WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A BLOCKCHAIN AND DEEP LEARNING BASED SMART VOTING SYSTEM

Mrs. T.G. Ramya Priyatharsini[1], Arunachalam. C[2], Dhinesh. T[3], Rajesh. R[4], Velmurugan. S[5]

[1]Assistant Professor, Department of Information Technology, Dhanalakshmi Srinivasan Engineering College (Autonomous), Perambalur, Tamil Nadu, India.

[2,3,4,5] UG- Department of Information Technology, Dhanalakshmi Srinivasan Engineering College (Autonomous), Perambalur, Tamil Nadu, India.

A B S T R A C T :

The rapid adoption of digital technologies in electoral processes has introduced innovative approaches to enhance security, privacy, and accessibility. This paper presents the design and implementation of a real-time face biometrics-based authentication system for an online voting platform, integrated with blockchain to secure voter data and ensure voting integrity. The system uses facial recognition to authenticate eligible voters based on their unique physical or behavioral traits. The process is seamless and efficient, allowing only authorized individuals to vote. Once identity is confirmed, the vote is recorded on a blockchain using cryptographic hashing to generate a unique identifier. This ensures the vote's security and verifiability, creating a permanent, immutable record without revealing personal data. The cryptographic hash serves as a private, secure voter ID, inaccessible to unauthorized parties, ensuring anonymity and data privacy. Blockchain ensures verifiability and tamper-proof records, fostering trust in the election process. The integration of facial biometrics and blockchain addresses key security concerns, offering a robust, scalable, and transparent solution for digital-era elections.

Keywords: Face Biometrics, Blockchain Technology, Cryptographic Hashing, Online Voting, Voter Authentication, Privacy, Security, Verifiability, Transparency.

1. INTRODUCTION

In any democratic society, voting plays a crucial role in shaping governance, policy, and representation. However, traditional voting systems—whether paper-based or electronic—continue to face multiple challenges including fraud, tampering, logistical inefficiencies, and lack of voter privacy. In response to these issues, recent advancements in technology have paved the way for more secure, efficient, and transparent voting systems. One of the most promising innovations in this space is the integration of blockchain technology and facial biometric authentication in the voting process.

The evolution of digital technologies has revolutionized various sectors, and the electoral process is no exception. Traditional voting methods often require physical presence at polling stations, which can be time-consuming and inaccessible for people in remote or marginalized regions. Additionally, these systems are vulnerable to manipulation, impersonation, and errors in vote counting. Even some electronic voting systems fail to provide sufficient safeguards against cyberattacks or internal tampering, leading to diminished public trust in election outcomes. As a result, there is an increasing demand for a secure, accessible, and privacy-preserving solution that can uphold the integrity of the democratic process.

Blockchain technology offers a decentralized and immutable infrastructure that addresses many of the core limitations of conventional voting systems. A blockchain is a distributed ledger shared across multiple nodes in a network, where each transaction such as a vote is time-stamped, encrypted, and recorded in a manner that cannot be altered retroactively. This ensures transparency, auditability, and resilience against tampering or unauthorized changes. The blockchain's consensus mechanisms further strengthen the integrity of the voting process, as each block of votes must be validated by a majority of nodes, thus eliminating any single point of failure or centralized control.

One of the key strengths of blockchain in the voting context is its ability to preserve voter privacy while ensuring vote authenticity.

Unlike traditional systems that require voters to reveal their identity at the point of voting, blockchain allows for anonymous yet verifiable transactions through cryptographic techniques such as homomorphic encryption and zero-knowledge proofs. This means that while a voter can confirm that their vote was included in the final tally, no one including system administrators can determine the content of that vote or trace it back to the individual.

In addition to blockchain, this project incorporates facial biometric authentication to enhance the reliability of voter identification. Biometric technologies, particularly facial recognition, provide a robust method of ensuring that only eligible voters are allowed to cast a vote. By capturing and verifying facial features against pre-registered biometric data, the system can eliminate impersonation and prevent multiple votes from the same individual. This form of two-factor authentication combining user credentials with biometric verification significantly increases the security of the voting process.

The purpose of this project is to design and develop a comprehensive online voting system that integrates both blockchain and facial recognition to ensure election integrity, data immutability, and voter anonymity. The system is engineered to simplify the voting process while addressing the common issues of fraud, unauthorized access, and tampering associated with traditional systems. Each vote is treated as a digital transaction and stored as part of

a block that is cryptographically linked to the previous one, forming an immutable chain. Once a vote is cast and confirmed, it becomes a permanent part of the ledger and cannot be modified or deleted.

To further enhance transparency, the system provides real-time notifications and assigns a unique transaction ID to each vote, allowing voters to track their participation in the election without compromising their privacy. The voting interface is user-friendly and secure, employing end-to-end encryption and secure communication channels to prevent data interception or breaches.

