

WEB ENABLED FINGERPRINT BASED ELECTRONIC VOTING MACHINE FOR PRIVATE COMMUNITIES

A Secure and Biometric-Authenticated Voting System

Group Number:15

Presented by

Brijesh Nishad : 2101321550026
Ashutosh : 2101321550021
Aayush Pandey : 2101321550001

Under the Supervision of
Mr. Rajat Kishor Varshney



ग्रेटर नोएडा इंस्टीट्यूट ऑफ टेक्नोलॉजी (इंजीनियरिंग इंस्टीट्यूट)



Introduction

Problem Statement

Traditional voting systems are vulnerable to fraud and impersonation, undermining democratic processes. These issues necessitate a more secure, tamper-proof alternative for voting in private communities.



Need for Secure Voting

There is an urgent requirement for a voting system that guarantees voter identity and prevents unauthorized access or tampering. The increasing risks to democracy in voting highlight the need for highly-secure systems.



WEF-EVM
Web Enabled Fingerprint EVM
Private Community



Solution Overview

The proposed solution combines biometric fingerprint authentication with a web-based electronic voting machine (EVM) to create a secure and efficient voting process for private communities.

Key Features

Key features include fingerprint verification for user authentication, a real-time results web dashboard, and the specialized ESP32 hardware for efficient offline fingerprint processing.



Problem Statement

Traditional voting systems are vulnerable to fraud and impersonation, undermining democratic processes. These issues necessitate a more secure, tamper-proof alternative for voting in private communities.



Need for Secure Voting

There is an urgent requirement for a voting system that guarantees voter identity and prevents unauthorized access or tampering. The increasing reliance on technology in voting amplifies the need for foolproof systems.



WEF-EVM
Web Enabled Fingerprint EVM
Private Community



Solution Overview

The proposed solution combines biometric fingerprint authentication with a web-based electronic voting machine (EVM) to create a secure and efficient voting process for private communities.

Key Features

Key features include fingerprint verification for user authentication, a real-time results web dashboard, and the specialized ESP32 hardware for efficient offline fingerprint processing.

Key Features

Our fingerprint-based EVM system provides unparalleled security and convenience



Biometric Authentication

Secure voter identification through fingerprint verification eliminates fake votes and ensures one vote per person.



Tamper-Proof Design

Military-grade encryption and blockchain technology make the system completely tamper-proof and auditable.



Real-Time Results

Get instant voting results with our cloud-based system that updates in real-time as votes are cast.



Web Enabled

Remote monitoring and administration through our secure web dashboard accessible from any device.

WEB ENABLED FINGERPRINT BASED ELECTRONIC VOTING MACHINE FOR PRIVATE COMMUNITIES

A Secure and Biometric-Authenticated Voting System

Group Number:15

Presented by

Brijesh Nishad : 2101321550026
Ashutosh : 2101321550021
Aayush Pandey : 2101321550001

Under the Supervision of
Mr. Rajat Kishor Varshney



Exploring Existing Voting Systems

Existing Systems Overview

Traditional EVMs in countries like India utilize hardware solutions without biometric checks for voter identification. Additionally, online voting platforms rely on password systems that are increasingly susceptible to phishing attacks.



Gaps in Current Solutions

Most existing voting systems fail to provide unique voter verification, leading to potential duplicate votes. Hybrid systems combining web technology with hardware are scarce, resulting in limited accessibility and security.



Addressed Challenges

Addressing these challenges requires advanced solutions, such as biometric voter verification, to significantly reduce impersonation risks. A hybrid architecture optimizes both security and user accessibility, addressing critical gaps in the current voting landscape.



Existing Systems Overview

Traditional EVMs in countries like India utilize hardware solutions without biometric checks, exposing vulnerabilities. Additionally, online voting platforms rely on password systems that are increasingly susceptible to phishing attacks.



Gaps in Current Solutions

Most existing voting systems fail to provide unique voter verification, leading to potential duplicate votes. Hybrid systems combining web technology with hardware are scarce, resulting in limited accessibility and security.





Addressed Challenges

Implementing biometric authentication, such as fingerprint verification, helps to significantly reduce impersonation risks. A hybrid architecture optimizes both security and user accessibility, addressing crucial gaps in the current voting landscape.

