iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** II **Month of publication:** February 2025

DOI: https://doi.org/10.22214/ijraset.2025.66992

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue II Feb 2025- Available at www.ijraset.com

Block Chain Enhanced Secure Electronic Voting System Using Real Time Face Recognition and OTP Authentication

Sanket Kale[1], Anand Deshmukh[2], Akash Kale[3], Meghraj Korade[4], Prof. Ashvini Pawale [5]
Information Technology, BSIOTR, Pune, India

Abstract: ***The Real-Time Face Recognition Electronic Voting System is an innovative solution to improve security, reliability, and transparency in electronic voting systems (EVS). Using advanced deep learning models, it accurately recognizes and verifies registered voters by identifying unique patterns in their facial features, which significantly reduces the chances of mistakes, like identifying the wrong person [1]. After a voter's face is successfully recognized, the system sends a one-time password (OTP) to their registered mobile number as an extra layer of security, preventing unauthorized access and reducing the risk of voter fraud [2]. Once voters pass both face recognition and OTP verification, they gain access to the voting interface, where they can securely cast their vote. Every vote is recorded instantly as a unique transaction on a blockchain ledger, which ensures that votes cannot be tampered with. The decentralized nature of blockchain also boosts transparency, allowing voters, election officials, and auditors to verify results without relying on a single central authority [3]. This decentralized setup not only helps prevent vote tampering and data breaches but also makes the system more trustworthy and secure [4]. Designed to work in real time, the system has minimal delays, making it a practical choice for large-scale elections and real-world voting needs.***

Keywords: Face Recognition, Electronic Voting, Neural Networks, OTP, Block chain, Security, Integrity, Biometrics, Tamper-Proof, Transparency.

I. INTRODUCTION

As the need for secure, transparent, and efficient voting systems grows, addressing election security challenges has become increasingly critical. Traditional voting methods, which depend on physical IDs or electronic PINs and passwords, are often vulnerable to fraud and manipulation, raising doubts about election integrity [3]. While electronic voting systems (EVS) can streamline the voting process, they are also susceptible to security threats, including unauthorized access, vote tampering, and disruptions to system functionality. Such vulnerabilities pose risks to the reliability of democratic processes [4].

To tackle these issues, the Real-Time Face Recognition Electronic Voting System combines advanced technologies to offer a secure, user-friendly, and tamper-resistant voting experience. The system is built around three main components: facial recognition using neural networks, OTP-based multi-factor authentication, and blockchain technology for vote recording. Neural networks enable highly accurate facial recognition, which significantly reduces false positives and negatives in voter identification [1]. Once a voter is authenticated through facial recognition, an OTP is sent to their device, providing an additional time-sensitive security layer to protect against unauthorized access [2]. Blockchain technology further enhances the system's transparency and security by recording each vote on a decentralized ledger. This immutable, public ledger eliminates risks associated with centralized data manipulation and provides transparency, allowing voters, officials, and auditors to independently verify each transaction [3]. This openness and traceability foster trust among all stakeholders, which is essential for the credibility of election outcomes [4].

This paper discusses the design, implementation, and benefits of the Real-Time Face Recognition Electronic Voting System. By integrating neural networks, OTP-based multi-factor authentication, and blockchain, this system addresses critical security and transparency concerns of traditional and electronic voting methods. The proposed solution aims to provide a scalable, secure voting framework suitable for local and national elections, contributing to the modernization of democratic processes.

II. EXISTING SYSTEM

Traditional voting systems, like ballot papers or Electronic Voting Machines (EVMs), require a lot of people and funds to work effectively. With EVMs, voters can see the candidates' names and symbols on a screen, and they simply press a button to cast their vote, which the machine then records and counts. In the ballot paper system, voters receive a paper listing all the candidates and mark their choice by hand. These marked papers are then collected and counted manually, which is both time-consuming and labor-intensive.

To verify voters, officials usually check ID cards in person and mark the voter's finger with ink to prevent them from voting more than once. However, these methods lack strong security. Because ID verification is done manually rather than with automated systems, it's easier for tampering or manipulation to occur. This lack of security weakens the reliability of the voting process, as it creates opportunities for unauthorized voting or altering votes.