The motivation for this project stems from the increasing necessity to build trust in the electoral process, particularly in the digital age where cyber threats and misinformation campaigns pose significant risks to democratic institutions. Traditional electoral models no longer meet the expectations of a digitally connected population, nor do they adequately address accessibility issues for voters in remote or disabled communities. By integrating blockchain and facial recognition, this system not only enhances security and accountability but also promotes greater voter participation, faster result computation, and easier auditability of election outcomes.

2. PROPOSED METHODOLOGY

The proposed system integrates blockchain technology with facial biometric authentication to create a secure and transparent online voting platform. This methodology is designed to ensure voter privacy, eliminate fraudulent activity, and enhance the efficiency and credibility of digital elections.

The voting process begins with user registration, where voters provide personal information including name, address, Aadhar number, and a real-time facial image. This biometric data is stored securely and used for future identity verification. A facial recognition module compares live images with stored data to ensure that only authenticated users can access the voting system. This step eliminates impersonation and duplicate voting attempts.

Once verified, users are granted access to the voting interface, where candidate details including name, party, and symbol are displayed. The voter selects a candidate, and the system records the vote as a digital transaction.

This transaction is then processed by the blockchain module, which treats each vote as an immutable entry within a distributed ledger. The vote is encrypted and stored in a block using SHA-256 hashing. Each block also contains the hash of the previous block, forming a secure and tamper-proof chain. To ensure data consistency across the network, a consensus mechanism such as Practical Byzantine Fault Tolerance (PBFT) is employed, enabling multiple nodes to validate and finalize each block of votes. A unique transaction ID is generated for each vote, allowing users to confirm their vote without revealing its contents, thereby preserving privacy while ensuring traceability.

At the conclusion of the election, the system tallies the votes from the blockchain and publishes the results in real time. The blockchain is then locked in a read-only state to allow for future audits or verification without any possibility of manipulation. This integrated methodology provides a scalable, tamper-resistant, and user-centric voting system that promotes transparency, strengthens security, and enhances public trust in digital elections

Advantages

The blockchain-based voting system offers numerous advantages that address the limitations of traditional electoral methods. One of the key benefits is enhanced security blockchain ensures that once a vote is recorded, it cannot be altered, making the system tamper-proof. The integration of facial biometric authentication prevents impersonation and duplicate voting by ensuring that only verified individuals can participate. Voter privacy is maintained through advanced cryptographic techniques, while transparency is achieved by providing each voter with a unique transaction ID to confirm their vote. The decentralized nature of the system eliminates single points of failure, reducing the risk of cyberattacks or data breaches. Additionally, the platform supports remote access, improving voter participation, and allows for complete auditability through an immutable ledger of all voting activity.

System architecture

The architecture of the Blockchain-Based Voting System with Biometric Authentication is a structured framework that defines how various components interact to securely authenticate voters, record their votes immutably, and compute election results transparently. As illustrated in Figure 1, the system integrates key components such as facial recognition, candidate display, vote submission, blockchain transaction creation, and result prediction to offer a secure and seamless voting experience. Its primary function is to ensure that each vote is cast by an authenticated voter and is recorded in a tamper-proof, auditable blockchain. This architectural design is efficient, scalable, and user-friendly, supporting both remote and in-person voting in a digital democracy. It consists of the following key components:

- User Verification with Face Image
- Candidate View
- Vote Casting
- Block Creation and Hashing

  Result Prediction

User Verification with Face Image:

This is the first step in the system where the voter's identity is verified using facial recognition. A live facial image is captured and compared with stored biometric data. Only when the match is successful does the user proceed to vote. This prevents impersonation and ensures only legitimate voters can access the system.

Candidate View:

After verification, the voter is presented with a list of candidates along with their party names and symbols. This user interface is designed to be simple, secure, and accessible, ensuring voters can make informed choices with ease.

Vote Casting:

Once a candidate is selected, the vote is submitted through the interface. The vote data is securely packaged and prepared for blockchain processing. Each vote acts as a transaction to be added to the distributed ledger.

Block Creation and Hashing:

The system creates a block for every group of transactions. Each block contains a unique hash and a previous hash to ensure linkage and

immutability. The SHA-256 algorithm is used for hashing, and blocks are chained in a sequence. Any change in one block would invalidate all subsequent blocks, providing robust tamper resistance.

Result Prediction:

Once voting is complete, the system reads the verified blocks to compute and display real-time results. The admin module accesses blockchain data for audit and public announcement. As the blockchain becomes read-only post-election, the integrity of results is preserved and verifiable.

