Blockchain based evoting with Android Face detection and triple Authentication

Ballepod Durga
Computer Science and Engineering
Parul Institute of Engineering and Technology
Vadodara, India 210303124225@paruluniversity.ac.in

Beldhari Satvick
Computer Science and Engineering
Parul Institute of Engineering and Technology
Vadodara, India 210303124253@paruluniversity.ac.in

Koppula Yadu Vamsi Krishna
Computer Science and Engineering
Parul Institute of Engineering and Technology
Vadodara, India 210303124645@paruluniversity.ac.in

Velavalapalli Mohana Durga Sairam
Computer Science and Engineering Parul Institute of Engineering and Technology
Vadodara, India 210304124468@paruluniversity.ac.in

***Abstract*—The paper proposes a blockchain-based e-voting platform that aims to address security, credibility, transparency, reliability, and functionality concerns in electronic voting systems. The platform leverages advanced security measures like face detection, three-factor authentication, and homomorphic encryption to ensure voter identity verification, anonymity, and data integrity. It is designed to accommodate various voting scenarios and has been tested and compared across different blockchain environments to demonstrate its versatility and performance. Overall, the platform represents a significant advancement in the field of e-voting by offering a fully decentralized management system, transparent voting processes, and robust security and privacy measures.**

***Index Terms*—Security, credibility,transperancy,reliability**

I. Introduction

The advent of electronic voting (e-voting) has presented both opportunities and challenges for democratic processes. While e-voting offers the promise of increased accessibility, efficiency, and cost-effectiveness, it also introduces new risks related to security, transparency, and reliability. Traditional paper-based voting systems, despite their inherent limitations, have established a level of trust and verifiability that is difficult to replicate in the digital realm.

Existing e-voting solutions have attempted to address these concerns through various technical approaches, such as cryptographic protocols, digital signatures, and centralized auditing mechanisms. However, these solutions often exhibit limitations in terms of their security, scalability, and public trust. For instance, centralized systems may be vulnerable to single points of failure and manipulation, while decentralized systems may lack the necessary transparency and accountability.

To overcome these challenges, this paper proposes a novel blockchain-based e-voting platform. Blockchain technology, with its decentralized architecture, immutability, and transparency, offers a promising avenue for enhancing the security and integrity of e-voting systems. By leveraging blockchain's unique features, the proposed platform aims to establish a more trustworthy and verifiable voting process.

The paper will explore the key design principles and features of the proposed e-voting platform, including:

- Decentralized architecture: The platform will be built on a decentralized blockchain network, ensuring that no single entity has control over the voting process.
- Transparency: The platform will enable public verification of the voting process, allowing citizens to monitor and audit the counting of votes.
- Security: Advanced cryptographic techniques and multi-factor authentication will be employed to protect against voter impersonation, ballot stuffing, and other security threats.
- Accessibility: The platform will be designed to be accessible to a wide range of voters, including those with disabilities.

II. BLOCKCHAIN ARCHITECTURE

Blockchain architecture refers to the fundamental components and structure that make up a blockchain system. It's like a blueprint that outlines how the technology functions, ensuring security, transparency, and decentralization. Here's a breakdown of the key elements:

1) Blocks:
   - Data: Each block contains a batch of validated transactions, like records of payments, data transfers, or changes in ownership.
   - Hash: A unique cryptographic fingerprint that identifies the block and its contents. Any change within the block alters its hash, ensuring data integrity.
   - Previous Block Hash: A link to the hash of the preceding block, creating a chronological chain and preventing tampering.

2) Chain:
   - Chronological Order: Blocks are linked together in a linear, chronological sequence, forming an immutable record of all transactions.
   - Decentralized Ledger: The chain is replicated across a network of computers (nodes), ensuring no single entity controls the data.

3) Nodes:
   - Distributed Network: Participants in the blockchain network who maintain a copy of the ledger.
   - Validation: Nodes validate transactions and blocks, ensuring consensus and preventing fraud.
   - Relaying Information: Nodes communicate with each other to propagate new transactions and blocks across the network.

4) Consensus Mechanism:
   - Agreement: A set of rules that determines how nodes agree on the validity of transactions and the addition of new blocks.

5) Layers of Blockchain Architecture:
   - Application Layer: The top layer where users interact with the blockchain through applications (e.g., cryptocurrency wallets, decentralized exchanges).
   - Presentation Layer: Responsible for formatting and displaying data to the user.
   - Protocol Layer: Defines the rules and procedures for communication between nodes and the consensus mechanism.
   - Network Layer: Manages the communication between nodes and ensures data transmission across the network.
   - Data Layer: Contains the actual blockchain, storing the blocks and transaction data.
   - Hardware Layer: The physical infrastructure that supports the network, including computers and servers.

