Elevating Democracy: Blockchain-Secured Voting with Enhanced Identity Authentication

Nayan G Patil
Computer Science and Engineering
S. G. Balekundri Institute of Technology
Belgaum, India
narayangpatil18@gmail.com

Shreya Sanjay Karalgekar
Computer Science and Engineering
S. G. Balekundri Institute of Technology
Belgaum, India
shreyakaralgekar7@gmail.com

Deepak S Bhadgaonkar
Computer Science and Engineering
S. G. Balekundri Institute of Technology
Belgaum, India
deepakbhadgaonkar123@gmail.com

Gouri S Rane
Computer Science and Engineering
S. G. Balekundri Institute of Technology
Belgaum, India
gourirane4444@gmail.com

Rajeshwari kisan
Computer Science and Engineering
S. G. Balekundri Institute of Technology
Belgaum, India
rajeshwari.kisan@gmail.com

Abstract— Current voting systems, both traditional and digital, suffer from a lack of transparency and vulnerabilities that can be exploited. This undermines public trust and raises concerns about democratic rights. Blockchain technology offers a potential solution to these problems by providing a secure and transparent platform for voting. Unlike conventional voting mechanisms that depend on physical polling stations, our proposed framework leverages blockchain and Epic voter Id with face recognition, OTP Verification to conduct voting digitally. This framework is scalable due to its use of flexible consensus algorithms and employs a Chain Security Algorithm to further enhance security. Smart contracts ensure a secure connection between voters and the network during transactions. The voting process itself is elaborated upon leveraging Blockchain technology. Performance evaluations demonstrate that This system is appropriate for large-scale implementation.

Keywords—Digital Voting, Blockchain voting system, Face scanning, OTP (One-Time Password).

I. Introduction

Democracy plays a vital role in the progress of nations, allowing citizens to elect and replace their government through elections. Nonetheless, this procedure requires a substantial amount of manpower and resources. Elections are essential for people to choose their leaders, necessitating accuracy and transparency. Existing systems have shortcomings such as the risk of violence, machinery damage, and fraudulent votes. To tackle these concerns, this document suggests a novel approach: an Web-based e-Voting System using Facial Recognition technology. While other methods like fingerprint recognition exist, our system offers advantages in bandwidth utilization for facial matching and identification.

II. LITERATURE SURVEY

“Lai et al.” proposed A transparent electronic voting system that is decentralized and ensures that emphasizes minimal trust among participants, suitable for large-scale electronic elections. However, their system lacks protection against DoS attacks because of the absence of a third-party auditing authority. It's only viable for small-scale use due to platform limitations. While Ring Signature maintains voter privacy, managing multiple signer entities is challenging. Their use of PoW consensus, while providing security, is energy-intensive and costly.

[1]Shahzad et al. introduced the BSJC proof of completeness as a dependable e-voting method, Ensuring anonymity, confidentiality, and robust security concerns. Yet, challenges remain, including the energy-intensive Proof of work and the engagement of a third party, risking data tampering and unfair results, particularly at scale.

[3]Gao et al. proposed a A cryptographic electronic voting protocol based on blockchain technology aimed at thwarting quantum computing threats with audit capabilities, enhancing the Niederreiter algorithm's resistance to quantum attacks. While effective for small-scale elections, security and effectiveness decrease with a higher number of voters.

[2]Khan, K.M. proposed the block-based e-voting architecture, experimenting with permission and decentralized blockchain frameworks without requiring authorization under various scenarios. Their scheme involves generating voter and voter addresses and updating blockchain ledger by a mining group, ensuring the voting process's integrity and reliability.

