Aadhar Based Voting System With Finger Print Authentication

Mrs. Prakruthi G R[1], Sonica S[2], Chandana N[3], Saroj J[4], Megha[5]
[1]Assistant Professor, Dept of AD
[2, 3, 4, 5]Dept of AD
[1, 2, 3, 4, 5] East West Institute of Technology, Bengaluru,

Abstract- *"Anywhere Voting System" using Aadhaar-linked biometric authentication, The system allows eligible voters to cast their vote from any polling station across the country by verifying their identity through Aadhaar-linked biometric data, such as fingerprints enabling voters to cast ballots from any polling station. By verifying identity through Aadhaar, it ensures authenticity, prevents duplicate votes, and removes location-specific voter lists. This system enhances transparency, reduces electoral fraud, and simplifies logistics, fostering inclusive, efficient, and secure elections in India.*

Keywords- Anywhere voting, Biometric verification, Aadhaar-linked authentication, Electoral transparency

I. INTRODUCTION

India, being the largest democracy in the world, continually seeks innovative ways to enhance the efficiency, transparency, and inclusivity of its electoral process. One such transformative idea is the "Anywhere Voting System," which harnesses the power of Aadhaar-linked biometric authentication. This advanced system aims to simplify the voting process, making it more accessible to all citizens while ensuring the integrity and security of elections. The "Anywhere Voting System" is a revolutionary approach designed to modernize India's electoral framework. By integrating Aadhaar-linked biometric authentication, the system allows eligible voters to cast their ballots from any polling station across the nation. This innovation eliminates the traditional dependence on location-specific voter lists, offering a seamless and flexible voting experience.Through the use of biometric data, such as fingerprints or iris scans, the system ensures accurate identity verification, preventing issues like duplicate voting and impersonation. Aadhaar integration also enhances the authenticity of the process, ensuring that only valid voters participate in elections.This approach not only simplifies the logistical complexities of elections but also fosters inclusivity by enabling citizens—especially those who are away from their registered constituencies—to exercise their right to vote. It holds particular significance for migrant workers, students, and individuals with mobility challenges, thereby strengthening democratic participation. Additionally, the system aims to reduce electoral fraud, enhance transparency, and streamline operations for election authorities. By adopting such a forward-thinking solution, India can set a global benchmark for secure, efficient, and inclusive elections, ensuring the democratic process remains robust and trustworthy for future generations

II. LITERATURE SURVEY

1.“Enhancing the Security of Online Voting System Using Defined Biometrics”
Author:Devanshi Malik,Kritika Tripathi
Published in:2023

This paper proposes a secure online voting system using Aadhaar-linked biometric authentication and two-step verification to prevent fraud and ensure voter eligibility. Voters register online and authenticate via OTP and fingerprint on election day. The system simplifies voting, eliminating duplicate or fake votes. It also reviews cloud, blockchain, and facial recognition-based systems for secure elections. This framework ensures accessibility, transparency, and efficiency in the voting process.

2.”Fingerprint based voting system”
Author:Abhishek Kaushik, Shiv Narain Gupta
Published in:2023

This paper addresses challenges in India's electoral process, such as booth capturing, rigging, and duplicate voting, highlighting limitations of current EVMs. It proposes a biometric voting system using Aadhaar-linked fingerprint authentication to ensure "one person, one genuine vote." A prototype integrates online voter registration and organizes voters by constituency, enabling national implementation

4.”Biometric-based Smart Electronic Voting SystemUsing Internetof Things”
Author: Vasanthi A, Dhanush Kumar R
Published in:2023

This paper proposes a secure voting system utilizing iris recognition and fingerprint authentication to address issues like duplicate and false voting. Voter data, including iris scans and Aadhaar numbers, is stored in a database and verified during the voting process. IoT integration automates data collection, storage, and result calculation, enhancing efficiency and reducing tampering risks. This approach aims to modernize the voting system, ensuring credibility, security, and transparency

3."Secured Voting System based on Multilayered Biometric Authentication"
Author: Gunda Sathwik,Manu Gupta
Published in:2024

This paper proposes a secure, multi-layered online voting system integrating facial recognition, thumbprint detection, and Aadhaar number verification to enhance voter authentication and prevent fraud. It utilizes a Django-based web application with admin and user portals, ensuring accessibility and scalability. Facial recognition via OpenCV strengthens authentication, while the three-step verification process eliminates duplicate votes and ensures system integrity. This approach aims to modernize elections, streamline operations, and enhance transparency and trust in the democratic process.