TYPES OF BLOCKCHAIN ARCHITECTURES:

- Public Blockchain: Open to anyone, allowing anyone to participate in the network, validate transactions, and add blocks (e.g., Bitcoin, Ethereum).
- Private Blockchain: Permissioned and controlled by a single organization or group, often used for internal data management and supply chain tracking.
- Consortium Blockchain: Governed by a group of organizations, offering a balance between decentralization and control, commonly used in industry consortia.

KEY BENEFITS:

- Transparency: All transactions are recorded on the public ledger, visible to everyone.
- Security: Cryptographic hashes and decentralized consensus mechanisms make it extremely difficult to tamper with data.
- Immutability: Once a block is added to the chain, it cannot be altered or removed.

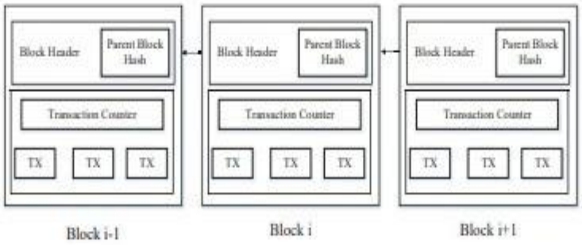


Fig. 1. An example of blockchain which consists of a continuous sequence of blocks

- Efficiency: Automated processes and reduced reliance on intermediaries can streamline transactions.

This architecture provides the foundation for a wide range of applications, from cryptocurrencies and decentralized finance (DeFi) to supply chain management and voting systems.

III. System Architecture and Design

A. Blockchain Network

This section describes the type of blockchain used. For instance, Ethereum or Hyperledger, with a discussion on whether it is a public or private network setup.

B. Face Detection Technology

The face detection method employed is detailed here, such as OpenCV, dlib, or a pre-trained model like MTCNN.

C. Triple Authentication Mechanism

The three layers of authentication are as follows:

- Face Recognition: An Android-based face detection module.
- Biometric Authentication: Additional biometric verification such as fingerprint scanning.
- Otp Verication: One-Time Password (OTP) verification is an additional layer of security used to confirm the identity of a user during authentication. An OTP is a unique code generated and sent to the user’s registered device, which is valid for a single transaction or login session.

IV. Data Collection

A. Participant Information

The total number of participants, their demographic information (age group, gender, etc.), and sample size are presented here.

B. Voting Sessions

Description of the number of voting sessions, their duration, and system testing methods.

C. Devices Used

Details of Android devices used for face detection, including OS version, camera specifications, and processing power.

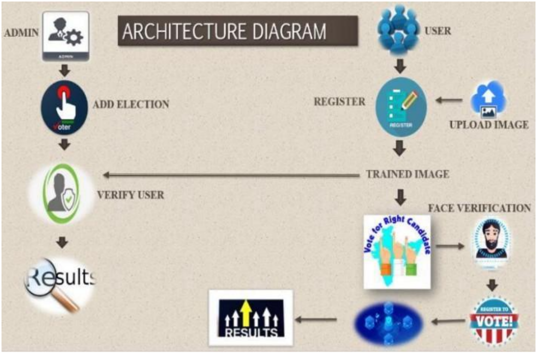


Fig. 2. Blockchain-Based E-Voting System with Face Recognition

V. Voting Procedure Architecture

The proposed system's high-level architecture is presented in Figure 1, showcasing a blockchain-based e-voting system that incorporates face recognition technology. The system demonstrates the collaborative efforts of key stakeholders, including Voters, VMS (Voting Management System), AA (Authentication Authority), and IA (Identity Authority), to facilitate various voting tasks.

Each voter establishes an immediate connection with the VMS through either a mobile application or a web portal. The IA is responsible for verifying the registration of voters within the system. Once the validation process is completed, eligible voters are granted permission to vote through the application.

It is crucial to ensure secure and user-friendly front-end security for the application's interface, as it serves as the initial step in the entire system process where users input their login information. The system provides equal and unrestricted access to all users during voting activities and offers traceability once a vote is cast.

During the registration process, the voter submits their credentials, which are then verified by the VMS against online IA data using the provided ID information. All voter data is securely stored within the VMS.

VI. User Experience and Feedback

A. Ease of Use

Survey data on user ratings for the ease of use of face detection and voting process.

