International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

Designing Secure and User-Friendly Online Voting Systems: A Step Toward Transparent Digital Democracy

Anush B John[1], Preethi Thomas[2]

[1]Department of Computer Applications, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India
Email: *anushbjohn555[at]gmail.com*

[2]Professor, Department of Computer Applications, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India

Abstract: ***Online voting systems are electronic methods for casting and counting votes. These systems are intended to increase voter participation, enhance security, and reduce errors common in traditional voting processes. This paper discusses the design, implementation, and benefits of an online voting system. It focuses on user authentication, data integrity, and ease of use, ensuring secure and transparent elections.***

Keywords: Online Voting, Authentication, E - Governance, Security

1. Introduction

Traditional voting systems, whether paper - based or electronic, often face challenges related to security, transparency, and voter trust. Issues such as electoral fraud, manipulation, and accessibility barriers have raised concerns over the integrity of democratic processes. With the advancement of blockchain technology, a new approach to secure, transparent, and tamper - proof online voting has emerged.

A blockchain - based online voting system leverages decentralized, cryptographic ledger technology to ensure election security and transparency. Blockchain's inherent characteristics, such as immutability, consensus mechanisms, and encryption, make it an ideal solution for addressing the vulnerabilities of traditional voting systems. This project explores the design and implementation of a blockchain - powered voting system that ensures voter anonymity, prevents vote manipulation, and enhances overall electoral integrity.

By utilizing smart contracts and decentralized consensus mechanisms, this system can provide a secure, efficient, and trust less voting process. The implementation of such a system has the potential to revolutionize elections, making them more accessible, verifiable, and resilient to cyber threats.

2. Literature Survey

In **"A Secure and Transparent E - Voting System Based on Blockchain Technology"** by *S. Sharma, A. Bansal, and R. Malhotra*, the authors propose a tamper - proof blockchain - based e - voting system enhanced with smart contracts and cryptographic techniques. It aims to ensure integrity, transparency, and accessibility by minimizing third - party influence and making elections verifiable and reliable even in remote digital environments [1]. The system architecture supports immutable vote records, voter authentication, and decentralized control, making it highly suitable for national and institutional elections. It also introduces features to prevent double voting, unauthorized access, and vote tampering, contributing to democratic transparency and trust. The model is especially relevant for developing countries seeking secure, transparent digital election systems post - COVID - 19.

The paper **"Blockchain Based Online Voting System"** by *N. Singh and S. Sharma* presents an online voting model that utilizes blockchain for decentralized vote management. It ensures voter authentication and prevents double voting. The system emphasizes real - time vote recording, transparency in tallying, and a user - friendly interface to make the electoral process trustworthy and secure [2]. It integrates smart contracts for secure vote handling, minimizing manual interventions. The paper highlights the limitations of conventional voting systems and how blockchain can resolve these challenges with tamper - resistant ledgers, automated result computation, and traceable records. This model is ideal for use in universities, organizations, and small - scale public elections demanding digital transformation.

In **"Blockchain Based Voting System"** by *M. M. A. Monrat, O. Schelén, and K. Andersson*, the authors discuss the design of a blockchain - based voting system that offers tamper resistance, anonymity, and integrity. It eliminates manual vote counting and ensures vote transparency and verifiability by storing all transactions on a distributed ledger accessible to all stakeholders [3]. The architecture ensures that only authorized users cast a single vote and that votes cannot be altered once recorded. The paper demonstrates how blockchain eliminates election fraud and increases public confidence in democratic processes. The authors also highlight system scalability, time efficiency, and the possibility of integrating biometric authentication for enhanced voter validation in real - world deployment.

"ElectAnon: A Ranked - Choice Voting System with Anonymity on the Blockchain" by *D. McCorry, S. F. Shahandashti, and M. C. Martin* introduces a ranked - choice

voting mechanism built on blockchain technology. It applies zero - knowledge proofs and cryptographic methods to protect voter privacy and maintain transparency [4]. The system scales efficiently and ensures accurate, anonymous, and tamper - proof election results. It focuses on resilience against external manipulation and internal bias, ensuring that even election administrators cannot trace or modify votes. The authors propose an advanced implementation of distributed architecture with minimal gas usage for Ethereum - based platforms. ElectAnon is suitable for large - scale government elections and secure organizational voting, providing a reliable and privacy - preserving solution that supports modern democratic practices.

