International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

Biometric Polling Verification Framework with Audit Monitoring Based Offline Validation Support

Manku Akhila, Narra Navya*
Vaagdevi Engineering College, Warangal, 506005, Telangana, India.
*Correspondence: Narra Navya

ABSTRACT

Elections are a fundamental component of democratic governance, and maintaining their integrity is essential for ensuring transparency, accountability, and public confidence in the electoral process. As voter populations continue to increase, conventional polling systems encounter numerous challenges, including voter impersonation, duplicate voting, manual identity verification errors, lengthy authentication procedures, and inadequate monitoring of polling activities. Traditional election processes rely heavily on physical identity documents, printed electoral rolls, and manual record verification, making them vulnerable to human error, procedural inefficiencies, and fraudulent practices. Furthermore, the absence of real-time identity verification and centralized digital record management limits the ability of election authorities to detect irregularities and maintain accurate audit trails during polling. To address these limitations, the proposed Biometric Polling Assurance System provides a secure digital platform that integrates biometric-based voter authentication with centralized monitoring and structured relational data management. Developed using React for the frontend, Node.js for backend processing, and MySQL for relational database management, the system securely verifies voter identities before vote casting, thereby enforcing the one-person-one-vote principle. The MySQL database employs normalized tables with primary and foreign key relationships to ensure data consistency, integrity, and efficient storage of election records. The platform also maintains detailed authentication logs and administrative records to support transparency, accountability, and post-election auditing. Role-Based Access Control (RBAC) restricts system access to authorized users, while transaction management ensures accurate processing of concurrent authentication requests. The proposed system enhances election security, operational efficiency, scalability, voter privacy, and the overall credibility of modern electoral processes.

Keywords: Biometric Authentication, Electronic Voting System, Election Security, Voter Authentication, Election Integrity.

1. INTRODUCTION

The integration of technology into electoral systems has progressed significantly over several decades, transforming the way elections are conducted across the world. Earlier voting processes relied entirely on manual methods, including paper ballots and blackballing, but technological advancements gradually introduced punch cards, lever voting machines, ballot optical scanners, electronic voting cabins, direct recording electronic (DRE) voting systems, and hybrid voting mechanisms that combine both manual and electronic processes [1]. These innovations were primarily introduced to improve voting efficiency, accelerate vote counting, reduce administrative workload, and enhance the accuracy of election results. However, the increasing dependence on digital technologies has also introduced new challenges related to election security, voter authentication, data integrity, privacy protection, and auditability. Modern electoral systems must therefore ensure not only accurate vote collection and counting but also secure voter verification, transparent election monitoring, and reliable mechanisms for detecting and preventing fraudulent activities. Since most traditional and electronic voting systems operate under centralized

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

administrative control, they remain susceptible to risks such as unauthorized system access, voter impersonation, manipulation of electoral records, and insider threats if appropriate security controls are not implemented [2]. Consequently, strengthening identity verification mechanisms and implementing secure monitoring frameworks have become essential requirements for maintaining public trust and ensuring the credibility of democratic elections.

In conventional electronic voting environments, voter registration records, authentication information, and election data are generally maintained within centralized databases administered by election authorities [3]. Although centralized management simplifies administrative control, it also creates a single point of failure and increases the potential impact of security breaches, particularly when voter verification depends solely on identity documents, passwords, or other static credentials. Over the years, numerous voting approaches—including paper-based elections, electronic voting machines, internet-based voting systems, and hybrid electoral platforms—have been developed with the common objective of preserving voter anonymity while ensuring accurate, transparent, and verifiable vote recording and counting [4]. As digital technologies continue to evolve, protecting sensitive voter information has become increasingly important due to growing concerns regarding cybersecurity threats, personal data privacy, identity theft, and unauthorized disclosure of electoral information. These challenges highlight the necessity of integrating advanced authentication technologies, secure access control mechanisms, encrypted data management, and comprehensive audit trails into modern election systems to safeguard voter information, strengthen election integrity, and improve overall confidence in the electoral process [5].

2. LITERATURE SURVEY

CH Srilatha, et al. [6] introduced a cutting-edge concept: a smart electronic voting system grounded in a thorough biometric identification survey. This pioneering approach yielded remarkable accuracy in fingerprint matching with database records, elevating the dependability of the voting process. Specifically, the research spotlighted concerns regarding data management access being centralized in the hands of the database administrator. This aspect underscored the need for a meticulous examination of data governance structures, aiming to enhance transparency and mitigate potential vulnerabilities. The authors introduced "IOT-Based Voting Machine with Fingerprint Verification," an IoT-based voting machine with fingerprint verification, and achieved high accuracy in fingerprint matching with stored data. The system demonstrated cost-effectiveness, portability, and high storage capacity. Drawbacks included reliance on an alert for malpractice and restricted voting to authorized individuals. Parag Narendra Achaliya, et al. [7] proposed a system that allowed the government to conduct free and fair polls in the country. Crores of rupees were spent on this to make sure that the elections were riot-free. But, nowadays, it had become common for some forces to indulge in rigging, which could eventually lead to a result contrary to the actual verdict given by the people. This paper aimed to present a new voting system employing biometrics in order to avoid rigging and to enhance the accuracy and speed of the process. That meant this system was better than present-day voting systems. During elections, the fingerprint of a voter was entered as input to the system. Then, this input was compared with the database. If the user's data was available in the database, access was granted to the user for casting the vote. However, if the record did not match the database, the vote was rejected, and the same applied for repeated users as well.