III. METHODOLOGY

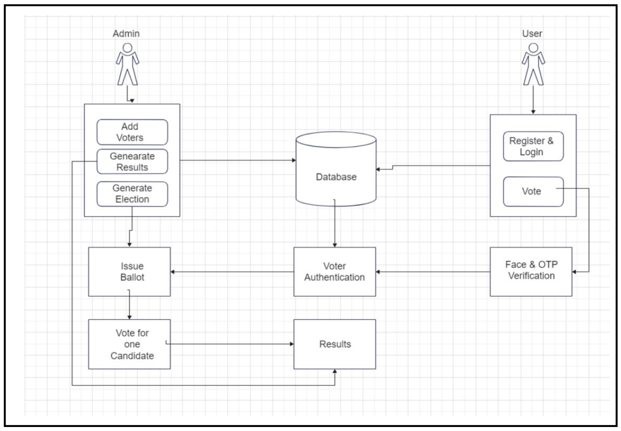

Fig.1 Architecture Diagram

Voter Registration

During registration, voters provide their unique ID number, email address, name, and phone number. The system utilizes facial recognition technology for login purposes, requiring a clear video selfie at signup.

Login and Authentication

Following registration, voters log in using a password. Successful login is followed by facial recognition for boosting security and real-time authentication.

Blockchain for Secure Voting

The system leverages blockchain technology for its inherent security and transparency. Blockchain encrypts cast votes using an asymmetric encryption algorithm. The public key for verification resides on the blockchain, while the private key is held by the system.

Ethereum for Transaction Execution

The Ethereum network serves as the framework for creating and storing the blockchain. Encrypted blocks containing voting data is distributed across numerous nodes, ensuring system resilience. Voters interact with smart contracts on a private Ethereum blockchain environment created using Ganache to cast their votes.

Admin Role and Responsibilities

The administrator manages the entire voting platform. This includes verifying voter and candidate registrations, scheduling elections, and controlling crucial notifications, such as results announcements.

Results Processing and Transparency

The results stage involves vote tabulation and generation. The system displays the outcome on the website. Voters can identify their votes using their public keys, upholding the system's transparency.

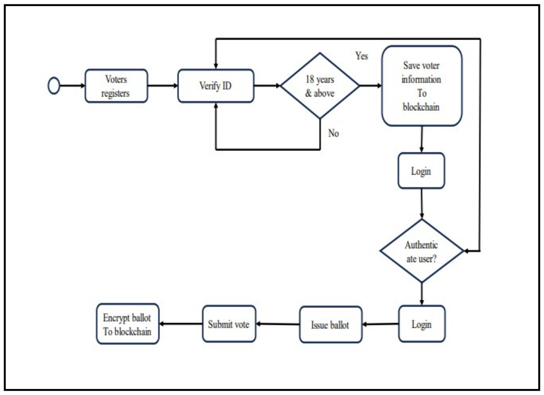

Fig.2 Data Flow Diagram

IV. EXISTING WORK

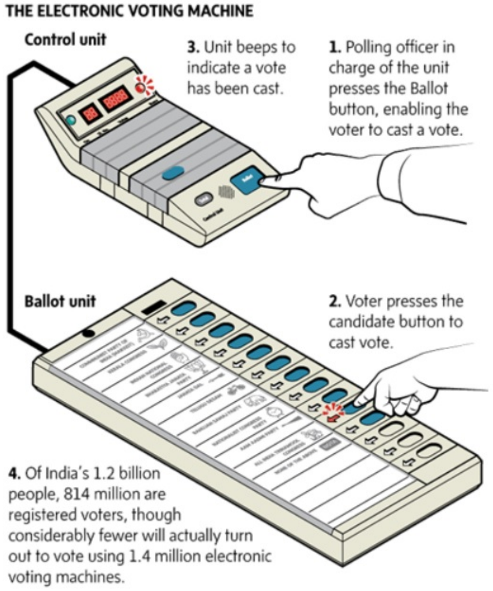
THE ELECTRONIC VOTING MACHINE
Control unit
3. Unit beeps to indicate a vote has been cast.
1. Polling officer in charge of the unit presses the Ballot button, enabling the voter to cast a vote.
Ballot unit
2. Voter presses the candidate button to cast vote.
4. Of India's 1.2 billion people, 814 million are registered voters, though considerably fewer will actually turn out to vote using 1.4 million electronic voting machines.