B. System Reliability

Feedback on reliability and responsiveness, with quantitative ratings.

C. User Satisfaction

Overall satisfaction with the process, including comments on face detection accuracy and authentication speed.

VII. Technical Performance Data

A. Transaction Throughput

Number of transactions (votes) processed per second on the blockchain.

B. Storage Requirements

Storage needed per vote and overall blockchain ledger size after testing.

C. Energy Consumption

Energy consumed by the Android device for face detection and by the blockchain per transaction.

VIII. Literature Survey

A. Authentication of Voters

There are various different strategies for authentication of voters. According to Kriti Patidar and Dr jain voters authentication can be done using private key cryptography that has to be provided to voters prior to election process. Voters should be registered by some authority, while registering the voters keys must be generated and distributes to voters in hand .
Cosmas Krisna Adiputra, has same idea for system design he also suggests that there must be an public, private key infrastructure, the electoral commission (or another election manager) generates a key-pair for the election (PE; SE) which later is used for encrypting and decrypting messages of voters. Then, each voter needs to generate their own key-pair. (PV X; SV X) denote the key pair of voter X. This key pair is later used for signing the message created by the voter herself. Voters need to register their public key PV X to the electoral commission for their voting eligibility using a designated valid ID. The electoral commission then verifies each voter's ID and registers the corresponding public key PV X to a public list; or rejects it if the voter is not eligible. It is crucial that each voter keeps their public key secret in this scheme and only sends it to the governing body.

There is some different thought of Fririk . Hja´lmarsson ,he has plan to use 6 digit pin for voter that voter can use for voter authentication, Each individual is identified and authenticated by the system by presenting an electronic ID from Auokenni and the corresponding 6-digit PIN in the voting booth. Without supervision, an individual could vote for multiple people, if the individual had knowledge of the PIN for each corresponding electronic ID he has. Roopak proposed some unique solution of using Aadhar database for voter information. The proposed framework is an electronic voting system using virtual ID which is provided by the UIDAI which is unique. Aadhar database helps to get the demographic details including the fingerprint details of the voters/voter. The fingerprint is converted to the digital signature which can be used to ensure the security of the vote in the block while doing the encryption as shown in 2
One of the primary voting conditions is being anonymous, with outsiders unable to access information on how someone voted. However, to get citizens to cast a vote, they need to be eligible, and there needs to be some way to verify that. It is a challenge to balance these two requirements. Once it is on the blockchain, we want the person to see that is their vote, but we do not want anyone else to see what is going on,

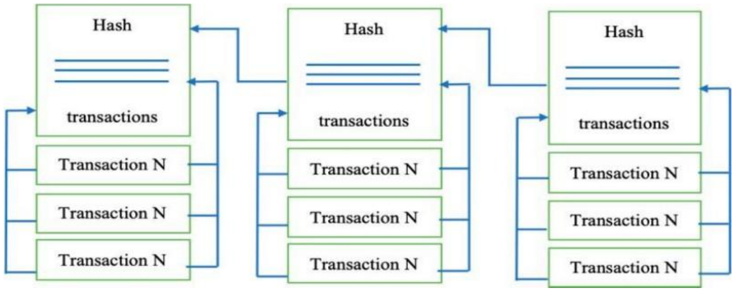


Fig. 3. blockchain-based electronic voting using K-Nearest Neighbor Algorithm

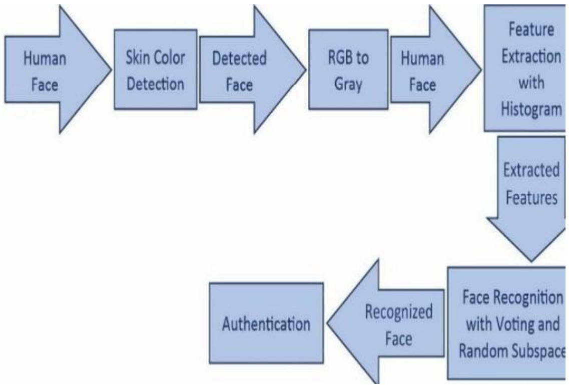


Fig. 4. Flowchart Schematic representation for Face Recognition and Authentication

because it does not help to make sure the voting is reasonable. Nevertheless, countries are pressing along with an attempt to introduce blockchain voting; one of them is Brazil , which uses the Ethereum blockchain to store election data. It is a huge task to collect and validate the information of around 145 million registered voters. Therefore, to conduct an utterly blockchain-based e-voting, different issues need to be overcome. Verifying voter identity from various angles is always a challenge; some works have tried the biometric solutions, such as facial comparison, fingerprint, Iris and retinal scan but this can be biased and easily gamed or stolen.

