biometric authentication, this approach aims to solve problems that traditional electoral systems often suffer from (impersonation, vote fraud, and ineffectiveness). Voter fraud is effectively reduced by the use of facial recognition that ensures ballot box/voting machine access is restricted to valid voters. Real facial stimuli and pre-defined voter data are accurately cross-matched in a wide variety of contexts by employing advanced machine-learning-based algorithms.

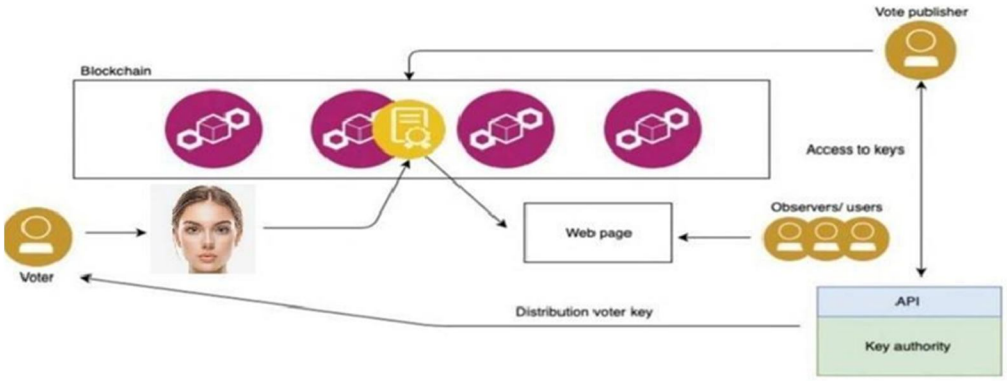


Fig. 1 System Architecture of proposed system

B. *Methodology*

1) *User Authentication through Facial Recognition*: Voters initiate the process by scanning their face through the system's web-based interface. Advanced facial recognition algorithms analyze and verify the biometric data to confirm voter identity. Anti-spoofing measures are implemented to prevent fraudulent access, such as impersonation or multiple voting attempts. This stage ensures that only legitimate voters gain access to the system, reducing risks of identity theft and election manipulation.
2) *Data Encryption and Privacy Compliance Design:* To protect voter information, facial and vote data are encrypted using the SHA-512 hashing algorithm. Multi-layered encryption safeguards the system from unauthorized access or tampering. In addition, the handling and storage of biometric data adhere to privacy regulations, including the General Data Protection Regulation (GDPR), ensuring ethical and legal data management.

3) *Blockchain-Based Vote Record:* After successful authentication, voters are granted access to cast their votes. Each vote is stored as a secure transaction on a blockchain network. This decentralized ledger ensures immutability, transparency, and resistance to tampering. Votes remain anonymous while still being traceable and verifiable, promoting accountability without compromising voter privacy.
4) *Key Authority and System Interface:* A Key Authority API is integrated to generate unique cryptographic keys for each voter. These keys confirm voter eligibility and ensure that each individual can vote only once. The web-based user interface offers a simple and intuitive voting experience. The combined use of cryptographic keys and blockchain technology strengthens overall system security and maintains the integrity of the election process.