WEB ENABLED FINGERPRINT BASED ELECTRONIC VOTING MACHINE FOR PRIVATE COMMUNITIES

A Secure and Biometric-Authenticated Voting System

Group Number:15

Presented by

Brijesh Nishad : 2101321550026
Ashutosh : 2101321550021
Aayush Pandey : 2101321550001

Under the Supervision of
Mr. Rajat Kishor Varshney



Proposed Methodology

System Architecture

The proposed system integrates a web UI for user interaction with a REST API for data processing. It also includes a PostgreSQL database for storing voter information and a Redis cache for real-time data retrieval.



Frontend and Backend Details

The frontend consists of an Angular application for voter registration and voting. The backend is built using Node.js with Express.js, utilizing PostgreSQL and Redis for data storage and processing.



Hardware Components

Key hardware components include the ESP32 microcontroller for data processing and the RGB LED strip for physical voter verification and verifying fingerprints. Together, they form the backbone of the system for voter authentication in voting.



Workflow Diagram



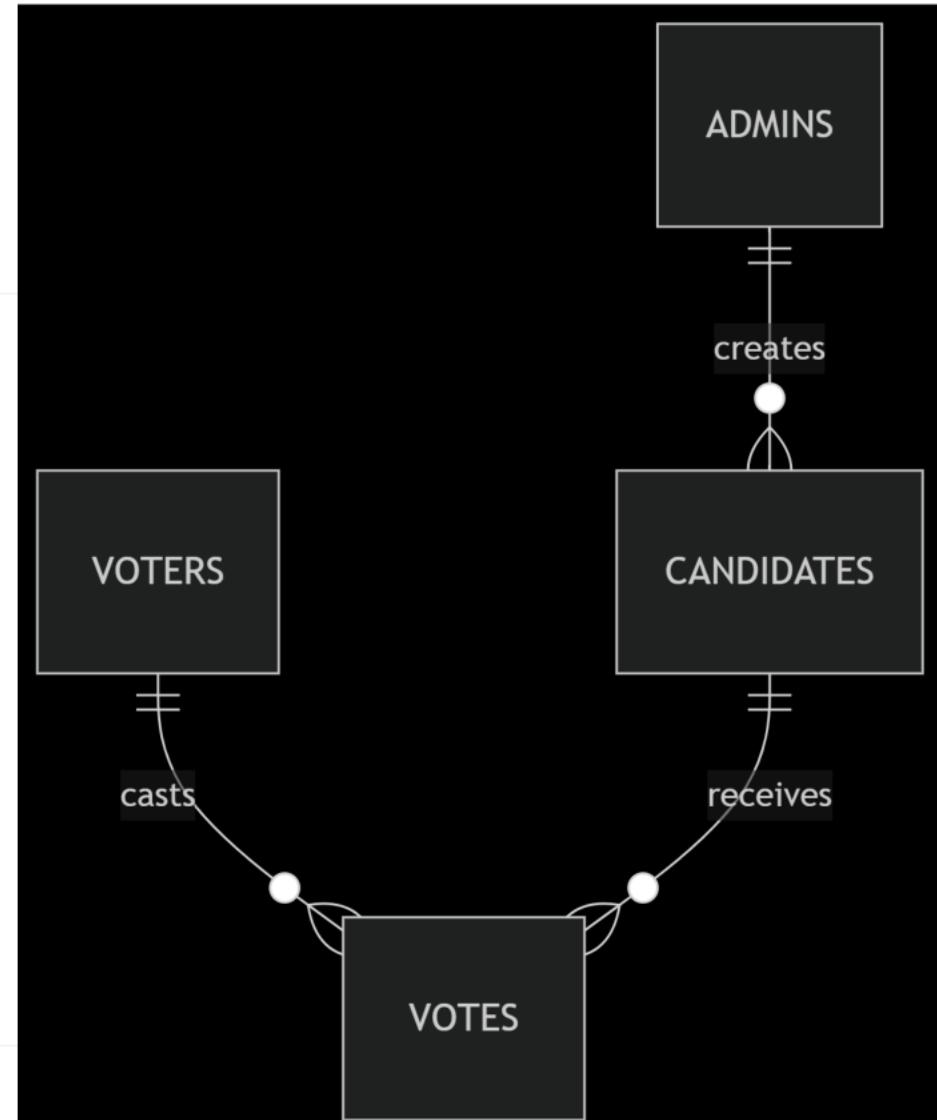
Database ER Diagram

The database architecture includes essential tables: Voters, Candidates, and Votes. A detailed ER diagram illustrates the relationships and data integrity essential for secure and efficient handling of the voting process.



