International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 11 | Nov 2024 www.irjet.net p-ISSN: 2395-0072

E-Voting System Using Blockchain and Face Recognition

[1]Dhanashree Bagal, [2]Sanika Patil, [3]Gauri Chavan, [4]Srushti Shete, [5]Kajal Pawar, [6]Dr. Swati Pawar

[1,2,3,4,5] UG Students, Department of Computer Science And Engineering, SVERI's College of Engineering, Pandharpur, Maharashtra, India
[6]Associate Professor, Department of Computer Science And Engineering, SVERI's College of Engineering, Pandharpur, Maharashtra, India

---

Abstract:

The paper presents an innovative e-voting system that integrates facial recognition and blockchain technology to address security and authenticity issues in online voting. The system uses facial recognition to uniquely identify registered voters, ensuring that each individual is authorized to vote. This technology prevents identity fraud and enhances the security of the voting process. Blockchain technology is employed to record votes securely, ensuring transparency, immutability, and verification of the voting data. The system allows voters to cast their votes remotely while maintaining confidentiality and trust in the election process. The paper discusses the methodology behind the design and implementation of the e-voting system, focusing on integrating these technologies for a secure, scalable, and efficient voting experience. Additionally, the challenges faced during development and the potential improvements for future implementations of this system are also highlighted. This approach aims to modernize the voting process, making it more accessible, secure, and transparent for elections in various sectors.

Keywords:

E-Voting, Face Recognition, Blockchain, Security, Reliability, transparency, Functionality, Estonia, Electronic Governance, Decentralized System, user authentication.

I. Introduction

The significance of "electronic voting using facial recognition and blockchain" is that it can change the way of voting by solving important problems such as security, package transparency, and access. In many traditional voting systems, problems such as voting, double voting, election fraud, and voter fraud threaten the integrity of the election [1][2][3]. The combination of blockchain creates a secure and reliable election [4]. Facial recognition reduces the risk of fraud and increases the accuracy of voter identification by ensuring that only registered people can vote [5][6]. The distributed and immutable structure of the blockchain can protect the integrity of votes by preventing vote data from being tampered with or altered [7]. Together, these technologies increase public confidence in elections by ensuring that all votes are secure and accurate. It is especially effective in remote or large turnout situations [8]. The initiative highlights the importance of integrating new technologies into the democratic process to ensure a secure and transparent electoral process, safeguard fair elections, and enhance public participation [9].

II. Literature Review

E-Voting System Using Blockchain and Face Recognition:

Electronic voting using facial recognition and blockchain addresses key issues in the electoral process, including voter identification, fair voting, transparency, and prevention of fraud. Current research and progress on e-voting, facial recognition, and blockchain technology also identify gaps and challenges to overcome in the planning process [1][2][3].

1. **N Prathyusha, P Pooja, A Vijay Vasanth. "Blockchain-Based E-Voting System with Facial Recognition."** This paper proposes a blockchain-based e-voting system with facial recognition for secure voter authentication. It ensures tamper-proof voting and accurate voter identification, improving transparency, security, and privacy in elections.

2. **Rifa Hanifatunnisa, Budi Rahardjo. A review paper on Blockchain Based E-Voting Recording System Design.** This paper highlights the use of blockchain for secure and immutable e-voting systems, ensuring data integrity and reducing fraud risks. It emphasizes transparency and decentralized data storage.

3. **Kanika Garg,PaviSaraswat,Sachin Bisht, Sahil Kr. Aggarwal, Sai Krishna Kothuri, Sahil Gupta. A Comparitive Analysis on E-Voting System Using Blockchain.** The authors analyze different blockchain-based e-voting systems, focusing on their benefits like security and transparency, while addressing challenges such as scalability and voter authentication.

4. **Ali Mansour AI-madani, Ashok T. Gaikwad, Vivek Mahale, Zeyad A.T. Ahmed. Decentralized Evoting System based on Smart Contract by using Blockchain Technology.** This study proposes a decentralized e-voting system using blockchain smart contracts to automate voting processes, ensuring transparency while reducing third-party dependencies.