Fig.3 Working of EVM

Currently, voting systems predominantly rely on Electronic Voting Machines (EVMs) and Secret Ballot Voting, both of which entail significant manpower and time-consuming processes. Eligibility for voting typically begins at the age of 18, with individuals required to present their voter ID and other details for manual validation before being granted permission to vote. However, conventional voting mechanisms are beset with inefficiencies and vulnerabilities that compromise the integrity of the electoral process.

Electronic Voting Machines (EVMs) have become a common fixture in many electoral systems worldwide. While intended to streamline the voting process, their deployment necessitates meticulous logistical planning. EVMs must be transported to various polling stations across the country, entailing significant manpower and security arrangements. Moreover, the manual validation of voter details before casting a vote introduces delays and potential opportunities for error or manipulation.

Similarly, Secret Ballot Voting, while preserving voter anonymity, remains a labour-intensive process. Each vote must be manually cast and subsequently counted, a task that requires considerable manpower and time. The manual handling of paper ballots introduces the risk of miscounting or tampering, undermining the credibility of election outcomes.

Despite efforts to ensure transparency and fairness, the current voting system is far from infallible. The reliance on manual processes not only prolongs the duration of elections but also increases the likelihood of errors and irregularities. Moreover, the logistical challenges associated with transporting and securing EVMs pose logistical challenges, particularly in geographically vast or politically volatile regions.

To address these shortcomings and enhance the accessibility and efficiency of the voting process, there is a pressing need for technological innovation. One potential solution lies in the development and implementation of digital voting systems that leverage cutting-edge technologies such as blockchain and biometric authentication.

Blockchain-based voting systems offer a secure and transparent platform for conducting elections. By storing voting records in a decentralized ledger, blockchain technology ensures immutability and tamper resistance, safeguarding the integrity of the electoral process. Moreover, the use of cryptographic techniques guarantees voter anonymity while enabling verifiable and auditable election results.

Biometric authentication, such as facial recognition or fingerprint scanning, can further enhance the security and accessibility of digital voting systems. By linking voter identities to unique biometric identifiers, such as facial features or fingerprints, these systems mitigate the risk of identity fraud and unauthorized voting. Additionally, biometric authentication streamlines the voter verification process, reducing the need for manual intervention and expediting the voting process.

In conclusion, while conventional voting mechanisms have served as the cornerstone of democratic elections for centuries, they are increasingly proving inadequate in the face of evolving technological and societal challenges. By embracing digital voting solutions, we can overcome the limitations of existing systems and usher in a new era of accessible, efficient, and transparent elections.

V. WORKING

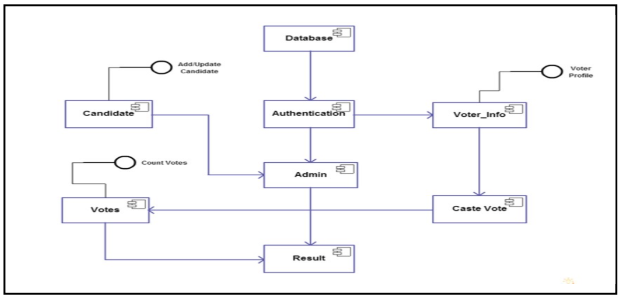

Fig.2 Overview of System

The proposed system offers a streamlined and secure method for voter interaction, enhancing the efficiency and accessibility of the voting process. Upon logging into the system, voters undergo facial recognition authentication, granting access to the list of candidates relevant to their electoral district. This authentication mechanism, coupled with role-based access control, ensures that only authorized individuals can participate in the voting process.

Once a voter selects their preferred candidate, their vote is mined by multiple miners for verification. Valid votes are then added to the public ledger, secured through blockchain technology utilizing cryptographic hashes for end-to-end verification. Each successfully cast vote is treated as a transaction within the blockchain, recorded both as a new block and in the database. This approach ensures the integrity of the voting system, preventing duplicate votes through the use of unique facial recognition identifiers.

