Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Secure and Transparent E-Voting system using Blockchain Technology

Manukonda Raviteja

Electronics and Communication Engineering,
SASI Institute of Technology & Engineering

Abstract

The use of block chain technology in the Online Voting System with Face Recognition would go a long way in improving the security, transparency, and integrity of the election process. Through block chain, all the votes made by a registered voter can be stored as a transaction in an unchangeable and immutable ledger that can guarantee the safety and auditability of the data. The voter registration information, encrypted Voter IDs, Aadhaar numbers, and hashed face recognition data could be safely placed on privately-owned block chain instead of on centralized data bases that can be at risk of attack. Such a decentralized system is free of the risks of data manipulation and guarantees the credibility of voter data during the election process. The tokenization aspect of Block chain means that a voter is allocated unique voting tokens so that they cannot cast multiple votes. The tokens are verified and stored in the block chain, which increases the election security even more. Smart contracts may be used to automate a number of processes in the election management process, including counting votes and announcing the winner, which provides transparency and prevents manipulation. The final election outcome may also be recorded in the block chain that end up being available to the populace and anyone able to confirm the integrity of the election process. Based on the use of block chain and React JS in frontend, and Spring Boot in backend to deal with API requests and MySQL to store non-sensitive information, the system establishes a secure, decentralized, and fully auditable election system that facilitates transparency, privacy, and fraud deterrence.

Keywords: Block chain Implementation, Permanent Voting, Decentralized Vote, Smart Contract, Voter Authentication and Authorization, Voter Data Privacy, React JS, spring boot, MySQL, Face Recognition, Voter Transparent.

1. Introduction

A democratic system is based on integrity and security of elections and yet the systems that have been traditionally used are vulnerable to fraud, data leakages and human mistakes. Online voting systems have become a possible solution to these problems with the development of digital technologies. Nevertheless, despite the digital platforms, there have been questions over the security of the voter information, vote manipulation, and visibility of the election process. Block chain technology provides a good alternative to solve these problems and increase the overall trustworthiness of the voting process.

The decentralized and immutable property of block chain makes it a good candidate to secure the

election process. Implementing block chain into an online election system will make every vote a secure and tamper resistant transaction, which will guarantee the integrity of the election process. Block chain eradicates the chances of a centralized system, including information leakage or malicious manipulations and deforms the data through a system of nodes over a network. This decentralization makes sure that no one will be able to manipulate or alter the voting data. In addition, election processes, including vote counting and result announcement, can be automated using smart contracts, which can make the entire process more transparent and eliminate the possibility of human error or fraudulent interference. Use of face recognition technology increases the level of security since only registered voters can cast their votes. The voter registration data, in terms of encrypted Voter IDs, Aadhaar numbers and hashed faces can be safely registered in the blockchain, which is guaranteed to be privately encoded and shielded against unauthorized access. The tokenization system of blockchain arsenal also insures that every voter is given a distinct voting token, thus eliminating the possibility of the voter making multiple votes.

The suggested system will combine the block chain with React JS as the frontend and Spring Boot as the backend API processing with MySQL as the data storage of non-sensitive data. This combination provides a secure and transparent and auditing election platform which guarantees privacy, eliminates fraud and instils confidence in the electoral process.

A. Objective

The major aim of the project is to create a safe, transparent, and non-tamper able electronic voting system through the skillful combination of the block chain technology with face recognition to enforce voter authentication. This system seeks to mitigate the structural weaknesses of conventional voting systems and the current digital voting systems including breaches of data, vote divisions, and transparency. With decentralized and immutable properties of block chain, the system will provide security in the fact that all the votes cast are stored, auditable, and inaccessible to manipulation. Once the face recognition technology is integrated, this should ensure that the technology will be an added security where only registered voters can cast their votes and this will avoid fraudulent votes. Moreover, smart contract use will automate the election management operations such as counting of votes and announcement of results making the election process efficient and transparent. By installing a decentralized voting platform with React JS as frontend and spring boot as the backend API controller and MySQL as the storage of non- sensitive data, this system envisions to establish an all-auditable, fraud-free election platform that advances trust, privacy, and integrity in the electoral process.

