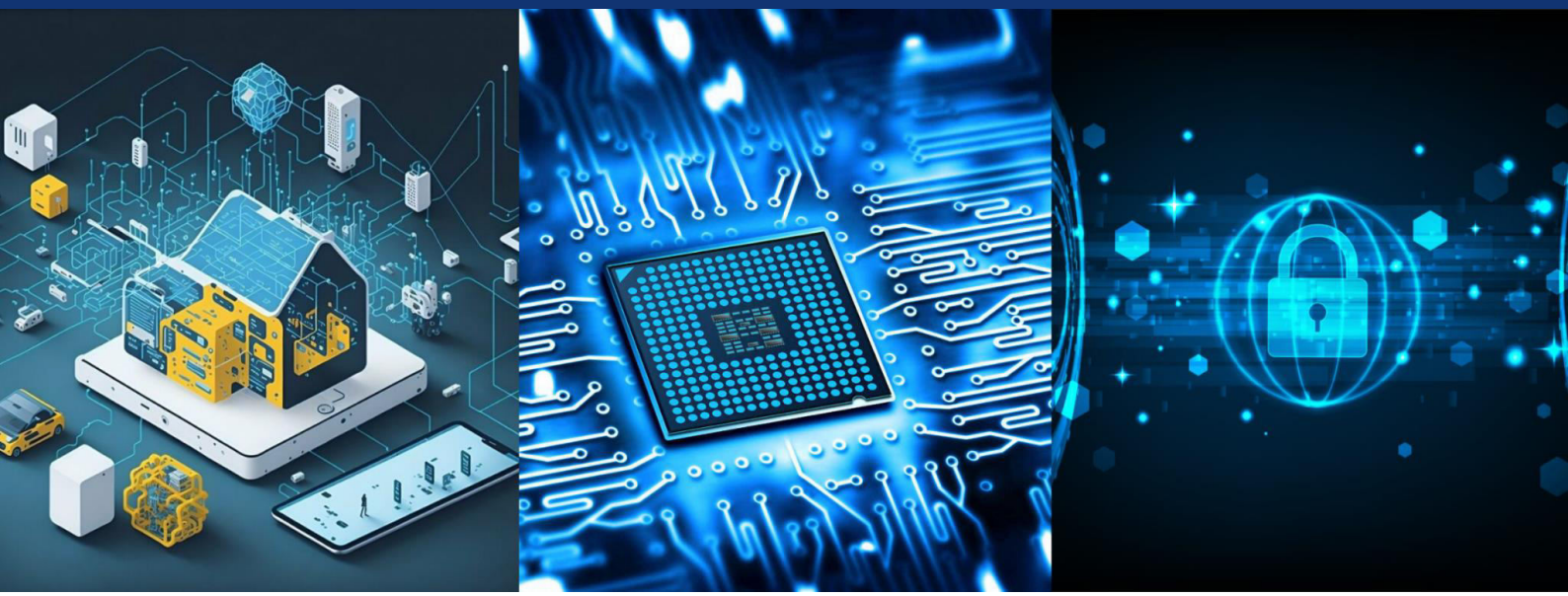
IJIRCCE

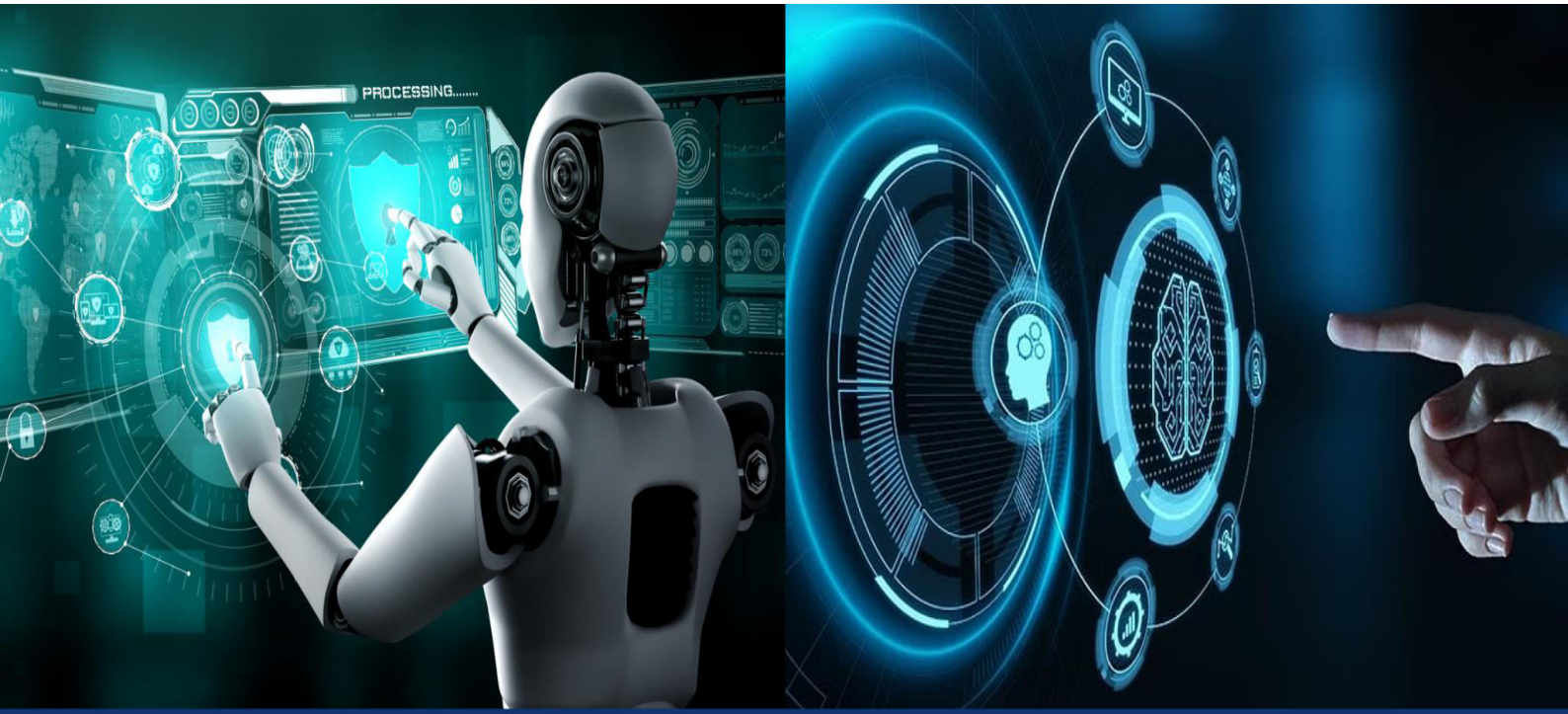
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.625

Volume 13, Issue 1, January 2025

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301151

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Fingerprint based Biometric Smart Electrtonic Voting Machine

Mr. Parth Sushant Parab[1], Mr. Swagat Deepak Gawade[2], Mr. Kavir DhirajSawant[3], Mr. Shamba Subhash Gaonkar[4], Mr. Amey Mahesh Gode[5], Mr.T.M.Patil[6]

Student, Yashwantrao Bhonsale Institute of Technology, Sawantwadi, Maharashtra, India[12345]

Faculty, Yashwantrao Bhonsale Institute of Technology, Sawantwadi, Maharashtra, India[6]

ABSTRACT: This research paper explores the design and implementation of "Fingerprint-based biometric smart election voting machine" project. India is a Democratic country with a huge population where voting plays an important role. Every citizen has the right to choose their leaders. This is done by using electronic voting machines (EVMs) at polling booths. But even there may be some malfunctions during elections. Under these circumstances holding elections is a complex task for the Election Commission because there is rigging taking place. Electronic voting systems have come into the picture to prevent rigging up to the maximum extent. For this, we are using the R307 Fingerprint Module which scans the fingerprint . A USB to TTL converter is an electronic device that converts USB signals into TTL (Transistor-Transistor Logic) level signals. This type of converter is commonly used for communication between devices that use USB and microcontrollers or modules , which require TTL signals. Our developed algorithm stores the particular fingerprint in the storage drive and makes sure that the fingerprint is unique from the previously stored data.

KEYWORDS: R307 Fingerprint, Monitor, USB TO TTL .