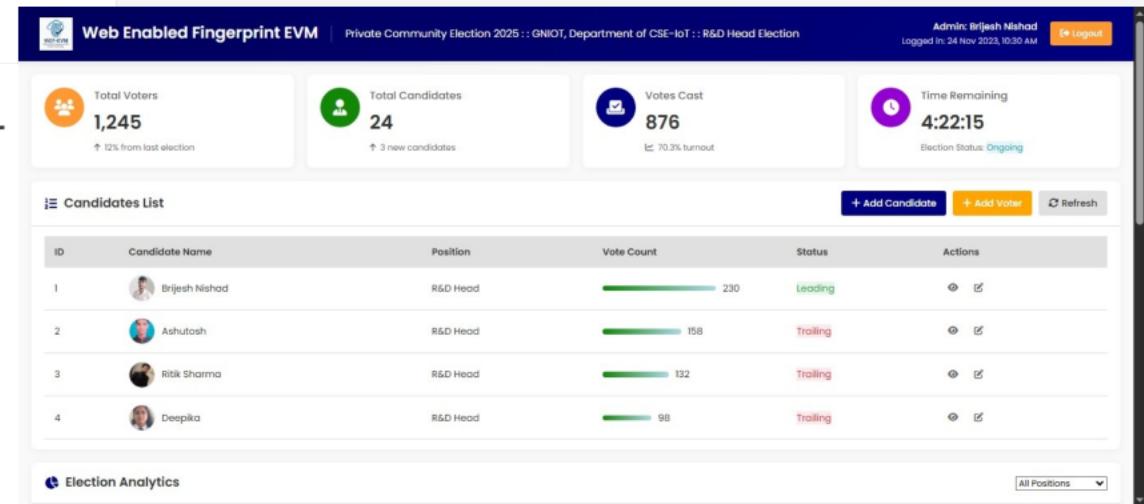
System Architecture

The proposed architecture integrates a web portal for user interaction with an ESP32 backend, processing fingerprint data and managing database connections. This hybrid setup ensures both security and accessibility for voting in private communities.



