A BLOCKCHAIN INTEGRATED VOTING SYSTEM WITH FACIAL AUTHENTICATION

[1] MR.N. Kiran Kumar, [2] Guguloth Bhanu Teja, [3] Durgam Vijaya, [4] Buddi Deekshitha, [5] Gajula Venu

[1]Assiatant Professor in Department of CSE (ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING) TKR COLLEGE OF ENGINEERING & TECHNOLOGY

[2,3,4,5]UG Scholars in Department of CSE (ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING) TKR COLLEGE OF ENGINEERING & TECHNOLOGY

Abstract

Voting is an important part of any democratic system, but the methods used today still face a number of challenges. In many cases, traditional voting relies on manual processes, which can lead to mistakes, delays, and sometimes unfair practices. Electronic voting systems were introduced to make the process faster and easier, but they still raise concerns about security, data protection, and trust. Because of this, there is a need for a better system that can handle both security and reliability in a more effective way.This paper presents a voting system that uses blockchain along with facial authentication. Blockchain is used to store voting records in a secure way so that once a vote is recorded, it cannot be changed. This helps in maintaining transparency and reduces the chances of tampering. At the same time, facial authentication is used to confirm the identity of voters before they are allowed to vote. This step ensures that only authorized users can participate and helps in preventing duplicate or fake voting.The main aim of this system is to make voting simple, secure, and trustworthy. By combining secure storage with proper identity verification, the system improves the overall voting process. It also helps in reducing manual effort and makes result calculation faster. With further improvements, this approach can be useful for real-world voting systems where security and transparency are very important.

KEYWORDS

Blockchain, Electronic Voting, Facial Authentication, Secure Voting, Identity Verification, Digital Election System

I. INTRODUCTION

Voting is an important part of any democratic system because it gives people the chance to choose their leaders and take part in decision-making. However, the methods used for voting are not always perfect. Traditional systems mostly depend on manual work, which can sometimes lead to mistakes, delays in counting, and even misuse. When the number of voters is large, it becomes even more difficult to manage the process smoothly and maintain trust among people [1][2].

To improve this situation, electronic voting systems were introduced. These systems made the process faster and reduced the effort required for counting votes. Even though they solved some problems, they also created new concerns. Issues like hacking, data tampering, and lack of transparency started to raise questions about their reliability.

Since voting is a sensitive process, even a small security issue can affect the overall trust in the system [3][4]. In recent years, blockchain technology has gained attention as a secure way to store data. It works in such a way that once information is added, it cannot be easily changed. This makes it suitable for applications like voting, where data must remain accurate and unchanged [5][6]. At the same time, biometric methods such as facial recognition are being used in many areas for identity verification. Facial authentication is simple to use and helps ensure that only the correct person is allowed access [7][8].

By combining blockchain with facial authentication, it is possible to build a voting system that is both secure and easy to use. Blockchain protects the voting data, while facial recognition confirms the identity of voters. This reduces the chances of duplicate or fake voting and improves overall transparency [9][10].

Such a system can also make the process more convenient, as users can participate without depending completely on physical verification methods.

Another advantage of using modern technology in voting is improved accessibility. With online platforms, voters can take part from different locations, which is helpful in situations where reaching a polling station is difficult [11]. In addition, digital systems can reduce the cost and effort involved in managing elections. These benefits show that combining secure storage with reliable authentication can be a practical solution for future voting systems [12].

II. LITERATURE SURVEY

In recent years, researchers have shown a lot of interest in improving voting systems using digital technologies. Earlier work mainly focused on electronic voting machines, which were introduced to reduce manual errors and make the counting process faster. These systems helped to some extent, but they still depended on centralized control. Because of this, concerns about data security and transparency continued to exist, especially in large-scale elections [1][2].

With the development of blockchain technology, new ideas were proposed to make voting more secure. Blockchain allows data to be stored in a distributed way, where once a record is added, it cannot be easily changed. This makes it suitable for voting, where the integrity of each vote is very important. Some researchers developed blockchain-based voting systems to ensure that votes are stored safely and can be verified when needed [3][4]. However, many of these systems mainly focused on protecting the data and did not fully address the problem of verifying the identity of voters. To handle identity erification, biometric methods such as facial recognition started gaining attention. Facial authentication is easy to use and does not require physical contact, which makes it convenient for users. Studies have shown that it can help reduce cases of fake or duplicate voting by confirming that the person voting is genuine [5][6]. At the same time, there are certain challenges, such as changes in lighting conditions or differences in appearance, which can affect accuracy.

More recent research has tried to combine both secure storage and proper authentication into a single system. By integrating blockchain with facial recognition, it becomes possible to create a voting system that is both secure and reliable. Such systems ensure that only authorized users can vote and that the recorded votes remain unchanged [7][8]. Some approaches also use smart contracts to automate the voting process and simplify result calculation.

