IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, May 2024

Aadhar Based Biometric Electronic Voting System

Shiva Kumar V[1], Akshaya J[2], B Thulasi Brundha[3], G Saiprasanna[4]
Students, Department of Computer Science and Engineering[1,2,3]
Assistant Professor, Computer Science and Engineering[4]
Rao Bahadur Y Mahabaleswarappa Engineering College, Ballari, India

Abstract: *Flawless voting is guaranteed through the use of Electronic Voting Machines. It is crucial for citizens to have confidence in the security of their votes and to prevent any fraudulent activities. The primary objective of this initiative is to create a secure Electronic Voting Machine that utilizes fingerprint identification technology. To access fingerprints, the AADHAR card database is utilized. During elections, the authentication process for e-voting involves finger vein sensing, which allows voters to cast their votes after electronic ballot reset. Furthermore, the voting data and details of voters can be transmitted to the nearby Database Administration unit via WIFI. The fingerprint scanning feature is implemented to ensure security and prevent issues like fake or repeated voting. This system not only improves accuracy but also enhances the speed of the voting process.*

Keywords: voting

I. INTRODUCTION

The Election Commission of India (ECI) was established to oversee voting in India, ensuring impartiality and no support for any political party. Security of the e-voting process is crucial, necessitating a secure system design. However, ensuring security and privacy can be time-consuming, expensive, and inconvenient. Various levels of e-voting security must be implemented to prevent exposure to the public. Measures are needed to safeguard votes from being made public. Electronic voting machines (EVMs) provide buttons for each choice, connected to an electronic ballot box. EVMs consist of a control unit and a balloting unit connected by a cable. Disadvantages of EVMs include the inability to recognize candidate identity, lack of voter verification,vulnerability to hacking, fraud, and tampering during manufacturing, especially with the Chip.

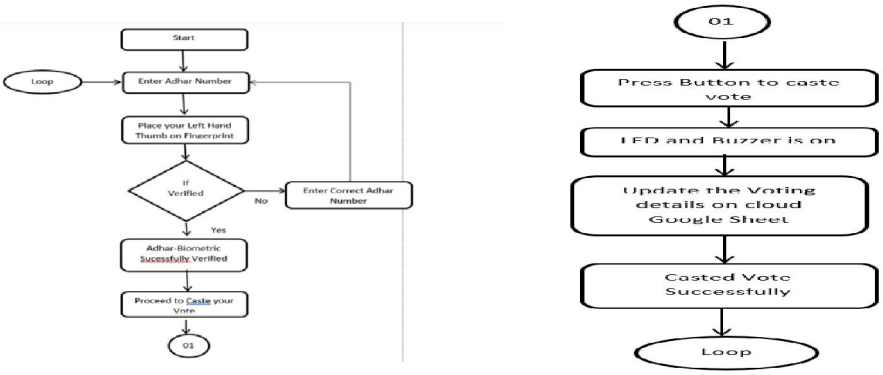
II. RELATED WORK

1. The development of a BEVS that incorporates fingerprint authentication and a centralized database. To ensure efficient and accurate fingerprint matching, multiple BEVS machines will be installed in each polling station in Bangladesh, based on the total number of voters. The proposed system consists of two main sections: voter registration and voting control/result calculation.The voter information will then be securely stored in a central database.
2. The proposed voting system that utilizes biometric identification as its main component.The system described involves capturing the fingerprint impression of a voter, which is then compared with existing data in the database. If a match is found, the voter is granted access to cast their vote. The system ensures instant results and utilizes Internet of Things (IoT) technology for vote counting.
3. The system that incorporates a biometric fingerprint sensor. This sensor ensures that each voter is authenticated before being allowed to participate in thevoting process by cross-referencing their fingerprint with the database of registered voters. Once the voter is verified, they can proceed to select their preferred candidate using a panel of buttons.
4. The proposed system is an electronic voting machine that utilizes biometric technology for security. Each voter's fingerprint is used to identify them, and the system compares the fingerprint with the database to determine if the person is registered. The system is also capable of detecting if a voter attempts to cast multiple votes. If a voter is not registered or tries to vote more than once, the system will identify them and prevent them from voting. However, if neither of these cases apply, the system will allow the voter to cast their vote.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, May 2024

III. PROPOSED SYSTEM AND IMPLEMENTATION

The primary hindrance to voters exercising their right to vote is the distance they have to travel to reach the polling station, resulting in a more time-consuming journey for them.During any election within society, two main issues tend to arise consistently. Firstly, disputes often arise regarding the eligibility of elderly voters, which can be attributed to differences in academic levels and delays in promotions. Secondly, the challenge of individuals located far from voting stations, such as in different cities, poses a significant obstacle in casting their votes. These factors collectively contribute to the perception of staff elections as lacking credibility and fairness. As a solution, we suggest implementing a system that enables voters to cast their votes at the nearest voting booth, equipped with features to address the inefficiencies of the existing system.

