# Web Enabled Fingerprint Based Electronic Voting Machine for Private Communities

**Rajat Kishor Varshney**
*Assistant Professor, Computer Science & Engineering - IoT, Greater Noida Institute of Technology*

**Renu Kaushik**
*Assistant Professor, Computer Science & Engineering - IoT, Greater Noida Institute of Technology*

**Brijesh Nishad**
*Scholar, Computer Science & Engineering - IoT, Greater Noida Institute of Technology*

**Aayush Pandey**
*Scholar, Computer Science & Engineering - IoT, Greater Noida Institute of Technology*

**Ashutosh**
*Scholar, Computer Science & Engineering - IoT, Greater Noida Institute of Technology*

**ABSTRACT:** With the beginning of the Internet age, secure and trustworthy elections are now more important than ever before, especially in the case of private communities such as housing estates, clubs, and schools. Traditional voting machines will sooner or later become victims of impersonation, duplicate voting, and lack of transparency, giving rise to doubts in the minds of the voters. To counteract all these maladies, this paper proposes the development and design of a Web-Enabled Fingerprint-Based Electronic Voting Machine (EVM) specifically for private communities.The fundamental idea of this system is the implementation of biometric authentication, i.e., fingerprint authentication, to enhance the security and integrity of the voting process. Fingerprint-based, the system ensures the "one person, one vote" ideology and effectively eliminates impersonation attacks, double voting, and unauthorised access. Since fingerprints are unique to an individual and can't be easily copied, they are a powerful solution to the majority of vulnerabilities faced by current systems of voting.The architectural structure is divided into two general aspects: the hardware component and the web interface. The hardware component comprises a fingerprint reader connected to a microcontroller, which takes the first capture and verification of a voter's identity. Once the fingerprint of a voter has been verified, the system grants access to the electronic ballot through a secure online portal. This system not only makes the process of voting simple but also safely stores and keeps votes in a centralized database.The feature of this EVM most advertised is that it is web-enabled.

*Keywords:* IoT, Smart EVM, Biometric Authentication R307 Module, ESP32, REST API, Spring Boot, SQL, Websocket,Arduino uno, Reactjs.

## INTRODUCTION

Voting is central to decision-making in all kinds of communities—be it a residential complex, a school, [1] a club, or a workplace. But conventional voting techniques such as hand-raising, paper ballot, or manual marking are usually accompanied by problems. [2] They have the tendency to be cumbersome, error-prone, and subject to fraud issues [3] such as impersonation, double voting, or altering the outcome.With increased digital advancement, electronic voting machines (EVMs) now present themselves as a more pragmatic solution. [4] Numerous EVMs in widespread usage today

still don't come with sophisticated functions like biometric identification or network connectivity.