B. Scope

The project scope will involve coming up with a secure, transparent, and immutable online voting system through the incorporation of block chain technology and face recognition in order to strengthen its security and privacy. The system will enable secure voter registration, with the help of encrypted Voter ID, Aadhaar numbers, and hashed face recognition information on a personal block chain. The authentication of voters will be done through face recognition so the genuine ones will be the ones who cast their votes. The voting will be registered on the block chain as a transaction that cannot be altered and audited, and the tokenization system of block chain will give each voter a unique voting token, and would not be able to vote twice. Smart contracts will replace the necessary

steps in the election, including voting counts and proclamation of victors, which will ensure transparency and remove the chances of human error. The interface will be built on React JS, a platform providing easy- to-use interface by which the voter will be able to engage with the system, whereas the backend will be based on the Spring Boot framework which will allow safe API calls. Non-sensitive data will be stored on MySQL, which will also contribute to the effectiveness of the system. The general goal of the project is to design a fully auditable and decentralized election system that does not only serve as a means of fostering trust and privacy but also uphold the integrity of the election process by eliminating queues and fraud. The scope also encompasses the ability to ensure that the system is flexible to all forms of elections, keep a high level of security as well as offer a smooth experience to voters.

2. Literature Survey

[1]The creation of the paper was started by authors S. P. K. Shankar et al. (2020) who presented a new and secure electronic voting system called "E-Voting System Using Facial Recognition". [2]The researchers had as their main goal the total eradication of impersonation and multiple voting incidents, but at the same time, [3]they pointed out the issue of scalability problems, which resulted from the size of the image datasets and the implementation of the technique's unencrypted data transmission.[4]P. Agarwal and R. Singh (2021) came up with a voting system that is very secure and is based on Aadhaar authentication combined [5]with OTP generation and facial recognition for voter verification.
[6]Their approach not only guaranteed the uniqueness of voters but also strongly depended on network connectivity and was subject to delays during the majority of voting hours. [7]M. Al-Hubaishi et al. (2019) proposed a Blockchain-based e-voting system that provided the transparency and immutability of votes interlinked by blockchain.[8] In the meantime, blockchain offered secure data storage but the absence of [9]biometric integration rendered the system open to unauthorized access through credential theft.[10]A. Ramesh and S. Kumar (2022) came up with a Smart Voting System That Uses Face Recognition and Cloud Integration. [11]The solution was made such that the encrypted data of voters was stored in cloud servers
[12]and the detection of faces was done through OpenCV. It was very precise, could be accessed from distant locations but still needed a high-speed internet connection and well- optimized face datasets for real-time processing.[13]N. Gupta et al. (2023) presented an AI-based Voting System that fused the recognition of faces and emotions with machine learning to put a stop to voting frauds. [14]Their approach improved system intelligence but required high computational [15]power and raised privacy concerns regarding facial data storage.

3. PROPOSED SYSTEM

In the suggested system, it will be ensured that the voting number will be stored safely on the block chain, which will ensure its transparency, immutability and results that cannot be tampered with. Every vote will be encoded into a block chain transaction, and it will be safely recorded in the block chain and will never be changed after they are verified. This decentralized model will remove the risks of having centralized databases like manipulation of data or unauthorized alteration of data. After casting the vote and verification by the real time facial recognition technology, it will be registered as a transaction on the block chain ledger, making the data auditable and transparent. The voting system that uses

blockchain does as well guarantee that the vote counting exercise is automated and does not involve human manipulation, and smart contracts will take care of the aggregation and final declaration of the final result. This will ensure the election process is of integrity and gives verifiable results which will further promote the confidence of the voters as they can publicly verify the results of the elections. The security of the system is also enhanced by the implementation of blockchain because the system avoids breaches of the voting data and the results of the election become transparent and fair.