5. **Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, Gísli Hjálmtýsson. Blockchain-Based E-Voting System.** The paper presents a blockchain-based e-voting prototype, leveraging cryptographic techniques to enhance privacy and security, with a focus on permissioned blockchains for efficient performance.

6. **Ayesha Shaikh, Bhavika Oswal, Divya Parekh and B. Y. Jani, "E-voting Using One Time Password and Face Detection and Recognition".** This paper proposes an e-voting system combining OTP authentication and face recognition for enhanced security, preventing impersonation and ensuring reliable voter verification.

7. **F. Schroff, D. Kalenichenko and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering".** The FaceNet algorithm introduces a deep learning model that maps facial images to a Euclidean space, achieving high accuracy in face recognition and clustering, optimized by triplet loss.

8. **I. William, D. R. Ignatius Moses Setiadi, E. H. Rachmawanto, H. A. Santoso and C. A. Sari, "Face Recognition using FaceNet (Survey Performance Test and Comparison)".** This study evaluates FaceNet's performance across various datasets, demonstrating its robustness and high accuracy in recognizing faces under different conditions like pose and lighting. Vernekar et al. (2020) presents an exploration of blockchain technology for developing a secure, transparent, and cost-efficient e-voting system, addressing technical, legal, and security challenges in its implementation [9].

III. Problem Statement

Traditional voting systems face numerous challenges, including logistical difficulties, high costs, long counting times, voter fraud, and tampering risks. Electronic voting (e-voting) systems have emerged to address some of these issues but are vulnerable to security threats such as hacking and unauthorized access. Ensuring voter privacy and authentication remains critical, as current methods often rely on insecure techniques like passwords.

Public trust in electoral processes has diminished due to a lack of transparency and accountability, with voters unable to verify that their votes are accurately recorded and counted. To tackle these challenges, an innovative voting system that combines facial recognition technology with blockchain could be effective.

Facial recognition offers a reliable way to authenticate voter identity and prevent impersonation, while blockchain provides a decentralized, tamper-proof ledger for recording votes, ensuring they cannot be altered after casting while maintaining voter anonymity. This integrated approach aims to enhance voter security, ensure transparency, and restore public confidence in e-voting systems, ultimately safeguarding the integrity of democratic processes.

IV. Objective

1. To enhance Voter Authentication with Facial Recognition.
2. To ensure the Integrity of Votes through Blockchain.
3. To eliminate Voter Fraud and Impersonation.
4. To create a Transparent and Verifiable Voting Process.
5. To increase Election Efficiency and Accessibility.

V. Methodology

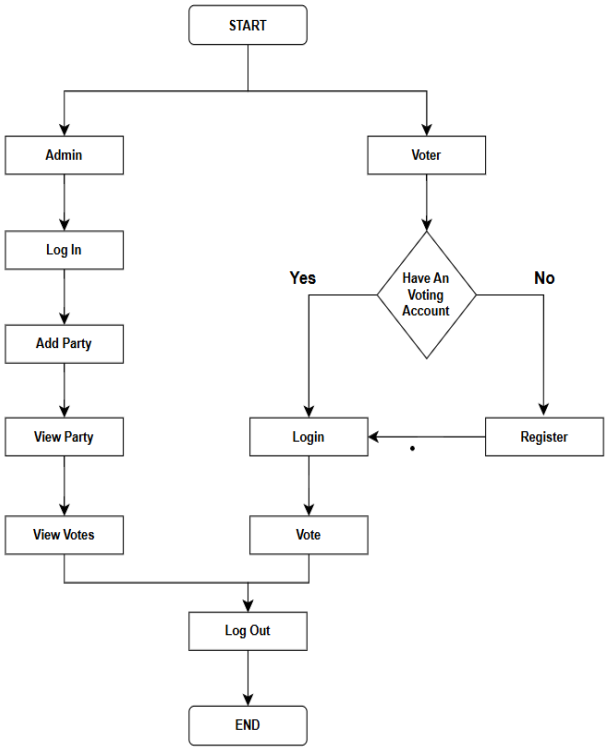

Fig 1: Block Diagram

This electronic voting system provides a secure and effective platform for digital voting and includes the ability to recognize faces to ensure the authenticity of voters. This method is divided into two main user roles: administrators and voters.