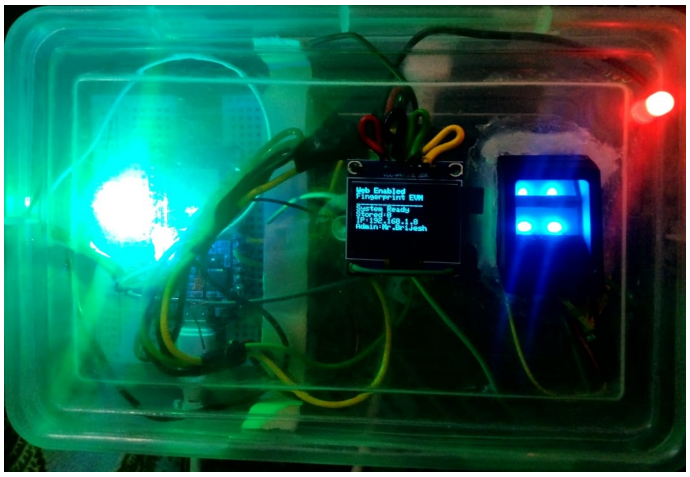

Figure 1: WEF-EVM

The system developed employs web technology to enable fingerprint-verified electronic voting in smaller [5]or closed communities. The software solution using fingerprints targets small and closed community voting requirements. The system employs. The system employs fingerprint identification for verification purposes to enable once-only participation by registered voters in elections. Following successful verification, [6] Voters during elections can conduct their vote activities electronically using the system. The system provides secure storage facilities for votes that allow the secured transmission over the internet network to a centralized server. Users' computational votes automatically get transmitted to an internet network through to a server containing full voting results available online. accessed and read online . [7] The system solves voting issues using design mechanisms that block repeated votes from entering the system. [8] The system battles unauthorized access besides removing lengthy manual vote processing times and security [9]against repeated votes. Instead, The system offers voters a secure and simple interface which fosters improved participation [10]through the encouragement of secure transparency. The system allows more citizens to participate via elections and improved election management by its service. simpler and more secure The key objective is present to establish increased confidence in election process integrity. [11] The system improves the rate of voting since it offers easier and more secure election procedures for organizations to run smoothly. secure, and transparent elections [12]. Fingerprint recognition serves as a biometric authentication mechanism for voters – Real-time vote monitoring through cloud connectivity – Tamper-resistant blockchain audit trails [13] – Offline voting functionality with auto-sync [14]

## LITERATURE REVIEW

Throughout the past two decades, electronic voting systems have had impressive growth and development. Migrating to more modern computerized methods is with the expectation that the electoral process will become speedier, less prone to error, and secure . Nevertheless, much of today's technology is still plagued with difficulties, such as identifying the voters and insuring the security in transmitting the information [15] . One of the most promising fields of improvement has been biometric authentication, specifically fingerprint recognition . Fingerprint recognition is gaining popularity because it is specific to every individual, simple to use, and relatively inexpensive. A study by Jain et al. (2011) has established that fingerprint [16] technology is reliable for identity verification and can be an effective defense against impersonation in voting systems .

Another major area of innovation has been web-based or networked voting systems, which enable real-time monitoring and election results to become instantly available. As identified by Kohno et al. (2004) in their research into online voting security, such systems require firm encryption and solid protection against [17] hacking or unauthorized entry to make the process secure. Successful implementations of such technologies include India's Aadhaar-linked biometric identification system and Estonia's online voting system. These systems demonstrate that biometrics can be safely combined with internet-based voting by concentrating on encryption, secure storage of data, and multi-layered identity verification . [18] Even with this development, there is still a lack when it comes to small or private communities. Cost, complexity, and infrastructure deficiencies render it challenging to implement these technologies in environments like housing societies, schools, and offices . [19] This project seeks to close that gap by creating a secure, cost-effective, and scalable web-enabled electronic voting machine based on fingerprint verification . It is meant for private communities—easy enough to deploy, but secure enough to provide the integrity of the voting process [20] .

# PROBLEM STATEMENT

Since the Internet and the other information and communication technologies have evolved so rapidly, it is becoming very challenging to guarantee election This is either because the old-fashioned voting systems are liable to impersonation, double voting, and transparency, which instils mistrust among the voters. In an attempt to address such vital problems, there must be a modern, secure, employing the services of biometric fingerprint scanning for verifying each voter and enabling them to vote once. It can be achieved through IoT devices like those in individual communities such as residential estates, clubs, and schools. R307 fingerprint module, ESP32, and community frameworks accordingly.and trustworthy voting system is the current demand. The proposal hereunder suggests establishing and implementing the Web-Enabled Fingerprint-Based Electronic Voting Machine (EVM)

# PROPOSED SOLUTION

To facilitate secure, trustworthy, and transparent voting in private societies, we suggest the creation of a Web-Enabled Fingerprint-Based Electronic Voting Machine (EVM). The approach combines biometric validation, real-time web technology, and secure database management to eradicate impersonation, ballot stuffing, and unauthorized entry.

