International Journal of Engineering & Extended Technologies Research (IJEETR)

ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802208

IoT - Based Fingerprint Voting System

Prof M. Vasanthakumar[1] M.E., MBA (Ph.D.), S.Gowtham[2], G.Gowthaman[3], B. Karthick[4], V. Kanishkar[5]

Department of Electronics and Communication Engineering, AVS Engineering College, Salem, Tamil Nadu, India

Department of Electronics and Communication Engineering, AVS Engineering College, Salem, Tamil Nadu, India

Corresponding Author: Gowtham.S

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT: The IoT-Based Fingerprint Voting System is a modern approach to conducting secure and efficient elections by integrating biometric authentication with Internet of Things (IoT) technology. Traditional voting systems often face challenges such as voter impersonation, multiple voting, and lack of transparency. This system aims to overcome these issues by using fingerprint recognition to ensure that each voter can cast their vote only once.

In this system, each voter is registered with a unique fingerprint stored in a centralized database. During the voting process, the fingerprint sensor captures the voter's biometric data and verifies it with the stored records. Once authenticated, the voter is allowed to cast their vote through an electronic interface. The voting data is then transmitted securely to a cloud server using IoT technology, enabling real-time monitoring and result analysis.

This system enhances the security, accuracy, and reliability of the election process while reducing human effort and errors. It also ensures transparency and faster vote counting. The proposed system is cost-effective, user-friendly, and suitable for implementation in both small-scale and large-scale elections.

KEYWORDS: Internet of Things (IoT), Fingerprint Recognition, Biometric Authentication, Electronic Voting System, Secure Voting, Cloud Computing, Voter Verification, Embedded Systems, Microcontroller, Data Security.

I. INTRODUCTION

Voting is a fundamental right in a democratic society, enabling citizens to choose their representatives and participate in governance. Traditional voting methods, such as paper ballots and Electronic Voting Machines (EVMs), have been widely used over the years. However, these systems face several challenges, including voter impersonation, multiple voting, lack of transparency, and time-consuming vote counting processes.

With the rapid advancement of technology, the integration of biometric authentication and the Internet of Things (IoT) has opened new possibilities for secure and efficient voting systems. Biometric techniques, especially fingerprint recognition, provide a unique and reliable method for identifying individuals, as no two fingerprints are alike. By incorporating fingerprint authentication into the voting process, the system ensures that only eligible voters can cast their votes and prevents duplication.

The proposed IoT-Based Fingerprint Voting System aims to enhance the security, accuracy, and reliability of elections. In this system, each voter's fingerprint is pre-registered and stored in a database. During voting, the fingerprint sensor verifies the identity of the voter. Once authenticated, the voter is allowed to vote through an electronic interface. The collected voting data is transmitted securely to a cloud server using IoT technology, enabling real-time monitoring and faster result processing.

This system reduces human intervention, minimizes errors, and improves transparency in the electoral process. It is costeffective, user-friendly, and suitable for implementation in educational institutions, organizations, and even national-level elections. The proposed system represents a significant step toward digital transformation in the voting process, ensuring fairness and trust in democratic systems.

ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802208

Objectives of the Study

1)To ensure one person–one vote by preventing duplicate and unauthorized voting.
2)To integrate IoT technology for real-time data transmission and monitoring.
3)To improve accuracy and transparency in the voting process.
4)To reduce human errors and manual effort in elections.
5)To provide fast and efficient vote counting and result generation.
6)To design a user-friendly and cost-effective voting system

II. BACKGROUND

Voting systems have evolved significantly over time, from traditional paper-based methods to electronic voting systems. While paper ballots were simple to implement, they were prone to errors such as invalid votes, ballot tampering, and lengthy counting procedures. To overcome these issues, Electronic Voting Machines (EVMs) were introduced, offering faster and more accurate vote counting. However, even EVMs face challenges related to security, voter authentication, and transparency.

One of the major concerns in existing voting systems is voter impersonation and multiple voting, which can affect the fairness of elections. To address these issues, biometric technologies such as fingerprint recognition have been widely adopted in various applications for identity verification. Fingerprint-based authentication is considered highly reliable because each individual has a unique fingerprint pattern that cannot be easily duplicated.