III. RELATED WORK

The use of biometric authentication, blockchain, and electronic voting systems (EVS) has become a key focus because it could greatly improve election security, transparency, and privacy. Traditional voting systems, which rely on PINs, passwords, or ID cards, are vulnerable to threats like hacking, identity theft, and vote manipulation [5]. To fix these issues, recent research has explored using advanced technologies such as biometrics and blockchain. Facial recognition, a type of biometric system, has proven effective in voting. Advanced deep learning models, like convolutional neural networks (CNNs), can identify faces accurately even with changes in lighting, angles, or facial expressions [6]. FaceNet, a popular facial recognition tool, is already used in many secure identification systems [1]. In voting, facial recognition can authenticate voters in real-time, reducing the chances of fraud or impersonation. Pairing facial recognition with additional security methods like One-Time Passwords (OTPs) further strengthens the system, ensuring that only verified voters can vote [7]. Blockchain is another technology that improves security in electronic voting. It creates a secure, tamper-proof ledger where votes are recorded. This ensures that once a vote is cast, it cannot be changed. Blockchain's decentralized nature allows independent verification by all involved parties, including voters, election officials, and auditors, which builds trust in the election process [8]. By combining multi-factor authentication (MFA), which uses both OTPs and biometrics, the system further reduces the risk of fraud [5]. While these technologies show great potential, there are still challenges like making the system scalable, ensuring voter privacy, and making the system accessible to everyone. As research continues, combining facial recognition, OTP authentication, and blockchain could address these challenges and make the voting process more secure, transparent, and efficient.

IV. MODULES AND METHODOLOGY

The Real-Time Face Recognition Electronic Voting System is made up of several key parts that work together to make voting secure, transparent, and efficient. Here's an easy-to-understand breakdown of how it works:

1) Face Recognition Module: This part of the system uses technology to identify voters by their face. It captures their facial image and compares it to the data already stored in the system to make sure the voter is who they say they are. This helps prevent fraud and ensures only the right person can vote.

2) OTP-Based Multi-Factor Authentication (MFA) Module: After the system recognizes the voter's face, it sends a One-Time Password (OTP) to the voter's phone. The voter then enters the OTP to confirm their identity. This extra step ensures only the person who is supposed to vote can do so.

3) Voting Interface Module: Once the voter is authenticated, they can access the voting interface. This is where they can choose who or what to vote for. It's designed to be easy to use and ensures their vote remains private and secure.

4) Blockchain-Based Vote Recording Module: After the vote is cast, it gets recorded on a blockchain. Blockchain is a technology that makes sure the vote can't be changed or tampered with. It also allows election officials or auditors to verify the votes independently, helping build trust in the results.

Each vote is safely recorded on a blockchain, which is like a digital notebook that everyone can see but no one can erase or change. Once a vote is added, it's permanent and can't be tampered with. Every vote forms a new "block" connected to the previous one, creating a secure chain of votes that can't be altered. This ensures all votes are recorded correctly and cannot be changed by anyone.

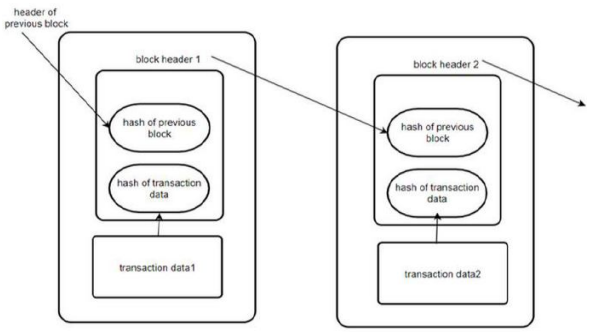


Fig 1. Blockchain Structure

The transparency of blockchain allows people in charge, like election officials or auditors, to check the vote count at any time without revealing who voted for whom. It provides a clear and trustworthy record of every vote, making sure the election results are accurate, fair, and protected from manipulation. This helps build confidence in the election process and ensures the integrity of the results.

1) Audit and Transparency Module: This part allows anyone involved in the election, like officials or auditors, to check the votes and confirm everything is fair. Since all votes are stored on the blockchain, they are publicly available for review, making the election process transparent.

2) Security and Privacy Module: This module ensures that all voter data and votes are kept safe. It uses encryption and other security measures to protect personal information and keeps an eye out for any potential threats. It also makes sure the system follows privacy laws.

