Design and Development of a Next Generation Biometric Integrated Electronic Voting System with Advanced Security Protocols and Multi Layered Authentication Mechanisms

[1]Komatla Babu Venkatesh Reddy,[2]Kona Jaya Santhosh Kumar,[3]Kulli Ranjith Babu,[4]Katti Samuel Saxena,[5]Katuri Yaswanth Kumar,[6]Dr. P. Srinivasa Rao

[1,2,3,4,5]U. G Student, Dept ELECTRONICS AND COMMUNICATION ENGINEERING, St. Ann's College of Engineering and Technology, (Autonomous)Chirala, Bapatla Dist, Andhra Pradesh – 523187, India

[6]Associate Professor, Dept ELECTRONICS AND COMMUNICATION ENGINEERING, St. Ann's College of Engineering and Technology (Autonomous), Chirala, Bapatla Dist, Andhra Pradesh – 523187, India

Abstract: The integrity and transparency of elections are essential for maintaining a strong democratic system. Traditional voting methods and existing electronic voting systems often face challenges such as voter impersonation, duplicate voting, unauthorized access, and security vulnerabilities. To address these issues, this project presents a Biometric-Based Electronic Voting System that combines RFID technology and fingerprint authentication to ensure secure and reliable voting. In the proposed system, each voter is assigned a unique RFID card that serves as a voter identification card. During the voting process, the RFID card is first verified, followed by fingerprint authentication using a biometric sensor. Only when both authentication stages are successfully completed is the voter allowed to cast a vote. The system is controlled using a Raspberry Pi 4, which manages voter verification, vote recording, and system monitoring. A keypad is provided for candidate selection, while a buzzer gives immediate feedback regarding authentication and voting status. The proposed solution significantly reduces electoral fraud, prevents duplicate voting, enhances voter privacy, and ensures accurate vote counting. By integrating advanced biometric verification with electronic voting technology, the system offers a secure, efficient, and transparent voting platform suitable for modern democratic processes.

KEYWORDS- Electronic Voting System, RFID Authentication, Fingerprint Recognition, Raspberry Pi 4, Biometric Security, Voter Verification, Election Automation, Secure Voting, Embedded Systems, Digital Democracy.

INTRODUCTION

Elections play a vital role in democratic societies by enabling citizens to choose their representatives and participate in governance. The credibility of any democratic system depends heavily on the fairness, transparency, and security of the electoral process. Traditional voting methods, including paper ballots and conventional electronic voting machines, are often vulnerable to issues such as voter impersonation, multiple voting, ballot manipulation, and lengthy vote-counting procedures.

With the rapid advancement of embedded systems, biometric technologies, and digital authentication techniques, electronic voting systems have evolved significantly. Biometric authentication has emerged as one of the most reliable methods for verifying voter identity because biometric traits such as fingerprints are unique to each individual and difficult to forge. Similarly, Radio Frequency Identification (RFID) technology provides a convenient and efficient mechanism for voter identification and record management.

The proposed Biometric-Based Electronic Voting System integrates RFID authentication and fingerprint verification to create a dual-layer security framework. Each registered voter is provided with an RFID card containing a unique identification number. During the voting process, the voter first presents the RFID card, after which fingerprint authentication is performed. Once both credentials are successfully validated against the database, the voter is granted access to cast a vote using a keypad interface.

The system utilizes Raspberry Pi 4 as the central controller, interfacing with the fingerprint sensor, RFID reader, keypad, LCD display, and buzzer. This integrated solution improves election security, eliminates duplicate voting, reduces human intervention, and ensures accurate vote recording. The proposed system provides a practical and scalable approach toward modernizing electoral processes while maintaining voter confidentiality and trust.

RELATED WORK

Several researchers have explored the application of biometric technologies and RFID-based authentication systems to improve the security and reliability of electronic voting systems.

Ashok Nalluri et al. proposed an RFID and fingerprint recognition-based electronic voting system that authenticates voters using RFID cards and fingerprint verification. Their system successfully

reduced unauthorized voting and enhanced election security.

Ravuri Chandrika et al. introduced an RFID-based electronic voting machine incorporating OTP and biometric verification. The proposed solution employed multi-level authentication to prevent fraudulent voting and duplicate vote casting.

Zakiah Mohd Yusoff et al. developed a fingerprint biometric voting machine using Internet of Things (IoT) technology. The system stored voting information in cloud databases while ensuring voter authentication through fingerprint verification.