At the same time, the development of the Internet of Things (IoT) has enabled seamless communication between devices and centralized systems through the internet. IoT technology allows real-time data transfer, remote monitoring, and efficient data management, making it suitable for applications that require continuous connectivity and control. By combining biometric authentication with IoT technology, the IoT-Based Fingerprint Voting System aims to provide a secure, transparent, and efficient voting solution. This integration helps in eliminating fraudulent activities, ensuring accurate voter identification, and enabling quick and reliable result processing.

III. RELATED WORKS

Several research works have been carried out to improve the security and efficiency of voting systems using biometric authentication and IoT technologies. A fingerprint-based voting system proposed in earlier studies focuses on eliminating duplicate voting by verifying the voter's identity using unique biometric data. This approach ensures that only authorized individuals can cast their votes, thereby increasing the reliability of the election process.

Recent advancements have introduced IoT-enabled voting systems where voting data is transmitted in real-time to centralized servers. These systems integrate microcontrollers, fingerprint sensors, and cloud platforms to provide secure communication and faster result processing. For example, an IoT-based voting system using fingerprint authentication demonstrated high accuracy and efficiency in small-scale elections, ensuring error-free vote collection and management

Other studies have combined fingerprint authentication with additional technologies such as GSM modules to enhance system functionality. These systems provide real-time updates through SMS notifications and improve transparency by allowing instant monitoring of voting results. Such implementations also focus on user-friendly interfaces and secure data handling mechanisms.

Journal of Science and Technology

Furthermore, modern research emphasizes multi-layer security approaches, integrating IoT, biometric verification, and cloud storage. These systems aim to prevent unauthorized access, ensure data integrity, and enable remote monitoring of election activities. The integration of these technologies significantly reduces manual errors and enhances the overall efficiency of the voting process.

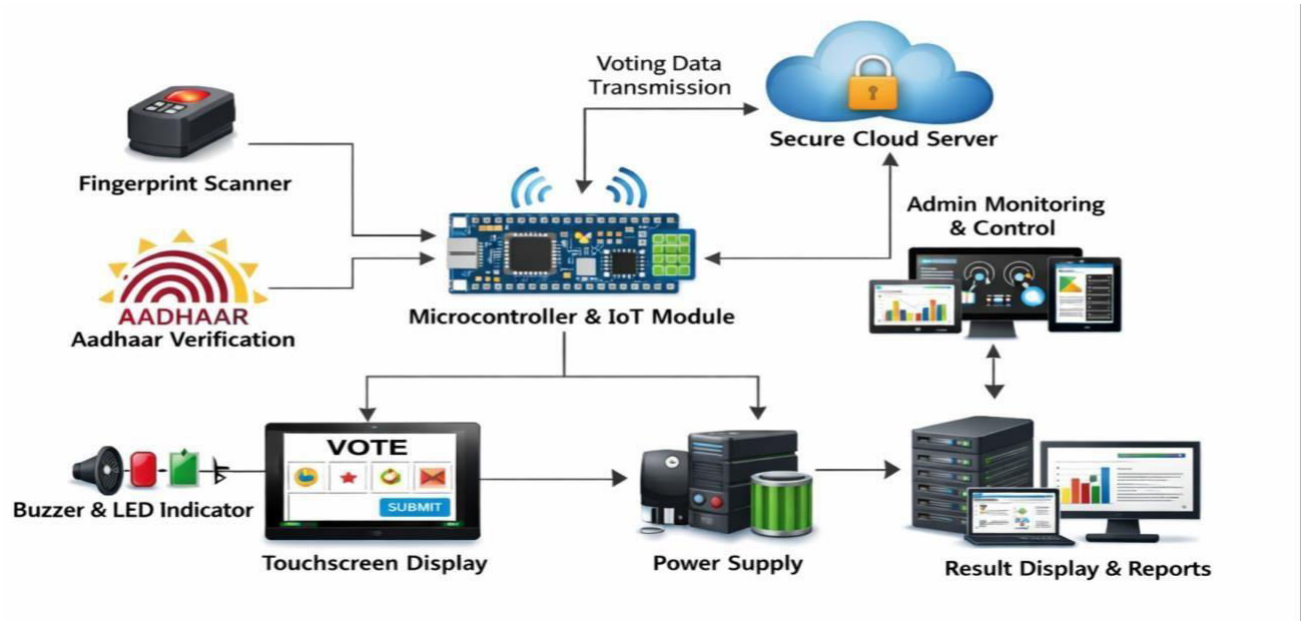
Overall, existing works highlight the importance of combining biometric authentication with IoT to develop a secure, transparent, and efficient electronic voting system, which forms the foundation for the proposed system.