1. Administrator registration and login:
   - i. The manager is responsible for managing the election, including adding and managing candidates.
   - ii. Manager must log in using their security credentials.
   - iii. You can check the voting results and monitor the voting status of all political parties in real-time.
2. Voter registration and login via facial recognition:
   - i. Voters need a voting ID. If voters do not have an account, they will go through a registration process.
   - ii. The registration process includes recording their facial information. time. This image is securely stored in the system database for future facial recognition.
   - iii. Steps to ensure unique information for each voter number and prevent double registration.
3. When logged in, the system compares the voter's live image with the image in the database using the recorded image for facial recognition. Blockchain-integrated voting process:
   - i. After identity verification, voters can choose their favorite candidate or candidates and vote.
   - ii. The system generates a unique hash ID using blockchain technology. This hash ID acts as immutable data, ensuring that votes cannot be changed, copied or tampered with. People vote irreversibly.
   - iii. Trust IDs are securely held, preserving the integrity and confidentiality of all votes.
4. System Workflow:
   - i. After voting, the voter logs out, protecting the system and preventing unauthorized access.

The approach uses blockchain technology and facial recognition to create a secure and tamper-proof electronic ballot. The system prevents vote mani pulation by generating a unique blockchain-base hash ID for each vote, ensuring that every vote is unaltered, traceable and secure.

VI. Algorithms

Algorithms Used in the E-voting System Using Face Recognition and Blockchain:

1. Haar Cascade Classifier (OpenCV):

The Haar Cascade Classifier is an algorithm used for object detection, specifically for identifying faces in images and videos. It employs machine learning techniques to create a cascade function using both positive and negative image samples. The algorithm analyzes images at multiple scales to detect features such as the edges of the face, eyes, and nose. If it identifies a sufficient number of matches, it verifies

the presence of a face. Its high efficiency makes it well-suited for real-time applications.

2. Face Encodings and Comparisons (dlib):

The dlib face encoding algorithm generates a 128-dimensional vector that represents an individual's face. This allows for effective comparisons of images using Euclidean distance; shorter distances signify closer matches and achieve high accuracy regardless of lighting or variations in expression. On the other hand, the Haar Cascade Classifier detects faces in images and videos by employing machine learning to develop a cascade function from both positive and negative samples, scanning for facial features at different scales. Its efficiency makes it appropriate for real-time applications.

3. Dlib's ResNet-based Model:

Dlib employs a modified ResNet-34 architecture for extracting facial features. It utilizes residual blocks to address the vanishing gradient issue, facilitating the effective training of deeper networks. This design allows for the learning of intricate facial characteristics through sequential convolutional layers, producing a vector representation for face recognition. ResNet models are effective at feature extraction and are particularly adept at handling complex visual patterns, which makes them well-suited for face recognition applications.

4. Euclidean Distance:

Euclidean distance quantifies the direct distance between two points in multi-dimensional space and is utilized here for comparing face encodings. In facial recognition, the algorithm determines the distance between two encoding vectors, identifying them as representing the same individual if the distance is below a specified threshold. Its simplicity, speed, and efficiency make Euclidean distance particularly appropriate for face verification tasks, especially in small-scale, low-dimensional environments.

5. Shape Predictor (dlib):

Dlib's shape predictor detects 68 facial landmarks, including the eyes, nose, and mouth, to pinpoint distinct features on a face. It employs a regression-based model to examine their relative positions, creating a structure that corresponds to a human face. This alignment is crucial for improving the accuracy of face recognition algorithms by ensuring proper positioning, no matter the individual's angle or pose.

