Biometric-Based Voter Authentication and Receipt Generation System

1. Background / Problem Statement

Traditional voter verification relies on ID cards and manual checks at polling booths. These methods can lead to:

- Impersonation or duplicate voting
- Human errors
- No proper proof of verification
- Slow processing during elections

To overcome these issues, a **Biometric-Based Voter Authentication System** is proposed. It uses **fingerprint matching**, displays voter details for confirmation, checks if the voter already voted, and prints a receipt as proof of authentication. Instead of focusing on the voting process itself, this system is designed to verify the identity of voters through biometric fingerprint authentication., display their complete details on a screen for confirmation, and generate a printed receipt confirming their eligibility status.

2. Working of the Project

1. **Fingerprint Scanning:**
   - The voter places their finger on the biometric sensor.
2. **Authentication:**
   - The system matches the fingerprint with the stored database to verify identity.
3. **Voter Details Display:**
   - Once authenticated, the **complete voter details** are shown on the screen, including:
     - Voter ID
     - Full Name
     - Age
     - Gender
     - Constituency / Ward
     - Voting Status (e.g., “Eligible – Not Voted”)
4. **Eligibility Check:**
   - If the voter is eligible and has not voted → the system approves authentication.
   - If the voter has already voted or is invalid → access is denied and displayed on the screen.
5. **Receipt Generation:**
   - After successful verification, the system prints a receipt with:
     - Voter ID (masked for privacy)
     - Date and Time
     - Booth ID
     - Authentication Status (e.g., “Verified & Eligible”)
6. **Data Security:**
   - ➢ All biometric and voter data are stored in encrypted form to prevent misuse.

3. Advantages

- Prevents impersonation & fake voting.
- 100% accurate fingerprint authentication.
- Displays full voter details for transparency.
- Generates a physical verification receipt.
- Fast & automated — reduces manual checking.
- Secure encrypted data storage.
- Helps in audit and monitoring.
- Eliminates impersonation during the verification process.
- Ensures voter information accuracy through on-screen display.
- Provides a secure method to prevent duplicate entries.
- Gives voters and officials physical proof of verification.

4. System Description

I. Voter Registration:

- Voters enroll their biometric data (fingerprint) and personal details at registration centers.
- The biometric data is converted to a template and securely stored in an encrypted database linked with other voter information.

II. Authentication Process:

- On election day, the voter places their finger on the biometric scanner.
- The system captures the fingerprint and extracts features to create a new biometric template.
- This live template is compared against the stored templates using matching algorithms.
- If a match is found, the voter's identity is verified.

III. Voter Details Display:

- Upon successful biometric verification, the system retrieves and displays complete voter details such as Voter ID, name, age, gender, constituency, and voting status (eligible/not voted).
- This enables poll officers and the voter to confirm identity visually.
- Eligibility and Voting Status Check:
- The system checks if the voter is eligible and whether they have already voted.
- Ineligible or already cast voters are denied access with appropriate messages on the screen.

IV. Receipt Generation:

- After successful authentication and eligibility verification, a thermal printer prints a receipt.
- The receipt includes masked voter ID, date and time, polling booth ID, and verification status.
- This physical receipt serves as proof of verified authentication.

V. Logging and Audit:

- The system logs each authentication attempt with timestamps and statuses in a secure log file or database.
- These logs help in post-election audits to detect fraudulent activities or system anomalies.

VI. Security Measures:

- All biometric data and personal information are stored encrypted.

- Communication between devices and servers is secured through encryption protocols.
- Backup and synchronization mechanisms maintain data integrity and availability.

VII. Fault Handling and Alternative Methods:

- In cases where biometric verification fails (e.g., unreadable prints), manual verification or secondary authentication methods can be employed.
- Exception handling routines ensure smooth operation without disruption in case of hardware/software failures.