Shubhangi Dhane et al. proposed an online voting system integrating fingerprint sensors, facial recognition, and QR code scanning technologies. Their work focused on improving voter authentication through multiple verification mechanisms.

Ajaykumar K.H. et al. developed an electronic voting machine utilizing RFID and fingerprint authentication to ensure secure voter verification and prevent repeated voting attempts.

These studies demonstrate the effectiveness of biometric authentication and RFID technologies in securing electronic voting systems. However, many existing systems either rely on a single authentication mechanism or involve complex implementations. The proposed system addresses these limitations by integrating RFID and fingerprint authentication within a Raspberry Pi-based platform to achieve improved security, efficiency, and ease of deployment.

LITERATURE SURVEY

[1] RFID and Fingerprint Recognition Based Electronic Voting System for Real-Time Application This work utilizes RFID cards and fingerprint verification for voter authentication. The system ensures that voting is permitted only after successful biometric verification, thereby preventing unauthorized voting activities.

[2] RFID-Based Electronic Voting Machine Using OTP and Biometric Verification The authors proposed a three-level authentication mechanism consisting of RFID validation, OTP verification, and biometric authentication. This approach significantly enhances election security and voter validation.

[3] Fingerprint Biometric Voting Machine Using Internet of Things This research integrates fingerprint authentication with cloud-based storage using IoT technology. The system enables secure vote recording while maintaining transparency and accessibility.

[4] Online Voting System Using Fingerprint Sensor, Face Recognition, and QR Code Scanner The study introduces a multi-factor authentication system combining fingerprint recognition, facial recognition, and QR codes to minimize election fraud and improve voter verification accuracy.

[5] Electronic Voting Machine Using RFID and Fingerprint This project employs RFID cards and fingerprint matching for voter validation. It prevents duplicate voting and provides secure election management through electronic authentication methods.

The literature survey indicates that combining RFID technology with biometric authentication significantly improves voting system security and voter verification accuracy.

EXISTING METHOD

The existing electronic voting systems primarily rely on traditional voter identification methods such as voter ID cards, passwords, OTP verification, or standalone biometric authentication techniques. In many cases, voter verification is performed manually or through a single authentication mechanism, which increases the possibility of unauthorized access and electoral fraud. Conventional Electronic Voting Machines (EVMs) are designed to simplify the voting process; however, they still face challenges related to voter impersonation, duplicate voting, and identity theft. Systems that use only RFID cards or only fingerprint verification are vulnerable if the authentication credential is lost, duplicated, or compromised. Furthermore, many existing voting systems lack real-time monitoring, secure data management, and multi-factor authentication, making them susceptible to manipulation and security breaches. These limitations can affect the transparency, reliability, and overall integrity of the election process, thereby reducing public confidence in the voting system.

PROPOSED METHOD

The proposed Biometric-Based Electronic Voting System introduces a secure and reliable voting platform by integrating RFID technology with fingerprint authentication using Raspberry Pi 4. In this system, every registered voter is assigned a unique RFID card that serves as a digital voter identification card. During the voting process, the voter must first scan the RFID card, after which the system verifies the card information against a pre-registered database. Once RFID authentication is successful, the voter is required to place a finger on the fingerprint sensor for biometric verification. The captured

fingerprint is compared with the stored fingerprint template to confirm the voter's identity. Only when both authentication stages are successfully completed is the voter permitted to cast a vote using the keypad interface. The selected vote is securely recorded in the database, and the voter status is immediately updated to prevent duplicate voting. A buzzer provides instant feedback regarding authentication success, authentication failure, and vote submission. By employing dual-factor authentication and automated vote management, the proposed system significantly enhances election security, eliminates unauthorized voting, ensures voter privacy, improves transparency, and provides an efficient and trustworthy voting environment suitable for modern democratic processes.