III. METHODOLOGY

The system begins with the data integration phase, where voter details, candidate lists, and biometric information are securely stored in a central database. Each voter's Aadhaar number is linked to their biometric data, including fingerprints, and mapped to their constituency. Candidate data, such as names, party affiliations, and constituencies, is also uploaded to the database. This ensures that the system can dynamically retrieve the relevant candidate list based on the voter's constituency.

The authentication phase forms the backbone of the voting process. Voters place their finger print on finger print scanner, initiating the biometric verification process. A biometric device captures the voter's fingerprint and matches it with the stored fingerprint in the database. The system employs secure matching algorithms to ensure accurate identification. If the fingerprint does not match, the system displays an error message, notifying the voter and preventing further access. If the fingerprint matches, the voter is authenticated, and the system proceeds to the next step.

In the voting phase, after successful authentication, the system dynamically retrieves the voter's constituency details and displays the list of candidates contesting in that constituency.

This step is crucial for ensuring that voters are presented with accurate and relevant options. The voter selects their preferred candidate through the web interface. The system then securely records the vote in the database, ensuring that the voter's choice remains confidential. A confirmation message is displayed to inform the voter that their vote has been successfully cast.

The system design incorporates a user-friendly web interface to enhance accessibility for voters and election officials. Error-handling mechanisms, such as clear messages and guidance in case of fingerprint mismatches, are included to assist voters during the process. Scalability is also a key consideration, ensuring the system can handle large-scale voter participation across multiple polling stations without performance degradation.

The final step mainly focuses on securely recording the vote, aggregating results, and ensuring transparency in the electoral process. Once the voter has successfully completed biometric authentication and selected their preferred candidate, the system encrypts the vote and records it in a central database. This encryption ensures that the voter's choice remains confidential and tamper-proof. A confirmation message is displayed to the voter, affirming that their vote has been successfully cast, providing reassurance about the process's reliability

IV. HARDWARE AND SOFTWARE REQUIREMENTS

The hardware includes a Power Supply Unit (PSU) to ensure stable power delivery to all components, including a backup power source to maintain operations during outages. An LCD display, typically a 16x2 or 20x4 character module, provides voters with clear instructions, candidate lists, and confirmation messages. A buzzer is used for audio feedback, signaling successful authentication or errors, enhancing user interaction. The system relies on an Arduino microcontroller (e.g., Arduino Uno or Mega) to act as the core processing unit, managing data flow between the fingerprint sensor, LCD display, and network modules. A fingerprint sensor (such as the R305 or GT-511C3) captures biometric data to authenticate voters securely by matching fingerprints against the Aadhaar-linked database. Connectivity is achieved using Wi-Fi modules (e.g., ESP8266 or ESP32) or Ethernet modules, ensuring seamless communication with the central database. Peripheral devices, such as keyboards or touchpads, may also be integrated to allow additional voter inputs. Here

comes the most crucial step for your research publication. Ensure the drafted journal is critically reviewed by your peers or any subject matter experts. Always try to get maximum review comments even if you are well confident about your paper.

The software stack includes the Flask framework, which is used for developing the web application. Flask facilitates the creation of a secure backend that communicates with the central database, handling authentication, candidate retrieval, and vote recording. The central database, implemented using MySQL or PostgreSQL, stores voter details, Aadhaar-linked biometric data, and candidate lists. Data transmission between the web application and hardware devices is encrypted using HTTPS and SSL/TLS protocols to prevent unauthorized access. Visual Studio Code (VS Code) serves as the integrated development environment (IDE) for writing and debugging the Flask application, offering developers a robust platform for efficient coding.

The Arduino microcontroller is programmed using the Arduino Integrated Development Environment (IDE) to manage real-time interactions between hardware components. The system's architecture ensures a seamless flow of data, beginning with the fingerprint sensor capturing biometric data, followed by authentication and candidate list retrieval, and ending with secure vote recording. Error-handling mechanisms, user-friendly displays, and scalability features make this system a practical and innovative solution for modern electoral challenges.

V. SYSTEM ARCHITECTURE

The system architecture of the Anywhere VotingSystem is designed to provide a seamless and secure voting process through the integration of hardware and software components. The core of the architecture is a microcontroller that serves as the control unit for interfacing between various hardware modules and the voting application. The system starts with a fingerprint module, which captures the voter's biometric data for authentication. The captured fingerprint is processed and compared with pre-stored Aadhaar-linked biometric data to validate the voter's identity. If the fingerprint matches, the microcontroller signals the next steps in the process.