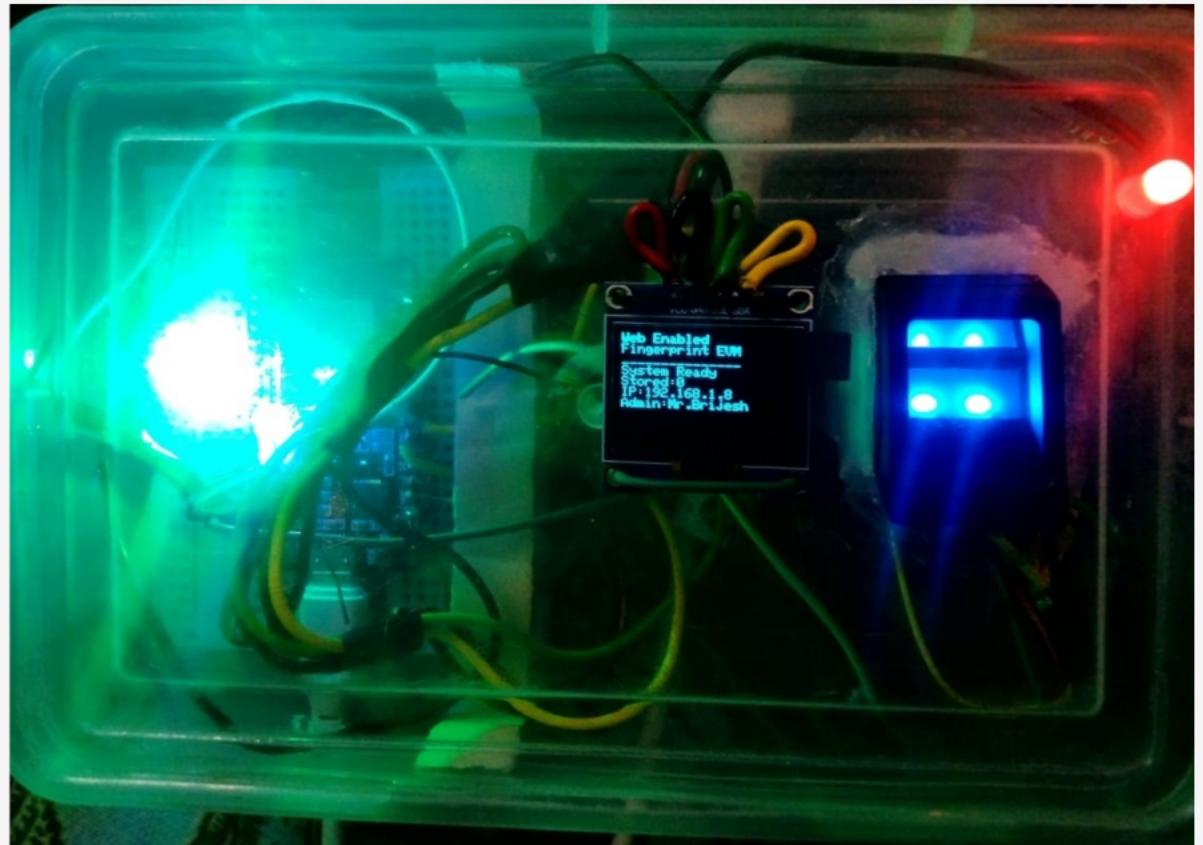
Frontend and Backend Details

The frontend consists of an admin and voter dashboard, while the backend utilizes a Spring Boot REST API for managing voter information and authentication processes. MySQL database enhances data management efficiency and security.



Hardware Components

Key hardware components include the ESP32 microcontroller for data processing and the R307 fingerprint sensor for capturing and verifying fingerprints. Together, they form the backbone of biometric authentication in voting.



Workflow Diagram

The voting process workflow involves admin registration of voters via fingerprint, followed by voter authentication and vote casting. This flow ensures a systematic approach to secure and reliable voting.

How It Works

Simple three-step process for secure and efficient voting

1

Voter Registration

Voters register their fingerprint with authorized personnel to create their unique voter profile.

2

Fingerprint Authentication

On voting day, voters authenticate using their fingerprint to access the voting interface.

3

Cast Your Vote

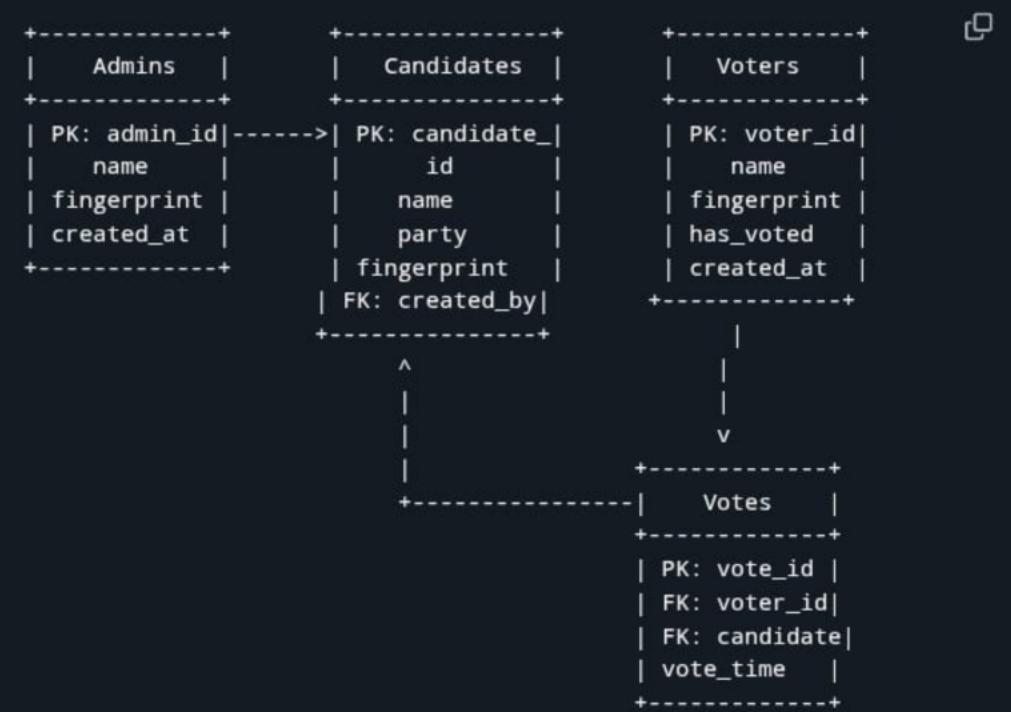
Select your candidate and confirm your choice. The vote is immediately encrypted and stored.

Database ER Diagram

The database architecture includes essential tables: Voters, Candidates, and Votes. A detailed ER diagram visualizes the relationships and data integrity essential for secure transaction handling in the voting process.