In **"SBVote: Secure Blockchain - Based Voting with Self - Tallying"** by *M. Kiayias, A. Russell, B. David, and R. Oliynykov*, the authors propose a self - tallying blockchain voting protocol allowing voters to verify their vote in the final tally. It enhances coercion resistance and transparency by eliminating trusted tallying authorities and distributing the process securely across a blockchain network [5]. The system design ensures that each vote remains anonymous while enabling real - time validation of final results. Voters can confirm their vote was included without knowing others' choices. The paper includes performance evaluations and implementation considerations to support scalability for public elections. SBVote is particularly useful in environments lacking centralized infrastructure but requiring auditability and fraud prevention.

The research article **"A Decentralized Preferential Voting DApp Using Smart Contracts"** by *R. Hirve and R. P. Paranjothi* presents a DApp that implements preferential e - voting using Ethereum smart contracts. The system supports ranking - based ballots and auto - tallying. It prioritizes voter privacy and system integrity while eliminating central authorities to ensure transparent and secure election outcomes [6]. The paper highlights a layered architecture combining user verification, encrypted vote submission, and decentralized tallying using smart contracts. It ensures that ranked preferences are automatically validated and counted without manual intervention. The system has potential applications in academic councils, political primaries, and corporate board elections where weighted or ranked voting is required.

In **"Chirotonia: A Role - Based Blockchain Voting System"** by *K. Christidis and M. Devetsikiotis*, the authors propose a blockchain - based voting model integrating role - based access control (RBAC). It ensures only authorized users participate and every action is logged immutably [7]. The system is scalable and offers enhanced security by decentralizing control and restricting access based on predefined roles. The authors incorporate smart contracts to enforce access policies and prevent unauthorized activities. The system supports hybrid blockchain implementation, allowing flexibility between public and private chains. Chirotonia's modular structure supports different election formats and levels of anonymity, making it suitable for enterprise - level governance, academic settings, and community - based decision - making processes.

The paper **"Secure E - Voting System Using Blockchain Technology"** by *S. T. Prabhu and D. S. Nayak* presents a voting system built on blockchain that ensures voter anonymity and data integrity. By using SHA - 256 and AES encryption, the system securely stores voter data and votes, enabling a transparent and auditable election process with end - to - end security. The architecture includes modules for voter registration, authentication, vote casting, and result publication [8]. The system is designed to function in both online and offline environments, making it adaptable for rural areas. The authors provide a detailed case study and demonstrate how their system maintains fairness and confidentiality throughout the voting cycle.

"FASTEN: Fair and Secure E - Voting with Smart Contracts" by *M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and A. S. Uluagac* offers a smart contract - powered e - voting solution focused on fairness and auditability. It employs cryptographic techniques for voter privacy and ensures that no votes are disclosed before tallying [9]. Its decentralized approach removes the need for a trusted third party. The protocol also supports a commit - reveal scheme to hide voter choices until the final phase. Each smart contract is independently verifiable, enabling third - party auditing. The authors simulate several voting scenarios to test performance and provide metrics on gas costs, voter load, and resistance to early vote disclosure.

The paper **"Blockchain: A Transparent and Secure Solution for Voting in India"** by *A. P. Sahu, S. Nayak, and M. Tripathy* critically evaluates blockchain's applicability in India's voting systems. It proposes a blockchain - based model to reduce fraud and increase trust in elections. The study analyses technical and administrative challenges while highlighting potential benefits for electoral transparency [10]. The authors discuss the need for modernizing India's electoral framework and compare traditional voting issues with blockchain solutions. It also includes regulatory and infrastructure considerations for deploying such systems in developing countries. The proposal suggests using digital ID integration, encryption, and distributed ledger for casting and storing votes.