IV. RESULTS

Fig. 2 Home page

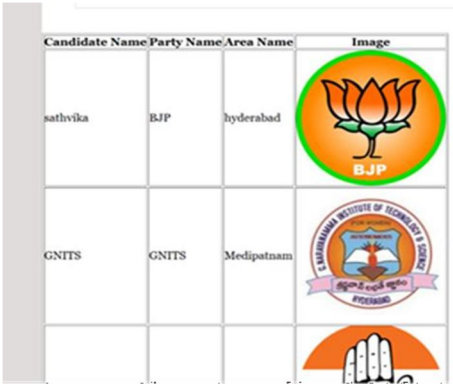


Fig. 3: Admin viewing the party details

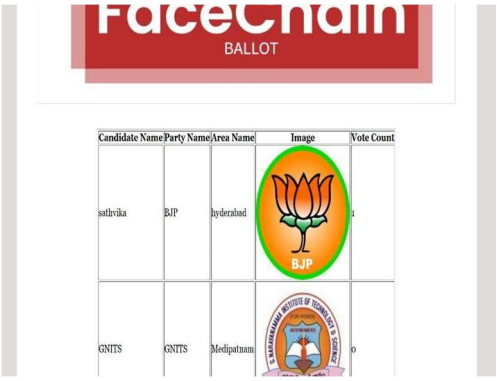


Fig. 4: Final vote count

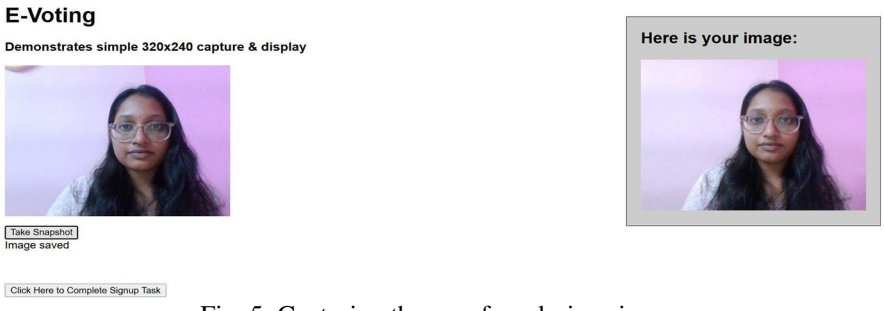


Fig. 5: Capturing the user face during signup

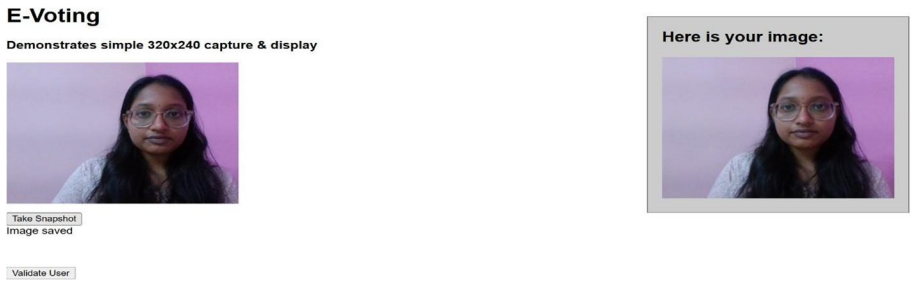


Fig. 6: Validating the user face before casting vote

Fig. 7: User casting vote

V. CONCLUSIONS

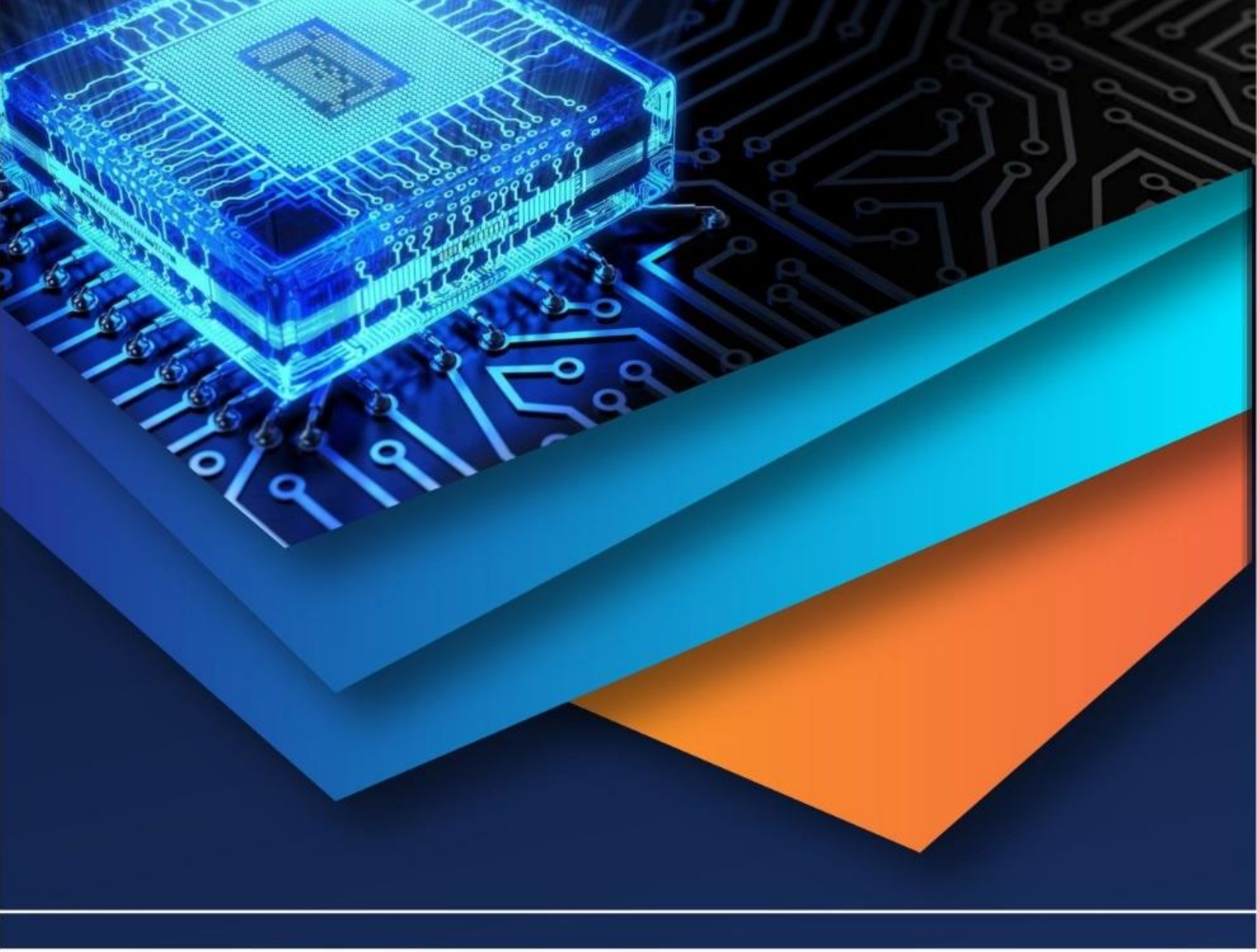
Motivated by technological advances and the increasing need for safe, transparent, and efficacious voting systems, the voting system project is grand in scope and loaded with potential. Scalability, enhanced security, accessibility and real-time analytics, among others, can be incorporated into the system to help it evolve to meet contemporary elections' requirement. With the application of state-of-the-art technology such as blockchain, artificial intelligence, and biometrics, voter fraud and low turnout can be prevented, with high accuracy, inclusivity, and credibility. Through "opening up" and "transparency"2 to all citizens, these better features not only enhance the system,2 but also protect democratic principles

User-friendly graphical interface can contribute to a voting system in a beneficial way, by facilitating the administration and the voting process for the involved parties, as well as ensuring the device compatibility with different types of devices, such as computers, tablets, and mobile phones.

When successful vote submission is validated and potential voters are reminded about upcoming elections, automated messages can lead to greater efficiency and visibility of voting. In addition to safety audit logs for post-election accountability, the technology could also generate