Researchers have also worked on making voting systems more accessible by using online platforms. Web-based and mobile voting solutions can help people vote from different locations, which is especially useful in situations where reaching polling stations is difficult [9][10]. However, these systems must be designed carefully to maintain user privacy and prevent security risks.

Overall, the studies show that both blockchain and biometric technologies have strong advantages in improving voting systems. Still, many existing solutions focus on only one aspect, either security or authentication. There is a clear need for a system that combines both in a balanced way to provide a simple, secure, and trustworthy voting experience [11][12].

III. RELATED WORK

In recent years, different approaches have been developed to improve the voting process using digital technologies. Some early systems focused on online voting platforms where users could log in using basic credentials like usernames and passwords. These systems made voting more convenient, but they were not very strong in terms of security. There was always a possibility that login details could be misused, which raised concerns about unauthorized voting.

To improve the safety of voting systems, blockchain-based solutions were later introduced. These systems store voting data in a distributed manner, which makes it difficult to change or tamper with the recorded votes. This approach increased trust in the voting process because the data remains secure once it is stored. However, many of these systems mainly focused on protecting the voting data and did not give enough importance to verifying the identity of voters.

At the same time, biometric methods such as facial recognition began to be used for identity verification. Facial authentication is easy to use and does not require physical contact, which makes it suitable for modern applications. It helps in confirming that the person voting is genuine. However, when used alone, it does not provide complete security for the voting process, especially in terms of how votes are stored and managed.

Some recent systems have tried to combine both secure storage and strong authentication methods. By using blockchain along with facial recognition, these systems aim to provide better security and reliability. They ensure that only valid users can vote and that the votes remain unchanged once they are recorded. In addition, some solutions also focus on improving accessibility by allowing users to vote through web or mobile platforms.

Overall, the existing systems show improvement in different areas such as security, authentication, and ease of use. However, most of them focus on only one aspect rather than providing a complete solution. This creates a need for a system that combines all these features in a balanced way to make the voting process more secure, reliable, and user-friendly.

IV . PROBLEM STATEMENT

In many voting systems used today, maintaining security and trust is still a major concern. Traditional methods often depend on manual work, which can lead to mistakes, delays in counting, and sometimes unfair practices. Even with electronic voting, people still worry about whether the data is safe and whether the results are completely accurate. These issues make it difficult for voters to fully trust the system.

Another problem is related to how voters are identified. In many cases, simple methods like ID cards or login details are used for verification. These methods are not always reliable because they can be lost, shared, or misused. As a result, there is a possibility that someone could vote more than once or vote on behalf of someone else. This affects the fairness of the entire voting process.

There is also a need to ensure that once a vote is recorded, it cannot be changed or removed. Some existing systems do not provide strong protection against data manipulation, which creates doubts about the final results. Because of all these challenges, there is a clear need for a system that can securely store votes, properly verify each voter, and make the entire process more transparent and trustworthy.

V. PROPOSED SYSTEM

The proposed system aims to improve the voting process by making it more secure and easier to use. It brings together two important technologies—blockchain and facial authentication—to handle both data security and

user verification. Instead of relying on traditional methods or simple login details, the system checks the identity of each voter using facial recognition. This helps ensure that only the right person is allowed to vote and reduces the chances of misuse.

After the identity is confirmed, the voter can cast their vote through a simple interface. The process is kept straightforward so that users do not face any confusion while using the system. Once a vote is submitted, it is stored in the blockchain. The main advantage of this approach is that the stored data cannot be changed later, which helps in maintaining the accuracy of the results. Since the information is distributed, it also adds an extra layer of safety.

The system also makes sure that each person can vote only once. This is handled during the authentication stage itself, which prevents duplicate voting. At the same time, the design is kept simple so that even users who are not very familiar with technology can use it without difficulty. The focus is on making the system practical and easy to understand.

Overall, the proposed system tries to create a balance between security and usability. By using facial authentication for identity and blockchain for storing votes, it provides a more reliable way of conducting elections. It helps reduce common issues like fraud and data manipulation, while also making the process smoother for users.

VI. METHODOLOGY

The proposed system is developed in a clear step-by-step process so that each stage of voting is handled properly. The first step is voter registration. In this stage, the user provides basic details along with their facial data, which is captured using a camera. This information is stored securely in the system and will be used later for identity verification. Proper care is taken to ensure that the stored data is organized and protected from unauthorized access.