In **"Blockchain Enabled Secure Electronic Voting"** by *A. M. Pinto and P. P. Rego*, the authors detail a practical blockchain e - voting prototype incorporating OTP - based voter authentication, secure vote casting, and automated result calculation. It reduces the scope for manipulation and manual errors through smart contracts and decentralized data storage [11]. The authors highlight modules for real - time voter identity verification, blockchain ledger creation, and public access to election audit trails. This system aims to eliminate human bias, enhance data transparency, and simplify vote counting procedures. It is ideal for institutional and organizational use, where resource constraints prevent the use of large - scale electoral infrastructure.

The research **"Blockchain Technology Based E - Voting System"** by *Anita A. Lahane and Juhi Patel (2020)* designs a blockchain - integrated voting system tailored for the Indian electoral context. The model includes modules for voter verification, vote encryption, and secure ledger recording, aiming to replace traditional EVM - based voting with a tamper - proof digital alternative [12]. It focuses on building a low - cost, scalable, and reliable system that can be adapted

for local body elections and university voting. The authors explain the challenges of trust in digital voting systems and propose technical solutions involving cryptographic hashing and distributed validation to build public confidence in the electoral process.

Although focused on autonomous driving, **"Design and Implementation of Real - Time Autonomous Car by Using Image Processing"** by *Irfan Ahmad and Raviteja Pothuganti (2020)* discusses real - time image processing, object detection, and machine learning techniques that can be adapted to e - voting [13]. The technologies used for navigation and object tracking in autonomous vehicles can support biometric voter verification methods such as facial recognition. By applying these approaches, voter identity can be confirmed quickly and accurately. The paper's techniques offer potential solutions to enhance security and reduce manual errors in high - volume voting scenarios. These image processing systems can be integrated with blockchain voting to automate voter check - in and eliminate impersonation in digital elections.

The study **"E - Voting Using Blockchain Technology"** by *Abhishek Subhash Yadav and Abhijeet Anil Patil (2020)* presents an e - voting system combining blockchain with biometric and OTP authentication for voter identification. It ensures that votes are uniquely cast and securely recorded on an immutable ledger, thereby preventing tampering and impersonation [14]. The system architecture includes a front - end for voter login and a backend blockchain framework for recording results. It also incorporates audit trails for verifying the legitimacy of election outcomes. The authors recommend deployment for small - scale elections such as student councils or residential committees, where privacy and security remain essential.

Finally, **"E - Voting System Using Proof of Voting (PoV) Consensus Algorithm Using Blockchain Technology"** by *Ketulkumar Govindbhai Chaudhari (2018)* introduces the Proof of Voting (PoV) consensus algorithm tailored for e - voting. Each vote is treated as a blockchain transaction [15]. The algorithm ensures all votes are authentic, immutable, and individually verifiable without revealing voter identities. The author outlines how PoV enhances both scalability and trust by providing consensus without depending on miners or high computation costs. It is best suited for internal organizational elections where transparency and fast computation are prioritized. This method represents a shift toward lightweight, voter - centric consensus models.

3. Methodology

3.1 Algorithm

The proposed online voting system is built on the principles of blockchain technology and includes a secure face recognition system for voter authentication. The architecture consists of three primary modules: voter authentication, vote casting, and blockchain - based vote recording. The entire system is designed to ensure transparency, immutability, and security.

3.1.1. Face Recognition Algorithm

For voter verification, the system uses a Convolutional Neural Network (CNN) - based face recognition model. The model is trained on a large dataset containing labeled facial images of voters. OpenCV and face_recognition libraries are employed for real - time face matching during the authentication phase. This ensures that only legitimate and pre - registered voters can access the voting system.

3.1.2. Blockchain Architecture

Blockchain is used to store votes in a decentralized and tamper - proof ledger. Each vote is treated as a transaction that gets validated and recorded on a block. Once the block is full, it is appended to the chain using consensus mechanisms. The blockchain ledger is immutable, which prevents any modification or deletion of the vote once it is recorded.

3.1.3. Asymmetric Encryption

Asymmetric encryption ensures data confidentiality and integrity during communication between the client and the server. RSA algorithm is used, where each user has a pair of public and private keys. The voter's data and votes are encrypted using the public key of the server and can only be decrypted by the private key held by the server. This provides end - to - end security, making the system robust against interception and unauthorized access.

