DECENTRALIZED VOTING SYSTEM WITH MULTIMODAL BIOMETRIC APPROACH

Mrs Ankitha Bekal[1], Deepak G Deekshith[1], Kiran Rai[1], G[1], and Krithik[1]

[1]*Department of Computer Science and Engineering, P. A. College of Engineering, Karnataka, Mangaluru, India*

E-mail:

Abstract

This project focuses on building a secure and trustworthy online voting system that people can use from anywhere. To ensure that only the right person can vote, the system uses three layers of verification: face recognition, palm recognition, and a one-time password (OTP) sent to the voter's phone. This triple-check process makes it very difficult for anyone to cheat or vote using someone else's identity. Once the voter is verified and casts their vote, the vote is stored using blockchain technology. Blockchain acts like a digital record book that cannot be changed, deleted, or hacked, which guarantees that all votes are safe and tamper-proof. Unlike traditional voting systems, there is no single person or group that can control or manipulate the results. This system is especially helpful for people who cannot visit polling booths, such as those living in remote areas or with disabilities. By combining biometrics and blockchain, the project makes voting more secure, fair, and convenient, while also increasing trust in the election process by making sure that every vote is real, properly counted, and protected.

Secure Online Voting, Blockchain, Face Recognition, Palm Scan, OTP Verification, Voter Safety, Digital Elections, Biometric Login, Fair Voting, Voting from Anywhere,

ISBN:97881-19905-39-3

Trustworthy Elections, Tamper-Proof System, Smart Contracts, Transparency, Cyber-Secure Voting.

1 INTRODUCTION

Elections are important mechanisms of a democractic foundation in many countries/jurisdictions. Traditional voting can have limitations, including fraud, identity theft, vote tampering, and dutability of voters to vote. As a result, this project will focus on developing a secure and intelligent voting system that utilizes biometric authentication and blockchain usage. The proposed voting system will include multimodal biometric authentication by using face recognition, palm detection, and One- time-password (OTP) authentication. The combination of these features will ensure that only the intended eligible authenticated voters will submit the vote. All votes submitted using the voting system will be stored on a blockchain. Once the votes are in the blockchain they are incapable of being change or tampered with, thus ensuring the integrity of the votes that have been captured. The combination of the blockchain as a distributed ledger also means that there is no reliance on any central authority; this removes any path of manipulation by a central authority. With the technical recommendations indicated in the proposal, not only will there be improvements in security to the electoral process, as well as better public access, and trust and transparency of the electoral process, but voters will be able to have the opportunity to participate voting from anywhere; this is the desired outcome and result of the research and systems project.

2 METHEDOLOGY

The system works step-by-step to ensure that only the right person can vote and that their vote is completely secure. First, voters register by scanning their face and palm, in addition to some basic information about themselves. When it's time to vote, the system again scans

ISBN:97881-19905-39-3

a person's palm and face, before sending an OTP via text or email to ensure that it is really them. Once all these checks have been successfully completed, the person is now eligible to vote.

Once the vote has been cast, it is securely recorded on the blockchain as it is meant to be immutable. The blockchain works like a ledger where no-one can change, store, or hack it. The vote isn't just recorded but instead is stored like a guaranteed secured transaction. The system allows for all users to use voting outside of any one person or organization being able to control all of the votes cast. With these capabilities, voting becomes safer, better, and trustworthy for

everyone.