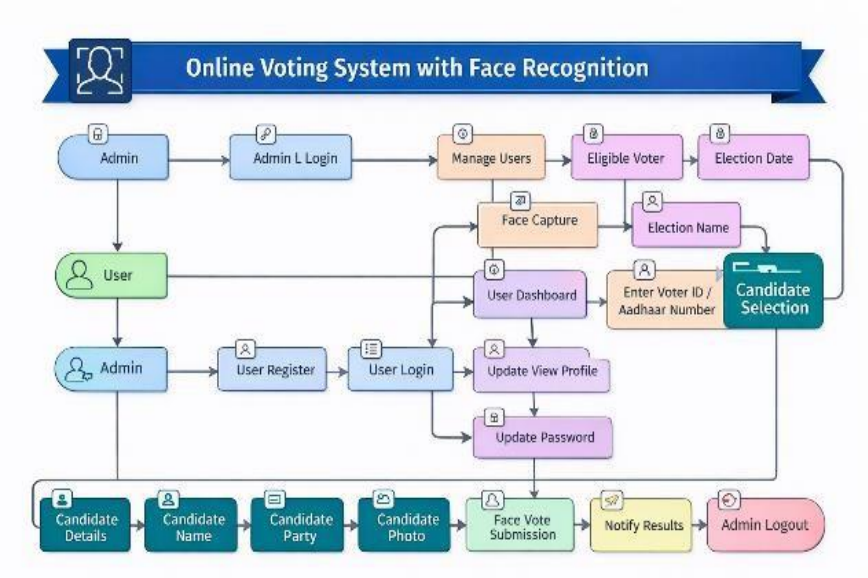

Fig 1: Block diagram for proposed system

4. METHODOLOGY

The Online Voting System with Face Recognition project was developed through a strict software engineering cycle, which included: requirement analysis, system design, implementation and testing. At the Requirement Analysis stage, the project requirements were divided into two major modules; the User Module and the Admin Module. The User Module encompassed the whole voter experience beginning with registration where the personal information of the user like Name, Voter ID/Aadhaar, Date of Birth, address, phone number, and password were captured. It then resorted to live face capture (OpenCV) LBPH algorithm followed by secure login through facial authentication, dashboard access, candidate view, voting, profile management, and changing password. The Admin Module included secure log-in of the administrator, and he/she logged in a dashboard to manage the election (election name, election date and voter list), candidate management (including candidate name, party, and photo), voter list management, voting process monitoring, and publishing results (with security).

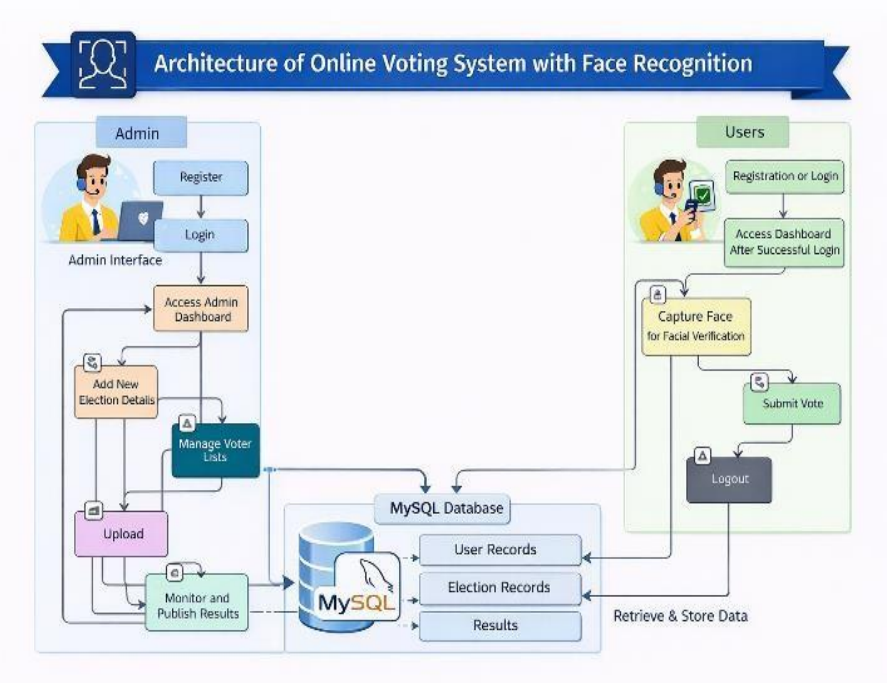

Fig 2: Architecture

Non-functional requirements were security-related (including AES encryption and SHA hashing), level of scalability (based on cloud deployment), high availability, performance efficiency, data integrity, and usability. The UML diagrams,
e.g. Use Case, Activity, Sequence, Class and Deployment diagrams, were used to attain the System Design and illustrated the structure, the workflow and the interaction of the system. Level 1 and Level 2 Data Flow Diagrams were successful in illustrating the data flow between the voter and the system administrator with the help of system components. The Implementation involved the user-friendly mobile frontend with ReactJS, the backend RESTful services with the help of Spring Boot (Java) as well as the secure data storage with MySQL. This strategy determined secure, efficient, and responsive online voting platform to fulfill all the requirements of the non-functional and functional requirements.

A. Working Principle

The working principle of the Online Voting System with Face Recognition consists in the necessity to secure, to be transparent, and to be integrated in the course of the election. The system has two modules namely the User Module and the Admin Module. In the User Module case, the process will begin with voter registration where personal information such as Name, Voter ID/Aadhaar, Date of Birth and contact detail will be collected. The Live face capture is implemented using the LBPH algorithm of OpenCV which forms a unique biometric template which will be securely stored to be utilized in the future authentication. On the voter logging in, facial recognition is provided in real time to ensure that he/she is the only registered voter who is capable of casting his/her vote thereby preventing impersonation or fraud. Once the authentication is complete, the voter will be redirected to the dashboard where he/she will have access to the available candidates and be able to vote. In this manner, voting is also heavily encrypted through AES encryption in a manner that all information exchanged between the voter and the system would not be known to anyone. When using the Admin Module, the

system will begin as a safe administrator access followed by election and candidate administration and lastly, the voter list administration. The administrator is also able to get the live perspective of the voting and announce the results safely after the elections are concluded. The backend is created on spring boot, which is a system to access MySQL and save non sensitive information but to save every vote on the block chain as a secure transaction because only in this way the results may be regarded as unchangeable and verifiable. The system will ensure results of a transparent, efficient and tamper proof voting through the conglomeration of face recognition, secure login and block chain.