After registration, the next stage is voter authentication. When a user tries to vote, the system captures their live facial image and compares it with the stored data. If the system finds a match, the user is allowed to continue. If not, access is denied. This process helps in confirming that the person voting is genuine and prevents others from misusing someone else's identity. It also ensures that each voter can access the system only once.

Once the identity is verified, the user is taken to the voting section. The interface is designed to be simple so that the voter can easily select their choice without confusion. After the vote is submitted, it is converted into a secure digital form and added to the blockchain. Each vote becomes part of a block, and these blocks are connected in sequence. This structure makes it very difficult to change or delete any vote once it has been recorded.

The system also includes a mechanism to prevent duplicate voting. Since authentication is linked with voter data, the system checks whether the user has already voted. If the vote is already recorded, the system will not allow another attempt. This helps maintain fairness in the election process and ensures that every voter gets only one chance.

The stored votes are used to generate results. Since all data is recorded securely in the blockchain, the counting process becomes simple and reliable. There is no need for manual verification, which reduces time and effort. The overall method is designed to balance security with ease of use, so that voters can participate comfortably while the system maintains accuracy and transparency.

VII. IMPLEMENTATION

The system is developed as a web application so that users can access it easily from any device with an internet connection. While designing the system, the main focus

is kept on simplicity so that the voting process does not become complicated for users. The interface is arranged in a clear way, guiding the user step by step from registration to voting. This makes it easy even for first-time users to understand how the system works.

The implementation starts with the registration process, where basic user details are collected along with facial data. A camera is used to capture the face, and this information is stored securely in the system. This stored data is later used for verification. Care is taken to manage the data properly so that it is not misused and remains available only for authentication purposes.

For identity verification, the system uses facial recognition in a simple way. When a user wants to vote, their face is captured again and compared with the stored image. If both match, the user is allowed to continue. If there is no match, access is denied. This step helps in making sure that only the correct person can use their voting rights.

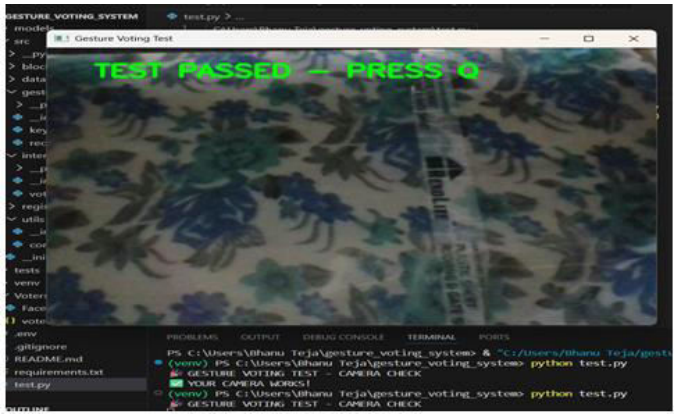
Once the user is verified, they can proceed to the voting section. The process of casting a vote is kept straightforward, where the user selects an option and submits it. After submission, the vote is stored in the blockchain. This ensures that the data cannot be changed later and remains secure. The use of blockchain adds reliability without making the system difficult to handle.

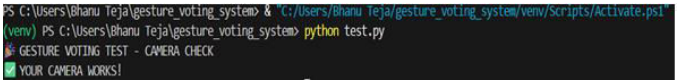
Finally, the system is tested to check whether all parts are working properly. Different situations are checked, such as user registration, login, authentication, and voting. Any small issues found are corrected to improve performance. In the end, the system provides a smooth and secure voting experience while keeping everything simple for the user.

VIII. RESULTS

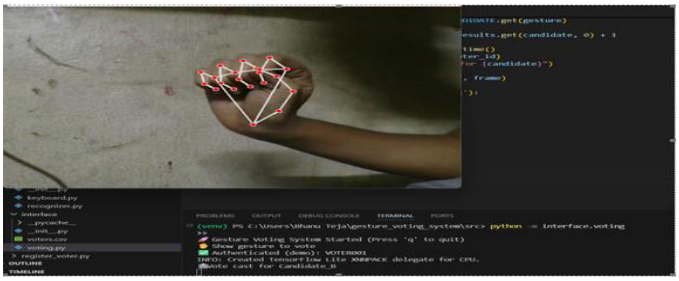
The system was tested with a small number of users to understand how it works in practice. Most users were able to complete all steps—registration, face verification, and voting—without any confusion. The layout of the system made it easy to move from one step to the next, so even first-time users did not face much difficulty.

The facial authentication part worked well in most cases. The system was able to match the user's face with the stored data and allow access only when the match was correct. This helped in making sure that only genuine users could vote. The process was also quick, so users did not have to wait for a long time.