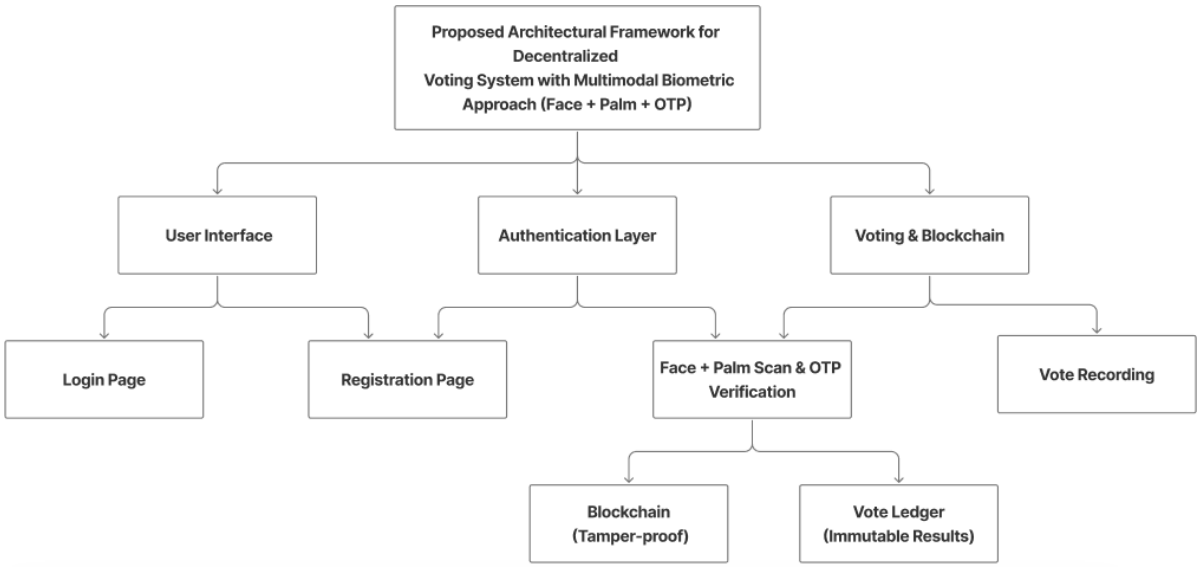

Figure 1: : Proposed architectural framework

3 User Interface Layer:

• Login Page: This is the page where voters will enter the credentials needed to authenticate their access to the system.

• Registration Page: This is where voters and candidates will initially register for access

ISBN:97881-19905-39-3

to the system. It will require them to take Face and Palm scans along with their information that we will keep to verify at a later time can be stored securely.

4 Authentication Layer:

• Face + Palm Scan: when doing the voting, I as the voter will be asked to authenticate my identity by having my Camera and Sensor scan my Face and Palm to ensure that I am the same person that registered for the system.

• OTP Verification: After the Face and Palm scan, the voting app will send a OTP (One Time Password) to the registered mobile number/rendered email, that must be entered to ensure the voter's identity prior to putting for the vote.

5 Voting & Blockchain Layer:

• Vote Recording: Once I the voter have authenticated myself, I can vote; It will record the relevant voting information found on the Blockchain

• Blockchain: This layer will ensure once the vote is submitted the vote, cannot be changed, deleted, or compromised; it records all votes found on a secure ledger that is unchangeable in every respect.

• Vote Ledger: The phase of where a vote that has been submitted and is held as a digital representation; it is unchangeable; the votes cannot be once sent.

5.1

5.1.1 Step-by-Step Breakdown of the System:

6 Voter registration:

• First, the voter gets registered by giving the Face and Palm scans and all this information will securely sit in a centralized database.

ISBN:97881-19905-39-3

• They will be connected to an OTP delivery system (email or SMS) to be used for subsequent verification during the election event.

7 Voter authentication:

• On Election Day, voters will start the authentication process by scanning their Face and Palm.

• An OTP is also being sent to their registered Mobile/Email that they need to enter to complete the authentication process before they can vote.

8 Voting:

• After authentication, voters can select their choices and vote.

• Their votes will be captured into a Blockchain at this time so that the vote represented is immutable or tamper resistant.

9 Vote ledger and Blockchain:

• The Blockchain creates an unalterable vote cast record and secure and transparent in real time.

• The Vote Ledger is the source of truth and captures the votes transparently and immutably thus ensuring nobody can tamper with the election results.

10 Result emergence:

• Once voting is safetly closed, by previous Design it will have tactily calculated the results into a Blockchain thus robustly supporting entry for the results.

ISBN:97881-19905-39-3

10.1

10.1.1 Key Features of the Architecture:

• Multimodal Biometric Authentication, you have both the Face and Palm scans and the OTP, providing a much higher level of secured access and fraud mitigation for voting.