➢ System Architecture

```
         +-----------------------------+
         |  Voter Database             |
         | (Biometric + Details)       |
         +--------------+--------------+
                        |
                        v
         +-----------------------------+
         | Fingerprint Scanner         |
         +--------------+--------------+
                        |
                        v
         +-----------------------------+
         | Microcontroller Unit        |
         | (Authentication + Display)  |
         +--------------+--------------+
                        |
          +------+-------+-------------+
          |              |             |
          v              v             v
   Display       Eligibility   Thermal Printer
(Voter Info)       Check      (Receipt Generation)
```

---

5. Project Life Cycle

The Biometric-Based Voter Authentication and Receipt Generation System follows the **Spiral Model**, which is ideal for systems requiring continuous testing, improvement, and risk control. The Spiral Model is used because a biometric authentication system requires continuous testing, risk analysis, and improvement. Unlike simple software, biometric systems must work accurately with different fingerprints, different lighting, different user conditions, and must avoid security risks like duplicate or fake identities.

Phase 1: Requirement Analysis

- Collect requirements from election authorities
- Identify what data is needed (Aadhaar/ID, fingerprint or face biometrics)
- Define system goals: voter authentication, duplicate prevention, receipt generation
- Specify safety, accuracy, and privacy needs

Phase 2: System Design

- Plan biometric sensor connectivity
- Database design for storing voter & biometric templates
- User interface design
- Security and encryption planning

Phase 3: Prototype Development

- Build a small working model
- Example: fingerprint scanner + basic matching + display
- Initial database setup
- Generate sample test receipts

Phase 4: Testing & Risk Analysis

- Test the sensor accuracy
- Check false match / false rejection rates
- Identify failures (poor fingerprint, duplicate matching errors)
- Fix security risks, database failures, user mistakes

Phase 5: Improvement (Next Spiral Loop)

- Update algorithms for better accuracy
- Improve UI speed, matching time, and noise handling
- Add new features (logs, encryption, backup security)

Phase 6: Final Implementation

- Full deployment with complete database
- Secure authentication, receipt printing, audit logs

Phase 7: Maintenance

- Add new voters
- Update database
- Improve software if new issues appear

Stage	Description
Data Registration	Register voters' biometric and personal data in a secure database before the election.
System Design	Plan and integrate fingerprint sensor, microcontroller, display, and printer.
Software Development	Develop modules for biometric authentication, voter detail display, eligibility checking, and receipt printing.
Hardware Integration	Connect components into a functioning prototype.
Testing	Run scenarios for valid voters, duplicate voters, and invalid voters.
Deployment	Demonstrate the system in a simulated environment.