SYSTEM ARCHITECTURE

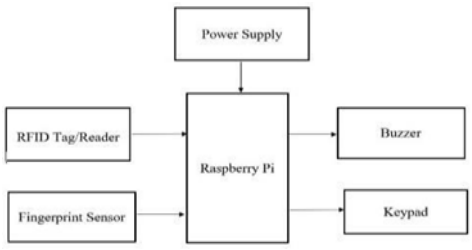

Fig.1 System Architecture

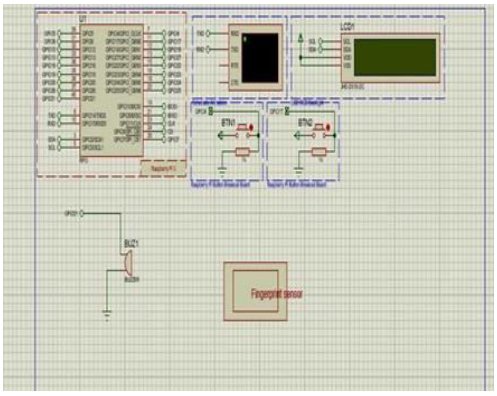

Fig.2 Circuit Diagram

MODULE DESCRIPTION

Voter Registration Module: The Voter Registration Module is responsible for enrolling eligible voters into the system before the election process begins. During registration, the voter's personal details, fingerprint data, and RFID card information are collected and securely stored in the database. Each voter is assigned a unique RFID card that acts as a digital voter identification card. This module ensures that only authorized and registered voters can participate in the election process.

RFID Authentication Module: The RFID Authentication Module serves as the first level of voter verification. When a voter arrives at the polling station, the RFID card is scanned using the RFID reader. The system reads the unique identification number stored on the RFID card and compares it with the records available in the database. If the RFID information

matches a registered voter, the system proceeds to the next authentication stage. Otherwise, access is denied and the voter is prevented from voting.

Fingerprint Verification Module: The Fingerprint Verification Module provides the second layer of security. After successful RFID verification, the voter places their finger on the fingerprint sensor. The captured fingerprint image is processed and compared with the pre-stored fingerprint template associated with the voter's RFID card. If a valid match is found, the voter is authenticated successfully. This module prevents unauthorized access, identity fraud, and duplicate voting attempts.

Voting Module: The Voting Module allows authenticated voters to cast their votes securely. After successful dual-factor authentication, the voter is presented with the list of candidates through a keypad interface. The voter selects the preferred candidate, and the system records the vote in the database. The voting process is designed to be simple, efficient, and user-friendly while maintaining voter confidentiality.

Vote Management Module: The Vote Management Module is responsible for securely storing and managing all voting data. Once a vote is cast, the system updates the voter's status to indicate that the vote has been submitted. This prevents multiple voting attempts by the same individual. The module maintains vote records securely and ensures data integrity throughout the election process.

Alert and Notification Module: The Alert and Notification Module uses a buzzer to provide immediate feedback to the voter. The buzzer generates different sound indications for successful authentication, failed authentication, invalid RFID cards, fingerprint mismatches, and successful vote submission. This module improves user interaction and helps voters understand the status of their actions during the voting process.

Database Management Module: The Database Management Module stores voter information, fingerprint templates, RFID details, voting records, and authentication logs. The database is maintained within the Raspberry Pi system and is protected using appropriate security mechanisms. This module ensures secure storage, quick retrieval, and reliable management of election-related data.

System Control Module: The System Control Module is implemented using the Raspberry Pi 4, which acts as the central controller of the entire voting system. It coordinates communication between all

hardware components, including the fingerprint sensor, RFID reader, keypad, buzzer, and database. This module manages authentication, vote recording, error handling, and overall system operation to ensure smooth and secure functioning of the electronic voting system.

RESULTS AND DISCUSSION

The proposed **Biometric-Based Electronic Voting System** was successfully designed, implemented, and tested using Raspberry Pi 4, RFID technology, and fingerprint authentication. The system demonstrated reliable performance in voter identification, authentication, and vote recording processes. During testing, all hardware components, including the RFID reader, fingerprint sensor, keypad, buzzer, and display unit, were properly integrated and operated without communication errors.

The RFID authentication module accurately identified registered RFID cards and rejected unauthorized or invalid cards. Similarly, the fingerprint verification module successfully matched registered fingerprints with stored templates, ensuring that only eligible voters were allowed to participate in the election process. The dual-factor authentication mechanism significantly enhanced security by preventing voter impersonation and unauthorized access.

After successful authentication, voters were able to cast their votes using the keypad interface. The system accurately recorded each vote in the database and immediately updated the voter status to prevent duplicate voting. Any attempt to vote multiple times was detected and rejected by the system. The buzzer provided instant feedback regarding authentication success, authentication failure, and vote submission, improving user interaction and system usability.

The database management module securely stored voter information and voting records, ensuring data integrity and confidentiality. Throughout the testing phase, the system maintained consistent performance and accurately processed all voting operations without data loss. The overall results demonstrate that the proposed system provides a secure, transparent, and efficient electronic voting solution.