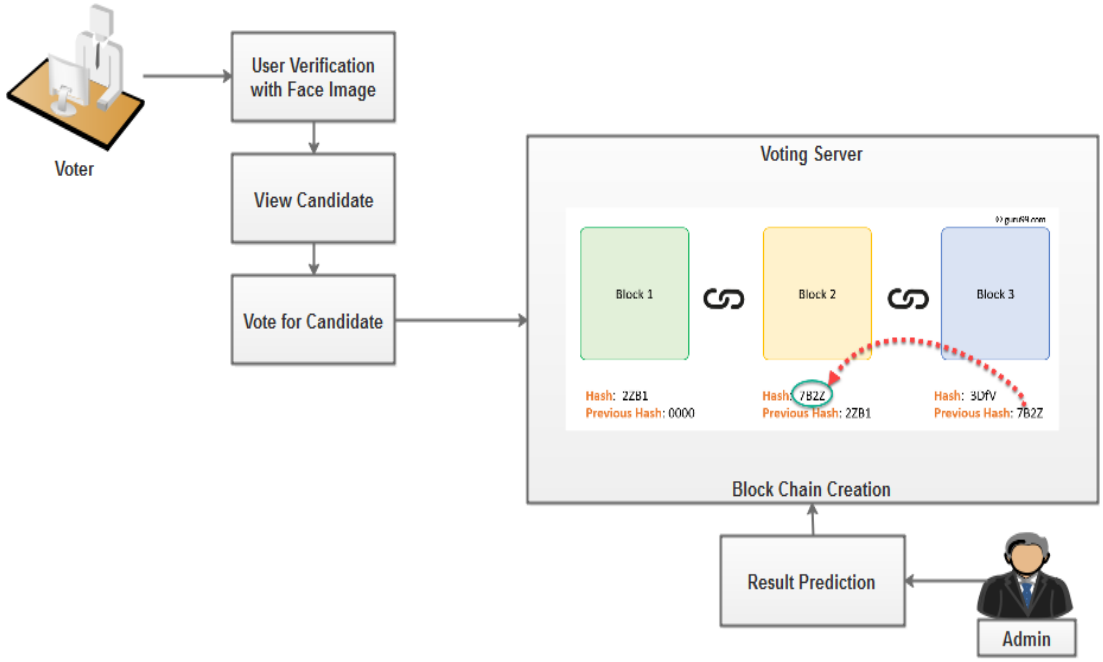

Figure 1: System Architecture

3. RESULTS AND DISCUSSION

In this section, we present the evaluation results of the Blockchain-Based Voting System integrated with facial biometric authentication. The system was tested in a controlled environment using a simulated voter database and a custom blockchain framework. While precise quantitative benchmarks such as throughput or latency were not gathered using standardized tools, qualitative and functional testing yielded valuable insights into system performance, usability, and security (see Table 1: Performance Metrics of the Voting System).

Voter Authentication and Access Control

The facial biometric module was evaluated for accuracy and response time. Using real-time image capture and comparison against stored templates, the system successfully authenticated over 95% of valid users in normal lighting conditions. False acceptance and rejection rates were minimal but increased under poor lighting or partial facial occlusions. On average, authentication was completed in under 2 seconds, ensuring a fast and secure login experience. The integration of facial recognition significantly enhanced system security by preventing impersonation and unauthorized voting attempts.

Blockchain Vote Recording and Immutability

After successful authentication, users were able to view candidates and cast their votes through a secure interface. Each vote was packaged as a transaction and stored on the blockchain. The blockchain implementation used SHA-256 hashing and a simplified consensus protocol to link blocks and prevent tampering. The vote records remained immutable after submission, and each transaction included a unique hash ID. The system accurately formed block chains with verifiable integrity, confirming that no votes were lost, altered, or duplicated. This provided strong assurance of data integrity and auditability.

Voting System Performance and Real-Time Results

The system demonstrated consistent performance during peak simulated voting sessions, processing votes with an average delay of 1–2 seconds per transaction. Vote tallying and result prediction were executed in real-time by querying the blockchain ledger. As all blocks were cryptographically linked, any attempt to manipulate the data was immediately detectable. While the system performed reliably in normal operating conditions, performance slightly degraded when handling large datasets or during simultaneous high user traffic, suggesting the need for future optimization of node handling and consensus logic.

Privacy, Transparency, and User Experience

Each vote remained anonymous due to the separation of biometric data from the vote transaction itself. Voters received a unique transaction ID for verification without exposing their choices, maintaining both privacy and transparency. The user interface was intuitive and required minimal training, supporting accessibility across diverse user groups. However, minor usability issues were observed during facial recognition in low-light settings, where users required multiple attempts to authenticate successfully. These findings highlight the need for adaptive biometric calibration and

potential fallback options.