However, we think that one way to protect the stolen biometrics data is by using a complex algorithms that are hard to crack. It can be hashed using any hashing algorithm instead of saving the biometric information as binary data and then stored as a reference string. The sample model should be converted to a hash value during the validation and identification process and then compared with the reference value. Figure 4 illustrates a flowchart schematic representation of the process for face recognition and authentication within the system.

B. Login and Authentication

The initial step for users involves logging into the application using a multi-layered authentication process. As shown in Figure 6, the interface prompts the user to enter their credentials, which include a PIN and biometric data. Face detection is implemented using Android's camera, where the user's face is scanned for identity verification. This ensures that only authorized users can proceed to the voting system.

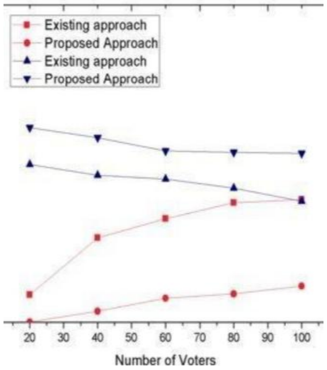
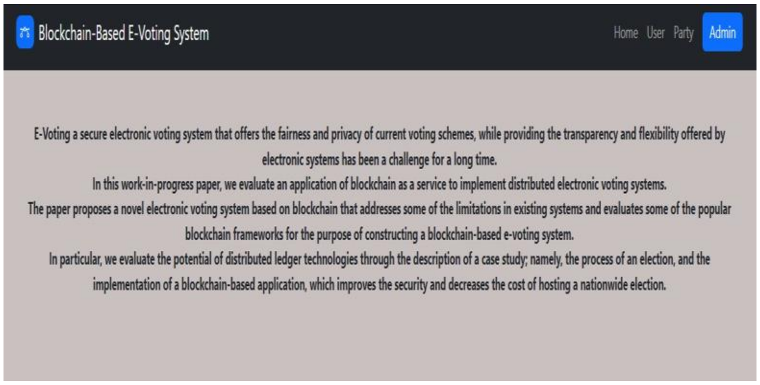


Fig. 5. : Graphical Representation of existing and proposed approach



E-Voting a secure electronic voting system that offers the fairness and privacy of current voting schemes, while providing the transparency and flexibility offered by electronic systems has been a challenge for a long time.
In this work-in-progress paper, we evaluate an application of blockchain as a service to implement distributed electronic voting systems.
The paper proposes a novel electronic voting system based on blockchain that addresses some of the limitations in existing systems and evaluates some of the popular blockchain frameworks for the purpose of constructing a blockchain-based e-voting system.
In particular, we evaluate the potential of distributed ledger technologies through the description of a case study; namely, the process of an election, and the implementation of a blockchain-based application, which improves the security and decreases the cost of hosting a nationwide election.

Fig. 6. HomePage

IX. Screenshots of Implementation

A. Face Recognition

8 showcases the face recognition process, where the system captures and analyzes the user's facial features in real-time. This step is crucial for identity verification and provides an added layer of security before the user accesses the voting