I. INTRODUCTION

In the modern tech world, we definitely need a very solid way of ensuring who is who, and that's exactly where biometrics comes in. Whether you're getting a National ID or do online shopping, it's of utmost importance to have a very rock-solid way of saying, "Hey, this is me!" Voting is super important, too, but the problem lies in making sure one person only votes once. Right now, we use electronic voting machines with ink marks on our fingers to show someone voted. But with tech speeding up, there's a worry that these ink marks can be erased, leading to some not-so honest stuff. So, it is all about creating a special Fingerprint-based Voting System. By developing a Fingerprint-based Voting System, we're aiming to tackle the issues of fair election processes. We bid farewell to those old ink marks and welcome a more secure means of proving a vote through this technology. In a world that evolves rapidly in terms of technology, this is a step forward in guaranteeing a trustworthy and full proof voting process for all. Integrating advanced interdisciplinary approaches, such as biometric fusion, IOT security enhancements, and user-centric design, elevate It ensures the reliability, security, and a clear user experience of an electoral process.

FEATURES

Voter Registration: Biometric Data Collection: Voters are registered using biometric data such as fingerprints, iris scans, or facial recognition to create a unique and secure voter profile.
De-duplication: The system ensures that each voter is registered only once by comparing biometric data to detect duplicates.
Voter Verification: Real-time Verification: On election day , voters' biometric data is scanned and compared with the data in the central database to confirm their identity before allowing them to vote.
Fraud Prevention: Prevents multiple voting and impersonation, ensuring that only eligible voters can cast their ballots.
Secure Voting Process: Electronic Voting Machines (EVMs): Integrated with biometric verification systems to ensure that only authenticated voters can vote.

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301151

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. SYSTEM ANALYSIS

A. Problem Definition:

The need to increase reliance on digital systems for election processes has brought along with it a critical responsibility: to ensure the integrity and security of these systems. Several threats, both internal and external, pose a great deal of risk against the confidentiality, integrity, and availability of election systems. These threats encompass insider misuse of privileges, external cyber attacks, physical tampering, database breaches, man-in-the-middle attacks, software vulnerabilities, among others.

weak authentication mechanisms, and social engineering attacks. If not properly mitigated, these vulnerabilities can compromise voter data, election outcomes, and public trust in the electoral process. Therefore, it is essential to implement robust security measures, including access controls, encryption, secure software development practices, continuous monitoring, and personnel training, to address these potential risks and protect election systems from exploitation or sabotage.