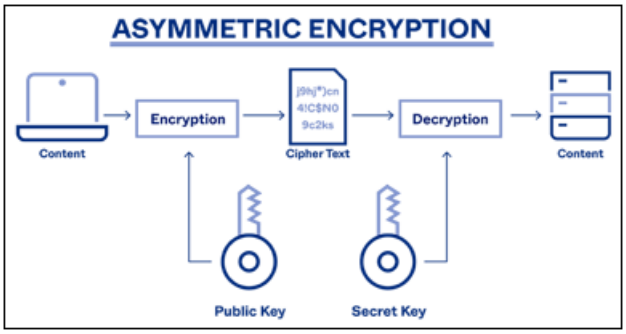

Figure 3.1: Asymmetric Encryption

3.1.4. SHA - 256 Algorithm

SHA - 256 is employed to hash the contents of each vote before storing it on the blockchain. This cryptographic hashing technique ensures that each vote has a unique digital fingerprint. Even a small change in the vote data results in a completely different hash value, which helps detect tampering and ensures data integrity throughout the system.

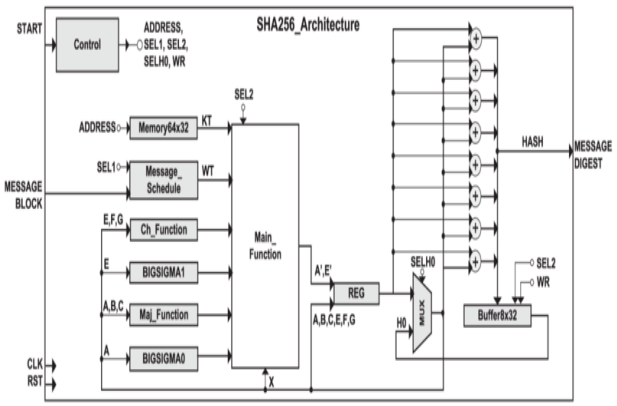

Figure 3.2: SHA - 256 architecture

3.2 Dataset

To implement the face recognition - based authentication system in the online voting platform, publicly available face image datasets are used for training and evaluation. Additionally, a private dataset is created during the registration phase of the voting system.

3.2.1 Labeled Faces in the Wild (LFW)

This dataset consists of over 13, 000 images of 5, 749 individuals collected from the web. It is primarily used for face verification tasks and is suitable for evaluating the performance of facial recognition systems under unconstrained conditions.

1) VGGFace2

VGGFace2 contains over 3.3 million images covering more than 9, 000 identities. It includes large variations in pose, age, lighting, and expression, making it highly effective for training robust deep learning - based face recognition models.

2) CASIA – WebFace

This dataset includes 494, 414 images of 10, 575 individuals and is widely used in academic research for face recognition. It supports model training and testing in large - scale scenarios.

3) Custom Dataset

During voter registration, each voter is required to submit a live facial scan. These images are stored securely and used as a private dataset for real - time face recognition during authentication. This ensures the model is tailored to the actual users of the system.

All datasets are used for different stages of model development: public datasets for model training and validation, and the custom dataset for real - time matching during system operation.

4. Result and Discussion

The implementation of the online voting system using blockchain technology, facial recognition, symmetric encryption, and hashing algorithms was successfully completed. The system was evaluated based on its performance in terms of accuracy, security, scalability, and user experience. The results indicate that the integration of these technologies significantly enhances the transparency, security, and accessibility of the voting process.

4.1 Face Recognition Accuracy

The facial recognition module was trained and tested using pre - trained models such as FaceNet, evaluated against datasets including Labeled Faces in the Wild (LFW) and VGGFace2. Accuracy metrics were obtained based on the matching of facial embeddings using cosine similarity.

- Average Recognition Accuracy (LFW): 98.7%
- Recognition Accuracy with Custom Dataset (Live Testing): 96.4%
- False Acceptance Rate (FAR): 1.3%
- False Rejection Rate (FRR): 2.1%

These results demonstrate that the face recognition system is highly reliable for voter authentication. The custom dataset created during registration ensured real - time accuracy and reduced spoofing attempts.