Following validation, voters receive immediate notification of their transaction ID via message or email, allowing them to track their vote on the ledger. While this notification provides transparency, it maintains voter privacy by safeguarding individual voting choices. Each voter's identity is represented by a cryptographic hash within the blockchain, ensuring anonymity even from system operators or administrators.

By leveraging blockchain technology and robust authentication mechanisms, the proposed system offers a comprehensive solution to enhance the integrity and accessibility of the voting process. Its emphasis on security, privacy, and verifiability ensures a fair and transparent electoral system, addressing the shortcomings of traditional voting methods.

Conclusion

The execution of the blockchain-based e-voting system with face-recognition and OTP authentication represents a significant advancement in the realm of secure and transparent electoral processes. Through rigorous testing and validation, we have demonstrated the effectiveness and reliability of the system in ensuring the integrity of the voting process while preserving voter privacy. The integration of facial recognition technology and OTP authentication enhances the security of user authentication, mitigating the risk of unauthorized access and ensuring that only eligible voters can take part in the election process. The utilization of blockchain technology provides a secure and tamper-resistant platform for recording and verifying votes, promoting transparency and trust in the electoral outcome. Furthermore, the system's notification mechanism allows voters to receive immediate confirmation of their vote's successful recording without compromising their anonymity or revealing their voting preferences. This ensures that voters can have confidence in the integrity of the election process while maintaining their privacy.

In conclusion, the blockchain-based e-voting system with face-recognition and OTP authentication represents a robust and innovative solution to modernize and safeguard the democratic process, paving the way for more transparent and inclusive elections.

References

[1] Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. *IEEE Access* 2019, *7*, 24477–24488.

[2] Khan, K.M.; Arshad, J.; Khan, M.M. Investigating performance constraints for blockchain based secure e-voting system. *Future Gener. Comput.Syst.* 2020, *105*, 13–26.

[3] Gao, S.; Zheng, D.; Guo, R.; Jing, C.; Hu, C. An Anti-Quantum E-Voting Protocol in Blockchain with Audit Function. *IEEE Access* 2019, *7*, 115304–115316.

[4] Alaya, B.; Laouamer, L.; Msilini, N. Homomorphic encryption systems statement: Trends and challenges. Comput. Sci. Rev,36, 100235. 2020.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Fernandes, A.; Garg, K.; Agrawal, A.; Bhatia, A. Decentralized Online Voting using Blockchain and Secret Contracts. In Proceedings of the 2021 International Conference on Information Networking (ICOIN), Jeju Island, Korea,pp. 582–587, 13–16 January 2021.

[7] Park, S.; Specter, M.; Narula, N.; Rivest, R.L. Going from bad to worse: From Internet voting to blockchain voting. J. Cybersecur. 2021.

[8] Barnes, C. Brake, and T. Perry. Digital Voting with the use of Blockchain Technology Team Plymouth Pioneers-Plymouth University. Accessed: Feb. 14, 2022.

[9] Ometov, A.; Bardinova, Y.; Afanasyeva, A.; Masek, P.; Zhidanov, K.; Vanurin, S.; Sayfullin, M.; Shubina, V.; Komarov, M.; Bezzateev, S. An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future Trends, 8, 103994–104015, IEEE Access 2020.

[10] Rawat, D.B.; Chaudhary, V.; Doku, R. Blockchain technology: Emerging applications and use cases for secure and trustworthy smart systems. J. Cybersecur. Priv,1, 4–18. 2021.

[11] Kim, T.; Ochoa, J.; Faika, T.; Mantooth, A.; Di, J.; Li, Q.; Lee, Y. An overview of cyber-physical security of battery management systems and adoption of blockchain technology. IEEE J. Emerg. Sel. Top. Power Electron. 2020.

[12] G. Rathee, R. Iqbal, O. Waqar, and A. K. Bashir, ''On the design and implementation of a blockchain enabled E-Voting application within IoT oriented smart cities,'' IEEE Access, vol. 9, pp. 34165–34176, 2021