IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

Biometric Voting System with Real-Time Vote Monitoring Using IoT

Mr. Ravi Kumar Dabas[1], Vatsal Gupta[2], Mukund Goel[3], Dhruv Gupta[4]
Assistant Professor, CSE-IoT[1]
Students, CSE-IoT[2-4]
Raj Kumar Goel Institute of Technology, Ghaziabad, India
ravikumardabas1@gmail.com, vatsalgupta6616@gmail.com,
mukundgo23122003@gmail.com, dhruvgupta2601@gmail.com

Abstract: *The conventional voting procedures have been known to have numerous problems ranging from identity frauds, duplicate voting, poor visibility, and delays in declaration of results. These problems can be attributed to inefficiencies in voter identification, poor security features, and inadequate monitoring systems. In the current era of rapid development of internet of things (IoT), embedded systems, and cloud computing, it is essential to come up with solutions to enhance automation and ensure secure transactions during elections. This article suggests biometric voting using real-time voting monitoring system. The system uses fingerprint technology integrated with IoT to provide a secure and reliable election process. The suggested solution involves using a fingerprint sensor to provide unique identification and authentication of the voters, hence eliminating multiple voting and unauthorized people from casting ballots. In addition, an ESP32 microcontroller provides the required processing power for voter identification, ballot casting, and communication of the results to the cloud server. After casting a vote, the results are uploaded in real-time to cloud servers such as Firebase, where they are immediately stored, processed, and presented in a visual format. In addition, IoT dashboard is used to provide real-time monitoring of the votes and instant publication of the results. Moreover, the suggested system ensures reduced human interference, less error rates, and increased precision and efficiency in the process of counting votes. The system is affordable, flexible, and applicable in both rural and urban settings. Overall, the system proves to be better than traditional voting techniques in terms of security, speed, and transparency.*

Keywords: Biometric Voting System, Fingerprint Authentication, Internet of Things (IoT), Real-Time Monitoring

I. INTRODUCTION

The process of voting forms an integral part of any democracy because it gives citizens a platform to voice their views and actively participate in the process of governance. Nevertheless, existing voting procedures like use of paper ballots and standard electronic voting machines (EVMs) suffer from certain setbacks such as impersonation, duplicate voting, non-transparent voting process, delay in declaring results among others. Such problems limit the credibility of election results. Moreover, manual checking and involvement of human beings in the process increases the possibility of frauds and mistakes.

Thanks to the developments in technology, there is a need for a better system of voting as modern technologies such as IoT, embedded systems and cloud computing continue to develop. One of the most reliable forms of identifying a person during voting is through biometrics, which involves use of individual's physical body traits that cannot easily be replicated. Several biometrics are available, but fingerprint recognition has become quite popular due to its efficiency, cost effectiveness and easy application. Combining biometrics with IoT technology can be a good way of improving the security and transparency of voting systems. IoT technology facilitates the instantaneous transfer of data, real-time

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

monitoring of processes, and visualizing the results, all of which make the voting procedure faster. Microcontrollers like ESP32 become an essential part of IoT systems because they enable communication between various hardware devices and the cloud platform. In this paper, a biometric voting system based on IoT technology and featuring the real-time monitoring of votes is suggested. For this purpose, a fingerprint sensor will be used to identify voters, ESP32 will be employed for processing data and communicating with other hardware devices, and a cloud-based database will monitor all the voting processes and store the results. The main goal of the system being designed is to prevent unauthorized voting, decrease the involvement of people in this procedure, and ensure the accuracy of the final results.

II. LITERATURE REVIEW AND RELATED WORK

Numerous researches have been carried out lately to make voting systems efficient and transparent with the help of advanced technologies. Both traditional systems and electronic voting machines (EVMs) were used in many countries for the voting process. But such voting systems are often connected with problems such as voter impersonation, errors made by humans, a lack of transparency, and delay in announcement of results. These challenges have encouraged researchers to look for ways to ensure voter identification and increase the safety of a voting process.

Biometric-based voting systems can be considered an innovative approach to solving this problem as they use different types of physiological features of a voter in order to identify him/her. There are a lot of biometric parameters which can be taken into account to create a system. Fingerprint-based voting is the most common approach among researchers because of its efficiency, lower costs, and easiness. Researchers claim that fingerprinting with a microcontroller eliminates the risk of duplicate voting. Automation has a major part in such systems.

Apart from the use of biometric identification methods, the incorporation of IoT technology has increased the potential of modern voting systems. Voting systems incorporating IoT technologies have enabled users to transmit data real-time, remotely monitor the voting process, and visualize results using cloud platforms. Several proposed models rely on microcontrollers, like Arduino and ESP32, to transmit voting information to cloud databases for faster and better management. Furthermore, these voting systems incorporate real-time remote access capability, giving authorities the ability to monitor voting events remotely.

However, current voting systems have several shortcomings that make them less effective in some situations. One of the limitations of the current voting systems is their reliance on the availability of internet connectivity, which may be a problem in rural settings. Issues relating to the security, privacy, and scalability of some voting systems have not been properly addressed in many cases. In addition, several proposed voting systems are complicated and lack real-time voting monitoring capabilities. The paper introduces an IoT biometric voting system.

III. METHODOLOGY

The working of the proposed biometric voting system can be explained through the following steps:

1. Voter Authentication:

The voter places their finger on the R307 fingerprint sensor. The sensor captures the fingerprint and sends it to the ESP32 microcontroller for verification. If the fingerprint matches with the stored database, the voter is authenticated. A green LED indication is given for successful authentication, while a red LED and buzzer alert indicate invalid access.

Fig. 1: R307 Fingerprint Sensor Module

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

2. Display of Instructions:

On being successfully authenticated, the I2C LCD displays clear messages on how to go about the voting process. Such messages include "Select your vote" and "Choose candidate." By doing this, it becomes easier to use the device as the instructions become clear to users, both beginners and non-technical users alike.

Fig. 2: I2C LCD Display

3. Vote Casting:

The voter selects a candidate by pressing the corresponding push button. Each button represents a specific party or candidate.

Fig. 3: Push Buttons

4. Vote Confirmation:

Once the vote is cast, the system confirms the selection. The I2C display shows a confirmation message like "Vote Recorded Successfully." A short buzzer beep and green LED indication are used to confirm successful vote submission.

5. Vote Processing:

The ESP32 processes the input and ensures that each authenticated voter can cast only one vote. Duplicate voting is prevented by checking fingerprint records.

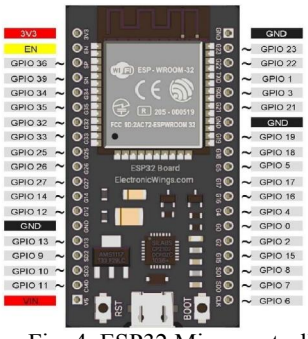

Fig. 4: ESP32 Microcontroller

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

6. Data Transmission:

The recorded vote is transmitted to a cloud-based database using the ESP32's built-in Wi-Fi module.

7. Data Storage:

The vote is stored in a real-time database such as Firebase, where the vote count is updated instantly for the selected candidate.

8. Real-Time Monitoring:

The updated voting results are displayed on an IoT dashboard, allowing real-time monitoring of vote counts for each party.

9. System Feedback and Security:

Throughout the process, LEDs, buzzer, and display provide continuous feedback to the user. The system ensures secure, accurate, and transparent voting with minimal human intervention.

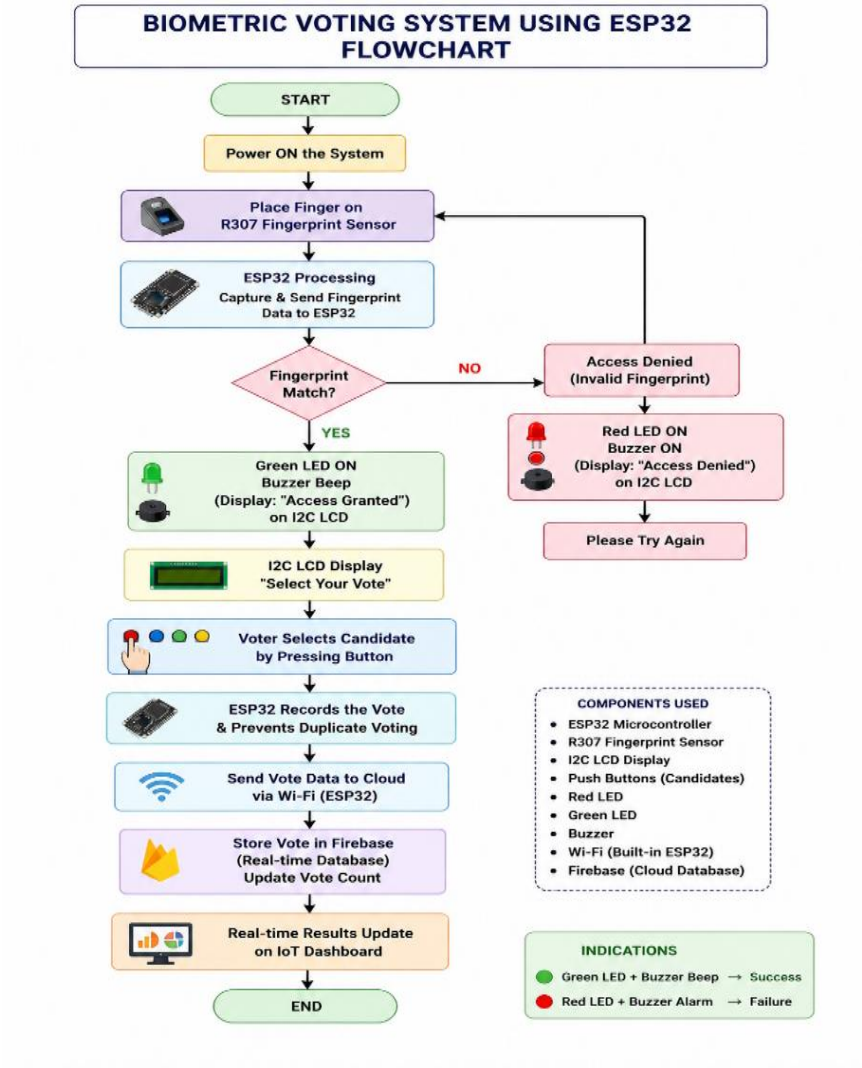

Fig. 5: Flowchart of Biometric Voting System

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

IV. RESULTS

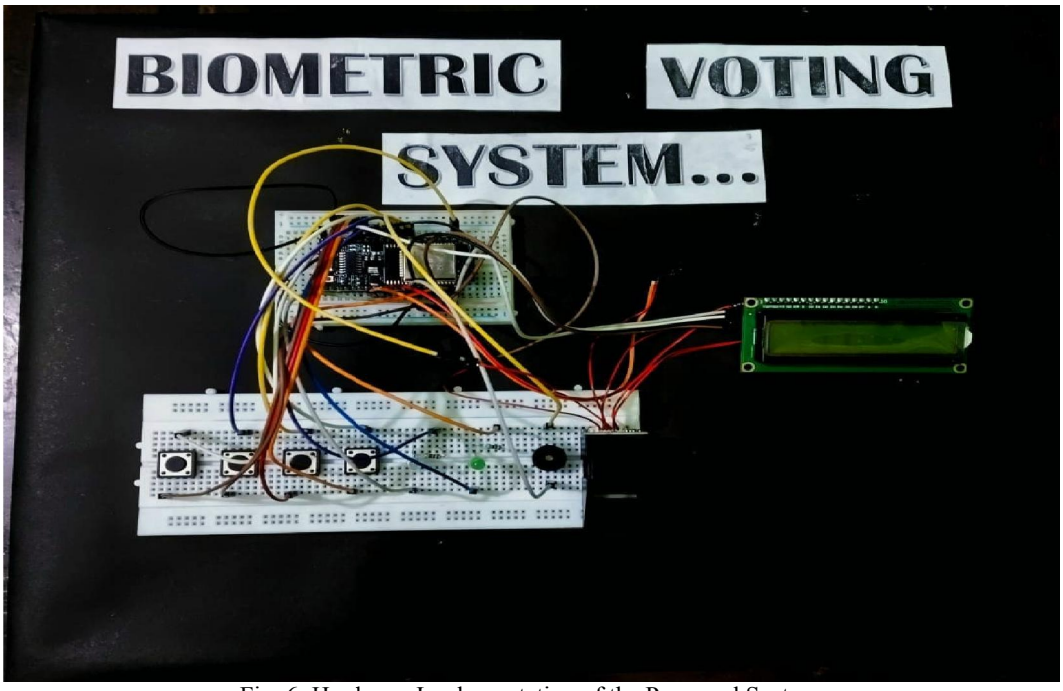

Fig. 6: Hardware Implementation of the Proposed System

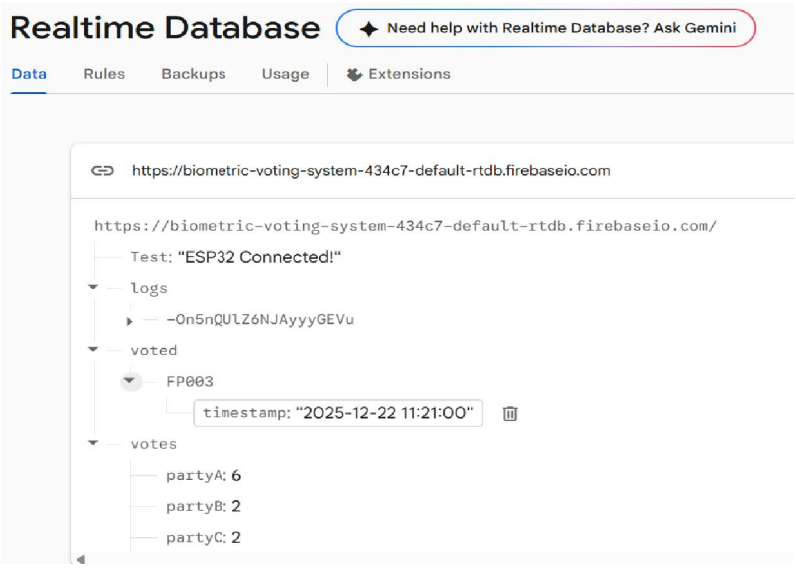

Fig. 7: Firebase Realtime Database Showing Voting Data

V. DISCUSSION

The results derived from the use of the developed biometric voting system show that it is effective and guarantees a safe, reliable, and efficient voting mechanism. The use of fingerprint authentication in the system ensures that all

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

registered users who can cast their votes are the same and there will be no instances of voting frauds. The use of R307 Fingerprint sensor provides high-quality and reliable identification of voters.

The incorporation of the ESP32 microcontroller makes it possible to make communication between various hardware parts and cloud services smooth. As it was shown in the result part, voting information is instantly transmitted to Firebase Real-time database without any difficulties. This means that counting of votes is instantaneous and there is no necessity for conducting manual vote counting.

In addition, the system has some components like I2C LCD, LEDs, and buzzer that increase user interaction and make it easy for the voter to interact with the device and perform voting procedures. Moreover, the IoT-enabled dashboard supports remote monitoring of the voting statistics, making it transparent and allowing the authorities to manage the voting process easily.

However, this system does have some weaknesses. Firstly, it requires an active internet connection to transmit the data instantly, which can be difficult in some remote locations. Secondly, proper management is required to ensure data security and privacy while working with cloud platforms. Nevertheless, compared to traditional methods, this system provides remarkable benefits in terms of precision and efficiency.

VI. CONCLUSION

The implementation of biometric voting using fingerprint verification and Internet of Things (IoT) offers an effective solution to modern voting applications in terms of security and efficiency. In particular, the proposed system manages to solve critical issues related to traditional voting, such as identity theft and duplication of votes. In addition, it enables quick and accurate result declaration thanks to the use of the R307 fingerprint sensor. The important function of the ESP32 microcontroller is associated with processing the information provided by voters and establishing communication between a device and a cloud-based database via the Internet. Firebase provides an opportunity to instantly store and modify voting data; therefore, it helps avoid the manual collection and counting of votes. Moreover, additional components like I2C LCD display, LEDs, and a buzzer allow the user to have better control over the whole procedure.