International Journal of Engineering & Extended Technologies Research (IJEETR)

ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802208



System Architecture Overview

The IoT-Based Fingerprint Voting System is designed using a structured architecture that integrates biometric authentication, embedded systems, and cloud communication to ensure secure and efficient voting.

The system consists of four main layers: Input Layer, Processing Layer, Communication Layer, and Output Layer. The Input Layer includes the fingerprint sensor and voting interface. It captures the voter's biometric data and voting choice.

The Processing Layer consists of a microcontroller (such as Arduino or NodeMCU), which verifies the fingerprint, controls the voting process, and manages data operations.

The Communication Layer uses an IoT module (Wi-Fi/ESP8266) to transmit the voting data securely to a cloud server. The Output Layer includes display units and result monitoring systems that show voting status and final results.

The architecture follows a client-server model, where the voting device acts as the client and the cloud server acts as the central system for data storage and analysis. Data security is maintained through encryption techniques, ensuring safe transmission and storage.

Overall, this architecture provides a scalable, reliable, and secure framework for modern electronic voting systems, enabling real-time monitoring and efficient result processing.

The proposed research design focuses on developing a secure, reliable, and efficient IoT-based fingerprint voting system to overcome the limitations of traditional voting methods. The study begins by identifying the major problems in existing systems such as voter fraud, multiple voting, manual errors, and delays in result declaration.

The research adopts an experimental and implementation-based approach, where both hardware and software components are designed and tested. The system integrates biometric authentication (fingerprint recognition) with Internet of Things (IoT) technology to ensure secure data transmission and real-time monitoring.

During the research process, voter data including fingerprint templates are collected during the registration phase and stored in a secure database. The system then verifies voters during the election process by matching the scanned fingerprint with the stored data. Only authenticated users are allowed to cast their vote.

The design also includes data validation, system testing, and performance evaluation, where parameters such as accuracy, response time, and security are analyzed. The research ensures that the system is user-friendly, scalable, and suitable for real-time voting applications

ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802208

The proposed system architecture is designed using a layered approach, consisting of multiple interconnected modules that ensure smooth operation of the voting process.

IV. APPLICATION OF THE IOT-BASED VOTING SYSTEM

1. Used in government elections to ensure secure and fraud-free voting.
2. Applied in college and university elections for student representative selection.
3. Useful in corporate organizations for internal decision-making and voting.
4. Implemented in local body elections such as panchayat and municipal voting.
5. Suitable for online or remote voting systems with secure authentication.
6. Used in private institutions and clubs for member-based voting.
7. Helpful in survey systems where only verified users can participate.

V. TESTING AND VALIDATION

Testing and validation are carried out to ensure that the system performs accurately, securely, and reliably under different conditions. The system is tested at each stage to verify proper functionality and performance.
The fingerprint module is tested by registering multiple users and verifying that only valid fingerprints are accepted while unauthorized users are rejected. This ensures correct biometric authentication.

The voting process is validated by checking that each authenticated voter can cast only one vote and that the vote is recorded correctly without duplication or errors.
The IoT communication system is tested to confirm that voting data is transmitted securely to the cloud server without data loss or delay. Network stability and encryption are also verified.
Finally, overall system testing is performed to evaluate response time, accuracy, reliability, and error handling.

The results confirm that the system operates efficiently and meets the required security and performance standards.
1.Test fingerprint accuracy and authentication.
2. Validate one person–one vote functionality.
3. Verify correct vote recording and storage.
4. Check IoT data transmission and cloud connectivity.
5. Evaluate system performance and error handling.

VI. FUTURE SCOPE

1. Integration of advanced biometric technologies such as face recognition and iris scanning for enhanced security.
2. Implementation of blockchain technology to ensure tamper-proof and transparent voting records.
3. Development of remote and mobile voting systems to increase accessibility for users.
4. Enhancement of data encryption and cybersecurity measures to protect sensitive information.
5. Expansion of the system for large-scale national elections with improved scalability.
6. Use of Artificial Intelligence (AI) to detect fraudulent activities and unusual voting patterns.
7. Introduction of multi-language interfaces to make the system user-friendly for diverse populations.
8. Implementation of real-time monitoring dashboards for election authorities.

VII. CONCLUSION

The IoT-Based Fingerprint Voting System provides a secure, reliable, and efficient solution for modern voting challenges. By integrating biometric authentication with IoT technology, the system ensures that only authorized voters can cast their votes, thereby eliminating duplication and fraud.