1. Database Implementation

ER Diagram



WEB ENABLED FINGERPRINT BASED ELECTRONIC VOTING MACHINE FOR PRIVATE COMMUNITIES

A Secure and Biometric-Authenticated Voting System

Group Number:15

Presented by

Brijesh Nishad : 2101321550026
Ashutosh : 2101321550021
Aayush Pandey : 2101321550001

Under the Supervision of
Mr. Rajat Kishor Varshney



ग्रेटर नोएडा इंस्टीट्यूट ऑफ टेक्नोलॉजी (इंजीनियरिंग इंस्टीट्यूट)



Implementation and Results



Security Considerations

An HTTPS protocol secure communication is followed for the HTTP and MQTT ports, which are used for session management. The communication is only secured as CON-GOAL, ensuring they remain in memory, coupled with fast hashing for efficient lookups.



Experiments and Results

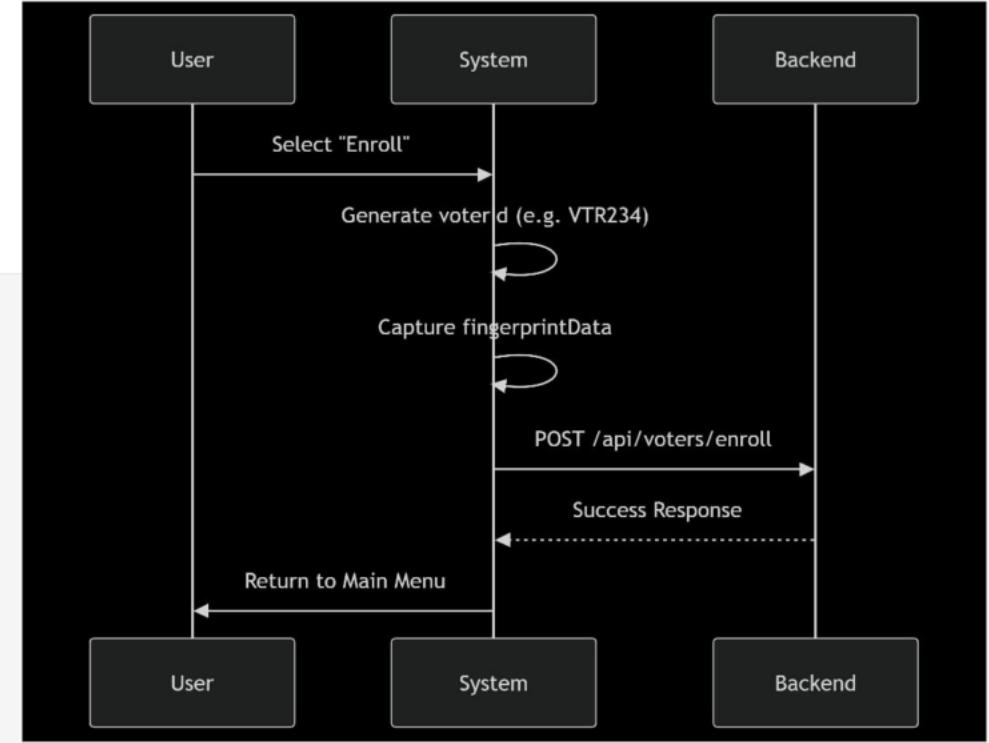


Conclusion and Future Scope



Database Implementation

The voting system includes critical tables: Voters, which contains IDs and fingerprint templates; Candidates with IDs and party affiliations; and Votes mapping voters to candidates. An example SQL statement creates the Voters table with fingerprint templates stored as LONGBLOB for privacy and security.



```
REST API Documentation
Base URL
https://portal.wef-evm.com/api

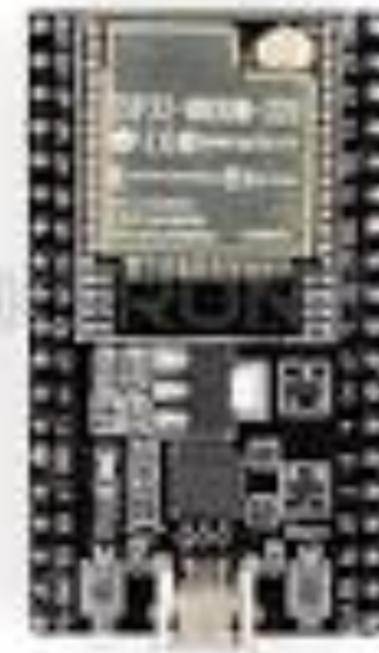
Authentication
Endpoint      Method  Description
/admin/admin-login    POST    Password-based admin login
/admin/admin-login-biometric  POST    Fingerprint-based admin login
Admin Endpoints
Endpoint      Method  Description
/admin/login-success-get-center-info  GET    Get voting center info
/admin/total-voters    GET    Get total registered voters
/admin/total-candidates GET    Get total candidates
/admin/votes-cast      GET    Get total votes cast
/admin/add-candidate   POST   Add new candidate
/admin/add-voter        POST   Register new voter
/admin/candidate-lists GET    List all candidates
/admin/analysis        GET    Get voting analytics
/admin/recent-activity GET    Get recent system activity
/admin/evm-health       GET    Check system health status
Voter Endpoints
Endpoint      Method  Description
/voter/verify-fingerprint  POST   Verify voter fingerprint
/voter/cast-vote        POST   Submit vote
Candidate Endpoints
Endpoint      Method  Description
/candidate/list  GET    List all candidates
```