• Blockchain Technology, Trusted voting. The architecture uses the blockchain technology to ensure data integrity, provide transparency and trust for the voting process. Once a vote is placed, it is forever recorded, it cannot be changed and duplicate recording cannot happen.

• Real-Time results. The architecture provides real-time visibility of round counting and securely recorded results that are later available for verification.

11 SYSTEM ARCHITECTURE

The architecture is divided into four core components to ensure a secure, decentralized voting system. These components work seamlessly together to authenticate users, ensure transparency, and prevent fraud during elections.

12 User Interface (UI :

• Role: The UI is an architecture's front end. This is where users will interact with the system. In the UI, users can: Register and login; Biometric data (Face + Palm scans) recording; Enter OTP that was sent to device (mobile/email); Vote.

• User Flow: Once the user enters the system using the registration process or by logging in, they will see the biometric authentications screens, they will be asked to enter the OTP and then they can proceed to the voting menu.

13 Biometric Authentication Module:

ISBN:97881-19905-39-3

• Role: This module is responsible for confirming the identity of registered voters using the Face and Palm scans.

• Face Recognition: Image processing uses AI based recognition to identify and match facial features.

• Palm Detect: Palm prints are captured, analysed and matched against a palm print template that was registered in the past.

• Verification: In combination with face and palm feature extraction that takes advantage of the deep learning models to replicate human function, where only people in the registration are able to vote.

14 OTP Verification Module:

• Role: Users are required to enter one-time passwords after biometric verification has completed.

• OTP creation: Once biometric verification is completed, a unique OTP is generated and sent as a SMS to the voter's registered mobile number or email.

• Verification: Users are required to enter the OTP received. This step is necessary so that only registered voters can complete voting; decode the OTP for further voting.

4. Blockchain Voting Backend :

• Role: Once the voter has completed the biometric verification and OTP, the Blockchain Voting backend is accountable for:

• Vote casting: The system sole vote cast is documented (and recorded).

• Blockchain: All votes are stored permanently, transparently, and securely on the Blockchain.

• Smart contracts: are utilized to arrange for the vote to be recorded, and ensure once a vote is cast it cannot be changed or manipulated.

The systems process occurs with the following stages:

ISBN:97881-19905-39-3

15 Biometric Registration/Login:

• Voters take Face + Palm biometric registrations, or login as a registrants. This computer program ensures that only verified users will be allowed in proceeding to vote.

16 Balloting:

• When a verified voter has gone through the process of the biometric verification and the OTP - the voter is securely allowed to cast their vote.

17 Vote Counting:

• The system captures the votes, and stores each voted in the Blockchain. All votes are counted automatically and stored, in the Blockchain, which ensures the voted cannot be tampered with or altered after being cast.

18 Result Posting:

• The election results are displayed in real-time on a public dashboard. Since the votes are stored in the Blockchain, the process is transparent and free from manipulation.

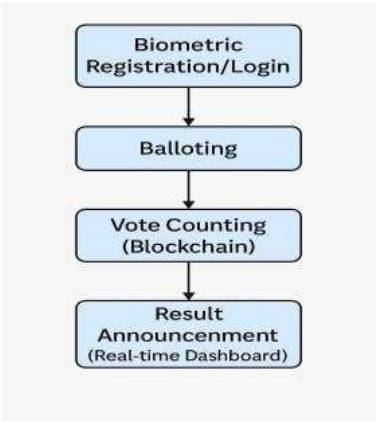

Figure 2: : Voting System Workflow with Biometric and Blockchain Integration

ISBN:97881-19905-39-3

19 IMPLEMENTATION

The Decentralized Voting System with Face + Palm + OTP authentication has been implemented using React front-end along with several advanced technologies to ensure that the voting process is conducted securely and transparently for all voters. The User Interface (UI) of the system has been developed using React and utilizes HTML, CSS and Javascript to provide a fast, responsive environment for the users. In the Decentralized Voting System, the voter will interact with the system using React components which will provide easy navigation through the biometric registration, one-time password (OTP) entry and vote-casting. For the biometric authentication aspect of the voting system we have incorporated TensorFlow.js, and OpenCV in the React code to produce a framework that allows a person's face and palm to be detected in real time inside a standard browser window. The framework we are utilizing replaces the biometric aspects of standard Python developed models that would otherwise require a separate Python backend to process the biometrics data.