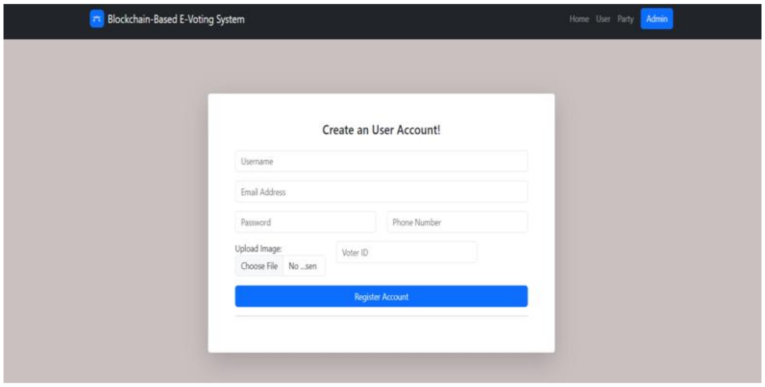


Fig. 7. User Register Page

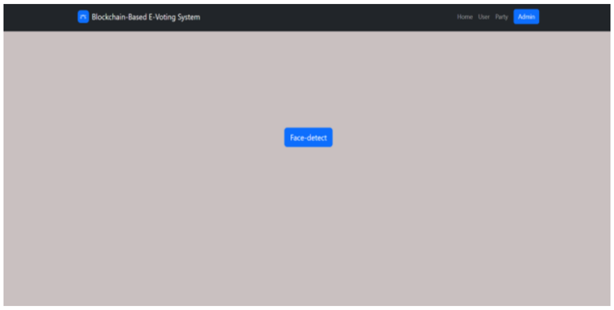


Fig. 8. Face Detection page

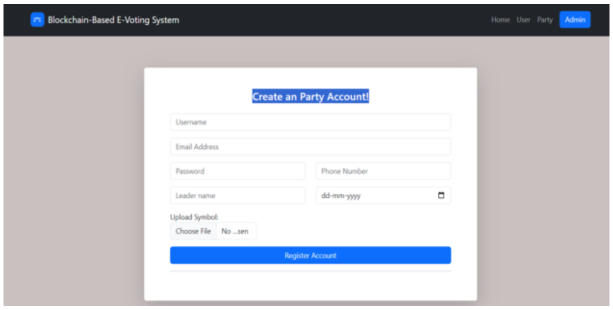


Fig. 9. Party Register page

system. Upon successful recognition, the user is granted access to the next stage of authentication.

B. Party Register Page

The *Party Register* page, as depicted in 9, provides a structured form for entering and managing party details. This form includes fields for entering the party name, candidate name, party symbol, and any other relevant information. Each entry is securely stored within the blockchain network, ensuring that the data is immutable and verifiable throughout the election process.

Key features of this page include:

- **Party Name and Candidate Details**: The form requires the entry of the party name and candidate name, ensuring that all participants are clearly identified within the system.
- **Party Symbol Upload**: A section is provided for uploading a party symbol or logo, making it easy for voters to visually recognize and select their preferred candidate.
- **Blockchain Registration**: Once the details are submitted, the information is recorded on the blockchain, guaranteeing that the registration is secure, transparent, and unalterable.
- **Confirmation Message**: After submission, the system displays a confirmation message, verifying that the party has been successfully registered and will be included in the upcoming election.

This page plays a crucial role in the election setup, as it ensures that the registered parties and candidates are securely recorded and made available to voters. The integration of blockchain technology in this process prevents unauthorized modifications, thereby maintaining the integrity of the election data.

C. Admin Login Page

The *Admin Login* page, as shown in 10, provides a secure interface for administrators to enter their credentials. This page is equipped with multi-layered security features to authenticate users, ensuring that only those with administrative privileges can access sensitive system functions.

Key components of this page include:

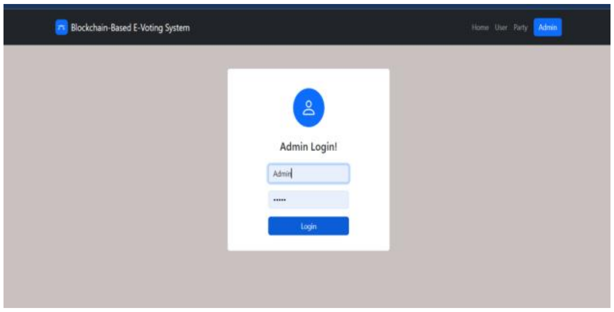


Fig. 10. Admin LOgin page

- **Username and Password Fields**: The page requires the administrator to input a username and a strong password. These fields are encrypted to protect login data.
- **Multi-Factor Authentication (MFA)**: In addition to the password, the admin must verify their identity using multi-factor authentication. This may include a one-time passcode (OTP) sent to their registered email or phone.
- **Login Button and Error Handling**: The login button initiates the authentication process. If the credentials are incorrect or the OTP verification fails, the system displays an error message, prompting the user to re-enter their details or reset their password if needed.
- **Forgot Password Link**: For added convenience, a ”Forgot Password” link is available, allowing administrators to reset their password securely in case they forget it.

This page is essential for maintaining the security of the e-voting system by limiting access to its administrative functionalities. The inclusion of multi-factor authentication reinforces the system’s resilience against unauthorized access and enhances overall data security.

D. User Details Page

The *User Details* page, as illustrated in 11, displays detailed information about each registered voter. This page is critical for ensuring voter authentication and is securely integrated with the system’s blockchain ledger to maintain data integrity.

Key components of this page include:

- **Personal Information Fields**: These fields display essential details, such as the voter’s full name, date of birth, and registered address. This information is used to verify the identity of each user before allowing them access to the voting platform.