6. SHA256 (Hashing Algorithm for Blockchain):

SHA256 is a cryptographic hash function that produces a fixed-length output of 256 bits (32 bytes) from any input. It is widely used in blockchain technology to ensure data integrity and security. In a blockchain, each block contains a hash of the preceding block, a timestamp, and transaction data, with SHA256 generating a unique hash for every block. Any modification to the block results in a significant change to the hash, facilitating tamper detection. Its strong security features, computational efficiency, and resistance to collisions make SHA256 an excellent choice for securing blockchain transactions and electronic voting systems.

7. Proof of Work (PoW) (Blockchain):

Proof of Work (PoW) is a consensus mechanism utilized in blockchain networks to validate transactions and incorporate new blocks. Miners engage in competition to solve intricate cryptographic puzzles, and when a valid solution is discovered, the new block is integrated into the blockchain, providing a reward to the miner. This process entails substantial computational resources, which serves as a deterrent against manipulation by malicious entities. PoW strengthens blockchain security by requiring considerable effort for transaction validation, thereby making it expensive for attackers to modify the chain.

8. RSA (For Encryption of Votes):

RSA is an asymmetric cryptographic algorithm utilized for data encryption and decryption, making it appropriate for encrypting votes in an e-voting system prior to their submission to the blockchain. It uses a key pair: a public key for encryption and a private key for decryption. When a vote is cast, it is encrypted with the public key, ensuring that only the designated recipient with the private key can decrypt it. RSA provides a high level of security for sensitive information, guaranteeing that only authorized individuals can access the encrypted data.

VII. Results

Table Number 1:

This table has columns like Candidate ID, Candidate Name, Area, and Number of Votes which show which

candidate has how many votes and that candidate is from which area.

Table 1: Table of Vector Identification Accuracy.

Candidate Id	Candidate Name	Area	Number of Votes
101	John	A	350
102	Alice	A	200
103	Bob	B	450
104	Sarah	B	300
105	David	C	500
106	Emma	C	220

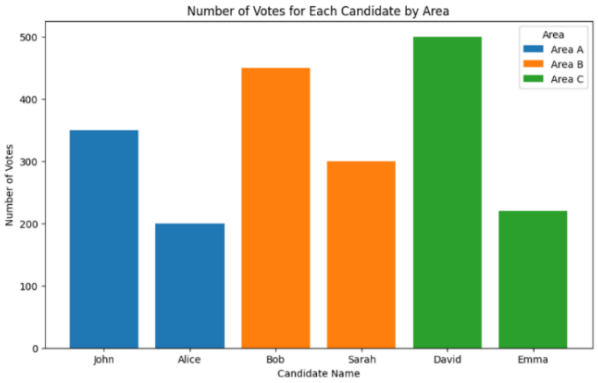

Fig 2: Graph of candidates and Number of votes

Figure number 2 is the image of graph that describes the above table i.e., table number 1

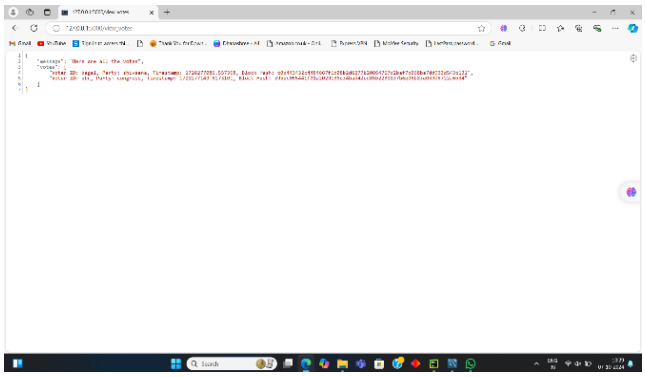

Fig 3: Show votes and their information

Figure number 3 is the figure that shows which voters have voted to whom, what is the hash ID of that vote and what is time of vote.