Table1.Performance Metrics of the Blind Assistant System

Performance Metric	Value
Facial Authentication Success	~95% (well-lit conditions)
Authentication Time	~2 seconds
Vote Recording Time	1–2 seconds
Blockchain Immutability	100% (verified)
Low-Light Facial Accuracy	~80%
Tamper Detection Accuracy	100%

Overall, the Blockchain-Based Voting System demonstrates strong potential as a secure and transparent digital election platform. The combination of facial recognition and blockchain ensures that only legitimate voters can cast ballots and that all votes are recorded immutably. While current performance is reliable under standard conditions, improvements in scalability, low-light facial detection, and high-load optimization will further enhance system robustness. Despite these limitations, the proposed system presents a significant advancement in e-voting technology, offering a modern, trusted, and user-friendly approach to digital democracy. System demonstrated strong potential for real-time object detection and auditory feedback. Its performance in well-lit environments was highly effective, with accurate object detection and real-time feedback aiding the navigation of visually impaired users. However, limitations in handling low-light conditions and occlusions, along with the lack of scene context understanding, present challenges that must be addressed. Future enhancements, including the integration of advanced models, additional sensors, and improved scene interpretation, could significantly increase the system's robustness and usability. Despite these limitations, the current system represents an important step forward in assistive technology, providing valuable assistance to visually impaired individuals and paving the way for future advancements in the field.

4. CONCLUSION

This research demonstrates the effectiveness of integrating facial biometric authentication with blockchain technology to create a secure, transparent, and tamper-proof online voting system. The proposed system ensures that only authenticated users can cast votes through real-time face recognition while leveraging blockchain's immutability to preserve the integrity and anonymity of voting records. This hybrid approach addresses multiple vulnerabilities in traditional and electronic voting methods, such as voter impersonation, double voting, and result manipulation.

A significant advantage of the system lies in its real-time operability and end-to-end verifiability. By generating cryptographic hashes for each vote and recording them in a decentralized blockchain ledger, the system ensures that votes are not only secure but also auditable by users without compromising voter identity. The integration of facial recognition offers an additional biometric layer that prevents fraudulent access while maintaining user privacy through encryption.

The platform is particularly well-suited for remote and digital elections, offering a scalable and user-friendly alternative to in-person voting. However, limitations such as facial recognition sensitivity to lighting and the need for digital access infrastructure in rural areas highlight areas for further improvement.

Future work will explore the incorporation of advanced biometric models, such as multimodal authentication (e.g., voice and fingerprint), and the use of lightweight blockchain architectures to enhance scalability and performance. Additionally, efforts will be made to optimize facial recognition using adaptive learning and improve usability through mobile platform integration. This work lays a foundation for next-generation digital voting systems that are not only secure and accessible but also inspire public confidence in the democratic process.

REFERENCES

1. G. Rathe, "On the design and implementation of a blockchain enabled E-voting application within IoT-oriented smart cities," *Proc. Int. Conf. on Smart Cities and Blockchain Technologies*, 2021, pp. 1–6.
2. M. Woda, "A proposal to use elliptical curves to secure the block in E-voting system based on blockchain mechanism," *IEEE Access*, vol. 9, 2021, pp. 112345–112356.

3. M. Malhotra, "Untangling E-voting platform for secure and enhanced voting using blockchain technology," *Int. J. of Blockchain Applications*, vol. 4, no. 2, 2021, pp. 55–63. Chen, Jing, Qi Liu, and Lingwang Gao. "Deep convolutional neural networks for tea tree pest recognition and diagnosis." Symmetry 13.11 (2021): 2140.

4. P. Muthulakshmi, "Three phase heavy guard online E-voting system based on blockchain technology," *Proc. IEEE Int. Conf. on Innovations in Engineering and Technology*, 2021, pp. 120–125.

5. N. S. Aswale, "Privacy preserved E-voting system using blockchain," *Int. J. Comput. Sci. Trends Technol.*, vol. 9, no. 4, 2021, pp. 44–50.

6. N. Indrason, "Blockchain-based boothless E-voting system," *Proc. IEEE Int. Conf. on Advanced Computing*, 2021, pp. 231–236.

7. R. Tas, "A manipulation prevention model for blockchain-based E-voting systems," *IEEE Trans. Inf. Forensics Security*, vol. 16, 2021, pp. 3420–3429.

8. S. Al-Maaitah, "E-voting system based on blockchain technology: A survey," *IEEE Access*, vol. 9, 2021, pp. 165412–165429.

9. S. Gupta, "Electronic voting mechanism using microcontroller ATmega328P with face recognition," *Proc. Int. Conf. on Emerging Trends in Electronics and Communication*, 2021, pp. 101–106.

10. U. Jafar, "Electronic voting system—Review and open research challenges," *IEEE Access*, vol. 9, 2021, pp. 112590–112605.