B. Implementation:

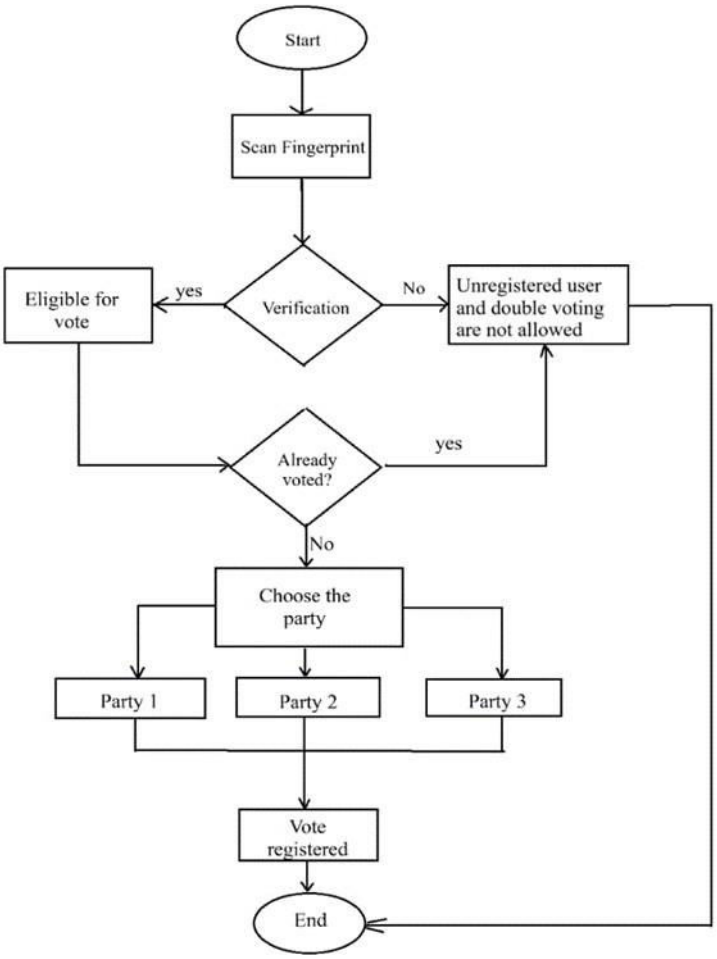


Fig1.1 Function of biometric smart electronic voting machine

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301151

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

1. Nationality Check Flowchart

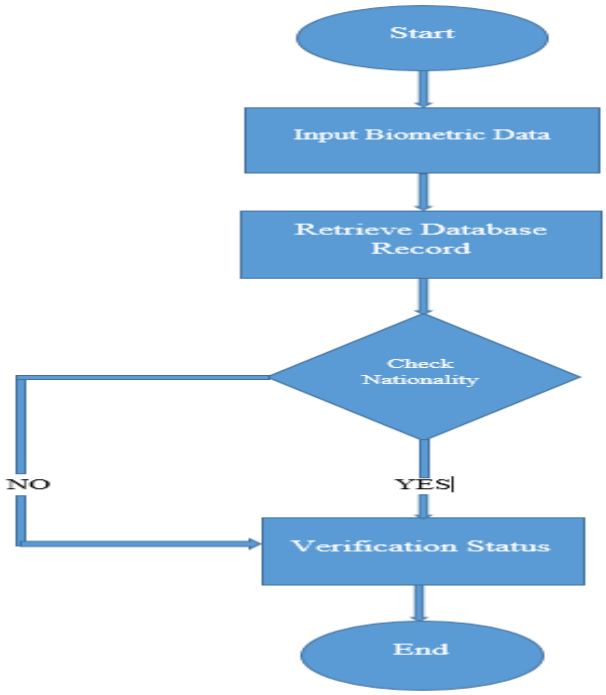


Fig1.2 Nationality Check Flowchart

This flowchart represents the **Nationality Check Module** in a biometric voting system, where biometric data is processed to verify the voter's nationality before proceeding to the voting system.

Steps:

1. **Start**: Begin the nationality verification process.
2. **Input Biometric Data**: Capture biometric data such as fingerprints or iris scans from the user.
3. **Retrieve Database Record**: Fetch the user's data from the database based on the biometric input.
4. **Check Nationality**: Verify if the user is a valid citizen:
    a. If **Yes**, proceed to the next step.
    b. If **No**, terminate the process and notify the user.
5. **Verification Status**: Confirm successful nationality verification for valid users.
6. **End**: Exit the module after verification.