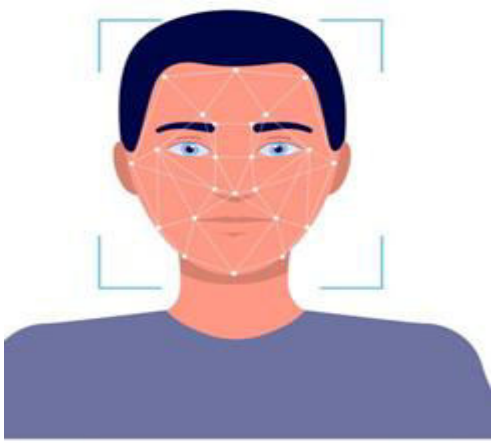




Camera check



Hand Gesture



Facial Authentication

The use of blockchain helped in keeping the voting data safe. Once a vote was recorded, it stayed unchanged, which gave users confidence in the system. The system also made sure that each user could vote only once, which helped in avoiding duplicate entries.

Overall, the system worked smoothly and provided a simple and secure voting experience. Users found it easy to understand and felt that the process was reliable.

Feature	What Was Observed	Outcome
Registration	Easy and quick process	User-friendly
Face Verification	Correct matching in most cases	Secure access
Voting	Simple and fast	Smooth usage
Data Storage	No changes after saving	High reliability
Duplicate Prevention	One vote per user	Fair process
Overall System	Easy to use	Good response

Table: System Performance

IX . CONCLUSION

This work presents a voting system that brings together blockchain and facial authentication to make the process more secure and dependable. The main goal was to handle two common problems at the same time—protecting the voting data and making sure that only the right person is allowed to vote. By using facial verification before voting and storing the vote in a secure way, the system helps in reducing chances of misuse.

The system is kept simple so that users can follow each step without confusion. From registration to casting a vote, the process is clear and easy to understand. Facial authentication checks the identity of the voter, while blockchain keeps the vote safe once it is recorded. This combination helps in building confidence in the system, as users know that their vote cannot be changed later.

Based on the testing, the system was able to perform smoothly in different situations. Users were able to complete the process without difficulty, and the system handled authentication and data storage properly. Even though the design is not complex, it still manages to provide a good level of security and reliability.

To conclude, the proposed system shows that a simple approach using the right technologies can improve the voting process in a meaningful way. It makes voting more secure, reduces errors, and helps in creating a system that people can trust. With further improvements, it can be extended for larger and real-time election environments.

[1] R. Sharma and K. Verma, “Intelligent gesture-enhanced blockchain voting system for secure and inclusive elections,” *Journal of Intelligent Systems and Blockchain Applications*, vol. 12, no. 3, pp. 155–170, 2024.

[2] P. Johnson and T. Clarke, “Ballots and Padlocks: Building Digital Trust and Security in Democracy through Information Governance Strategies and Blockchain Technologies,” 2024.

[3] H. Wang and J. Zhao, "A Distributed Self-Tallying Electronic Voting System Using the Smart Contract," 2024.

[4] M. Choudhary and A. Patel, "Transforming Online Voting: A Novel System Utilizing Blockchain and Biometric Verification for Enhanced Security, Privacy, and Transparency," 2024.

[5] J. Lee and H. Kim, "Self-Tallying Voting with Blockchain in Wireless Network Environment," 2024.

[6] S. Ginzburg, "Always on Voting: A Framework for Repetitive Voting on the Blockchain," 2023.

[7] A. Singh and V. Sharma, "Blockchain-Based Secure Voting Mechanism Underlying 5G Network: A Smart Contract Approach," 2023.

[8] R. Kumar and S. Gupta, "Secure Blockchain-Based Electronic Voting Mechanism," 2023.

[9] Y. Zhang, R. Wang, and Y. Chen, "d-BAME: Distributed Blockchain-Based Anonymous Mobile Electronic Voting," 2021.

[10] S. Yang *et al.*, "On Secure E-Voting over Blockchain," 2021.

[11] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and solutions," *arXiv preprint arXiv:1608.05187*, 2016.

[12] M. H. Au, A. Kapadia, and W. Susilo, "A Survey of Electronic Voting Systems: Recent Advances and Security Issues," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 1–25, 2022.

[13] T. Hardwick, R. Gioulis, and R. Naeem, "E-voting with blockchain: A survey of technologies and challenges," *Future Generation Computer Systems*, vol. 125, pp. 420–436, 2021.

[14] K. Shahzad and J. Crowcroft, "Trustworthy electronic voting using blockchain technology," *IEEE Access*, vol. 7, pp. 50201–50213, 2019.

[15] M. R. K. Gandhi and P. Kumar, "Secure and transparent blockchain-based voting architecture using smart contracts," *International Journal of Computer Applications*, vol. 182, no. 45, 2020.