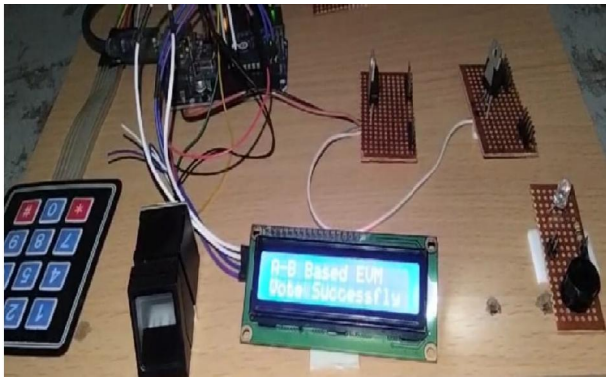


IV. METHODOLOGY

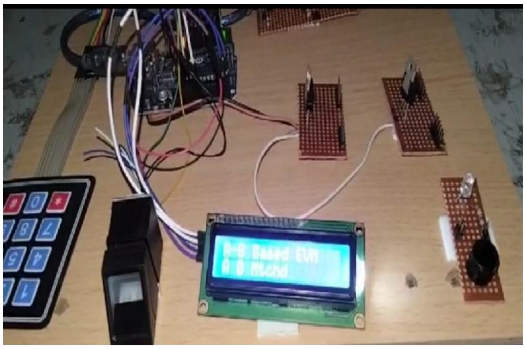
The methodology of this system involves a voter initially swiping their Aadhar Card on the Aadhar Card Reader Module, which then transmits the card data to the Microcontroller unit connected to it. The Microcontroller accesses the central server where Aadhar Card holder information is stored, retrieving the voter's details. Subsequently, the voter undergoes a fingerprint test to verify their identity. If the fingerprint matches the Aadhar information, the voter is permitted to cast their vote, and the system updates the database accordingly to prevent duplicate or fake identities. If the fingerprint does not match, the system denies voting permission, effectively preventing illegal voting. This methodology ensures secure and reliable voter authentication using Aadhar-based biometric verification integrated with electronic voting processes.

V. RESULTS

It is necessary to save fingerprints and Aadhar Numbers for verification purposes. Matching both the fingerprint and Aadhar number will enable the individual to vote, while a mismatch will result in the individual being unable to cast a vote.



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, May 2024



VI. CONCLUSION

The implementation of the Aadhar-based biometric electronic voting system holds great promise in improving the effectiveness and trustworthiness of the voting process. Through the utilization of biometric authentication connected to Aadhar, this system has the potential to minimize fraudulent activities and establish a more secure voting atmosphere. Nevertheless, the successful execution of this system necessitates meticulous attention to privacy concerns, technological infrastructure, and regulatory frameworks in order to guarantee inclusivity and safeguard democratic principles. In conclusion, although this system offers numerous advantages, its triumph ultimately hinges on comprehensive planning, active involvement of stakeholders, and strong protective measures against potential challenges.

VII. FUTURE SCOPE

Aadhar-based biometric electronic voting systems should give priority to improving security, user friendliness, scalability, dependability, and integrity. This involves investigating advanced encryption methods, integrating blockchain technology, and implementing strict verification measures to protect voter data and prevent manipulation. Research on user-friendliness is crucial to simplify the voting process, particularly for marginalized communities. Scalability research should concentrate on accommodating larger numbers of voters without sacrificing performance or security. Compatibility with government databases can streamline registration and verification. Ethical concerns related to privacy, consent, and data security need to be resolved to ensure compliance with democratic values. Public awareness campaigns are essential for building trust and encouraging participation in the electoral process.

REFERENCES

[1] Kumar, D. Ashok, and T. Ummal Sariba Begum. "A novel design of electronic voting system using fingerprint." *International Journal of Innovative Technology & Creative Engineering* 1.1 (2011): 12-19.
[2] Chandrasekar, S., and Gian Carlo Montanari. "Analysis of partial discharge characteristics of natural esters as dielectric fluid for electric power apparatus applications." *IEEE Transactions on Dielectrics and Electrical Insulation* 21.3 (2014): 1251-1259.
[3] Bederson, Benjamin B., et al. "Electronic voting system usability issues." *Proceedings of the SIGCHI conference on Human factors in computing systems*. 2003.
[4]Narayanan, V. Jayaprakash, B. Karthik, and S. Chandrasekar. "Flashover prediction of polymeric insulators using PD signal time-frequency analysis and BPA neural network technique." *Journal of Electrical Engineering and Technology* 9.4 (2014): 1375-1384.
[5] Jones, Bill. "California Internet Voting Task Force: A Report on the Feasibility of Internet Voting." (2000).
[6] Chaum, David. "Secret-ballot receipts: True voter-verifiable elections." *IEEE security & privacy* 2.1 (2004): 38-47.
[7] Darcy, Robert, and Ian McAllister. "Ballot position effects." *Electoral Studies* 9.1 (1990): 5-17.
[8] Dill, David L., et al. "Frequently Asked Questions about DRE Voting Systems." *Verified Voting* (2003).
[9] Deepika, J., et al. "Smart electronic voting system based on biometrie identification-survey." *2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM)*. IEEE, 2017.