B. Technical Tools and Frameworks:

Front-End: react js will be employed to create modern, responsive, and mobile-friendly user interfaces, and a smooth and user-friendly experience to the voters, administrators, and candidates. ReactJS is an efficient solution to the management of the user interface with dynamic changes and flowing interaction.

Back-End: Spring Boot (Java) is used as a back-end framework, where all the main business logic is implemented, which is the user authentication and election- related operations. It allows quick creation of RESTful APIs, which is a guarantee of the scalability and security of the system.

Face Recognition: Real-time voter authentication is done using OpenCV, which is combined with Python and the LBPH (Local Binary Patterns Histograms) algorithm. This makes sure that only the registered voters are allowed to cast their votes by conducting right and effective facial recognition when logging in.

Machine Learning: Deep learning models will be implemented to ensure an improvement in the strength and precision of the facial recognition procedure. Such models can be used to enhance the system to improve the detection and verification of the voters and minimize the possibility of errors or false identifications.

Database: The database is MySQL that is utilized to safely store and manage the data about users and elections, as well as their results. The database is fast to access and manipulates non sensitive information and captures high security and integrity.

Block chain: Block chain is implemented to save every vote in terms of the secure transaction, guaranteeing the impartiality and openness of the election outcomes. The decentralization of block chain ensures that when a vote is cast it can never be changed or distorted and it is a transparent and auditable election process. The block chain captures the result of the final count of votes, which makes the results of the election publicly verifiable and immutable.

C. Keccak Algorithm

Keccak algorithm is a type of cryptographic hash functions that are developed as a family of cryptographic hash functions, which are designed in accordance with SHA-3 (Secure Hash Algorithm 3), designed to offer a safe hashing of different purposes. In contrast to its forerunners, all of Keccak uses a sponge construction, which reads in data to a fixed-length state and sponges out the hash output. The main characteristic of Keccak is that it was able to deliver high security due to the

resistance to the conventional attacks such as collision and pre-image attacks that gave it a greater level of adaptability as regards output length. Keccak algorithm works with the input information broken up into fixed-size blocks and dynamically changes a state matrix of the transformations depending on a fixed set of non-linear functions.
A prominent algorithm in the Keccak algorithm is the so- called formula of the sponge construction formula which summarizes the absorbing and squeezing process. This can be represented as:

$$State = Keccak - F(State \,||\, Input\ Data)$$

Where:

- The final mode of the algorithm is state and in the start state of the algorithm, is of zeros.
- The basic permutation mechanism, but again changing state with each round, is the Keccak-F.
- Input Data: It is data, which should be hashed and presented to the state as part of the absorption phase.

D. **Methods**

- The LBPH algorithm that is applied in the recognition of human faces is a vital part of the authentication of voters during the entire process of registration and voting.
- Face Detection: Initially, the presence of the voter's face is sensed by the application through usage of OpenCV Haar cascades.
- Feature Extraction: It converts the face image into black-and-white and derives the local binary patterns from the face image.
- Face Matching: The system associates the features extracted at registration and voting with the already existing templates to authenticate the voter's identity.
- Machine Learning Integration: The Deep Learning Models applied for the recognition of the face features have a great accuracy level. They are trained to detect and authorize the face of a voter which makes impersonation quite difficult.

Voting Process:

- User Registration: A voter registers him/herself by submitting his/her personal details and taking a photograph of his/her face for confirmation.
- The system produces a distinct facial template and stores it securely for future validation.
- User Login: The voter logs in using his/her (i.e., Voter ID/Aadhaar) credentials. Face verification is done by the system simultaneously to validate the voter.
- Voting: After the voter logs in successfully and gets his/her face verified, he/she is then allowed to view the candidates and choose one by casting his/her vote. Votes are guarded through secure methods, data integrity is ensured, and double voting is not allowed.
- Admin Management: The administrator has the power to supervise not only elections but also candidates, taking care of voter lists and managing voting activities as well. The election will be over before the results are unconditionally secure and the publication made.