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

Also, an alert was sent to the nearby police. Shrushti Sankhe, et al. [8] proposed e-voting (Electronic Voting) as a term that encompassed a broad range of voting systems that applied electronic elements in one or more steps of the electoral cycle. There were many levels to e-voting in the broad sense, which could include e-collation, e-verification, internet voting, remote online voting, etc. Following the definition of a system as anything that took an input and gave an output, an e-voting system was any system that could offer both electronic and online voting. It could also incorporate e-registration, e-verification, e-collation, remote online voting, and real-time result display. An e-voting system (EVS) generally comprised the following for it to work efficiently.

Kashif H.M., et al. [9] proposed a voting system with biometric authentication. It was an electronic voting system that sought to make use of the uniqueness of the minutiae of the human fingerprint to further enhance the level of trust and confidentiality of the voters in the system, as well as to make the actual process as universally accessible as possible, which was achieved through deployment on the Internet. It was expected to solve the critical issues faced due to elections. For the voter registration and authentication processes, which were performed on the desktop module, the voter was expected to have his or her fingerprints captured and the minutiae extracted, which were stored in the database. This was done to prevent the occurrence of multiple registrations or identity issues. Thus, during the authentication period, voters were expected to undergo a matching verification of their fingerprint samples against the values stored in the database, which was identified through the use of a unique voter identification number assigned during registration. Samarth Agarwal, et al. [10] proposed a system that prevented booth capturing, rigging, fake voting, tampering with the Electronic Voting Machines (EVMs), etc. Being responsible engineers, it was their duty to do something to curb this menace. In the commonly used EVMs, the voting process took place electronically, and this eliminated the use of ballot paper to cast votes in elections, as it was very time-consuming and errors might crawl in intentionally or unintentionally. At that time, the authenticity of the voter was a big concern, and it also had to be ensured that the same voter was not able to vote two times. This issue could be dealt with by introducing a biometric-based voting system, where the authenticity of a voter was established based on fingerprints. Hence, the principle was one person, one authentic vote. In the present work, a prototype fingerprint-based biometric voting machine was developed. It was proposed that a feature that linked the Aadhaar database of the Unique Identification Authority of India (UIDAI), Govt. of India, New Delhi, could be embedded. This facilitated all the voters to get registered on the portal automatically, which could be classified on the basis of regions and constituencies based on their unique identification, i.e., their fingerprints. Parikshit Martolia, et al. [11] discussed the development and implementation of a new technology for voting machines. It devised a new modern approach that could replace the traditional mechanical voting system with a biometric one. The main objective was to design a biometric voting machine that used an individual's fingerprint as the medium of identification. It aimed to remove the traditional use of documents or voter ID at the polling booth during elections. The project suggested a more modern system that was biometric in nature and also less time-consuming.

Peter Wolf, et al. [12] introduced a system in which, in a biometric verification system, an individual claimed an identity, for example by providing a name and date of birth. The individual's biometric features were captured and compared to previously captured and confirmed biometric features of that individual.

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

Such a one-to-one comparison determined whether the individual was indeed who they claimed to be. In a biometric identification system, the individual did not need to claim an identity. His or her biometric features were captured and compared to the features of all previously captured biometric features stored in a biometric database. This one-to-many comparison sought to determine who the individual was. A. Piratheepan, et al. [13] proposed a system using Arduino to create a biometric voting system. Most elections throughout the globe did not use biometric technology instead, they opted for the more traditional paper ballot. The authenticity of voters was only one example of a security risk in the existing voting system. The suggested approach allowed for the rapid verification of a voter's identification. The registration data of all eligible voters was safely kept. They prioritised secure, accessible voting that upheld democracy and promoted civic engagement. Their efforts aimed to foster trust and confidence in the electoral system while safeguarding its integrity. They empowered citizens to vote quickly and confidently through their commitment to security, transparency, and accessibility. With this system in place, voters did not need to worry about the safety of their fingerprint-based ballots since they were digitally stored and verified. Fingerprint voting sped up the counting process and cut the need for human labour altogether. Sangameshwar Neelagund, et al. [14] introduced biometric registration kits for enrolment of voters, used electronic voter identification devices before and on Election Day, and issued voter identification documents (i.e., biometric voter cards), among others. The chronological stages for adopting a biometric voting registration project usually included assessment, feasibility studies, securing funding, reviewing legislation, conducting pilot projects and mock registration exercises, procurement, distribution of equipment, installation and testing, recruitment and training of staff, voter information, deployment, and post-election audits.