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301151

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

2. Voter Registration Flowchart

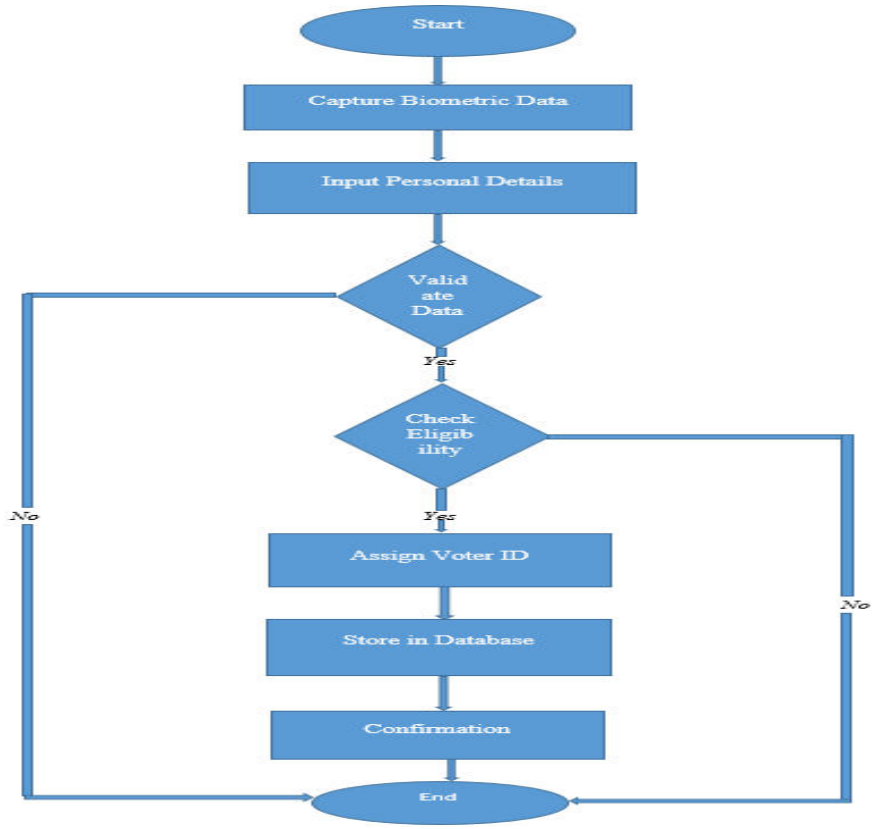


Fig1.3 Voter Registration Flowchart

Steps:

1. **Start : s**Initiate the voter registration process.
2. **Capture Biometric Data:** Collect biometric data such as fingerprints, facial recognition, or iris scans.
3. **Input Personal Details :** Input voter's personal information (e.g., name, age, address, national ID).
4. **Validate Data**

- Verify the data by checking:
  - **Age Eligibility**: Is the voter above the minimum voting age?
  - **Duplicate Check**: Ensure the voter is not already registered in the system.

5. **Check Eligibility**

- If the voter meets all criteria:
  - **Yes**: Proceed to the next step.
  - **No**: Notify the user and terminate the process.

6. **Assign Voter ID:** Generate and assign a unique voter ID to the user.
7. **Store in Database:** Save the biometric data, personal details, and voter ID into the database securely.
8. **Confirmation:** Notify the voter of successful registration and provide the voter ID.
9. **End**

- Exit the registration process.

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301151

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

3.Candidate Registration Flowchart

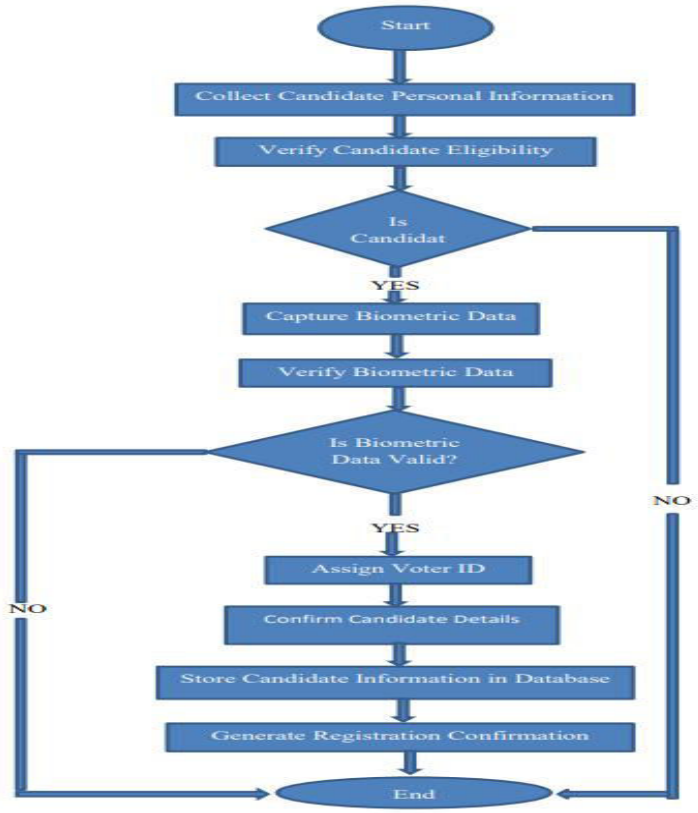


Fig1.4 Candidate Registration Flowchart

Steps:

1. **Start**: Begin the voting registration process.
2. **Collect Candidate Personal Information**: Gather personal details such as name, age, address, and ID information.
3. **Verify Candidate Eligibility**: Check if the candidate meets the criteria for voter registration (e.g., age, nationality).
4. **Is Candidate Eligible?**
    a. **Yes**: Proceed to biometric data capture.
    b. **No**: End the process.
5. **Capture Biometric Data**: Record biometric data such as fingerprints or iris scans for unique identification.
6. **Verify Biometric Data**: Validate the captured biometric data against system requirements.
7. **Is Biometric Data Valid?**
    a. **Yes**: Assign a unique voter ID.
    b. **No**: Restart the biometric data capture process or end the registration.
8. **Assign Voter ID**: Generate a unique voter ID for the candidate.
9. **Confirm Candidate Details**: Display the collected information to confirm accuracy.
10. **Store Candidate Information in Database**: Save the verified data securely in the database.
11. **Generate Registration Confirmation**: Provide a confirmation to the candidate, including their voter ID.
12. **End**: Complete the registration process.

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301151

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

4. Voting Using Fingerprint Data

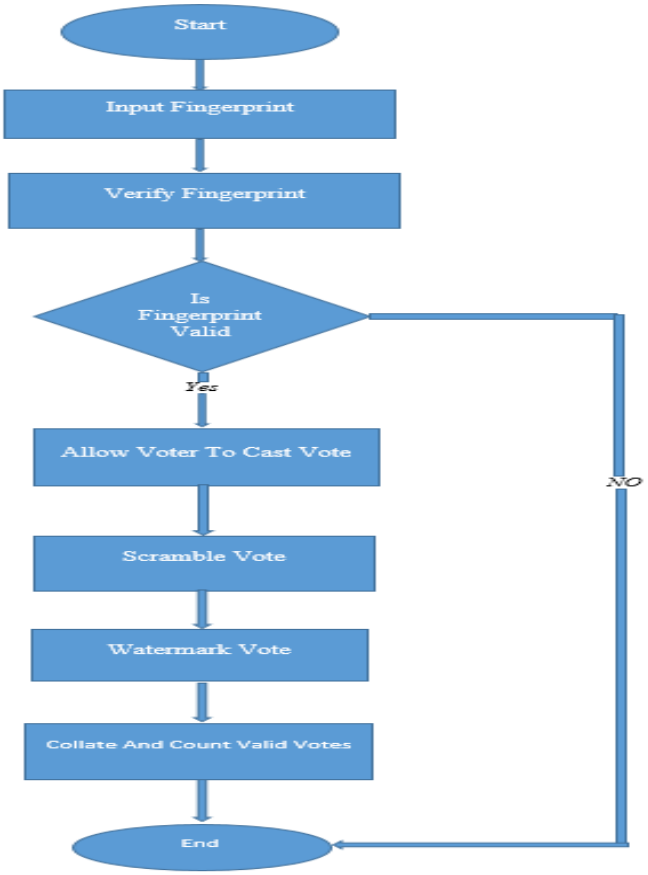


Fig1.5 Voting Using Fingerprint Data

Steps:

1. **Start**: Begin the voting process.
2. **Input Fingerprint**: The voter provides their fingerprint for identification.
3. **Verify Fingerprint**: The system cross-checks the fingerprint with the database.
4. **Is Fingerprint Valid?**
    a. **Yes**: Proceed to allow the voter to cast their vote.
    b. **No**: Reject the attempt and terminate the process.
5. **Allow Voter to Cast Vote**: Permit the voter to select and submit their choice.
6. **Scramble Vote**: Encrypt or anonymize the vote to ensure privacy and security.
7. **Watermark Vote**: Add a unique, system-generated watermark to prevent tampering or duplication.
8. **Collate and Count Valid Votes**: Collect all valid votes and prepare them for counting.
9. **End**: Complete the voting process.

III. FUTURE WORK

Voter Registration: Biometric Data Collection: Voters are registered using biometric data such as fingerprints, iris scans, or facial recognition to create a unique and secure voter profile.
De-duplication: The system ensures that each voter is registered only once by comparing biometric data to detect duplicates.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Voter Verification: Real-time Verification: On election day, voters' biometric data is scanned and compared with the data in the central database to confirm their identity before allowing them to vote.
Fraud Prevention: Prevents multiple voting and impersonation, ensuring that only eligible voters can cast their ballots.
Secure Voting Process: Electronic Voting Machines (EVMs): Integrated with biometric verification systems to ensure that only authenticated voters can vote.