REST API Endpoints

The system utilizes three essential API endpoints: /api/admins/add-voter for registering voters, /api/votes/cast for submitting votes, and /api/votes/results for fetching real-time voting results. These endpoints facilitate streamlined interactions between the frontend and the backend.

Hardware Wiring and Functionality

The hardware comprises an ESP32 microcontroller and an R307 fingerprint sensor. Wiring connects the VCC to 3.3V, with TX and RX routed through GPIO16 and GPIO17, respectively, enabling robust fingerprint processing and server communication.



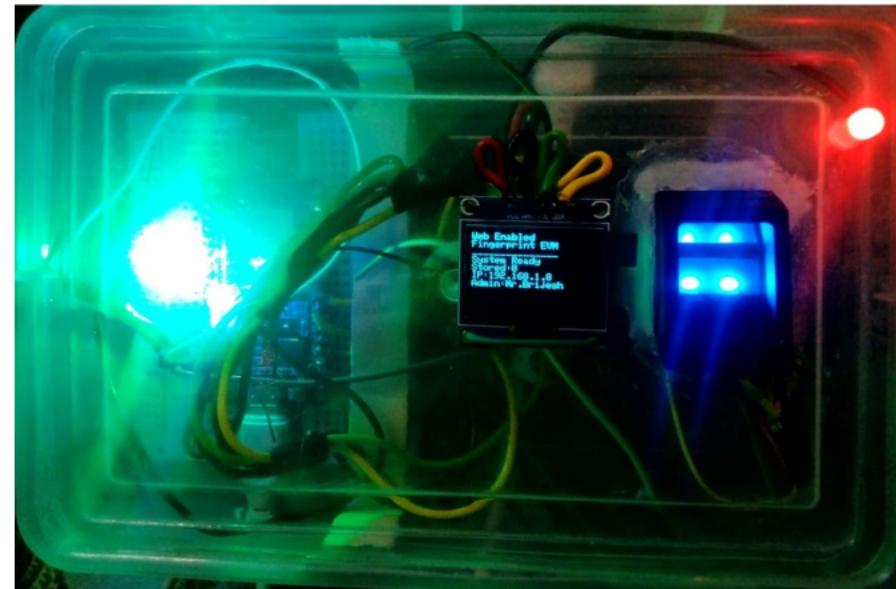
Security Considerations

An HTTPS protocol secures communication between the ESP32 and server, while JWT tokens are used for session management. Fingerprint templates are securely stored as LONGBLOB, ensuring they remain irretrievable, coupled with fast indexing for efficient lookup.



Experiments and Results

Testing revealed a flawless 0% false accept/reject rate with 100 voters, while vote casting latency remained under 2 seconds. These results emphasize the reliability and efficiency of the biometric voting process, ensuring accurate voter identification.



Conclusion and Future Scope

The web-enabled voting system presents a secure, scalable, and fraud-resistant solution for private communities. Future enhancements may include integrating facial recognition and implementing blockchain technologies to ensure even greater transparency and tamper-resistance.



WEF-EVM
Web Enabled Fingerprint EVM
Private Community

WEB ENABLED FINGERPRINT BASED ELECTRONIC VOTING MACHINE FOR PRIVATE COMMUNITIES

A Secure and Biometric-Authenticated Voting System

Group Number:15

Presented by

Brijesh Nishad : 2101321550026
Ashutosh : 2101321550021
Aayush Pandey : 2101321550001

Under the Supervision of
Mr. Rajat Kishor Varshney