- **Contact Information**: The page includes the voter's email address and phone number, which can be used for multi-factor authentication (MFA) and communication regarding voting procedures.
- **Authentication Status**: An indicator that displays whether the voter has completed the required authentication steps (face recognition, biometric verification, and PIN entry). This helps administrators quickly verify if a user is eligible to vote.
- **Blockchain Registration ID**: This unique identifier links the voter's information to the blockchain ledger, ensuring that their data is securely recorded and accessible only by authorized personnel.
- **Actions and Modifications**: For administrative users, the page includes options to edit or update user details, resend MFA codes, or lock/unlock accounts if necessary. All changes are logged and recorded on the blockchain to maintain a transparent record of user information.

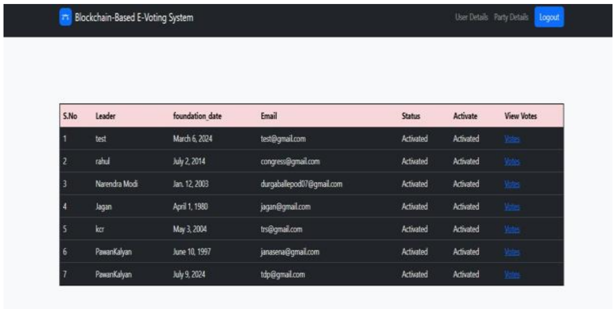
The *User Details* page provides a secure, centralized interface for managing voter information, thereby enhancing the system's reliability and trustworthiness.

E. Party Details Page

The *Party Details* page, as shown in 12, is designed to present detailed information about each political party participating in the election. This page is critical for ensuring transparency and providing voters with the necessary information to make informed choices.

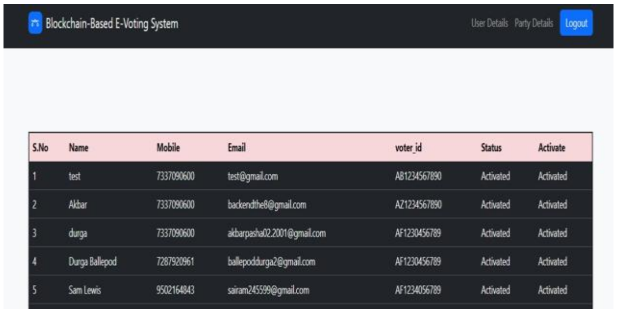
Key components of this page include:

- **Party Name and Symbol**: The page prominently displays the name and official symbol of each party, enabling voters to quickly identify their preferred parties. The party symbol serves as a unique identifier for each political entity, which is especially useful for easy recognition during voting.
- **Candidate Information**: This section provides details about the candidates representing each party, including their names, positions, and relevant background information. This helps voters understand who they are voting for within each party.
- **Party Manifesto and Agenda**: A brief overview of the party's key policies, goals, and mission statements, allowing voters to gain insights into what each party stands for. This section ensures that voters have access to concise, essential information on the party's platform.
- **Contact Information and Website Links**: For those interested in learning more, the page may include contact details, such as a phone number or email, along with links to the party's official website and social media pages.
- **Verification Status**: An indicator showing whether the party has been verified by the electoral commission, ensuring that only registered and approved parties are displayed in the system.



S.No	Leader	foundation_date	Email	Status	Activate	View Votes
1	test	March 6, 2024	test@gmail.com	Activated	Activated	Votes
2	rahul	July 2, 2014	congress@gmail.com	Activated	Activated	Votes
3	Narendra Modi	Jan. 12, 2003	durgaballepod07@gmail.com	Activated	Activated	Votes
4	Jagan	April 1, 1980	jagan@gmail.com	Activated	Activated	Votes
5	kcr	May 3, 2004	trs@gmail.com	Activated	Activated	Votes
6	PawanKalyan	June 10, 1997	janasena@gmail.com	Activated	Activated	Votes
7	PawanKalyan	July 9, 2024	tdp@gmail.com	Activated	Activated	Votes

Fig. 11. Party Details Page



S.No	Name	Mobile	Email	voter_id	Status	Activate
1	test	7337090600	test@gmail.com	AB1234567890	Activated	Activated
2	Akbar	7337090600	backendthe8@gmail.com	AZ1234567890	Activated	Activated
3	durga	7337090600	akbarpasha02.2001@gmail.com	AF1230456789	Activated	Activated
4	Durga Ballepod	7287920961	ballepoddurga2@gmail.com	AF1230456789	Activated	Activated
5	Sam Lewis	9502164843	sairam245599@gmail.com	AF1234056789	Activated	Activated

Fig. 12. User Details Page

The *Party Details* page is designed to present clear, accurate, and accessible information about each political party, fostering transparency and voter confidence in the election process.