- Block chain Integration: The block chain technology is used to store all votes in the form of transactions on a decentralized registry that is never altered. Once a vote is cast, it is registered as a block chain transaction such that it implies that it cannot be changed or used by other people. This will make the voting to be genuine and bring transparency. Votes and information about the voter authentication is securely stored to the block chain which offers an audit free record of the election. The end result of the election data is also stored in the block chain that provides a publicly verifiable list that can never be changed and therefore ensures the correctness and authenticity of the election process.

5. MODULES AND ITS IMPLEMENTATION

A. Admin Module Description:

The Admin module will give a secure access to the administrators and redirect them to the administration panel. It also provides politics management and this is whereby it presents factors such as election name, date and candidates. The administrators will be able to refresh the lists of voters, follow the progress of the voting, and present the outcomes of the elections safely, which will make the whole process less corrupt and correct.

Features:

- Admin Login: Type user name of the administrator along with password. Log in to the administrative panel successfully.
- Manage Elections: Add new specifics of election (Name, Date, List of eligible voters) Add candidates specifics (Name, Party, Photo)
- Supervise and publicly report Findings: Check the turnout of voters Report that is familiar and report the findings of the elections safely.

B. UserModule Description:

The Voter module allows those that take part in the elections to register by disclosing their personal details as well as a live image of the face that are stored in the database in a secure manner. Live face recognition is performed as the identification process once the procedure is signed in. Through election, the authenticated voter is able to access the voting interface, select a candidate and subsequently cast his/her vote by the use of the voting interface.

Features:

- User Registration: Face capture and Personal information (Name, Voter ID/Aadhaar, Date of Birth, Address, Phone number, Password) capture. There is face template and data security of the database.
- User Name: Aadhaar password/ Voter ID. The authentication checks the real-time face recognition on authentication and checks the credentials Checks.
- Voting Process: Fill the dashboard with an effective log in Retake the face image such that you can view the list of candidates and choose the one that you like the most of all Cast to Vote and preservation is even assured.

6. RESULTS AND DISCUSSION

A. Homepage:

This is the first page will be displayed after execution started.

Fig 3: Homepagefunctionality

B. Register Page

This is the register page for the user.

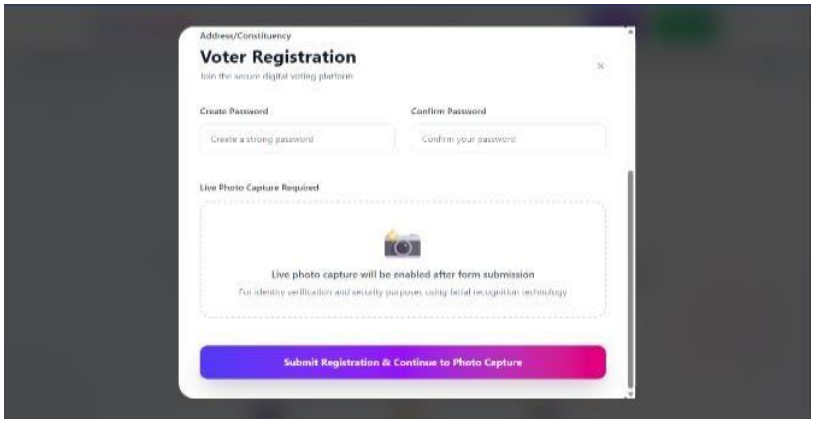

Fig 4: Register page functionality

C. Login Page:

This is the login page foruser.

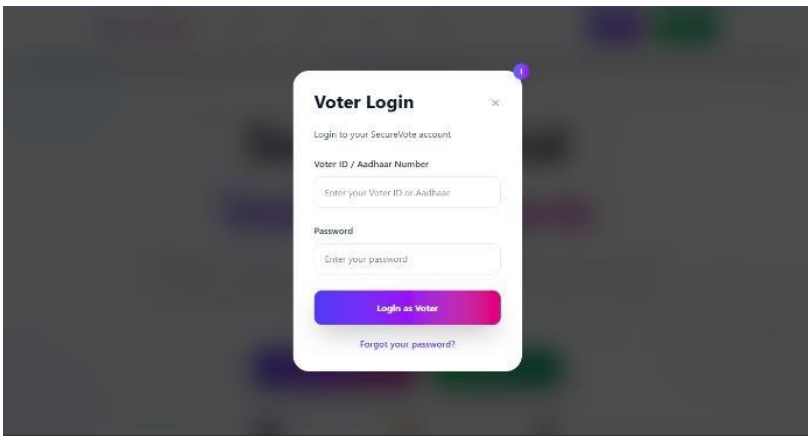

Fig 5: Login page functionality

D. Admin Login Page:

This is the login page for admin.

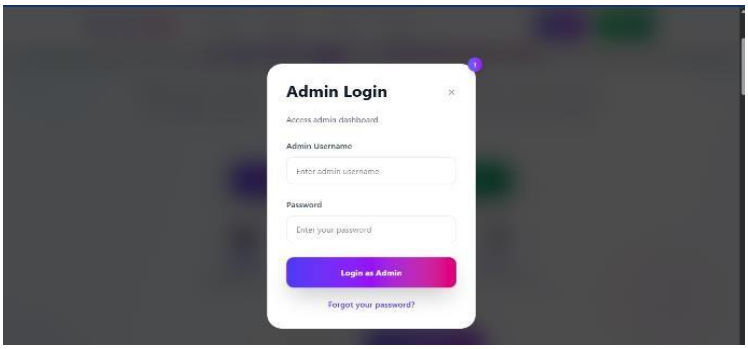

Fig 6: Admin Login pagefunctionality

E. Admin Dashboard

After the successful login of admin with default credentials this page will be displayed.

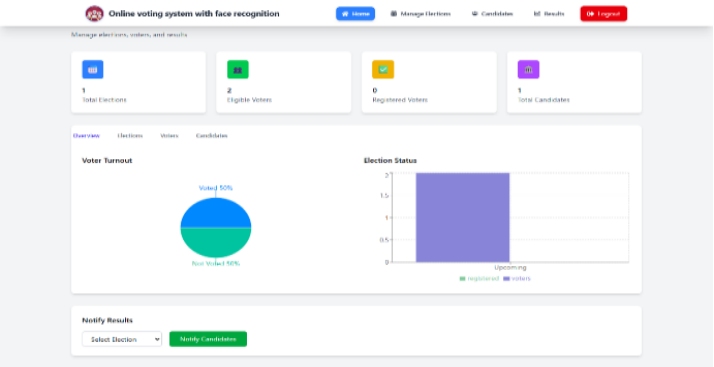

Fig 7: Admin Dashboardfunctionality

F. Manage Candidates

In this page the admin can see all the candidates.

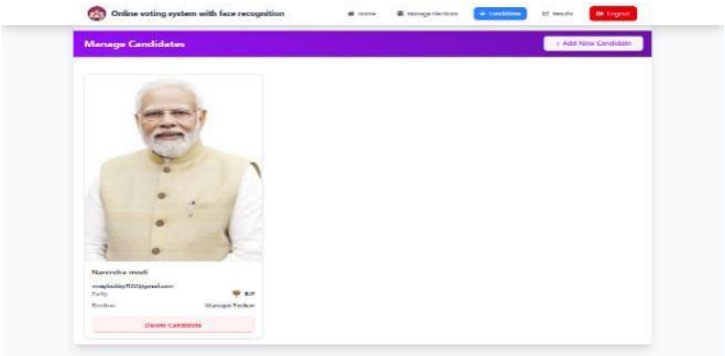

Fig 8: Manage Candidatesfunctionality

G. Manage Elections:

In this page the admin can manage elections.

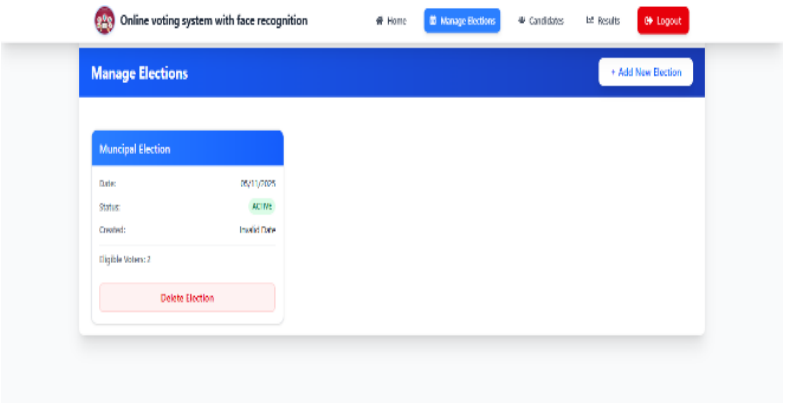

Fig 9: Manage Electionsfunctionality

H. View Results:

In this page the admin can view results.

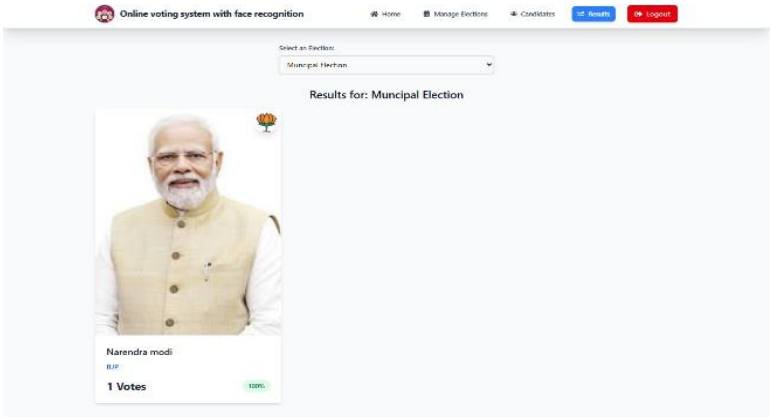

Fig 10: View Results functionality

I. User Dashboard:

After the successful login of user this dashboard will be displayed.

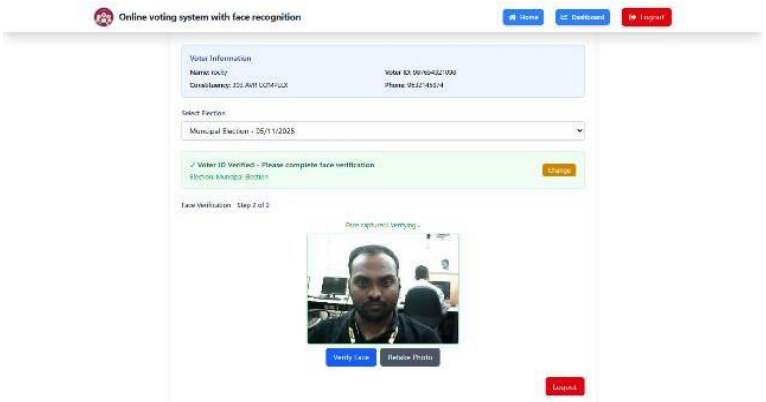

Fig 13: User Dashboardfunctionality

6. Conclusion

The initiative referred to as Online Voting System with Face Recognition is a combination of the sophisticated technologies aimed at changing the way of voting and thus, not only to make it more secure and efficient, but also to make it easier. Common problem areas covered in the system include voter impersonation, complicated and costly organization, and long queues, which leave a more transparent and dependable election process. Facial recognition technology of the voter during the registration process and at the polling station with AES encryption and SHA hashing to keep the data safe and confidential makes the voting process safe and confidential. Also, using the technology of blockchain, the system ensures that every vote is placed in a secure, non-editable transaction on a decentralized ledger to rule out the possibility of tampering and manipulation of the vote. Blockchain also establishes transparency, auditing and resistive capabilities of the election outcomes, giving voters confidence in the integrity of voting. The system is scalable and can be accessed remotely, as well as easily because of its cloud-based architecture, which makes it appropriate during large-scale elections and other voter requirements. The ease of use due to the creation of a user-friendly interface with the help of React JS and the high-performance of the backend with Spring Boot and MySQL also speaks of the reliability and easy maintenance of the system. The LBPH technology applied in facial recognition offers an extra security, where those who cast their votes are only valid voters. This system does not only increase the voting process as a simple and easy to use process but also makes the masses have confidence in the democratic process as there will be the use of the newest technology to make the whole process transparent, secure, and reliable. The successful implementation of such a system may be used in future digital elections and may assist in modernizing election in the world.

7. Future Enhancements

The On-line Voting System with Face Recognition is aimed at establishing and incorporating some of the future enhancements of the system in terms of functionality, security and usability. Some of the most useful upgrades will be the use of multi-factor authentication (MFA). This will also enhance an added level of security as the voters will need to authenticate their identity in a number of various methods such as sending them an OTP which they would need to input on their registered mobile number or email. This additional procedure will ensure that the system is only fed with legitimate voters to cast their votes and this will reduce the chances of other unofficial voters infiltrating the system and again this will enhance the confidence of the elector on the system. The other notable advancement is the launch of the block chain technology which makes the process of election even safer. The immutable and decentralized registry of block chain will enable ensuring that as soon as the votes are cast, they are impossible to modify and will make the results transparent and increase the trust in the results of the elections. The voting will be recorded as a secure and audit transaction that will make the system more precise and will give the population results that can be verified.

Monitoring and analytics can be carried out in real-time to improve the election management. This would develop a dashboard that would provide the election staff with such insights and indications about the voter turnout and enable potential fraud to be tracked and any technical problems to be detected and resolved in a short time. The active surveillance will provide prompt response, which will ensure the simplified processes of election and will be able to counter the difficulties once they arise.

Moreover, the system can be multi-lingual in that the voters belonging to different language groups can cast their votes during the election process thereby making the process inclusive hence increasing voter turnout. This would offer the better ground to more voters since the system would be user friendly to all voters.

References

1. Aanjanadevi, S., Palanisamy, V., & Jothi, | R Anandha. (2017). 68 International Journal for Modern Trends in Science and Technology Detection and Recognition Algorithms. International Journal for Modern Trends in Science and Technology, 03. http://www.ijmtst.com
2. Citra, D., Nair, A. □, Hamid, N. A., Faisal, A., Abidin, A., Mohamed, M. A., Fadzil, M., Kadir, A., Dhalila, S., & Satar, M. (2023). A SECURE ONLINE VOTING SYSTEM USING FACE RECOGNITION TECHNOLOGY. Malaysian Journal of Computing and Applied Mathematics, 6(1), 1–9. https://doi.org/10.37231/MYJCAM.2023.6.1.80
3. Fortuna, I., & Khaeruzzaman, Y. (2022). Implementation of OCR and Face Recognition on Mobile Based Voting System Application in Indonesia. International Journal of New Media Technology), 9(1), 20.
4. Ipinnimo, O., Ogbemhe, J., Mumuni, Q., Owoeye, S. O., & Olurombi, A. (2024). FACIAL RECOGNITION- BASED ONLINE VOTING SYSTEM WITH TWO- FACTOR SECURITY. JOURNAL OF INNOVATION SCIENCE AND TECHNOLOGY, 3(1). http://jist.fuoye.edu.ng/index.php/jist/article/view/81
5. Mandavkar, A. A., & Agawane, R. V. (2015). Mobile based facial recognition using OTP verification for voting system. Souvenir of the 2015 IEEE International Advance Computing Conference, IACC 2015, 644–649. https://doi.org/10.1109/IADCC.2015.7154786
6. Nair, K. C. D., & Mamatha, I. (2023). Online Voting System Based on Face Recognition and QR Code Authentication. Lecture Notes in Electrical Engineering, 1066 LNEE, 619–629. https://doi.org/10.1007/978-981-99-4634-1_48
7. Parmar, A., Gada, S., Loke, T., Jain, Y., Pathak, S., & Patil, S. (2021). Secure E-Voting System using Blockchain technology and authentication via Face recognition and Mobile OTP. 2021 12th International Conference on Computing Communication and Networking Technologies, ICCCNT 2021. https://doi.org/10.1109/ICCCNT51525.2021.9580147
8. Prakash, K., Mitra, N. V., Kumar, N. P., Babu, M. A., Bansal, S., & Kumar, S. (2025). Secure Online Voting System-Based on Facial Recognition by using Deep Learning. International Conference on Electronics, AI, and Computing: Innovating for a Sustainable and Connected Future, EAIC 2025. https://doi.org/10.1109/EAIC66483.2025.11101357
9. Preiya, V. S., Kumar, V. D. A., Vijay, R., Vijay, K., & Kirubakaran, N. (2023). Blockchain-Based E-Voting System with Face Recognition. Fusion: Practice & Applications, 12(1), 53. https://doi.org/10.54216/FPA.120104
10. Purandare, H. V., Saini, A. R., Pereira, F. D., Mathew, B., & Patil, P. S. (2018). Application for Online Voting System Using Android Device. 2018 International Conference on Smart City and Emerging Technology, ICSCET 2018.

https://doi.org/10.1109/ICSCET.2018.8537284

11. Revathy, G., Bhavana Raj, K., Kumar, A., Adibatti, S., Dahiya, P., & Latha, T. M. (2022). Investigation of E- voting system using face recognition using convolutional neural network (CNN). Theoretical Computer Science, 925, 61–67. https://doi.org/10.1016/J.TCS.2022.05.005
12. Shahram Najam, S., Zeb Shaikh, A., & Naqvi, S. (2018). A Novel Hybrid Biometric Electronic Voting System: Integrating Finger Print and Face Recognition. Mehran University Research Journal of Engineering & Technology, 37(1). https://doi.org/10.3316/INFORMIT.308126203732316
13. Shanthi, T., Saranya, R., Selvasridevi, S., Srinandini, K., & Sripriya, S. (2020). Voting System based on Finger Print and Face Recognition. International Journal of Pharmaceutical Research (09752366), 12(1), 1408. https://doi.org/10.31838/IJPR/2020.12.01.233
14. Subramanian, S. S., Suresh, C., Singh, S., Pavan, P., Akash, V., Karuna, G., & Mittal, A. (2025). Face Recognition Voting System. AIP Conference Proceedings, 3157(1). https://doi.org/10.1063/5.0262834/3344659
15. Sulaiman, M. M. K. M. M., Othman, M. F. I., Shah, W. M., Hassan, A., Harum, N., & Alseadoon, I. M. (2021). An Online Voting System using Face Recognition for Campus Election. Journal of Advanced Computing Technology and Application (JACTA), 3(1), 37–42. https://jacta.utem.edu.my/jacta/article/view/5215