3) Voter Registration and Database Management Module: This part manages all the voter information, such as their facial data and phone numbers for OTPs. It ensures that only registered voters can participate in the election and keeps the data updated and secure.

V. METHODOLOGY

The Real-Time Face Recognition Electronic Voting System is designed to ensure a secure, transparent, and efficient voting process by integrating advanced technologies. It starts with the voter registration process, where individuals provide their personal details and facial biometric data. This ensures that only verified voters can participate, and their facial data is captured through a camera, processed, and securely stored. This prevents fraud and ensures the integrity of the registration process.

When a registered voter attempts to vote, the system uses facial recognition to verify their identity. The system analyses the voter's face using pre-trained neural networks and compares it with the stored biometric data. If there's a match, the voter is authenticated. Then, a One-Time Password (OTP) is sent to the voter's registered mobile number for extra security. The voter enters the OTP into the system to proceed with the voting process. This two-step authentication ensures that only the registered voter can cast a vote, protecting the system from unauthorized access.

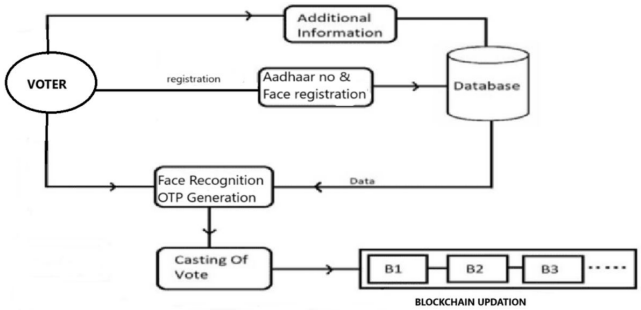


Fig 2. System Architecture

Once the voter is successfully authenticated, they are granted access to the voting interface, where they can select their preferred candidates or voting options. The system encrypts the vote to protect its confidentiality and prevent any tampering. After the vote is cast, it is recorded on a blockchain, which guarantees that the vote is securely stored and cannot be altered. Blockchain ensures transparency and accountability, as every vote is treated as a unique transaction verified by multiple nodes on the network. This decentralized structure makes the voting process tamper-proof and provides full transparency without compromising voter privacy.

The system also features a real-time vote counting and result generation module, which automatically tallies votes as they are recorded on the blockchain. This ensures that results are available quickly and transparently. Voters and election officials can track the status of the election and see real-time updates, which enhances the confidence in the process and allows for quick responses if any issues arise.

Public auditing is another important feature of the system. The transparency of blockchain allows anyone—including voters, election officials, and auditors—to independently verify the votes and results, ensuring the integrity of the election process. This public access to the voting records promotes trust in the results.