3. PROPOSED METHODOLOGY

The biometric polling assurance system as shown in Fig. 1 is designed to improve the security and reliability of elections by using biometric-based voter authentication to prevent impersonation and duplicate voting. The system connects polling stations with election authorities through a centralized digital platform, allowing real-time verification and monitoring of voter authentication activities. Voters are verified using biometric inputs before voting, while their privacy and vote anonymity are preserved. The system also maintains detailed authentication logs for transparency and auditing and supports offline verification to ensure uninterrupted polling. Overall, it provides a secure, scalable, and practical solution for conducting fair and fraud-free elections.

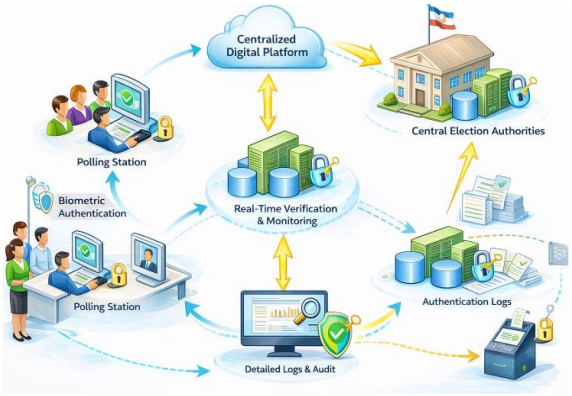

Fig. 1: System architecture for proposed biometric polling system

The proposed system operates through a centralized digital platform that integrates polling stations with election authorities in real time. Voters authenticate their identity using biometric inputs at polling locations, and their verification status is securely recorded. Once authenticated, voters are allowed to proceed with the voting process while ensuring that their identity remains decoupled from their vote, thereby preserving voter anonymity. This

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

approach balances strong security with essential privacy requirements.

4. RESULT ANALYSIS

Fig. 2 illustrates the user permission management interface of the online voting system, where the administrator is responsible for controlling access to different users based on their assigned roles. The interface provides a complete overview of registered users along with their authorization status, enabling the administrator to verify whether a user is approved to participate in the election process. It supports permission management by allowing administrators to grant or revoke access whenever necessary, thereby preventing unauthorized participation. This module strengthens system security by ensuring that only authenticated and approved users can perform their designated operations.

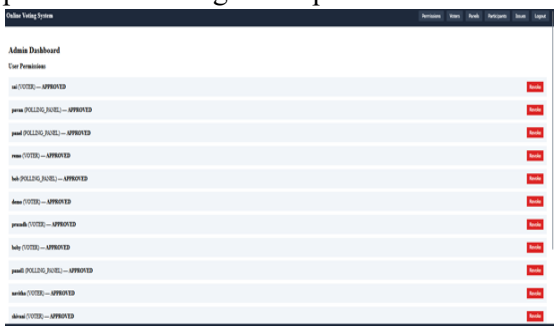

Fig 2: User Permission

Fig. 3 depicts the voter details module, which serves as a centralized repository for maintaining the information of all registered voters within the online voting system. The administrator can review voter records to verify registration details, monitor voter information, and ensure that only eligible individuals are included in the electoral database. This module assists in identifying inconsistencies or duplicate registrations, thereby improving the accuracy and authenticity of voter information. Maintaining well-organized voter records simplifies election administration and supports efficient verification during the voting process.

Fig. 3: Voter Details

Fig. 4 illustrates the polling panel details module, which maintains the records of polling officials responsible for conducting and supervising election activities. The administrator can examine the details of authorized polling personnel to ensure that each official is properly registered before participating in election operations. This module enables systematic management of polling staff and supports the assignment of responsibilities in an organized manner. By maintaining accurate records of polling officials, the system minimizes administrative errors and improves accountability throughout the election process.

Fig. 4: Polling Panel Details

Fig. 5 depicts the election participants management module, where the administrator manages the information of all contesting candidates participating in the election. The module supports candidate registration, maintains participant records, and enables administrative management throughout different stages of the election process. It also provides the functionality required to determine and declare the winning candidate after the completion of voting and result evaluation.

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

Maintaining a centralized repository of participant information simplifies candidate management and ensures consistency across the election workflow.