To provide feedback to the voter, a buzzer is connected to the microcontroller, which emits a sound to indicate either successful authentication or an error (such as a mismatched fingerprint). The entire system is powered by a stable power supply unit (PSU), ensuring uninterrupted operation and reliability. The microcontroller communicates with a PC that acts as an intermediary for data transfer and system control. The PC displays the list of candidates based on the voter's constituency, retrieved dynamically from a central database or portal.

The voter then selects their preferred candidate using an interface on the PC, which sends this information back to the system. The selected candidate's vote is recorded and encrypted before being uploaded to a central election portal, ensuring the integrity and confidentiality of the data. This architecture notonly streamlines the voting process but also ensures secure, accurate, and efficient data handling, making it suitable for large-scale implementation in democratic elections.

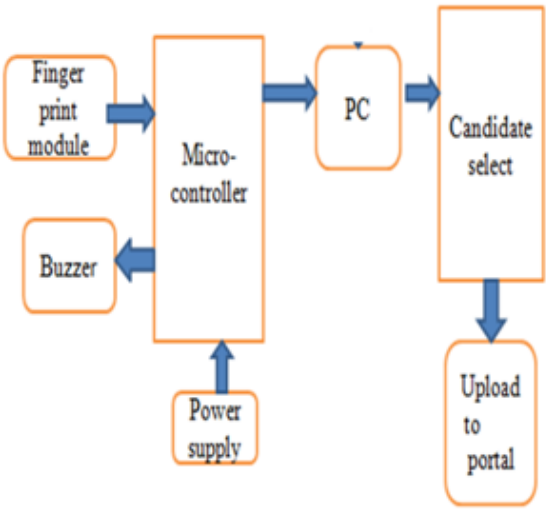

FIG: BLOCK DIAGRAM

VI. CONCLUSION

The Anywhere Voting System provides an innovative solution to revolutionize the voting process by combining Aadhaar-linked biometric authentication with advanced technology. This system enables voters to cast their votes from any polling station nationwide, ensuring convenience and accessibility while maintaining the highest standards of security and transparency. By addressing issues such as voter impersonation, duplicate voting, and location-specific restrictions, it simplifies the electoral process and fosters trust in democratic practices.The integration of reliable hardware components and secure software frameworks ensures seamless operation, accurate vote recording, and real-time data management. This system enhances efficiency in election logistics, reduces administrative complexities, and strengthens the overall integrity of the voting process. Furthermore, its user-friendly interface ensures ease of operation for voters and administrators alike, making it a practical and scalable solution for modern elections. Its robust security features

protect voter data and uphold the confidentiality of the election process. By promoting inclusivity, the system ensures that voters, regardless of their geographical location, can exercise their democratic right without barriers. The Anywhere Voting System not only modernizes elections but also strengthens democratic institutions, setting the foundation for a future of transparent, efficient, and technology-driven governance.

VII. ACKNOWLEDGEMENT

This project received support from the East West Institute of Technology. We express our sincere appreciation to our internal guide, Mrs. Prakruthi G R, Assistant Professor Department of Artificial Intelligence and Data Science (AD),for her valuable guidance and significant contributions in enhancing the manuscript. We also acknowledge Mrs.Shruthi T V, Prof & Head of AD Department, for her continuous support and mentorship throughout the project. Our special thanks go to Principal Dr.Channakeshavalu for hisunwavering encouragement. We are indebted to colleagues for their constructive feedback on earlier versions. Of the project. Any shortcomings in the manuscript remain our responsibility should not reflect negatively on the esteemed professional mentioned above.

REFERENCES

[1] Fingerprint-BasedVotingSystem. https://doi.org/10.1109/AECE59614.2023.10428219
[2] Enhancing the Security of Online Voting System Using Defined Biometrics. https://doi.org/10.1109/TEMSMET56707.2023.10150198
[3] Secured Voting System based on Multilayered Biometric Authentication. https://doi.org/10.1109/ICACCS48705.2020.9074281
[4] Biometric-based Smart Electronic Voting SystemUsing InternetOf Things. https://doi.org/10.1109/ICCEBS58601.2023.10449050
[5] Development of Fingerprint Voting Application using Aadhaar card. https://doi.org/10.1109/ICAISS58487.2023.10250537