printable receipts or provide voters with digital receipts for casting a ballot. The system can be configured in a customizable fashion for local, regional, and national elections to support various elections at different levels. Importantly, integration with census or citizen ID systems and integration with government-based databases for real-time voter-validation can enhance system effectiveness as well as reliability.

REFERENCES

[1] Blockchain-Enabled E-Voting, N. Kshetri and J. Voas, IEEE Software, vol. 35, pp. 95-99, July Blockchain-Enabled E-Voting | IEEE Journals & Magazine | IEEE Xplore.
[2] "Voting Process with Blockchain Technology: Auditable Blockchain Voting system", M. Pawlak, J. Guziur, and A. Poniszewska-Mara nda, Lecture Notes on Data Engineering and Communications Technologies, pp. 233-244, Springer, Cham, 2019. Voting Process with Blockchain Technology: Auditable Blockchain Voting System | SpringerLink
[3] "How Blockchain Works," by B. Singhal, G. Dhameja, and P. S. Panda, in Beginning Blockchain, pp. 31-148, Berkeley, CA: Apress, 2018. How Blockchain Works | SpringerLink
[4] R. Perper, "Business Insider reports that Sierra Leone is the first country to implement blockchain during an election," 2018. Nagelkosmetik – Risiko und Chance | Die Dermatologie
[5] Bitcoin: A Peer-to-Peer Electronic Cash System, by S. Nakamoto, tech.rep., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System | Satoshi Nakamoto Institute
[6] G. Wood and colleagues, "Ethereum: A secure decentralized generalized transaction ledger," Yellow Paper on the Ethereum Project, vol. 151, pp. 1–32, 2014. Ethereum Yellow Paper: a formal specification of Ethereum, a programmable blockchain



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY