International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 05 | May - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Fingerprint-Based Biometric Smart Electronic Voting Machine Using IOT

Mr.B M CHANDRASHEKAR [1], SANJAY K U [2], RISHYANTH S M [3], PRAVALIKA K [4],

RAKSHITHA R [5]

2, 3 ,4 ,5 Student, Department of Electronics and Communication Engineering, Jyothy Institute of Technology Engineering College, Bengaluru, Karnataka

1 Asst. Professor, Department of Electronics and Communication Engineering, Jyothy Institute of Technology Engineering College, Bengaluru, Karnataka

ABSTRACT

A safe, open, and effective voting system is more crucial than ever in the current digital environment. Voter impersonation, ballot manipulation, and logistical problems plague traditional voting techniques including manual ballots and electronic voting machines (EVMs), particularly in rural or heavily populated areas. To address these issues, this project suggests an Internet of Things (IoT)-enabled smart electronic voting machine that uses fingerprint biometrics. Only eligible voters are permitted to cast ballots, and duplicate or unauthorized entries are prevented thanks to its exact voter authentication using fingerprint biometrics. In order to ensure integrity and dependability, the system includes a microcontroller, fingerprint sensor, LCD for user interface, and a secure Internet of Things module that permits encrypted, real-time vote transfer to centralized cloud databases.

With features like secure vote tallying, remote monitoring, and real-time administrative notifications, the voting system is improved by the incorporation of IoT technology. By overcoming obstacles related to geography and infrastructure, these capabilities guarantee effective operation in both urban and rural locations. Real-time result aggregation is made possible by cloud-based data storage, which also maintains system dependability and voter privacy. The approach is easily adaptable to institutional, local, or national elections since it is scalable. Robust encryption procedures strengthen public confidence by preventing manipulation and unwanted access. Additionally, by using less paper, the transition to digital operations encourages environmental sustainability, making the system both environmentally benign and technologically modern.This intelligent voting system is made to be easy to use, require little upkeep, and be deployed affordably. It sets a new standard for election security and accessibility by fusing secure IoT connection with biometric verification. The system provides a technically sound and socially meaningful solution in an effort to restore public confidence in democratic processes. It facilitates transparent operations and remote voting for a variety of demographics and geographical areas. It is flexible and scalable, making it appropriate for many kinds of elections. In an increasingly digital environment, this approach lays the groundwork for future political involvement by guaranteeing a safe, inclusive, and effective voting experience.

INTRODUCTION

Ensuring the efficiency and integrity of electoral procedures is essential to upholding democratic norms in the rapidly changing digital age. Voter impersonation, ballot tampering, human mistake, and logistical difficulties are enduring problems with traditional voting techniques, such as paper ballots and conventional electronic voting machines (EVMs), particularly in rural or densely populated locations. These issues have the potential to erode public confidence and compromise electoral fairness. The need to update electoral systems with safe, transparent, and effective digital solutions that can ensure correct vote counting, safeguard voter identity, and expedite election logistics for greater accessibility and inclusion is developing as a result of the rapid advancement of technology.

This project presents an Internet of Things (IoT)-enabled smart electronic voting mechanism that uses fingerprint biometrics. Enhancing voter authentication, preventing election fraud, and facilitating real-time voting process monitoring are its main goals. By preventing duplicate and unauthorized entries, the fingerprint biometric method guarantees that only eligible, registered voters may cast their ballots. A microprocessor, fingerprint sensor, LCD for user interaction, and a secure Internet of Things module that sends encrypted voting data make up this device. Every vote is safely captured and transmitted to a centralized cloud database, preserving data integrity and facilitating quick, accurate, and transparent election outcomes.

The technology works well for both urban and rural installations since IoT connectivity also enables secure

vote tallying, administrative notifications, and remote monitoring. Voter privacy is preserved while real-time result aggregation is guaranteed by cloud storage. The system is made to be easy to use, scalable, and economical. It also helps the environment by using less paper. In addition to increasing election accessibility and dependability, this creative solution opens the door for safe, inclusive digital voting in democracies in the future.

LITERATURE SURVEY

Recent studies have focused on using biometric technologies to improve voting system security, especially as fingerprint authentication gains popularity. Fingerprint biometrics are a dependable way to authenticate voters in electronic voting systems, as shown by Kumar et al. (2017), who showed that they greatly reduce voter impersonation and fraudulent voting [1].

The use of the Internet of Things (IoT) in electronic voting systems was also investigated by Zhang and Li (2019), who emphasized the IoT's capacity for safe transfer of vote data and real-time monitoring. According to their research, IoT integration improves election processes' efficiency and transparency by enabling remote vote tallying and administrative warnings [2].

Chen and Huang (2020) addressed data security by concentrating on encryption methods in voting frameworks offered by the Internet of Things. In order to avoid vote fraud and guarantee data integrity during transmission from voting machines to centralized servers, their study highlighted the significance of end-to-end encryption [3].

Singh et al. (2018) examined biometric voting machine user interface designs to improve usability and discovered that fingerprint sensors and user-friendly LCD screens boost voter accessibility and decrease errors, especially in rural or less tech-savvy communities [4].

The environmental advantages of switching from paper ballots to digital voting systems were also examined by Green and Walker (2021), who found significant decreases in carbon emissions and paper waste. Their results provide credence to biometric IoT voting systems' sustainability as a workable green substitute [5].

In line with the objectives of the current project, these research collectively offer a thorough foundation for creating a biometric smart voting system that is safe, effective, and easy to use when combined with IoT technology.

METHADOLOGY

A microcontroller at the heart of the system architecture controls every piece of hardware, including an LCD screen, an IoT connectivity module, and a fingerprint sensor. Voters first enter their fingerprint information into the safe database of the system. In order to verify identity, the fingerprint sensor takes a voter's fingerprint during voting and compares it with the records that are saved. The LCD interface is activated by the system upon verification, enabling the voter to choose their favorite candidate. By ensuring that only eligible voters cast ballots, this biometric verification successfully removes bogus or duplicate votes. Additionally, the microcontroller manages the data flow, synchronizing vote recording, biometric verification, and user input.

To ensure secrecy and integrity, the microcontroller encrypts the voting data using strong security protocols after a vote is cast. The IoT module subsequently sends the encrypted data to a central cloud server. To avoid interception or manipulation during transmission, this module makes use of secure communication channels like MQTT over TLS. Real-time vote logging is made possible by IoT connectivity, which increases election transparency and auditability. Administrators can also remotely check the status of the system and get notifications if anything seems off.

All votes are kept in an encrypted database on the cloud-based server, which ensures redundancy and guards against data loss. It provides accurate and timely tallying at the end of the election by aggregating vote results in real time. Because the system is scalable, it may be implemented in a variety of voting locations, including rural and remote ones, without compromising security or performance. Cost-effectiveness and ease of maintenance are encouraged by user-friendly interfaces and low hardware requirements. Overall, the approach improves election accessibility and integrity by combining biometric authentication with IoT-driven data security.

FLOW CHART

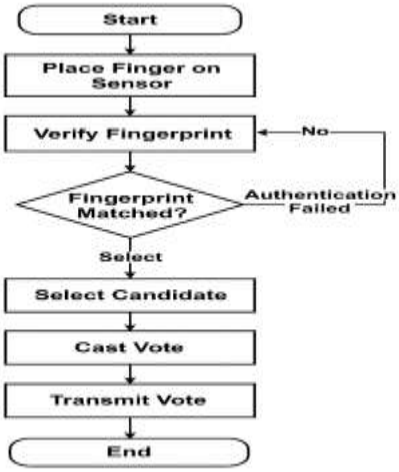

Fig.1: Fingerprint Voting Machine

The flowchart shows how a clever electronic voting machine that uses fingerprints operates. When the user touches the sensor with their finger, the system starts. After then, the fingerprint is checked against the database that has been registered. Authentication fails and the process restarts if the fingerprints do not match. In the event that the fingerprints match, the voter uses the voting interface to choose their favorite candidate. Following selection, an Internet of Things module securely casts the vote and sends it in real time to a centralized server. By ensuring that only verified voters cast ballots, this safe, automated procedure improves transparency and lowers the possibility of fraud.

BLOCK DIAGRAM

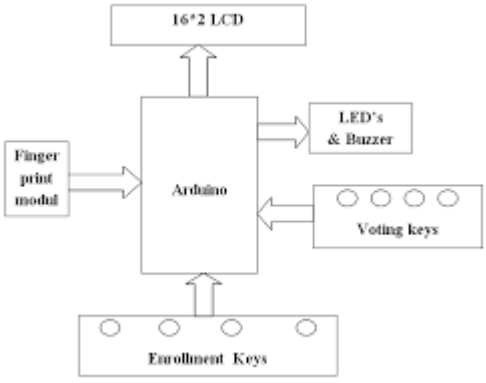

Fig 2:Fingerprint voting machine

The architecture of an Arduino microcontroller-based fingerprint-based electronic voting machine is shown in this block diagram. Voter authentication is done through the fingerprint module. After verification, the voter can choose their candidate by interacting with voting keys. New voters are registered in the system using enrollment keys. All inputs and outputs are managed by the Arduino, which serves as the main control unit. Throughout the procedure, instructions and status updates are displayed on a 16x2 LCD display. The user is guided by visual and aural feedback from LEDs and a buzzer. Through the use of electronic and biometric technology, this method guarantees safe, easy-to-use, and unchangeable voting.

HARDWARE COMPONENTS

1.Arduino uno:

Fig.3:Arduino uno

With its 14 digital input/output pins, operating at 5V, processing input from the fingerprint sensor, handling vote logic, and initiating data transmission, the Arduino Uno is an open-source microcontroller board based on the ATmega328P microchip. It is the brain of the biometric voting system, controlling the interaction between all hardware components, including the fingerprint sensor, LCD display, and IoT module. Its ease of use, affordability, and broad community support make it the perfect choice for embedded projects that need dependable control and quick development in systems like smart electronic voting machines.

2.Fingerprint Sensor:

Fig.4:Fingerprint Sensor

A biometric module called a fingerprint sensor takes a voter's fingerprint and confirms it in order to authenticate their identification. It is essential to this project's goal of limiting voting to authorized users. When a finger is placed on the sensor, it scans the fingerprint and transforms it into digital data that is compared to templates that have been recorded. The Arduino Uno grants access to the voting interface in the event that the match is successful. These sensors are renowned for their rapid response times and

exceptional accuracy. By drastically lowering threats like voter impersonation and duplicate voting, its adoption improves the security and dependability of electronic voting systems.

3.Push Button: After voter authentication, the push button is used as the manual input method for voting. It instructs the Arduino to record the vote when it is pressed. Reliability and seamless interaction with the voting system interface are guaranteed by its straightforward design.

4.LED: An LED serves as the system's visual indicator. By blinking in various patterns or colors, it can indicate successful fingerprint authentication, vote confirmation, or system faults. Users don't require written feedback to rapidly comprehend system status thanks to LEDs.

5.LCD Display: An interface for voter involvement is provided by the LCD display. It displays feedback, prompts, and instructions, such as the progress of a vote or fingerprint verification. This enhances usability and provides clear guidance for the voter at every stage of the procedure.

6.Buzzer: The buzzer gives the user auditory feedback. When a button is pressed, fingerprint authentication is completed, or there are any process failures, it beeps. This provides an additional communication layer that is particularly helpful for visually challenged people or in loud settings.

IMPLEMENTATION

Fig 5:Voting Machine

This project is an IoT-enabled smart electronic voting machine that uses fingerprint biometrics. Only registered voters will be able to cast ballots thanks to the fingerprint sensor voter authentication feature in the prototype. A user interface is provided via an LCD display to help the voter navigate the procedure. Blue indicator LEDs illuminate to verify selection, and three push buttons represent several candidates. Red LEDs are used to indicate errors and status. After fingerprint verification is complete, the voter uses the buttons to choose a candidate. The vote is registered and safely sent to a central database over the Internet of Things. This solution makes voting safe, unchangeable, and easy to use—perfect for community or institutional elections. It enables real-time vote data monitoring, enhances transparency, and guards against fraud.

RESULTS AND DISCUSSIONS

For increased security and transparency, this project offers a fingerprint-based biometric smart electronic voting system that is connected to the Internet of Things and WhatsApp API. Only registered voters can access the voting process thanks to the system's usage of a fingerprint sensor for voter authentication. The user can vote using designated push buttons for each candidate after successfully authenticating, with LEDs indicating selection and an LCD display directing the process. Following the vote, the system uses the Internet of Things to safely send the data to a central server. The voter's registered number also automatically receives a WhatsApp confirmation message, which acts as a receipt and security check. Through safe data processing and real-time communication, this feature promotes transparency, inhibits manipulation, and increases confidence.

Voter impersonation, duplicate voting, and a lack of real-time monitoring were among the major problems with traditional voting systems that were effectively resolved by the installation of the fingerprint-based biometric smart electronic voting machine. Following voter authentication using the fingerprint sensor, a push button was used to safely complete the voting procedure. The LCD display, LED indicator, and buzzer were then used for confirmation. After that, a real-time log of every legitimate vote was made.

Two significant outputs were produced by the system when the voting process was finished:

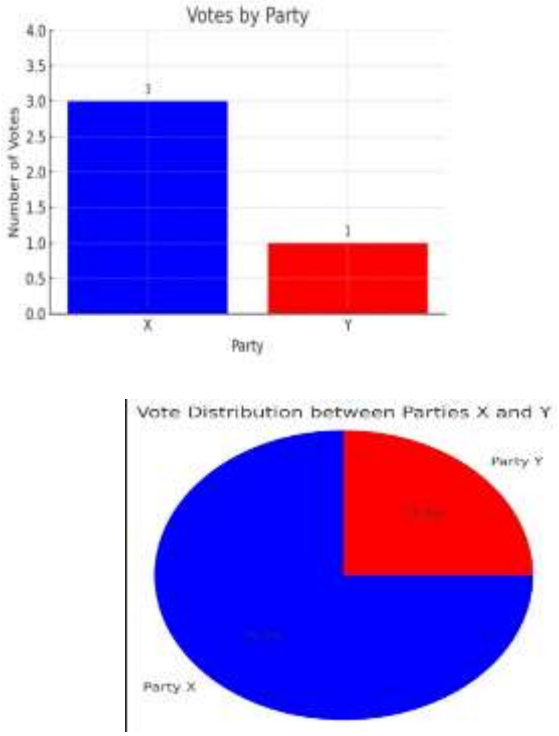

Fig 6&7:Bar graph of The result

1.A bar graph that displays the total number of votes cast for each candidate.

Fig 8:excel Sheet report

2.Voter IDs, voting status, and timestamp (if applicable) are presented in an Excel sheet report.

Because the bar graph offered a visual overview, administrators found it simple to examine the findings. This was accomplished by reading stored vote data and visualizing the total using Python's Matplotlib and Pandas tools. The openpyxl or xlsxwriter libraries in Python were used to create the Excel report, which provided a clear and shareable overview of the election procedure.

CONCLUSION

This initiative offers a dependable, safe, and cutting-edge technological answer to the problems with conventional voting systems. The solution eliminates the hazards of impersonation, multiple voting, and unauthorized access by combining fingerprint-based biometric authentication with Internet of Things technology to guarantee that only registered and confirmed voters are permitted to cast their ballots. The fingerprint sensor, LCD display, push button, LED indicators, and buzzer are among the hardware elements that can be effectively controlled by an Arduino Uno microcontroller. Every vote is safely recorded and unchangeable thanks to real-time encrypted data transmission via the IoT module to a centralized cloud-based server, greatly boosting election process trust.

The system is intended to be affordable, easy to use, and appropriate for implementation in a variety of contexts, ranging from municipal institutions to national elections. Additionally, by reducing reliance on paper votes, the use of digital components promotes environmental sustainability. Furthermore, tools like Excel report generation, bar graph visualization, and real-time vote counting enhance administrative effectiveness and transparency. Additionally, remote monitoring features guarantee that election officials may supervise the voting procedure even from a distance, facilitating prompt and well-informed decision-making.

All things considered, this biometric smart voting equipment that uses fingerprints redefines how elections can be held in the digital age. It offers a safe, flexible, and scalable platform that embraces automation and real-time data processing while maintaining the integrity of democratic systems. This study establishes a solid basis for upcoming developments in inclusive and safe electronic voting systems.

ACKNOWLEDGEMENT

With great appreciation, we would like to thank everyone who helped us construct this project, "Fingerprint-Based Biometric Smart Electronic Voting Machine using IoT." Our guide and faculty members deserve special recognition for their insightful comments, unwavering support, and knowledgeable direction, all of which greatly influenced the direction of this project. We also like to thank our college for providing the facilities and resources that were required. We would especially want to thank our friends and peers for their encouragement and helpful criticism. Finally, we would want to express our gratitude to our families for their unwavering support and understanding during this process. Their assistance was essential to this project's successful conclusion.

REFERENCES

1. Yusoff, Z. M., Yusnoor, Y., Markom, A. M., Nordin, S. A., & Ismail, N. (2024). *Fingerprint biometric voting machine using internet of things*. Indonesian Journal of Electrical Engineering and Computer Science, 30(2), 699–706. IJEECS
2. Al-jawaherry, M. A. (2018). *Arduino – Based Electronic Voting Machine*. Tikrit Journal of Pure Science, 23(10), 102–109. TJPSJ
3. Srilatha, C. H., Venigalla, D. C., Tuttagunta, S. K., Akshay, N., Adnan, M. M., Rajalakshmi, B., Thethi, H. P., & Kumar, A. (2024). *Fingerprint-based biometric smart electronic voting machine using IoT and advanced interdisciplinary approaches*. E3S Web of Conferences, 507, 01037. E3S Conferences+1E3S Conferences+1
4. Chatterjee, S., Jogalekar, I. S., & Lavanya, K. (2023). *E-Voting: Portable Fingerprint-Based Biometric Device for Elderly and Disabled People*. In Cyber-Physical System Solutions for Smart Cities (pp. 11). IGI Global. IGI Global
5. To'lqin o'g'li, J. S. (2024). *Application of IoT Tools in Fingerprint Voting System*. Modern Education and Development, 8(1), 352–363. Modern Education
6. Jatain, A., Arora, Y., Prasad, J., & Yadav, S. (2023). *Design and Development of Biometric Enabled Advanced Voting System*. International Journal of Innovative Research in Computer Science & Technology, 11(2), 45–52. ACS Publisher
7. Mukesh, R. A., Meena, M. L., Sasirekha, G., Selvameena, A., & Tt, T. (2019). *Finger Print Based Voting System Using Aadhaar Card*. International Journal of Engineering & Science Research, 9(3), 112–118.
8. Gupta, S., Jain, D., & Themalil, M. T. (2021). *Electronic Voting Mechanism using Microcontroller ATmega328P with Face Recognition*. In Proceedings of the 5th International Conference on Computing Methodologies and Communication (ICCMC), 1–6.E3S Conferences+1IJSRCEIT+1
9. Jagtap, A. M., Kesarkar, V., & Supekar, A. (2019). *Electronic Voting System using Biometrics, Raspberry Pi and TFT module*. In 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 1–5.
10. Kamble, P., Agawane, K., & Ingole, J. (2019). *Fingerprint based Electronic Voting Machine*. Journal of Analog and Digital Devices, 4, 25–30.E3S Conferences+1IJSRCEIT+1
11. Deepika, J., Kalaiselvi, S., Mahalakshmi, S., & Shifani, S. A. (2017). *Smart electronic voting system based on biometric identification survey*. In Third International Conference on Science Technology Engineering & Management (ICONSTEM), 1–4.E3S Conferences+1IJSRCEIT+1
12. Venugopal, S., & Rajan, R. R. (2020). *IoT-Based Voting Machine With Fingerprint Verification*. International Journal of Applied Engineering Research, 15(6), 623–628.IJSRCEIT+1E3S Conferences+1
13. Desai, M., Patoliya, J., & Mewada, H. (2020). *Internet of Things (IoT)-Based Advanced Voting Machine System Enhanced Using Low-Cost IoT Embedded Device and Cloud Platform*. In International Conference on Information and Communication Technology for Intelligent Systems, 1–6.E3S Conferences
14. Sharathchandra, S., Mathew, J. A., & Kumar, B. C. P. (2022). *IoT Based Fingerprint Voting System*. International Journal Of Creative Research Thoughts (IJCRT), 10(2), 789–795.E3S Conferences
15. Chakraborty, S., Singh, S. K., & Kumar, K. (2021). *Facial Biometric System for Recognition using Extended LGHP Algorithm on Raspberry Pi*. arXiv preprint arXiv:2101.03413. arXiv
16. Joshi, M., Mazumdar, B., & Dey, S. (2018). *Security Vulnerabilities Against Fingerprint Biometric System*. arXiv preprint arXiv:1805.07116. arXiv
17. Xiao, Y., He, Y., Zhang, X., Wang, Q., Xie, R., Sun, K., Xu, K., & Li, Q. (2024). *From Hardware Fingerprint to Access Token: Enhancing the Authentication on IoT Devices*. arXiv preprint arXiv:2403.15271. arXiv
18. Russo, A., Anta, A. F., Vasco, M. I. G., & Romano, S. P. (2021). *Chirotonia: A Scalable and Secure e-Voting Framework based on Blockchains and Linkable Ring Signatures*. arXiv preprint arXiv:2111.02257. arXiv
19. Patil, S., Bansal, A., Raina, U., Pujari, V., & Kumar, R. (2018). *E-smart voting system with secure data identification using cryptography*. In 2018 3rd International Conference for Convergence in Technology (I2CT), 1–4.SpringerLink
20. Naidu, P. R., Bolla, D. R., G, P., Harshini, S. S., Hegde, S. A., & Harsha, V. V. S. (2022). *E-voting system using blockchain and*

homomorphic encryption. In 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), 1–5.SpringerLink

21. Uddin, M. N., Ahmmed, S., Riton, I. A., & Islam, L. (2021). *A blockchain-based e-voting system applying time lock encryption*. In 2021 International Conference on Intelligent Technologies (CONIT), 1–6.SpringerLink
22. Dhinakaran, K., Raj, P. M. B. H., & Vinod, D. (2021). *Proposed Authentication Platform for E-Voting IoT System*. International Journal of Intelligent Systems and Applications in Engineering, 9(3), 2640–2645. IJISAE
23. Srikrishnaswetha, K., Kumar, S., & Mahmood, M. R. (2019). *A Study on Smart Electronics Voting Machine Using Face Recognition and Aadhar Verification with IoT*. Lecture Notes in Networks and Systems, 65, 87–95.IJISAE
24. Kanchana, S. (2018). *Fingerprint Based Biometric Authentication in IoT for Resolving Security Challenges*. International Journal of Research and Analytical Reviews, 5(4), 1000–1003.IJISAE
25. Altun, A. A., & Bilgin, M. (2011). *Web based secure e-voting system with fingerprint authentication*. Scientific Research and Essays, 6(12), 2494–2500.