VIII. Result Analysis

1. System Security: The integration of blockchain ensures the tamper-proof nature of the voting records, providing high-level security and transparency throughout the voting process
2. Scalability: The system demonstrated the ability to handle multiple users and large datasets, making it a scalable solution for elections with high voter turnout.
3. Voter Identification: Facial recognition proved to be an effective and reliable method for identifying voters, significantly reducing the chances of fraudulent voting.
4. Performance: The system operates with minimal latency for voter identification and blockchain verification, providing real-time results without noticeable delays.
5. Fraud Prevention: The combined use of blockchain and facial recognition reduces the possibility of identity theft, vote duplication, and other types of election fraud.

IX. Conclusion

The proposed e-voting system integrates blockchain and facial recognition, ensuring a secure and transparent voting process. The system effectively addresses the challenges of fraud and identity verification, making it a scalable solution for secure online voting. Blockchain technology enhances the security and transparency of the voting process, reducing the risk of tampering and fraud. Facial recognition ensures accurate voter identification and eliminates the need for traditional authentication methods.

X. Future Scope

1. Improve Blockchain Performance: Enhance the scalability and speed of blockchain for handling large-scale elections efficiently, ensuring faster transaction processing.
2. AI Integration: Integrate AI for real-time fraud detection during voting, enabling the system to identify and mitigate suspicious activities immediately.

3. Facial Recognition Enhancement: Improve the accuracy and reliability of facial recognition in low-light conditions and varying environments to ensure consistent performance.
4. Multi-Factor Authentication: Incorporate multi-factor authentication (e.g., OTP, biometrics) to strengthen voter security further and prevent unauthorized access.
5. Biometric Authentication: Explore the possibility of integrating additional biometric systems (e.g., fingerprint, iris scan) for a more robust voter identification process.

References

Research Papers:

1. N Prathyusha, P Pooja, A Vijay Vasanth. "Blockchain-Based E-Voting System with Facial Recognition." International Conference on Inventive Computation Technologies (ICICT), 2023.

2. Rifa Hanifatunnisa, Budi Rahardjo. A review paper on Blockchain Based E-Voting Recording System Design, 11th International Conference on Telecommunication Systems Services and Applications (TSSA),2017.

3. Kanika Garg,PaviSaraswat,Sachin Bisht, Sahil Kr. Aggarwal, Sai Krishna Kothuri, Sahil Gupta. A Comparitive Analysis on E-Voting System Using Blockchain, 4th International Conference on Internet of Things: Smart Innovation and Usages, 2019.

4. Ali Mansour AI-madani, Ashok T. Gaikwad, Vivek Mahale, Zeyad A.T. Ahmed. Decentralized Evoting System based on Smart Contract by using Blockchain Technology, International Confrernce on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), 2020.

5. Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, Gísli Hjálmtýsson. Blockchain-Based E-Voting System. IEEE International Conference on Cloud Computing, CLOUD 2018.

6. Ayesha Shaikh, Bhavika Oswal, Divya Parekh and B. Y. Jani, "E-voting Using One Time Password and Face Detection and Recognition", *INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT)*, vol. 03, no. 02, February 2014.

7. F. Schroff, D. Kalenichenko and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering", *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 815-823, 2015.

8. I. William, D. R. Ignatius Moses Setiadi, E. H. Rachmawanto, H. A. Santoso and C. A. Sari, "Face Recognition using FaceNet (Survey Performance Test and Comparison)", *2019 Fourth International Conference on Informatics and Computing (ICIC)*, pp. 1-6, 2019.

9. Vernekar, A. G., Phutane, M., Godase, R., Waghmode, V., & Shinde, S. M. (2020). Blockchain based E-Voting System. *International Research Journal of Engineering and Technology (IRJET)*, 7(12), 1786.