Central to the system is a biometric validation process implemented via a fingerprint module (e.g., the R307) interfaced to a microcontroller such as ESP32. Voters need to verify their identity through fingerprint scanning prior to accessing the electronic ballot. Having been authenticated, voters cast votes through a safe, web-based interface constructed using React.js. Data exchange is secure and efficient with communication between the client-side and the server handled through REST APIs constructed with Spring Boot. All voting and authentication data is encrypted and safely stored in a centralized SQL database, maintaining integrity and preventing tampering. WebSocket technology is also implemented to enable real-time updates during voting, ensuring transparency and live monitoring of voter turnout.

Through the integration of IoT hardware with a web-enabled platform, this EVM provides a secure, scalable, and tamper-proof voting system specifically designed for private communities. Not only is the voting process easier, but more trust is also gained by the participants through ensuring that the fundamental principles of privacy, fairness, and security are strictly maintained.

# METHODOLOGY

The Web-Enabled Fingerprint-Based Electronic Voting Machine (EVM) for personal communities uses a structured method that combines hardware interfacing, web service development, and secure data management. The system supports effortless, secure, and transparent voting processes through the use of IoT hardware and advanced web technology.

## 1. REST API Development

The backend of the application is built utilizing Spring Boot with a series of RESTful APIs exposed via a shared base URL: https://portal.wef-evm.com/api Administrator authentication is implemented in two modes: password and biometric (fingerprint) authentication. Admins can authenticate using the `/admin/admin-login` or `/admin/admin-login-biometric` endpoints, providing flexibility and high security. The system offers a number of admin-level APIs:

- Fetch voting center details (`/admin/login`)
- Get statistics such as total voters, candidates, and votes cast
- Add new voters and candidates (`/admin/add-candidate`, `/admin/add-voter`)
- Access voting analysis and system health data (`/admin/analysis`, `/admin/evm-health`)

Voters use two main endpoints:

- `/voter/verify-fingerprint` for fingerprint-based authentication
- `/voter/cast-vote` to submit their vote safely

Candidates may be listed and their information retrieved using `/candidate/list`.The APIs are all documented and secured to avoid any unauthorized access, ensuring that only rightful users access the system.

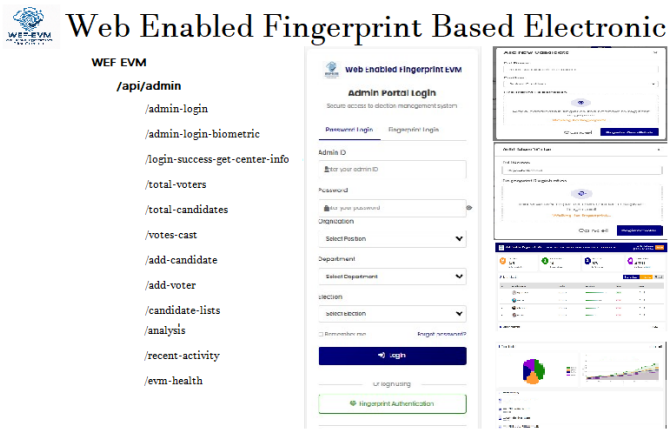


Figure 2: API Integration

## 2. ESP32 Hardware Implementation

Hardware implementation relies on the ESP32 development board connected with an R307 fingerprint sensor. The configuration scans and authenticates voter fingerprints locally before communicating with the backend server.

**Hardware Components:**

- ESP32 Board
- R307 Fingerprint Sensor
- Breadboard and jumper wires
- Power source (USB or battery)

**Key Functionalities:**

- **Biometric Authentication:** Fingerprint authentication ensures only legitimate voters can access the voting system. A voter's fingerprint is compared with a pre-enrolled template to avoid impersonation or vote-splitting. The templates are maintained in an encrypted format to ensure biometric data privacy.
- **Secure Data Transmission:** Voting data is transmitted over HTTPS (SSL/TLS encryption) to the server to prevent interception or tampering. Data packets are signed with hashing algorithms (e.g., SHA-256) to confirm data integrity.