Overall, the proposed voting system appears to be efficient, inexpensive, and easily deployable to different environments from small communities to larger organizations. Thus, based on the research results, the system can help enhance the security of digital elections, reduce the level of human involvement, and improve the speed of result declaration.

VII. FUTURE SCOPE

The suggested biometric voting system proves itself to be a reliable and effective way of conducting safe voting procedures; however, there is still much room left for improvement and additional development. Further developments can concentrate on improving scalability, security, and usability of the project in a real-life setting. One of the main directions of development could be the incorporation of Aadhaar identity cards into the system to ensure that voters cannot duplicate their identity and vote several times. Furthermore, additional measures could be taken concerning the security of data transmissions from the ESP32 to the cloud database through the use of advanced encryption methods. Improvement of the system could involve development of a special mobile application for monitoring purposes of authorized people. The introduction of blockchain technologies can significantly enhance the security level of the voting process and make it highly transparent and reliable.

Other possible developments include conducting state or even national-level voting events using this software or even deploying this system in offline mode without relying on the Internet. All in all, with all these developments, the system will become even more advanced, secure, and scalable for contemporary online voting systems.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, Jan. 2004, doi: 10.1109/TCSVT.2003.818349.
[2] A. K. Jain, P. Flynn, and A. A. Ross, Handbook of Biometrics. New York, NY, USA: Springer, 2008.
[3] D. Chaum, "Secret-Ballot Receipts: True Voter-Verifiable Elections," IEEE Security & Privacy, vol. 2, no. 1, pp. 38–47, Jan.–Feb. 2004, doi: 10.1109/MSECP.2004.1264852.
[4] R. L. Rivest, "On the Notion of 'Software Independence' in Voting Systems," Philosophical Transactions of the Royal Society A, vol. 366, no. 1881, pp. 3759–3767, Oct. 2008.
[5] H. Al-Ameen, S. Talab, and M. Alarabiat, "Electronic Voting Systems Evaluation: Requirements and Evaluation Procedures," International Journal of Advanced Computer Science and Applications, vol. 4, no. 7, pp. 1–9, 2013.
[6] N. Kshetri and J. Voas, "Blockchain-Enabled E-Voting," IEEE Software, vol. 35, no. 4, pp. 95–99, Jul./Aug. 2018, doi: 10.1109/MS.2018.2801546.
[7] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.
[8] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A Literature Review," Journal of Computer and Communications, vol. 3, no. 5, pp. 164-173, May 2015.
[9] K. Ashton, "That 'Internet of Things' Thing," RFID Journal, vol. 22, no. 7, pp. 97-114, 2009.
[10] Espressif Systems, "ESP32 Technical Reference Manual," Espressif Systems, Shanghai, China, 2020.
[11] Espressif Systems, "ESP32 Datasheet," Espressif Systems, 2021.
[12] Adafruit Industries, "R307 Fingerprint Sensor Datasheet," 2018.
[13] Google, "Firebase Realtime Database Documentation," 2023. [Online]. Available: https://firebase.google.com/docs/database
[14] Blynk Inc., "Blynk IoT Platform Documentation," 2023. [Online]. Available: https://docs.blynk.io
[15] Arduino, "Arduino IDE Documentation," 2023. [Online]. Available: https://www.arduino.cc/en/software
[16] M. A. Ferrag, L. Maglaras, H. Janicke, and J. Jiang, "A Survey on Security Challenges in IoT-Based Systems," IEEE Access, vol. 8, pp. 191-204, 2020, doi: 10.1109/ACCESS.2020.2965686.
[17] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[18] J. Bonneau et al., "SoK: Research Perspectives and Challenges for Internet Voting," IEEE Symposium on Security and Privacy, pp. 1-15, 2012.
[19] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, "Analysis of an Electronic Voting System," IEEE Symposium on Security and Privacy, pp. 27-40, 2004.
[20] A. K. Das, "A Secure and Robust Biometric-Based Authentication Scheme," IEEE Transactions on Information Forensics and Security, vol 12, no. 12, pp. 1–15, Dec. 2017.