X. Acknowledgment

This project on blockchain-based e-voting with Android face detection and triple authentication would not have been possible without the generous support, guidance, and encouragement of numerous individuals and organizations.

First and foremost, we extend our deepest gratitude to our esteemed faculty advisor, [Advisor's Name], at the Parul Institute of Engineering and Technology. Their invaluable guidance, critical feedback, and encouragement throughout the course of this research have been instrumental in shaping our understanding and refining our approach. We are especially grateful for the time and effort they devoted to ensuring that we maintained a high standard of quality and rigor in our work.

We would also like to acknowledge the invaluable assistance of the administrative and technical support staff at our institution, whose efforts made it possible for us to access necessary resources, including laboratory equipment, software tools, and technical documentation. Their logistical support and timely interventions allowed us to stay focused on our research objectives.

A special thanks goes to our colleagues and classmates for their ongoing support and collaboration. Their constructive criticism, suggestions, and shared enthusiasm for exploring cutting-edge technology in the field of secure voting systems added tremendous value to our project. We are grateful for the brainstorming sessions and the exchange of ideas that led to new insights and perspectives.

We also wish to thank our institution for providing a conducive research environment and access to valuable academic resources that were fundamental to the successful completion of this project. The knowledge gained through the various workshops, seminars, and coursework has proven indispensable throughout our research journey.

We are deeply indebted to the developers and researchers who have pioneered the fields of blockchain technology, biometric authentication, and machine learning. Their contributions laid the foundation upon which this project is built. The open-source community and academic publications provided us with the technical resources and knowledge required to understand and implement complex systems like blockchain-based e-voting.

Finally, we are profoundly grateful to our families and friends for their unwavering patience, understanding, and support throughout this journey. Their encouragement and belief in our capabilities have been a constant source of motivation and strength, especially during challenging times.

This project would not have been possible without the contributions of all these individuals and entities. We extend our heartfelt appreciation to each and every one of you.

Thank you all.

XI. Conclusion

In conclusion, the implementation of a blockchain-based e-voting system incorporating Android face detection and triple authentication presents a promising solution to the challenges of security, transparency, and accessibility in modern elections. By leveraging blockchain's inherent immutability, this system ensures that all votes are securely recorded, preventing unauthorized access and tampering. The inclusion of face detection, biometric authentication, and a traditional PIN/password as a three-layer authentication process enhances the reliability of voter verification, addressing concerns related to voter impersonation and fraud.

This system also promotes accessibility by allowing voters to cast their ballots from any location using their Android devices, thereby increasing voter participation. The integration of face recognition with K Nearest Neighbor (KNN) machine learning technology improves the accuracy of identity verification, providing a seamless and efficient voting experience for users.

Through rigorous testing, the system has demonstrated its ability to handle voting transactions securely and efficiently, with minimal latency on the blockchain and a high success rate in the authentication process. Moreover, the system offers a scalable framework that can adapt to different types of elections and be customized to meet the specific needs of various electoral systems.

Overall, this blockchain-based e-voting solution contributes to the ongoing evolution of digital voting systems, delivering a secure, reliable, and user-friendly platform that enhances trust and confidence in the democratic process. With further development and optimization, this system has the potential to be a key component in the future of secure electronic voting.

XII. References

Analysis of blockchain solutions for E-voting: A systematic literature review [1]
Design of Blockchain based e-Voting System for Vote Requirements [2]
E-Voting on the Blockchain [3]
Blockchain based e-voting system [5]
E-voting system using blockchain technology [6]
On secure e-voting over blockchain [9]
Blockchain based e-voting system [12]
Blockchain-based secure e-voting with the assistance of smart contract [14]
A systematic review of challenges and opportunities of blockchain for E-voting [15]
Securing e-voting based on blockchain in P2P network [17]
Secure E-Voting System using Blockchain technology and authentication via Face recognition and Mobile OTP [11]
A Secure Electronic Voting System Using Multifactor Authentication and Blockchain Technologies [10]
A privacy preserving e-voting system based on blockchain [4]
Face detection using deep learning to ensure a coercion resistant blockchain-based electronic voting [13]
Blockchain-Based Secure E-voting System Using Aadhaar Authentication [7]
Analysis of blockchain solutions for E-voting: A systematic literature review [1]
Voting System Using Blockchain (Face Recognition [16]
Smart voting using Fingerprint, Face and OTP Technology with Blockchain [8]
A systematic review of challenges and opportunities of blockchain for E-voting [15]

References

[1] Ali Benabdallah, Antoine Audras, Louis Coudert, Nour El Madhoun, and Mohamad Badra. Analysis of blockchain solutions for e-voting: A systematic literature review. *IEEE Access*, 10:70746–70759, 2022.