The use of fingerprint recognition enhances accuracy in voter identification, while IoT enables real-time data transmission and faster result processing. The system reduces human errors, improves transparency, and ensures secure storage of voting data.

Overall, the proposed system is cost-effective, user-friendly, and suitable for implementation in various types of elections. It represents a significant step towards digital and secure voting, increasing trust and reliability in the electoral process.

ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802208

In conclusion, the IoT-Based Fingerprint Voting System offers a robust, secure, and efficient solution for conducting elections. With further improvements and proper security measures, it has the potential to revolutionize the voting process by making it more transparent, accurate, and accessible, thereby strengthening democratic practices in the digital era.

REFERENCES

1. Kumar and S. Raj, "IoT-Based Secure Voting System Using Fingerprint Authentication," International Journal of Advanced Research in Engineering and Technology, 2025.
2. P. Sharma et al., "Smart Biometric Voting System with IoT Integration," IEEE Access, 2025.
3. R. Karthik and V. Prakash, "Design of Fingerprint-Based Electronic Voting Machine Using IoT," International Journal of Scientific Research and Development, 2025.
4. Anushka Fase et al., "Fingerprint Based Voting System Using IoT," International Journal of Computer Science and Engineering, 2024.
5. H. Srilatha et al., "Fingerprint-Based Biometric Smart Electronic Voting System," E3S Web of Conferences, 2024.
6. J. K.Adiniyi, "Biometric-Based Cryptography for Secure Voting Systems," ScienceDirect, 2024.
7. Dr. M. Yuvaraju et al., "IoT-Based Voting System with Fingerprint Identification," International Educational Scientific Research Journal, 2023.
8. C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746
9. C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2
10. C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9
11. S.Tamilselvi, R.Prakash, C.Nagarajan,"Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller" Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025
12. S.Tamilselvi, R.Prakash, C.Nagarajan," Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance" Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
13. S.Thirunavukkarasu, C. Nagarajan, 2024, "Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
14. C. Nagarajan, M.Madheswaran and D.Ramasubramanian- 'Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model'- Acta Electrotechnica et Informatica Journal , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.
15. C.Nagarajan and M.Madheswaran - 'DSP Based Fuzzy Controller for Series Parallel Resonant converter'- Springer, Frontiers of Electrical and Electronic Engineering, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.
16. C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
17. C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
18. Suganthi Mullainathan, Ramesh Natarajan, "An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques", Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
19. M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
20. P. Sandeep et al., "EVM Through ID and Fingerprint Verification Using RFID," International Journal of Engineering Research & Technology (IJERT), 2023. IJERT

ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802208

21. Hanaf Hamran et al., "Design and Implementation of Secure Electronic Voting System Using Fingerprint Biometrics," Journal of Artificial Intelligence and Computing, 2023.
22. Zakiah Mohd Yusoff et al., "Fingerprint Biometric Voting Machine Using Internet of Things," Indonesian Journal of Electrical Engineering and Computer Science, 2023.
23. Keshika Manimaran et al., "Fingerprint Voting System with Results in Telegram Using IoT," Multidisciplinary Applied Research and Innovation Journal, 2023.
24. Lavanya N et al., "IoT Based Fingerprint Voting System," International Journal of Creative Research Thoughts (IJCRT), 2023.
25. Selvi, G. V., Anbarasan, A. B., Murthy, B. A., & Prabavathy, S. (2023). An Application Oriented Integrated Unequal Clustering Algorithm for Wireless Sensor Network. In *Underwater Vehicle Control and Communication Systems Based on Machine Learning Techniques* (pp. 140-154). CRC Press.
26. Mathew, A. (2021). Deep reinforcement learning for cybersecurity applications. *International Journal of Computer Science and Mobile Computing, 10(12), 32-38.*
27. Archana, R., & Anand, L. (2025). Residual u-net with Self-Attention based deep convolutional adaptive capsule network for liver cancer segmentation and classification. *Biomedical Signal Processing and Control, 105, 107665.*
28. Jagadeesh, S., & Sugumar, R. (2017). A Comparative study on Artificial Bee Colony with modified ABC algorithm. *European Journal of Applied Sciences, 9(5), 243-248.*
29. Rajasekar, M. (2024). Real-Time Predictive DevOps Intelligence for Risk-Aware Digital Business Processes in Cloud and SAP Ecosystems. *International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(4), 10713-10718.*