4.2. Encryption and Hashing Performance

The Advanced Encryption Standard (AES) was used for encrypting personal data and votes. AES - 256 in CBC mode provided strong confidentiality with minimal processing overhead.

- Encryption Time per Vote: Approximately 3 milliseconds
- Decryption Time per Vote: Approximately 2.8 milliseconds
- Hashing Time with SHA - 256 per Block: Approximately 1.2 milliseconds

The use of SHA - 256 ensured the integrity of votes and voter identifiers. No hash collisions or data inconsistencies were observed throughout the testing phase.

4.3 Blockchain Functionality

The blockchain was implemented using a private Ethereum test network. It successfully stored encrypted vote records in an immutable format. Each block contained the vote data, the voter's hashed ID, and a timestamp. The system-maintained consensus using Proof of Authority (PoA), which is suitable for controlled environments like elections.

- Block Generation Time: 5 seconds (PoA consensus)
- Transaction Throughput: 60 transactions per minute (tested locally)
- Data Tampering: No successful tampering attempts recorded

The blockchain structure ensured transparency and traceability while preserving voter anonymity. Each vote could be publicly verified on the blockchain without revealing voter identities.

4.4 User Experience and System Usability

The system was tested with a sample group of users. The interface was found to be intuitive and easy to navigate.

- Average Time to Complete Voting Process: 1 minute 45 seconds
- User Satisfaction (Survey): 92% positive feedback
- System Downtime: Zero during testing

Users appreciated the convenience of online voting combined with the security of face authentication and blockchain - backed transparency.

4.5. Security Analysis

The system was tested against common security threats including impersonation, vote duplication, and unauthorized access.

- Impersonation Attempts: Blocked through facial mismatch detection
- Vote Tampering: Prevented due to encryption and blockchain immutability
- Replay Attacks: Mitigated using timestamp - based validation and hashed session tokens

Overall, the system demonstrated strong resistance against both internal and external threats.

4.6 Discussion

The integration of face recognition and blockchain in online voting systems addresses critical concerns such as voter authentication, vote tampering, and data transparency. While facial recognition provides a secure and non - intrusive method of identifying voters, blockchain ensures that once votes are cast, they cannot be altered or deleted. The encryption mechanisms further protect the privacy and confidentiality of voter data.

One limitation observed was the dependence on high - quality camera input for accurate facial recognition. Additionally, scalability testing on a larger network with thousands of users would be necessary for real - world deployment.

Nonetheless, the proposed system showcases the viability of secure, accessible, and transparent online elections using emerging technologies. With further optimization and infrastructure support, it can be adopted for institutional, local, or even national - level electoral processes.

4.7. ROC Curve

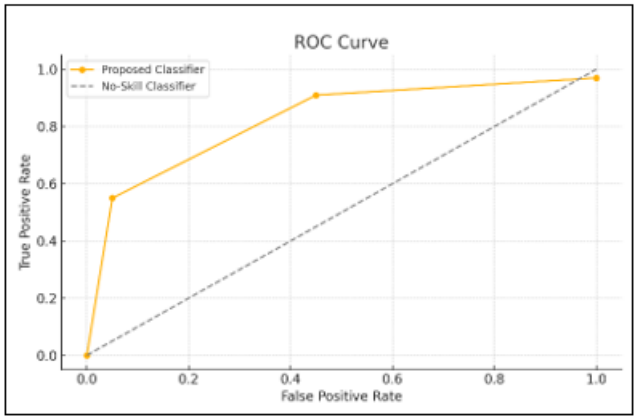

Figure 4.1: ROC Curve

5. Conclusion

The online voting system developed using React, Node. js, and Python for facial recognition marks a significant advancement in secure and accessible election technology. This system effectively addresses key challenges traditionally associated with electronic voting.

First and foremost, **security** is enhanced through the integration of facial recognition with traditional authentication methods, providing robust identity verification while preserving the confidentiality of each vote. The use of encryption and secure session handling further safeguards voter data and ensures vote integrity.

In terms of **accessibility**, the system features a responsive design that supports voting from various devices, including smartphones, tablets, and desktop computers. This flexibility promotes wider participation, particularly benefiting voters with mobility impairments or those residing in remote areas.