After the voter has been authenticated with face and palm verification, an OTP will be generated and sent to the registered device of the voter through a backend built using node.js. The voter will enter the OTP within the react interface, which will communicate to the backend to verify the OTP and initiate the voting process for the voter. The votes will be securely stored using smart contracts in the Ethereum blockchain using Solidity to guarantee the votes will be tampered with after submission and be publicly available for transparent voting process. Ganache was used for the local blockchain testing previous to user testing on the Ethereum network and went in conjunction with Metamask for user identification secured on the Ethereum network.

20 RESULTS AND DISCUSSION

The Decentralized Voting System based on Face + Palm + OTP authentication produced

ISBN:97881-19905-39-3

favorable testing results. The face and palm recognition confirmed correct identification of users. The added OTP verification provided a layer of security to prevent impersonation. The votes generated from the system were stored securely on the blockchain, allowing for immutability of the votes and preventing manipulation incase of changes. The system operated well under heavy traffic, which is a critical requirement for an actual election. While we had minimal traffic during trials, it was significant enough to test the systems traffic capability.

We took several privacy precautions. Biometric data was encrypted, and the OTP number was communicated via telegram. In utilizing these procedures, we can increase voter trust in the voting process, both in privacy and in the ability for the votes to not be altered by third-party interference (in this case the voting system).

Transparency is also another important factor in electioneering. The system can sufficiently provide transparency by logging every vote on the blockchain with timestamps. While your vote is traceable, your integrity as a voter remains private.

To imagine potential improvements one can envision more advanced integration of e-voting systems with cutting edge technologies for improved accuracy (e.g CNNs to improve recognition by carving out distinctions in the overall computational environment), and even anti-spoofing methods (liveness detection) to improve user security. In conclusion, the biometric authentication and blockchain provide revolutionary opportunities for secure, transparent, and reliable digital voting, and our Decentralized Voting System is indicative of this.

21 CONCLUSION

The outcomes of this project show a safe and secure online voting system can be developed with the help of technology. Face, palm and OTP verification stages ensure that only the correct voter can cast a vote, and then once votes are cast, it can be immutably stored

ISBN:97881-19905-39-3

onto the blockchain. During the implementation process, the voting system eliminates issues prevalent in in-person voting, such as fake votes, impersonation (identity fraud) and transparency. Although tested in a controlled demo environment, it demonstrates a strong opportunity for a future in-person election. Additionally, the system will only continue to grow as we further improve the ease of use of the application, especially for remote regions with poor connectivity, and add additional security features.

22 FUTURE ENHANCEMENTS

While this system operates well as is, it could be improved in multiple ways. For example, with the current identification methodology, a more advanced identification procedure such as iris scanning or voice detection could enhance unauthorized impersonation protection. In addition, to enhance accessibility in the system, particularly for elderly users or persons with disabilities, we could also have voice instructions and allow for language choice on the adoption of the voting mechanism.

As new systems will be commissioned for the IRL elections, there must be a solution to maximize voter simultaneous access (in a jurisdiction of 12 million voters) and mitigate areas with slow internet access. In terms of voter access, the system could be configured as a mobile app, which would enable voters to vote from their smartphones and thereby increase voting participation levels. There is also the potential to include AI monitoring to observe votes and the potential for suspicious voting activity, which would mitigate security while voting.

In order for the system to have the potential for larger-scale adoption, it could be tied into government ID systems such as the Aadhaar system or be granted legal allowance to be used in official elections. These enhancements will contribute to the Decentralized Voting System being secure, accessible, and scalable for future use in elections on a national scale.

ISBN:97881-19905-39-3