6. System Requirements

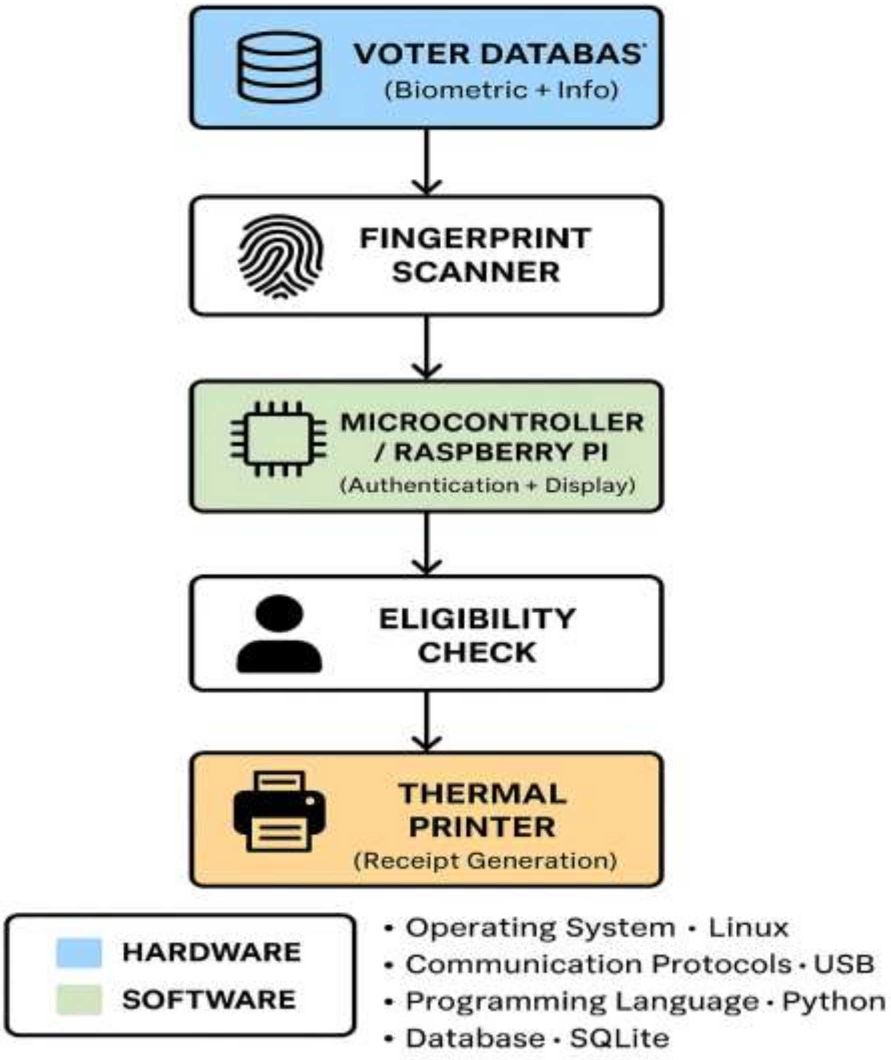
➢ Hardware

- **Fingerprint Sensor (e.g., R305)** – For fingerprint scanning and matching.
- **Microcontroller Board (e.g., Arduino / Raspberry Pi)** – Controls authentication logic.
- **LCD / Touchscreen Display** – Displays voter details after authentication.
- **Thermal Printer** – Prints authentication receipts.
- **Power Supply Unit** – For powering components.
- **LED / Buzzer Indicators** – Show authentication status.
- **External Storage (SD Card / USB)** – Optional, for database storage.

➢ Software

- **Arduino IDE / Python** – For coding and microcontroller programming.
- **Fingerprint Library** – For integrating biometric scanning.
- **Database System (MySQL / SQLite)** – For storing voter details and biometric data.
- **Printer Drivers** – For receipt printing.
- **Encryption Libraries** – For securing sensitive data.

➢ Pictorial representation


VOTER DATABAS
(Biometric + Info)
FINGERPRINT SCANNER
MICROCONTROLLER / RASPBERRY PI
(Authentication + Display)
ELIGIBILITY CHECK
THERMAL PRINTER
(Receipt Generation)
🟦 HARDWARE
🟩 SOFTWARE
• Operating System • Linux
• Communication Protocols • USB
• Programming Language • Python
• Database • SQLite

7. Limitations / Disadvantages

- Fingerprint scanner may fail if finger is wet/damaged
- Needs stable power & printer refills
- Requires secure database maintenance
- Initial registration and setup time is high
- Thermal printers provide simple receipts only

8. Applications

- National and State Election Voter Verification
- University / College Election Authentication
- Corporate Voting Systems
- Community or Local Body Elections
- Polling Booth Entry Verification Systems

9. Future Work

- Add face + fingerprint dual authentication
- Cloud-based voter records
- Mobile app for administrators
- OTP-based backup verification
- Integration with national digital ID databases
- Blockchain-based secure voting logs

10. Conclusion

The Biometric-Based Voter Authentication and Receipt Generation System is a secure and modern solution for voter verification. By replacing manual ID checking with biometric fingerprint matching, it removes impersonation, fake voting, and human error. Displaying voter details and printing receipts improves transparency and trust. This system can be deployed with existing voting machines to make elections more accurate, faster, and reliable. The receipt generation feature adds transparency and accountability. This system can be integrated with existing voting setups to improve overall election security.

11. References

- R305/GT-511C3 Fingerprint Sensor Datasheet
- Raspberry Pi Official Documentation
- MySQL / SQLite Database Manuals
- IEEE Research Papers on Biometric Voting Systems
- Election Commission of India reports on electronic verification