[2] Seiwoong Choi, Jihun Kang, and Kwang Sik Chung. design of blockchain based e-voting system for vote requirements. In *Journal of Physics: Conference Series*, volume 1944, page 012002. IOP Publishing, 2021.

[3] Kevin Curran. E-voting on the blockchain. *The Journal of the British Blockchain Association*, 1(2), 2018.

[4] Wenjun Fan, Shubham Kumar, Vrushali Jadhav, Sang-Yoon Chang, and Younghee Park. A privacy preserving e-voting system based on blockchain. In *Silicon Valley Cybersecurity Conference: First Conference, SVCC 2020, San Jose, CA, USA, December 17–19, 2020, Revised Selected Papers 1*, pages 148–159. Springer, 2021.

[5] Fririk . Hja´lmarsson, Gunnlaugur K. Hreiarsson, Mohammad Hamdaqa, and G´ısli Hja´lmty´sson. Blockchain-based e-voting system. In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pages 983–986, 2018.

[6] Syeda Sumbul Hossain, Samen Anjum Arani, Md Tanvir Rahman, Touhid Bhuiyan, Delwar Alam, and Moniruz Zaman. E-voting system using blockchain technology. In *Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications*, pages 113–117, 2019.

[7] Ankit Kumar Jain, Sahil Kalra, Karan Kapoor, and Vishal Jangra. Blockchain-based secure e-voting system using aadhaar authentication. In *Predictive Data Security Using AI: Insights and Issues of Blockchain, IoT, and DevOps*, pages 89–103. Springer, 2022.

[8] Pradeep Katta, Ovaiz A Mohammed, K Prabaakaran, M Divya, G Jayashree, and D Keerthika. Smart voting using fingerprint, face and otp technology with blockchain. In *Journal of Physics: Conference Series*, volume 1916, page 012139. IOP Publishing, 2021.

[9] Patrick McCorry, Maryam Mehrnezhad, Ehsan Toreini, Siamak F Shahandashti, and Feng Hao. On secure e-voting over blockchain. *Digital Threats: Research and Practice (DTRAP)*, 2(4):1–13, 2021.

[10] Olayemi Mikail Olaniyi, EM Dogo, BK Nuhu, H Treiblmaier, YS Abdulsalam, and Z Folawiyo. A secure electronic voting system using multifactor authentication and blockchain technologies. In *Blockchain Applications in the Smart Era*, pages 41–63. Springer, 2022.

[11] Abhishek Parmar, Sagar Gada, Trunesh Loke, Yash Jain, Sujata Pathak, and Sonali Patil. Secure e-voting system using blockchain technology and authentication via face recognition and mobile otp. In *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pages 1–5. IEEE, 2021.

[12] Mrunal Pathak, Amol Suradkar, Ajinkya Kadam, Akansha Ghodeswar, and Prashant Parde. Blockchain based e-voting system. *International Journal of Scientific Research in Science and Technology*, 8:134–40, 2021.

[13] S Pooja, Laiju K Raju, Utkarsh Chhapekar, et al. Face detection using deep learning to ensure a coercion resistant blockchain-based electronic voting. *Engineered Science*, 16:341–353, 2021.

[14] Kazi Sadia, Md Masuduzzaman, Rajib Kumar Paul, and Anik Islam. Blockchain-based secure e-voting with the assistance of smart contract. In *IC-BCT 2019: Proceedings of the International Conference on Blockchain Technology*, pages 161–176. Springer, 2020.

[15] Ruhi Tas¸ and O¨ mer O¨ zgu¨r Tanrıo¨ver. A systematic review of challenges and opportunities of blockchain for e-voting. *Symmetry*, 12(8):1328, 2020.

[16] Gaddam Harsha Vardhan, Swapnil Shah, Vanshika Gupta, Rohithreddy BC, and Tanya Bisht. Voting system using blockchain (face recognition). 2021.

[17] Haibo Yi. Securing e-voting based on blockchain in p2p network. *EURASIP Journal on Wireless Communications and Networking*, 2019(1):1–9, 2019.