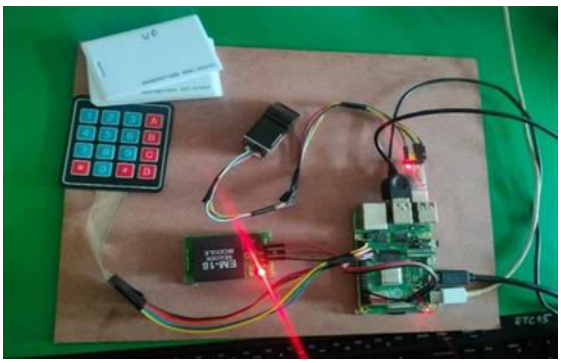

Figure 3. Hardware Result

Figure 4. Actual Product

Figure 5. Software Result

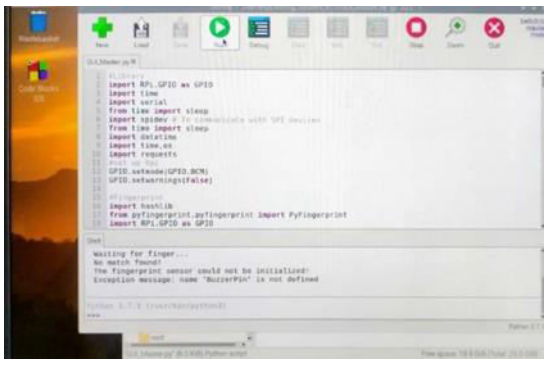

Figure 6: Fingerprint not found

The obtained results confirm that the proposed system is capable of providing a secure, reliable, and efficient voting environment while maintaining the integrity and confidentiality of the electoral process.

CONCLSUION AND FUTURE SCOPE

The proposed Biometric-Based Electronic Voting System successfully integrates RFID and fingerprint authentication to provide a secure, reliable, and efficient voting platform. By implementing dual-factor voter verification, the system effectively prevents unauthorized access, duplicate voting, and electoral fraud while ensuring accurate vote recording. The developed solution enhances transparency, voter confidence, and the overall integrity of the election process.

The system can be further enhanced by integrating advanced technologies such as blockchain, cloud computing, and end-to-end encryption to improve security and transparency. Additional biometric features such as facial recognition and iris scanning can be incorporated to strengthen voter authentication. Furthermore, secure remote voting through web and mobile applications can be implemented to increase accessibility and voter participation in future elections.

REFERENCES

1. Nalluri, B. B. Teja, and A. Balakrishnan, “RFID and Fingerprint Recognition Based

Electronic Voting System for Real Time Application," *International Journal of Engineering Development and Research (IJEDR)*, vol. 2, no. 4, pp. 1–5, 2022.

2. R. Chandrika and N. C. Gowtham, "RFID Based Electronic Voting Machine Using OTP and Biometric Verification," *Journal of Electronics and Communication Engineering Research*, vol. 8, no. 5, pp. 1–7, 2022.
3. Z. M. Yusoff, Y. Yusnoor, A. M. Markom, S. A. Nordin, and N. Ismail, "Fingerprint Biometric Voting Machine Using Internet of Things," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 30, no. 2, pp. 699–706, 2023.
4. S. D. Dhane and S. B. Rathod, "Online Voting System Using Fingerprint Sensor, Face Recognition and QR Code Scanner," *International Journal of Creative Research Thoughts (IJCRT)*, vol. 10, no. 5, pp. 1–20, 2022.
    A. K. H., A. R. B., and D. J. T., "Electronic Voting Machine Using RFID and Fingerprint," *Journal of Emerging Technologies and Innovative Research (JETIR)*, vol. 9, no. 6, pp. 1–4, 2022.
5. P. Mansingh, T. Titus, and V. Devi, "A Secured Biometric Voting System Using RFID Linked with the Aadhaar Database," in *Proceedings of the 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2020, pp. 1–5.
6. O. S. Olumide, K. B. Olutayo, and S. E. Adekunle, "A Review of Electronic Voting Systems: Strategy for a Novel Framework," *International Journal of Information Engineering and Electronic Business*, vol. 12, no. 1, pp. 19–29, 2020.
7. J. Liu, T. Han, M. Tan, B. Tang, W. Hu, and Y. Yu, "A Publicly Verifiable E-Voting System Based on Biometrics," *Cryptography*, vol. 7, no. 4, pp. 1–15, 2023.
8. H. Hamran, M. Abdullah, M. E. Naveed, and A. R. Afzal, "Design and Implementation of Secure Electronic Voting System Using Fingerprint Biometrics," *Journal of Artificial Intelligence and Computing*, vol. 1, no. 1, pp. 1–5, 2023.
9. Shalini, M. S. Prabha, and R. Krithika, "Secure Authentication for Advanced Voting System Using Fingerprint.and RFID," *International Journal of Trend in Scientific Research and Development (IJTSRD)*, vol. 2, no. 3, pp. 703–706, 2018.
10. D. B. Kadam, "RFID Based Electronic Voting System Using Raspberry Pi," *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, vol. 7, no. 4, pp. 1901–1908, 2019.
11. J. Arshad, M. Farooq-i-Azam, A. Khan, M. Irshad, and S. M. Noman, "Design and Implementation of a Software-