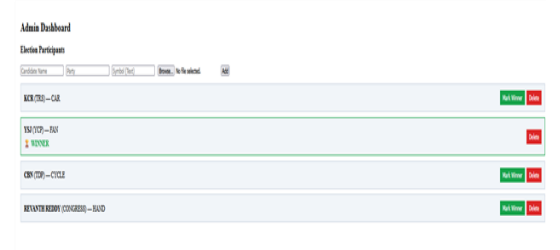

Fig. 5: Election Participants

Fig. 6 illustrates the voter dashboard, which provides users with information regarding their voting status and important election-related guidelines. The dashboard informs voters whether they have already cast their vote while also presenting instructions that help them understand the election process and their responsibilities. It promotes voter awareness by providing information about eligibility requirements, voting procedures, and security practices that should be followed during the election. The module serves as an informative platform that guides users throughout the voting process while maintaining transparency regarding their participation status.

Fig. 6: Voter Status

5. CONCLUSION

The Biometric Polling Assurance System successfully demonstrates how biometric-based authentication and secure digital technologies can be applied to strengthen the integrity of electoral processes. The system effectively addresses key challenges associated with traditional polling methods, such as voter impersonation, duplicate voting, and lack of real-time monitoring. By integrating biometric verification with a centralized backend and structured data management, the system ensures that only eligible voters are allowed to participate while maintaining voter privacy and vote anonymity.

REFERENCES

[1]. Solutions, I. Software that Powers Democracy Should Be Free. Available online: http://inno.vote/whitepaper/Inno.vote%20%E2%80%94%20Bringing%20Democracy%20to%20Elections.pdf (accessed on 28 January 2022).

[2]. Neziri, V. E-Voting: System Architecture—Kosovo Case. Master's Thesis, Faculty of Electrical and Computer Engineering, University of Prishtina, Pristine, Kosovo, September 2011.

[3]. Dhillon, A.; Kotsialou, G.; McBurney, P.; Riley, L. Introduction to Voting and the Blockchain: Some open questions for economists. EconPapers. In CAGE Online Working Paper Series 416, Competitive Advantage in the Global Economy; Örebro University: Örebro, Sweden, 2019.

[4]. Westin, A. Privacy and Freedom. Wash. Lee Law Rev. 1968, 25, 166.

[5]. Webb, P.D.; Eulau, H.; Gibbins, R. Election Political Science. Available online: https://www.britannica.com/topic/election-political-science (accessed on 7 September 2021).

[6]. CH Srilatha, Dwaraka Chand Venigalla, Sai Kaushik Tuttagunta, Nallagatla Akshay, Myasar Mundher Adnan, B Rajalakshmi, H Pal Thethi and Ashwani Kumar, "Fingerprint-based biometric smart electronic voting machine using IoT and advanced

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

interdisciplinary approaches", The Islamic university, pp. 507 – 511, 2024.

[7]. Parag Narendra Achaliya, Chaitanya Hemant Malvatkar, Mayur Annasaheb Gaikwad, Sudershan Bhausaheb Aher, Hritik Dilip Ajmera, "Biometric Voting System", International Journal of All Research Education and Scientific Methods (IJARESM), Vol. 10, no.8, pp. 1781 – 1793, 2022.

[8]. Shrushti Sankhe, Pratiksha Kute, Mayuri Kokane, Runali Dhaygude, Prof. Sujay Pawar, "Biometric Voting System", International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Vol. 2, no.5, pp. 129-135, 2022.

[9]. Kashif H.M., Dileep Kumar and Syed Muhammad Usman, "Next Generation a Secure E-Voting System Based on Biometric Fingerprint Method", International Conference on Information and Intelligent Computing IPCSIT, vol. 18, no.2, pp. 26-27, 2022.

[10]. Samarth Agarwal, Afreen Haider, Abhishek Jamwal, Param Dev, Rajeevan Chandel, "Biometric Based Secured Remote Electronic Voting System", International Conference on Smart Structures and Systems (ICSSS), 2020.

[11]. Parikshit Martolia, Pragati Bhojak, Sneha Bisht and Mr. Ajeet Singh, "Study of Biometric Voting System", International Journal on Emerging Technologies, Vol. 8, no.3, pp. 111 – 112, 2017.

[12]. Peter Wolf, Abdul Alim, Brown Kasaro, Mohammed Saneem, Pontius Namugera and Tamir Zorigt, "Biometric Technology in Elections", International Institute for Democracy and Electoral Assistance, 2017.

[13]. A. Piratheepan, S. Sasikaran, P. Thanushkanth, S. Tharsika, M. Nathiya, C. Sivakaran, Thiruthanigesan K., "Fingerprint Voting System Using Arduino", Middle-East Journal of Scientific Research, Vol. 25, no.8, pp. 1793–1802, 2017.

[14]. Sangameshwar Neelagund, B. Rudrappa Gujanatti, Shivaram N. Tolanur, Murughendra S. Nemagoud, and Shanta S. Reddy, "A voting system based on fingerprints", International Journal of Engineering Research, Vol. 4, no.05, pp. 887–892, 2015.