IV.OBJECTIVE OF PROJECT

In the "Fingerprint-Based Biometric Smart Electronic Voting Machine" project, the objectives concerning the above-mentioned aspects are:

1. Nationality Checking

It ensures only eligible citizens can register as voters on the basis of nationality criteria. It may be linked to a government database, such as Aadhaar or national ID, for verification purposes. It eliminates non-citizens or persons who are not eligible from participating in elections.

2. Candidate Registration

It enables secure registration of political candidates in the system. Saves their information, such as name, party, and biometric authentication for voter identification. Does not allow unauthorized parties to falsely contest elections.

3. Voter Registration

Every voter must register with the system via their biometric fingerprint, personal details, and ID confirmation.
The system identifies and removes lists of identical entry ensuring that every voter is registered only once. Saves voters' information for future elections

4. Biometric Fingerprint Verification

Utilizing the R307 Fingerprint Module. These will scan and save unique fingerprints of voters. Ensures that only registered, authenticated voters can cast their votes. Prevents multiple voting, impersonation, and election fraud.

V.CONCLUSION

In a nutshell, the Fingerprint-Based Biometric Smart Electronic Voting System using IOT, with its current technical sophistication, is a robust platform with the potential for ongoing enhancements. The integration of advanced interdisciplinary approaches has transformed the Fingerprint Based Biometric Smart Electronic Voting System using IOT into a cornerstone of modern democracy. By leveraging expertise across biometrics, and human computer interaction, this system ensures the integrity, accessibility, and transparency of electoral processes with trust and confidence among voters. Future improvements for the Fingerprint-Based Biometric Smart Electronic Voting System using IOT shall take advantage of state-of-the-art technologies as well as advancements on different technical issues to further detail and strengthen the system.

ACKNOWLEDGEMENT

We would like to express our sincere gratitude and appreciation to the experts who have contributed to the development of Fingerprint-based biometric smart electronic voting machine. would also like to extend our heartfelt thanks to our project guide Mr. T. M. Patil co-ordinator Mr. R. C. Dhandekar and HOD Mr.P.D. Kate and for their constant support, guidance, valuable suggestions, and modifications to enhance the quality of our project work. Their insights and encouragement have been instrumental in the success of our project. We would also like to thank the faculty members of our department for their valuable feedback and support throughout the project.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

REFERENCES

1. Pljonkin,Biometric VotingMachine Based on Fingerprint Scanner and Arduino, Published : 2nd International Conferece on Intelligent Communication and Computational Techniques (ICCT) (2019).
2. R.Akila Mukesh,Muraree Lal Meena, G. Sasirekha, A. Selvameena, Tamilselvi Tt ,Finger Print Based Voting System Using Aadhaar Card, International Journal Of Engineering & Science Research (2019).
3. Shubham Gupta, Divanshu Jain, Milind Thomas Themalil, Electronic Voting Mechanism using Microcontroller ATmega328P with Face Recognition, Published :5th International Conferenceon Computing Methodologies and Communication (ICCMC) (2021)
4. A.M.Jagtap, Vishakha Kesarkar, Anagha Supekar, Electronic Voting System using Biometrics, Raspberry Pi and TFT module, Published in: 3rd International Conference on Trends in Electronics and Informatics (ICOEI), (2019)
5. Poornima Kamble, Krishna Agawane, Jagdish Ingole, Fingerprint based Electronic Voting Machine, Journal of Analog and Digital Devices, 4 (2019)
6. J. Deepika; S.Kalaiselvi,S.Mahalakshmi; S.AgnesShifani, Smart electronic voting system based on biometric identification survey, Published in: Third International Conference on Science Technology Engineering & Management (ICONSTEM) (2017)
7. Shilpacvenugopal, Resmik.Rajan, Iot-Based Voting Machine With Fingerprint Verification, International Journal of Applied Engineering Research,15 (2020)
8. Miral Desai, Jignesh Patoliya, Hiren Mewada, Internet of Things (IoT)-Based Advanced Voting Machine System Enhanced Using Low-Cost IoT Embedded Device and Cloud Platform, International Conference on Information and Communication Technology for Intelligent Systems (2020)

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details