Based Advanced Electronic Voting Machine Using Automatic Registration and Fingerprint Identification," 2021.

12. V. S. K. Vivek et al., "E-Voting System Using Hyperledger Sawtooth," in *Proceedings of the International Conference on Advances in Computing, Communication and Materials (ICACCM)*, 2020, pp. 29–35.
13. S. Gupta, D. Jain, M. T. Themalil, and others, "Electronic Voting Mechanism Using Microcontroller ATmega328P with Face Recognition," in *Proceedings of the Fifth International Conference on Computing Methodologies and Communication (ICCMC)*, 2021, pp. 1471–1476.
    A. Jatain, "Design and Development of Biometric Enabled Advanced Voting System," *SSRN Electronic Journal*, 2020.
14. Babburi, S. Privacy-Preserving Collaborative Framework with Auditable Federated Learning.
15. Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
16. Immadi, S. K. (2025). Optimizing ERP for Human Capital Management. Applied Research for Growth, Innovation and Sustainable Impact, 377–384. https://doi.org/10.1201/9781003684657-63
17. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
18. Poojari, R. INTELLIGENT SYSTEMS+B108 AND APPLICATIONS IN ENGINEERING.
19. Mahimalur, R. K., Vasgam, M., & Manoharan, D. Devops Lifecycle Management And Cloud Migration Assessments: A Security-Driven CICD Perspective.
20. Viswanathan, V. (2023). AI-Augmented Decision Intelligence for Enterprise Systems: Integrating Cognitive Analytics for Resource and Talent Optimization.
21. Agrawal, A. M., Gajula, S., Shinde, R. P., Shah, H., & Ghosh, H. (2025, July). Machine Translation for Long Sequences with Enhanced Attention Mechanisms. In 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1-6). IEEE.
22. Maturi, S. Y. (2021). Blockbond hardening: Securing pooled-hash protocols against traffic tampering, MITM hash-rate hijacking, and template coercion. International Journal of Communication Networks and Information Security, 13(3), 718–728.
23. Pavan Kumar Adabala. (2026). Smart Retail Fuel Systems: IoT-Enabled Solutions for Loss Prevention and Environmental Safety. Computer Fraud and Security, 868–875. https://doi.org/10.52710/cfs.995
24. Kavuri, S. (2026). An Explainable Machine Learning Framework for Predicting Software Defects in

Large-Scale Software Systems. 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC), 1–6. https://doi.org/10.1109/icaic67076.2026.11395777

25. Pokala, H. K., & Gummadi, V. P. K. (2026). Autonomous AI-Powered Resource Management for Apache Flink on Amazon EKS. 2026 International Conference on Artificial Intelligence, Systems, and Emerging Technologies (ICAISET), 1–4. https://doi.org/10.1109/icaiset66439.2026.11541881
26. Shashank, A. (2025). Self-Healing Data Pipelines for Enhanced Reliability: A Paradigm Shift in Enterprise Data Management. Journal of Computer Science and Technology Studies, 7(8), 1097-1104.
27. Susarla, R. S., Boyapati, P. K., & Kandula, S. T. R. (2025, July). Cloud-Based Secure Data Storage in Smart Cities Using Central-Smoothing Hypergraph Neural Networks. In 2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC) (pp. 279-284). IEEE.
28. Boyapati, P. K. Building a centralized data operations hub for healthcare enterprise integration. IJSAT-Int. J. Sci. Technol. 16 (2). https://doi.org/10.71097/IJSAT.v16.i2.3219