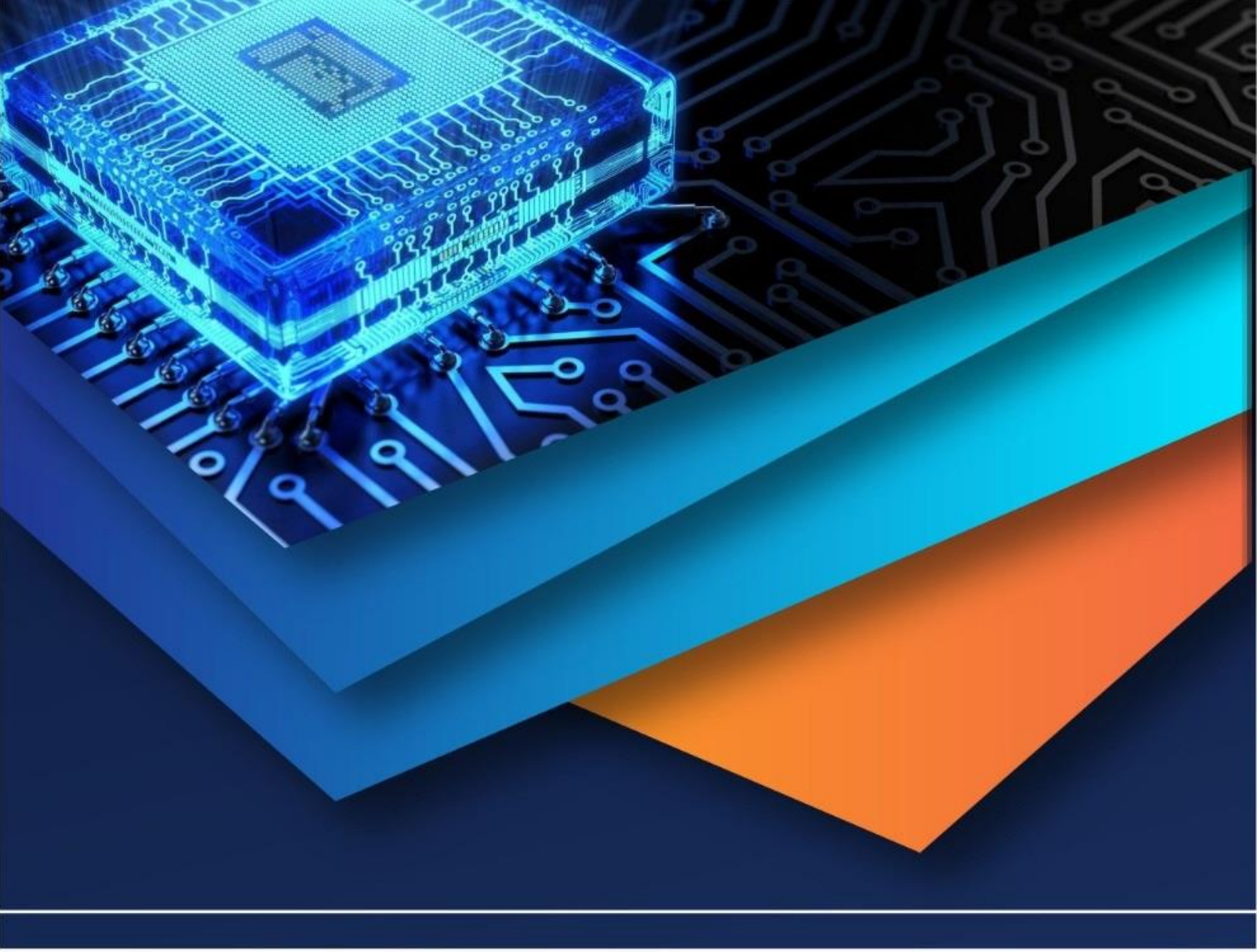
Finally, the system places a strong emphasis on security and privacy. Throughout the process, sensitive data such as facial recognition data, OTPs, and voting choices are encrypted and securely transmitted. This ensures that all voter information and votes remain protected from unauthorized access while maintaining the transparency and integrity of the system.

VI. CONCLUSION

The Real-Time Face Recognition Electronic Voting System provides a transformative solution to the challenges faced by traditional and electronic voting systems. By combining facial recognition, OTP authentication, and blockchain technology, it enhances security, transparency, and efficiency. The system ensures only authorized voters can participate, keeps a tamper-proof record of each vote, and allows for public verification. Its ability to handle large-scale elections and speed up vote counting sets a new standard for modern voting systems, helping to build greater trust in the electoral process.

REFERENCES

[1] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 815-823).
[2] Dhamija, R., & Perrig, A. (2000). Déjà Vu: A User Study Using Images for Authentication. In Proceedings of the 9th USENIX Security Symposium.
[3] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In IEEE International Congress on Big Data (pp. 557-564).
[4] Pilkington, M. (2016). Blockchain Technology: Principles and Applications. In Research Handbook on Digital Transformations. Edward Elgar Publishing.
[5] Sadeghi, A. R., Bocek, T., & Kießling, W. (2018). Secure Electronic Voting Using Blockchain and Biometrics. IEEE Access, 6, 56899-56909.
[6] Sun, Y., Wang, X., & Tang, X. (2014). Deep Learning Face Representation by Joint Identification-Verification. IEEE Transactions on Pattern Analysis and Machine Intelligence, 38(12), 2280-2292.
[7] Jain, A. K., Nandakumar, K., & Ross, A. (2018). 50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities. Pattern Recognition Letters, 81, 1-20.
[8] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin. Applied Innovation Review, 2, 6-10.
[9] Mills, L., Xie, L., & Viswanath, B. (2020). Blockchain for Secure Voting Systems: A Case Study of Voatz. IEEE Transactions on Engineering Management, 67(4), 1012-1021



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY