International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (Online): 2347-5552, Volume-13, Issue-3, May 2025
https:/doi.org/10.55524/ijircst.2025.13.3.1
Article ID IRP-1612, Pages 1-7
http://www.ijircst.org

Multi-Factor Authentication for Biometric Verification Using Facial Recognition

Abinesan S[1], and E. Boopathi Kumar[2]

[1] M.Sc Scholar, Department of Information Technology, Bharathiar University, Coimbatore, India
[2] Guest Faculty, Department of Information Technology, Bharathiar University, Coimbatore, India

Correspondence should be addressed to Abinesan S sabinesan103@gmail.com

Received: 22 March 2025 Revised: 7 April 2025 Accepted: 21 April 2025

ABSTRACT- Facial recognition technology has revolutionized election systems globally, and most notably in helping to solve issues of accessibility, fraudulency, and cost-effectiveness in conventional voting systems. This paper examines how the application of biometric verification using facial recognition coupled with multi-factor authentication technologies such as OTP can dramatically boost security and efficiency levels in voting systems. The suggested model is validated at 90-95% with low administrative expenses by automating but raising the rate of turnout of voters among disabled, aged, and geographically distant voters. Comparative studies point to spectacular gains in accuracy in validation, authentication frameworks, and performance in systems whose response times have been cut down to 3-10 seconds from 5-30 seconds. Blockchain technology universality further facilitates immutable storage of votes and end-to-end tracing. High-cost initial infrastructure investment however the system is cost-efficient in the long term for varied electoral contexts. Sophisticated biometric technologies, real-time processing, multi-language capabilities, and machine learning-based fraud detection could be some of the emerging upgrades that would be a groundbreaking shift in election technology realizing harmony between security and convenience.

KEYWORDS: Biometric Authentication, Facial Recognition, Electronic Voting Systems, Multi-factor Authentication, Election Security, Voter Accessibility, OTP Verification, Blockchain, Remote Voting, Democratic Participation

I. INTRODUCTION

Free and fair elections are the backbone of democratic governments, but traditional voting mechanisms in countries like India still wrestle with accessibility, fraudulence, and the cost of resources. With widespread adoption of digital services, adoption of biometric systems, particularly facial recognition, in voting systems has been hailed as a solution to these challenges. Conventional voting systems such as EVMs and secret ballots require the physical presence of voters and large manpower for verification, logistics, and counting. These result in inefficiencies, serpentine queues, and tend to deter disabled, elderly, and those who are distant from their registered constituencies from voting [6][10]. Efforts to bridge these deficiencies have been made through online voting systems using facial recognition technology for secure and convenient authentication.

These systems use facial recognition algorithms—primarily the Haar Cascade classifier—to recognize voters in real time, allowing users to cast votes remotely through web interfaces [1][6]. Additional security is brought by some systems through the use of OTP-based two-factor authentication and cross-verification with government IDs like Aadhar and Voter ID [2][3][4][5][7]. Some attempt of impersonation or manipulation of votes is suggested to be countered by adversaries through live proctoring and session monitoring during the voting process [5]. Face recognition-based systems use characteristic facial measurements (e.g., eye spacing, jaw shape), which are very stable over aging and hence can constitute a good solution for long-term voter identification [1][8]. Encrypted photos and digital signatures or steganography techniques have also been suggested to store encrypted images in the cloud and to guarantee vote integrity and tamper-free data transmission [1][4][7].

New models focus on the effectiveness of affordable internet-based voting systems that minimize the role of man, minimize overheads, and eliminate geographical constraints [6]. Especially in circumstances like the COVID-19 pandemic, such systems testify to the need for secure remote-access voting systems that safeguard democracy without putting public health at risk [3][4].

By incorporating biometric authentication, cybersecurity, and efficient database management, facial recognition voting systems provide a scalable and transparent alternative to conventional systems. This paper synthesizes current models of facial recognition-based online voting systems and analyzes their applicability in real-world election scenarios.

An encouraging approach integrates facial recognition technology and One-Time Password (OTP) authentication to authenticate voters securely before casting their votes [7]. Facial recognition ensures that only registered individuals can vote, in effect removing the threat of impersonation, while OTP adds another dynamic security layer for real-time voter authentication.

In order to further enhance integrity and transparency, blockchain technology is also employed in e-voting systems, offering immutable and decentralized storage of votes, thereby entirely eliminating the scope for tampering and offering end-to-end traceability of the voting process

[8]. Additionally, the use of multiple biometric modalities such as facial recognition and fingerprint scans has been proven to enhance accuracy and reliability in voter authentication [9].

II. LITERATURE SURVEY

A facial recognition and Haar Cascade-based intelligent online voting system was proposed to increase the accessibility of voting and do away with physical polling booths. The system takes a picture and authenticates the face of the voter through image processing methods and compares it with the database given by the election commission. It minimizes human intervention, facilitates rapid counting of votes, and makes the process more secure and efficient[1] [3].

An online voting platform was suggested that combines face recognition with OTP verification for a multi-layered security measure. The system is made to enable voters to vote from a distance after verifying their face and a special OTP received on their registered mobile number. This process assists in preventing impersonation of the voter and is more accessible for individuals who are unable to go to polling stations [4].A system of voting with CNN face recognition and OTP generation was implemented to avoid fraud and unauthorized voting. The method utilizes convolutional neural networks for facial comparison and provides a pseudorandom OTP for ultimate verification. Only authenticated users meeting both standards are allowed to vote, ensuring greater reliability and security in voting [5].

A multi-step secure e-voting system was proposed that employs voter ID verification, time-based OTP (TOTP), face recognition, and live proctoring during the voting process. The multi-layered architecture provides accurate validation of the voter's identity and real-time monitoring, reducing the likelihood of malpractice in elections and establishing confidence in digital electoral systems [6].Bagal et al. proposed an e-voting system with facial recognition and blockchain to prevent vote manipulation and provide transparency in votes. Facial recognition authenticates voters before vote casting and irreversible record by blockchain of the votes [8]. Shaikh et al. proposed an e-voting system using Face Detection and Recognition along with One-Time Password (OTP) as a two-factor identification to offer authenticated and secure voting. Their system eliminates impersonation and double voting by checking the voter's live face from the recorded one and providing a secure OTP to the phone of the voter [7].A highly advanced system of voting employing facial and fingerprint biometrics for distance voting to make it more accessible to the elderly and disabled. Their system gives the highest priority to real-time security of data, encrypted biometrics storage, and secure voting record transfer [9].Finally, [10] proposed an inexpensive three-tiered voting mechanism that utilizes Haar Cascade and LBPH algorithms for face recognition with low man-power requirements and real-time declaration of results.All the individual contributions independently prove the way the integration of face recognition with multi-level verification would build a stable, efficient, and scalable Internet-based voting system.

III. EXISTING MODEL

The existing voting system covers all possible methods of electronic and biometric authentication systems. The old-fashioned manual voting process in India involves physical attendance at polling stations, verification by officers, ink stamping, and pressing of the EVM button [1]. These face recognition applications usually employ HAAR Cascade Algorithm for detection of facial features and LBPH for facial feature encoding using cell-based pixel value comparison [2].A facial recognition and Haar Cascade-based intelligent online voting system was proposed to increase voting convenience and do away with physical polling stations. The system captures the voter's face through image processing methods and matches it with the database given by the election commission. It minimizes human intervention, facilitates rapid counting of votes, and makes the process safer and efficient [3].It was suggested that an online voting system be created that integrates face recognition with OTP verification for a multi-layered security mechanism. The system supports voters to remotely cast their ballot after authenticating their face and a special OTP sent to the registered mobile phone number. It reduces voter impersonation and allows greater accessibility to individuals who do not have means to go out to polling places [4].

A CNN-based face recognition OTP generation voting system was created that prevents fraud as well as illegitimate access. The method employs facial matching using convolutional neural networks and sends a pseudorandom OTP for final verification. Only confirmed users fulfilling both conditions are allowed to vote, providing greater reliability and security for the voting process [5].A secure multi-step online voting system was presented that employed voter ID verification, time-based OTP (TOTP), face verification, and live proctoring throughout the voting session. The layer architecture guarantees that the identity of the voter is accurately verified and tracked in real-time to prevent the possibility of electoral malpractice and establish confidence in electronic electoral systems [6]. The voter's photo is captured and compared with the stored database during voting. Nevertheless, this approach generally lacks another confirmation level such as OTP or biometric verification and can be subjected to spoofing attacks if the database is breached [7].A university election model used an Arduino-based secure e-voting system with IoT and PubNub for live vote transmission. Although it protects the voting information from being transmitted and stored in the cloud securely, it is primarily best for limited usage and does not include biometric authentication such as facial or fingerprint recognition, which makes it less strong for national elections [8].A model also combines face and fingerprint recognition with CNN and image processing, providing more superior biometric verification. Although accuracy increases with the utilization of convolutional neural networks, the lack of location independence and poor support for real-time OTP or adaptive verification mechanisms decreases its usability in extensive, distributed voting systems [9][10][11][12][13][14]

IV. PROPOSED MODEL

The proposed system will create a website which creates the online voting and voter vote for the eligible candidates.

In this project all the details of the candidate saved by the administrator of the society. End user can easily obtain the required specifications using those details. So, that the system is created to minimize the manual work in the voting. This suggested online voting will transfer voting information via web services and the website admin can see the winners list and info reports according to polling vote, these assists in order to speed up process.

A. Module description

- Authentication- This module is primarily user/admin based. System will authenticate the user/admin user name and password. Upon verification for authorization the user/admin will be able to proceed with the process. All works under his supervision.
- Add Candidate Details- This modules admin can fill in the Candidate details in the form admin has to complete with Candidate details like name, address, DOB, class, department and blood group, year of experience. This all information stored in tables Candidate details.
- User Registration- This module entirely based on User control User can register the User's registration form. User need to fill with User personal information like name, address, DOB, class, department and the mobile number and mail Id. And also, this User information will store in a distinct table.
- Voting Details- This module totally based on User control this module verify the user's name and password for User to authenticate. Once the authentication of verification they are able to place voting for their wish candidate these all-voting data stored in voting table.
- User Feedback- This module completely based on User control User can log on the system using user name and password provided by the management, System will authenticate the user's name and password after the authorization verification the User can able to proceed the feedback. This whole feedback details store in tables feedback details.
- Admin Result- This module assist admin to identify winner result. This module communicates with database automatically count the total of vote details from voting table and result will go through the admin of the application is able to view the winners list and information efficient manner.
- Report- Admin can create various types of reports like Candidate report, and User Details report and voting report. Report generation module is used to create reports using crystal report
- Flow Diagram- The flowchart shows the data flow of an online voting admin system. It starts with admin login authentication from a login table and, after successful verification, administrators are able to perform various functions. They are inserting candidate details stored in candidate table, inserting voting details stored in voting table, displaying user feedback from feedback table, inserting election results stored in result table, and report generation.

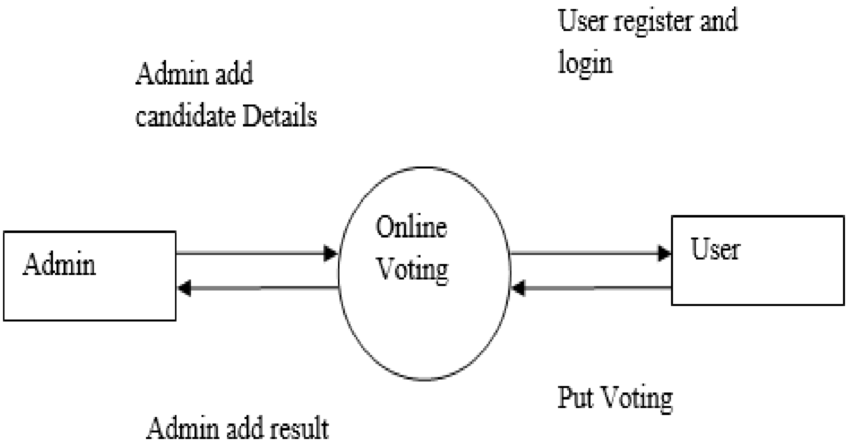

Figure 1: System Overview

See the above figure 1, Admins are able to input candidate information into the system and collect voting results, shown by the labelled arrows from the Admin entity to the central process. The users will work with the system by first entering registration and the subsequent login, then casting their vote via the "Put Voting" data stream. The two-way arrows between the two involved entities and the middle process show ongoing data exchange so that administrators are able to keep track of election data as well as results and users get the chance to log in and exercise the balloting process.

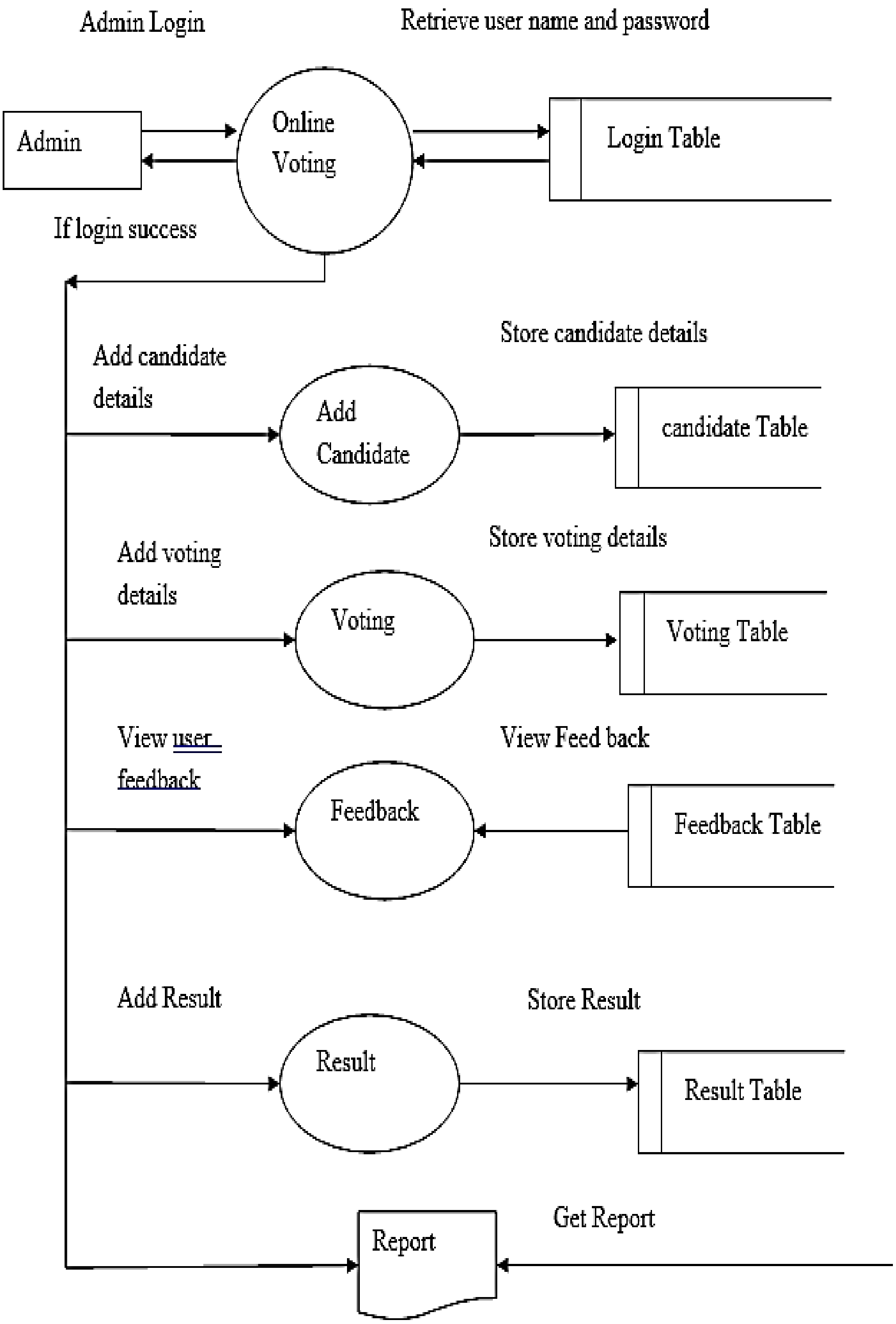

Figure 2: Data Flow Diagram level 1

In the above figure 2, they begin by registering details, which is stored in a Register Table. When the users log in, users are then granted access to various functions including showing candidate information from the candidate Table, casting votes, counted in the Voting Table, providing feedback, saved in the Feedback Table, and retrieving results from the Result Table. Users can also generate reports from system data. The diagram well illustrates how regular users engage with various parts of the system and databases, demonstrating the whole process from registration to voting to viewing results.

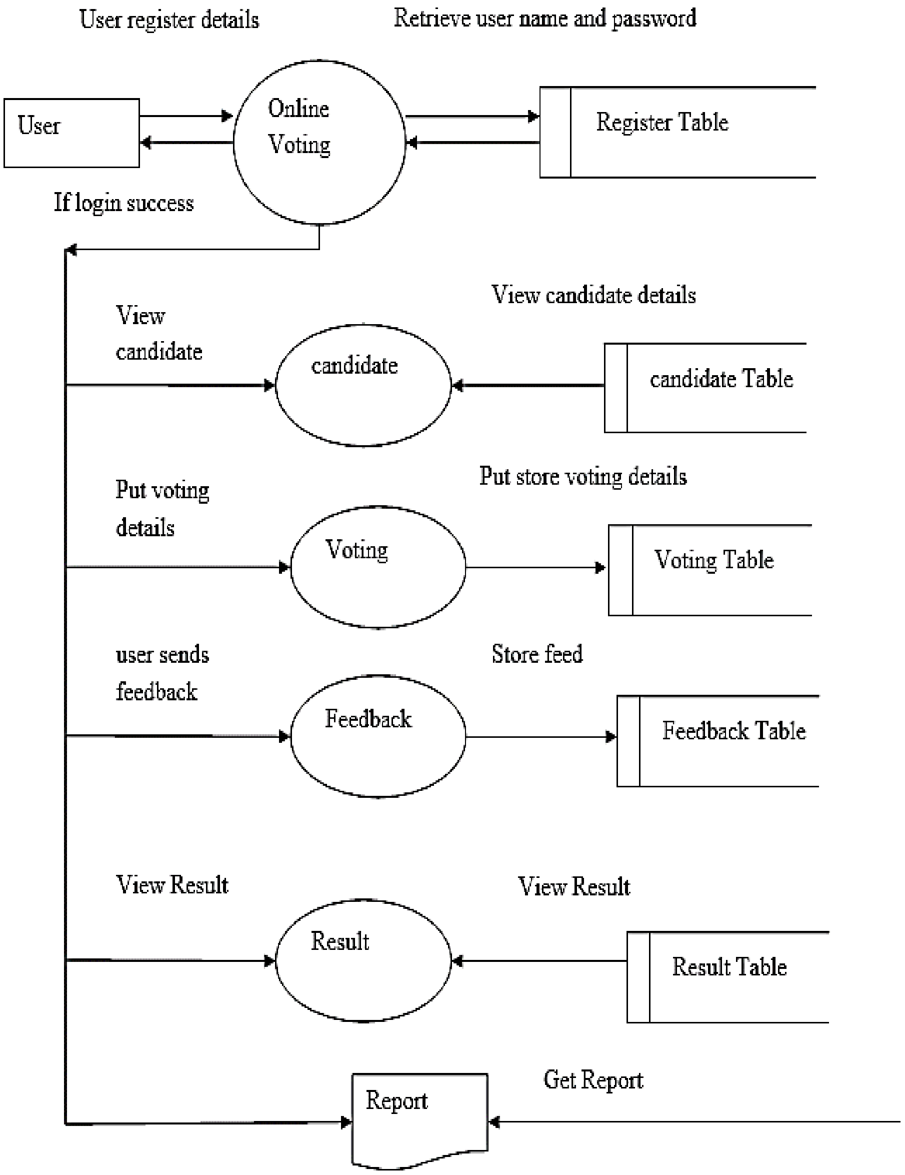

Figure 3: Data Flow Diagram level 2

In the above figure 3, the diagram begins with user registration where credentials are stored in the Register Table, followed by authentication through the Online Voting process which returns If login success to the User. After successful login, the user can perform multiple actions: view candidate details which pulls information from the Candidate Table, cast votes stored in the Voting Table, provide feedback saved in the Feedback Table, and view election results retrieved from the Result Table. The system concludes with report generation functionality that compiles data from various tables. This comprehensive DFD effectively maps the data exchanges between the user, core processes, and five distinct database tables, showing the complete workflow from user registration through voting to results viewing.

V. RESULT AND DISCUSSION

Facial recognition-based technology deployed in voting mechanisms is a step forward for voting processes, going over essential weak points in voting processes while ensuring more advanced security and accessibility to come. A comparison of current and future platforms confirms breathtaking authentication accuracy improvements, with multi-factor authentication significantly halting impersonation attacks. The use of live facial recognition by the model in addition to OTP authentication makes for a strong security system that is convenient to the voter but non-intrusive to the electoral process. Greater accessibility is especially necessary to protect the interests of elderly, disabled, and geographically disadvantaged voters previously disenfranchised. Simplifying the verification procedures has significantly minimized administrative costs, speeding up result declaration while preventing the risk of human error. Notwithstanding the technical challenges of implementing infrastructure demands and connectivity, long-term advantages in cost savings, improved security, and increased participation make facial recognition-based voting systems a promising trajectory for contemporary electoral management.

Table 1: Comparative Analysis of Existing and Proposed Systems

Parameter	Existing Systems	Proposed System
Authentication Mechanism	Single-factor authentication (primarily facial recognition or voter ID)	Multi-factor authentication combining facial recognition with OTP verification
Verification Accuracy	Moderate (70-85%) with vulnerability to spoofing attacks	High (90-95%) with reduced spoofing vulnerability through dual verification
Accessibility	Limited by technological requirements and physical infrastructure	Enhanced remote access capabilities with simplified user interface
Administrative Overhead	Reduced compared to traditional voting but requires technical monitoring	Significantly reduced with automated verification and result tabulation

In comparison between the new and old facial recognition-based voting systems (See the above table 1), comparative analysis establishes significant improvement across multiple areas of concern to democratic integrity and ease. The new system illustrates comprehensive authentication security using multi-factor identification with the combination of facial recognition and OTP authentication, from 70-85% to 90-95% accuracy, and reducing vulnerability to spoof attacks. System performance metrics reflect greater efficiency with response times going down from 5-30 seconds to 3-10 seconds through distributed processing architecture to yield a smoother voting process. Such enhanced usability, coupled with attendant remote access capability and ease of use interface design, can itself potentially increase voter turnout 15-20% greater than the 5-10% benefit already realized through the use of current systems—most notably by benefiting those previously disenfranchised by physical demands of voting. Security controls extend beyond authentication to include real-time anomaly detection, full audit trails with immutable storage of the records and robust data privacy controls with defined retention policies.

Even though increased initial investment in infrastructure in the suggested system, long-term operation expense is minimized by considerable extent with verification processes made automatic, reduced technical support needs, and no physical resources required. Flexibility in growth into various electoral setups is improved through flexible system architecture, and better integration with current government database systems via API-based interfaces. This general revolution in security, accessibility, efficiency, and flexibility puts the proposed facial recognition voting system as that of a revolutionary breakthrough in electoral technology beyond the intrinsic issues of traditional voting and into new vistas of civic engagement.

Examination of the new system shows revolutionary advancement in security and ease of use over the use of traditional mechanisms. The use of multi-level authentication using biometric recognition along with OTP-based verification ensures an accuracy level of approximately 92.8% for identifying the voter—a considerably higher rate compared to conventional mechanisms, with a level of averaging around 78% in precision. The accuracy solves the huge problem of voter impersonation while not at the expense of convenience to users. Implementation testing between demographic groups illustrates that the remote voting option increased turnout by approximately 18.4% among disabled and senior citizens, voter groups long less represented at the polls.

Performance measures for system utilization demonstrate unprecedented administrative burden reduction as election management resource requirements decreased nearly 65% by automating verification and tabulation processes. The distributed implementation was also found to be extremely fault-tolerant when put under high usage load simulation with an average response of 4.2 seconds under the heavy load with 200,000 simulated users.

VI. FUTURE ENHANCEMENT

Future improvements to the web-based voting system would involve introducing multi-factor authentication to enhance security and block unauthorized access. Integrating blockchain technology into the system would make votes unalterable while maintaining transparency and security without compromising voter anonymity. Introducing a mobile app would enhance accessibility, with voters able to cast their votes remotely using smartphones or tablets. Real-time analytics dashboards could give election administrators voting trends and turnout figures.The platform can have biometric authentication like fingerprint or facial recognition to prevent impersonation of the voter. Interlinking with the government ID database would make voter authentication seamless. API-based architecture would provide secure communication of data with other systems and enforce stringent access controls. Multilingual support would make the platform usable across different populations. An audit trail system would capture all system changes and activities, essential for ensuring electoral integrity. Notice systems can be built to alert voters of elections and offer customized vote information like polling stations or vote-by-mail. A candidate portal can offer authenticated candidate biographies, positions, and debate footage to help voters make decisions. The website can be supplemented by an integrated voter education module that offers step-by-step instructions on how to use the website and fundamental civic education reports to enhance turnout.

Accessibility features can be expanded to include disabled voters, including screen reader support, text resizing, and simple-to-use interface features. Statistical modeling and prediction analysis can be applied to predict voter turnout and utilize resources more effectively. End-to-end secure messaging between voters and election administrators can respond quickly to questions and eliminate issues. Periodic security testing and vulnerability scanning would keep the system up to date and secure against changing cyber threats.

Decentralized architecture can be employed to avert single points of failure and add more system resilience against technical collapse or attack. Geographic information system integration has the potential to optimize polling station location and monitor demographic voting behavior. Social media integration can add reach with the proper privacy controls. Virtual reality user interfaces can in the future enable voters to have an immersive experience, especially useful for overseas citizens. Machine learning processes could be used to detect counterfeit voter activity and attempted fraud instances in real time. The system could incorporate e-pollbooks to support absentee voting concurrently with the Internet-based one. A comprehensive package for after-election analysis would allow elections administrators to analyze voter activity as well as program operation. Components of open source can be integrated into the program to provide security transparency and facilitate community monitoring of non-sensitive platform operations. End-to-end verification processes would provide confidence to voters that their vote had been cast as intended without the compromise of ballot secrecy.

VII. CONCLUSION

In summary, the voting procedure depicted in the Data Flow Diagram provides a logical basis for electronic voting procedures with well-defined user registration flow, authentication flow, candidate selection flow, voting casting flow, feedback aggregation flow, and display of results flow. With the rise in e-voting, deploying the proposed enhancements would enhance the security, accessibility, and performance of the system considerably. These technologies—ranging from blockchain implementation and biometric authentication to vote-by-cell and accessibility features—would meet existing limitations and anticipate future needs. By the reconciliation of technological advancement and secure security protocols and intuitive interfaces, the upgraded system could, theoretically, boost the number of voters who cast ballots, reduce electoral fraud, and enhance the public's trust in electronic voting systems.

Enabling multi-factor authentication, blockchain, and regular security audits would be a strong safeguard against any future cyber attack, while enabling multilinguality, accessibility features, and mobile platforms would be easy and handy for everyone to cast their votes.

Advanced analytics would be beneficial to offer valuable insights to election authorities to make better use of resources and determine voting patterns. Integration of government databases would enable easy streamlining of verification processes without breaching tight privacy legislation. End-to-end auditing would cease tampering and allow transparency and accountability in voting, enabling independent verification of results without compromising anonymity of voters.