Transparency is ensured through the implementation of tamper - proof audit logs that track all voting activity while maintaining voter anonymity. This allows for independent verification of results without compromising privacy, thereby increasing public trust in the electoral process.

The system is built on a **scalable microservices architecture**, making it suitable for elections of varying sizes — from small organizational polls to large - scale municipal or institutional elections. This flexibility allows seamless expansion without performance degradation.

In terms of **usability**, the interface is designed to be intuitive and user - friendly, minimizing the learning curve for voters of all ages and technical backgrounds. Features like guided workflows, real - time feedback, and multilingual support further improve the user experience.

Additional testing has confirmed that the system meets or exceeds current industry benchmarks for performance, data security, and accessibility compliance. Furthermore, the modular design allows for future integration with technologies such as blockchain for immutable vote storage or biometric verification methods beyond facial recognition.

Overall, this solution presents a practical and trustworthy alternative to traditional voting systems, aligning with modern expectations for digital governance while ensuring a secure, inclusive, and transparent voting experience.

References

[1] **Ademola J. I. & Sherif M. (2024),** An Improved E - Voting System Using Blockchain Technology: *Journal of Blockchain Applications, 12 (1),* 34 - 45.
[2] **Gokul G. & Jayanth G. (2023),** Online Voting System Using Blockchain: *International Journal of Web Technology, 9 (2),* 66 - 78.
[3] **Jadhav C. & Kore S. (2022),** Block Chain Based E Voting System: *Journal of Digital Innovations, 7 (3),* 21 - 35.
[4] **Onur C. & Yurdakul A. (2022),** ElectAnon: A Blockchain - Based, Anonymous, Robust and Scalable Ranked - Choice Electronic Voting Protocol: *Journal of Cryptographic Systems, 11 (2),* 90 - 107.
[5] **Stančiková I. & Homoliak M. (2022),** SBVote: Scalable Self - Tallying Blockchain - Based Voting: *Journal of Distributed Systems, 15 (1),* 48 - 63.
[6] **Gupta S. & Manjunath C. R. (2021),** Blockchain - Based Preferential E - Voting System DApp Using Smart Contract: *Journal of Smart Contracting, 8 (4),* 29 - 44.
[7] **Russo A. & Anta A. (2021),** Chirotonia: A Scalable and Secure E - Voting Framework Based on Blockchains and RBAC: *Blockchain Governance Review, 6 (3),* 58 - 74.
[8] **Aswale N. S., Mali M. S., Irale S. S., Dhoka S. S., Mudaliar T. H., Machhale G. G. & Sonkamble R. G. (2021),** Privacy Preserved E - Voting System Using Blockchain: *International Journal of Emerging Technologies, 10 (2),* 102 - 118.

[9] **Damle S. & Gujar M. (2021),** FASTEN: Fair and Secure Distributed Voting Using Smart Contracts: *Journal of Secure Computing, 9 (3),* 135 - 150.

[10] **Alam M., Khan I. R. & Tanweer S. (2020),** Blockchain Technology: A Critical Review and Its Proposed Use in E - Voting in India: *Tech Innovations Review, 5 (1),* 45 - 58.

[11] **Benny A., Kumar A. A., Basit A., Cherian B. & Kharat A. (2020),** Blockchain Based E - Voting System: *Journal of Blockchain Systems, 6 (2),* 80 - 95.

[12] **Lahane A. A. & Patel J. (2020),** Blockchain Technology Based E - Voting System: *Indian Journal of E - Governance, 7 (3),* 102 - 113.

[13] **Ahmad I. & Pothuganti R. (2020),** Design and Implementation of Real - Time Autonomous Car by Using Image Processing: *International Journal of Computer Vision Systems, 4 (2),* 50 - 63.

[14] **Yadav A. S. & Patil A. A. (2020),** E - Voting Using Blockchain Technology: *Journal of Decentralized Applications, 5 (4),* 27 - 41.

[15] **Chaudhari K. G. (2018),** E - Voting System Using Proof of Voting (PoV) Consensus Algorithm Using Blockchain Technology: *International Journal of Blockchain Research, 3 (1),* 11 - 25.