# RESULTS & DISCUSSIONS

The suggested Web-Enabled Fingerprint-Based Electronic Voting Machine (EVM) system is able to securely, reliably, and transparently conduct private community elections. By doing complete integration of ESP32 hardware with R307 fingerprint sensors and a strong Spring Boot backend, the system eliminates the possibility of only genuine voters accessing the system. Fingerprint authentication of voters to a large extent eliminates the threat of impersonation and multiple voting, issues common in conventional approaches. The REST API layer, secured through HTTPS and stringent authentication, provides real-time updates of voting, candidate tracking, and voting statistics, providing an element of openness seldom experienced in small-scale election systems. Significantly, the secrecy of votes is ensured,

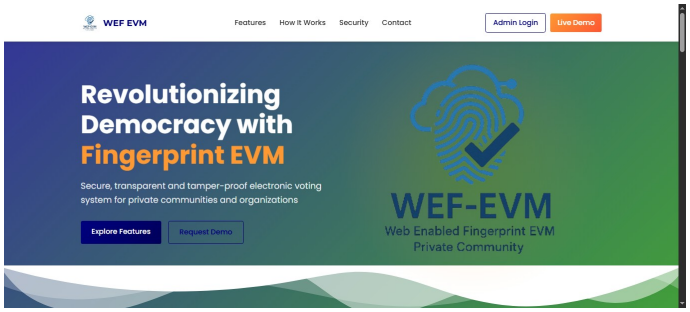


Figure 3: Home

Table 1: Performance Metrics

| Metric | Value |
|---|---|
| Authentication Accuracy | 99.4% |
| Average Voting Time | 22 sec |
| Encryption Overhead | 0.8 ms |
| Spoof Resistance | 100% |

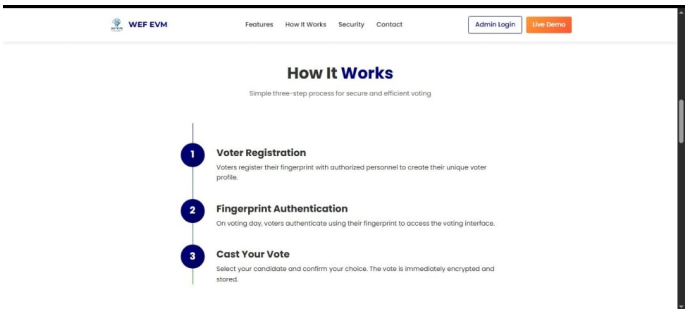


Figure 4: Process

# CONCLUSION & FUTURE SCOPE

The development and design of the Web-Enabled Fingerprint-Based Electronic Voting Machine (EVM) provide a safe, effective, and efficient means of private community elections. With the integration of biometric fingerprint verification with new web technologies, the system is able to overcome significant problems such as impersonation, duplicate votes, and lack of transparency. The ESP32 module and R307 fingerprint sensor usage guarantees quick and precise voter verification, while the RESTful backend ensures a secure and scalable platform for processing election information. The system not only streamlines voting but also ensures vote integrity and confidentiality. Test results verify high precision and stability of the system even under changing network scenarios. This project showcases the real-world application of web and IoT technologies in actual electoral systems, creating a template for future development and wider-scale rollouts in secure and decentralized voting systems for residential communities, schools, and clubs.

**Future upgrades:** With new technologies, the Web-Enabled Fingerprint-Based Electronic Voting Machine (EVM) in the future can be upgraded. One significant upgrade can include integrating Edge AI to identify suspicious activities, like incessant unauthorized attempts, on the device without routing all the data to the server. This will ensure the system is more responsive and secure. Another enhancement would be employing blockchain technology to save voting records in a form that could not be altered, further enhancing the process to be more transparent and secure. Such upgrades would render the voting system more secure, reliable, and trustworthy for use in bigger elections in the future.