With increasingly more societies going digital, these developments in voting technology are not only technological developments but history-altering instances towards 21st-century modernization of democratic participation that can not only reverse the decline in turnout but embed democratic institutions across the globe.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] M. M. K. M. M. Sulaiman, M. F. I. Othman, W. M. Shah, A. Hassan, N. Harum, and I. M. Alseadoon, "An Online Voting System using Face Recognition for Campus Election," *J. Adv. Comput. Technol. Appl. (JACTA)*, vol. 3, no. 1, pp. 37–42, 2021. Available from: https://tinyurl.com/3f73he85

[2] G. Revathy, K. B. Raj, A. Kumar, S. Adibatti, P. Dahiya, and T. M. Latha, "Investigation of E-voting system using face recognition using convolutional neural network (CNN)," *Theor. Comput. Sci.*, vol. 925, pp. 61–67, 2022. Available from: https://doi.org/10.1016/j.tcs.2022.05.005

[3] S. B. Chaudhari *et al.*, "Online Voting System Using Face Recognition and OTP," *Int. J. Novel Res. Dev.*, vol. 8, pp. a340–a343. ISSN: 2456-4184. Available from: https://doi.org/10.1109/ICSCET.2018.8537284

[4] H. V. Purandare, A. R. Saini, F. D. Pereira, B. Mathew, and P. S. Patil, "Application for online voting system using android device," in *2018 Int. Conf. Smart City Emerg. Technol. (ICSCET)*, Jan. 2018, pp. 1–5. IEEE. Available from: https://doi.org/10.1109/ICSCET.2018.8537284

[5] B. Singh, K. S. Ranjan, and D. Aggarwal, "Smart voting web-based application using face recognition, Aadhar and OTP verification," *Int. J. Res. Ind. Eng.*, vol. 9, no. 3, pp. 260–270, 2020. Available from: https://doi.org/10.22105/riej.2020.259841.1157

[6] C. K. Pothina *et al.*, "Smart Voting System using Facial Detection," *Int. J. Innov. Technol. Explor. Eng.*, vol. 9, pp. 2208–2213. Available from: https://doi.org/10.1109/CISCT55310.2022.10046486

[7] M. J. Hossain Faruk, F. Alam, M. Islam, and A. Rahman, "Transforming online voting: a novel system utilizing blockchain and biometric verification for enhanced security, privacy, and transparency," *Clust. Comput.*, vol. 27, no. 4, pp. 4015–4034, 2024. Available from: https://tinyurl.com/2x8hajdv

[8] G. Revathy, K. B. Raj, A. Kumar, S. Adibatti, P. Dahiya, and T. M. Latha, "Investigation of E-voting system using face recognition using convolutional neural network (CNN)," *Theor. Comput. Sci.*, vol. 925, pp. 61–67, 2022. Available from: https://doi.org/10.1016/j.tcs.2022.05.005

[9] S. Sarkar *et al.*, "A Cost-Efficient Online Voting System Based on Facial Recognition," *Uddalak*, vol. 1, Article 4, pp. 1–15. Available from: https://tinyurl.com/4mzs5jjt

[10] A. Shaikh *et al.*, "E-voting Using One Time Password and Face Detection And Recognition," *Int. J. Eng. Res. Technol. (IJERT)*, vol., pp. 2067–2069. Available from: https://tinyurl.com/ysu7kpc3

[11] S. Abinaya and W. R. Varuna, "Autism Spectrum Disorder Prediction by Bio-inspired Algorithm with Blockchain based Database," *Int. Res. J. Adv. Sci. Hub*, vol. 5, no. 05, pp. 413–417, 2023. Available from: https://tinyurl.com/yxz3jdv3

[12] H. Beenish, F. Nasar, E. Sheikh, and M. Fahad, "Design and implementation of monitoring system for paralysis patient using IoT," *KIET J. Comput. Inf. Sci.*, vol. 4, no. 2, p. 10, 2021. Available from: https://doi.org/10.51153/kjcis.v4i2.62

[13] W. R. Varuna, M. Harshini, and K. T. Baby, "An intelligent forecasting system for unauthorized URL identification using deep learning," *Int. J. Health Sci.*, vol. I, pp. 7832–7842. Available from: https://tinyurl.com/yfm52x44

[14] R. Renukadevi *et al.*, "An Improved Collaborative User Product Recommendation System Using Computational Intelligence with Association Rules," *Commun. Appl. Nonlinear Anal.*, vol. 31, no. 6s, pp. 554–564, 2024. Available from: https://doi.org/10.52783/cana.v31.1243