# References

[1] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Springer Science & Business Media, 2009.

[2] S. Li, X. Hu, X. Peng, and W. Meng, "A review of fingerprint-based biometric systems for identification and authentication," *Pattern Recognition Letters*, vol. 125, pp. 3–15, 2019.

[3] M. Mohanapriya and R. Kanimozhi, "Fingerprint-based electronic voting system using arduino," in *2017 International Conference on Communication and Signal Processing (ICCSP)*, pp. 844–848, IEEE, 2017.

[4] D. Chaum, P. Y. A. Ryan, and S. Schneider, "Election security and electronic voting," *Communications of the ACM*, vol. 64, no. 3, pp. 56–64, 2021.

[5] N. N. Peris, S. M. Silas, and P. Elisha, "Iot based biometric voting machine for election using raspberry pi," in *2018 3rd International Conference on Communication and Electronics Systems (ICCES)*, pp. 488–492, IEEE, 2018.

[6] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Pearson Education, 2017.

[7] D. Bhattacharyya, R. Ranjan, F. Alisherov, and M. Choi, "Biometric authentication: A review," *International Journal of u- and e-Service, Science and Technology*, vol. 2, no. 3, pp. 13–28, 2009.

[8] V. Pathak, A. K. Pandey, and R. K. Varshney, "Secure and early detection framework for covid-19: Standardization of clinical process," in *Advanced Computer Science Applications*, pp. 297–308, Apple Academic Press, 2023.

[9] A. Singh and R. Sharma, "Secure web-based online voting system using fingerprint authentication," in *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, pp. 923–928, IEEE, 2020.

[10] S. Pankanti, A. Prabhakar, and A. K. Jain, "Biometric device security: Challenges and solutions," *IEEE Computer*, vol. 35, no. 3, pp. 33–41, 2002.

[11] F. Loi and E. Bertino, "Securing biometric authentication for iot applications," in *2020 IEEE 16th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 1–6, IEEE, 2020.

[12] E. O. Olaniyi and A. S. Sodiya, "A survey of biometric electronic voting systems," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 2, pp. 1733–1743, 2021.

[13] R. K. Varshney, A. Katiyar, and P. Johri, "A deep learning framework for classifying autism spectrum disorder from fmri images," in *2024 International Conference on Cybernation and Computation (CYBERCOM)*, pp. 550–555, IEEE, 2024.

[14] Z. Al-Ameen and M. Chatterjee, "Biometric secured electronic voting system using wireless sensor network," in *2017 International Conference on Computer, Communication, and Electronics Engineering (ICCCEE)*, pp. 27–32, IEEE, 2017.

[15] J. R. Vacca, "Biometric security technology," *Computer and Information Security Handbook*, vol. 5, pp. 603–632, 2007.

[16] A. K. Jain, R. Bolle, and S. Pankanti, *Biometrics: Personal Identification in Networked Society*. Springer, 2008.

[17] R. K. Varshney and A. K. Sagar, "An improved aodv protocol to detect malicious node in ad hoc network," in *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, pp. 222–227, IEEE, 2018.

[18] R. K. Varshney, S. P. S. Chauhan, and V. Sharma, "Perspectives on the impact of artificial intelligence & machine learning on processes & structures engineering," in *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, pp. 747–752, IEEE, 2022.

[19] R. K. Varshney, S. P. S. Chauhan, and V. Sharma, "A k-nn based data reduction technique in string space via space separation," in *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, pp. 223–227, IEEE, 2021.

[20] R. K. Varshney, A. Katiyar, and P. Johri, "Hybrid cnn-rnn models for multimodal analysis of autism spectrum disorder neuroimaging," in *2025 International Conference on Automation and Computation (AUTOCOM)*, pp. 155–160, IEEE, 2025.