AN ESP 32 BASED RFID AUTHENTICATION USING ELECTRONIC VOTING SYSTEM WITH FINGERPRINT

Mrs. K. Dhivya[1], Safrin Banu A[2], Saranya R[3]

[1]Electronics and Communication Engineering, IFET College of Engineering, Gangarampalayam, Tamil Nadu
Email: k.dhivya91@gmail.com

[2]Electronics and Communication Engineering, IFET College of Engineering, Gangarampalayam, Tamil Nadu
Email: safrinbanu013@gmail.com

[3]Electronics and Communication Engineering, IFET College of Engineering, Gangarampalayam, Tamil Nadu
Email: saranyaece2026@gmail.com

ABSTRACT

Putting in a digital voting setup can really help make elections better, like cutting down on mistakes in voting and making the whole thing run smoother. But the old-school polling spots and even some basic electronic ones still have issues, stuff like people pretending to be someone else or voting twice, or just messing with things by hand that could change who wins. So this project I am thinking about uses an ESP32 microcontroller along with fingerprint stuff and RFID to check who voters are and stop anyone from voting more than once. The way it works is with two kinds of checks for people: one is the fingerprint scan, which is biometric, and the other is RFID for ID, so voting feels quick and safe, I guess. The ESP32 handles identifying users, letting them vote, and then reporting out the results because it is good at that. Voters start by using either the RFID card or the fingerprint to get recognized. Once it approves them, they can push a button for their pick of candidate. The screen on the LCD shows what is going on with the system and the vote tallies. What is nice is that it makes sure nobody can copy someone else's vote or throw in a fake one, since it matches your info to the database right before you vote. If they try to hit the button more than once or screw it up, a buzzer goes off and they lose the chance to vote that time. Then there is the GSM module that sends out how many votes are left and warns the election people if something seems off, which helps with keeping things open and watched. Adding the LM317 voltage regulator gives steadier power, so the whole unit runs more reliably and safely. It seems like a good, secure, and cheap way to do voting for smaller things, you know, like picking student council at school or club leaders, or even local reps in town. This part gets a bit messy explaining the tech, but I think it covers the main idea without too much complication.

Keywords: Electronic Voting System, Fingerprint Authentication, RFID Technology, ESP32 Microcontroller, Biometric Security, GSM Module, Embedded Systems, Secure Voting.

How to cite this article: Dhivya K, Safrin Banu A, Saranya R. An ESP 32 Based RFID Authentication Using Electronic Voting System with Fingerprint. Int J Drug Deliv Technol. 2026;16(52s): 1187-1193. DOI: 10.25258/ijddt.16.52s.153

Source of support: Nil.

Conflict of interest: None.

I.INTRODUCTION

Information technology and embedded systems have played a role in the technological development of democracy elections worldwide.Voting is the most important thing about democracy; that's why our job is to keep the votes safe, clean, and fair. Voters are a waste of people's and people's time; they can be rigged with ballot stuffing and voter impersonation. Although electronic voting is much easier for the voters than paper voting, it still has some disadvantages, like hacking, vote rigging, multiple votes, etc., so it would not be a fair election for everyone. Due to the requirement for secure, automated validation mechanisms, biometric authentication systems have become prevalent as reliable identification tools. Because it is singular, straightforward, and economical, fingerprint recognition is the most popular biometric method. However, dependence on a single authentication system presents risks, including identity theft or deception. This approach addresses these

issues by providing fingerprint-based validation while offering RFID identification as an alternative primary authentication method, thereby preventing unauthorized access. However, it is a reliable online voting system that incorporates fingerprint and RFID identification functionalities, interfaced with an ESP32 microcontroller. A second rationale for selecting The ESP32 microcontroller acts as the main contr IJDDT, Volume 16 Issue 52s, 2026

ol unit that manages this project is its proven resilience, low power consumption, and inclusion of communication modules, which are essential hardware components for embedded systems, particularly those intended for real-time operations. Because with this, they will not be able to impersonate voters or be able to vote twice because they will always verify twice before voting. The voting system concept is simple, and it's not just as simple as pushing the button and LCD module to display the system's instruction and the voting result. Furthermore, to ensure integrity and security, a GSM module is integrated to provide real-time updates to electoral authorities regarding voting metrics and outcomes. In this scenario the buzzer goes off, and the election is nullified, as not one vote has been rigged .This project aims to develop a safe, easy-to-use, and flexible online voting system for users that reduces human contact and enhances voter confidence. This would be great for small elections like the ones they have in school, work, and city hall. Implementing a voting system with biometric identification, automation, and communication technology presents a feasible solution for establishing a more efficient and accessible electoral process.

II.LITERATURE SURVEY

Satyanarayana et al. developed a biometric electronic voting system where fingerprint authentication was carried out to check impersonation in elections. Though the proposed Electronic Voting System enhanced accuracy and security in voting, it was vulnerable to spoofing, as it involved authentication by fingerprints alone without making use of a second factor authentication method [1].

Bhargavi et al. proposed a secured electronic voting system that utilized fingerprint authentication along with GSM-SMS voting notifications. Although the proposed Electronic Voting System increased transparency as it notified the concerned about the voting activities, it did not support scalability and real-time monitoring for large-size electoral lists [2].

Ismail et al. proposed an electronic voting system that utilized smart card authentication and fingerprint verification for a dual-layer secure authentication process by using smart cards (MyKad) and fingerprint authentication. Although this work increased the reliability of voter authentication, relying on smart cards made the voting system more complex in terms of maintenance [3].

Poudel et al. proposed an electronic voting system that used blockchain technology for secure validation of voter identity authentication. The voting system provided better protection for its data integrity; however, its complexity made it inefficient for a small voting process [4].

A fingerprint-based IoT electronic voting system was designed by Wibowo et al. using ESP32 microcontroller technology. They achieved higher efficiency and less human involvement but did not consider the provision of real-time notifications to prevent illegal voting activities [5].

Sandeep et al. designed an election voting system using the concepts of RFID and fingerprint to avoid voting fraud and duplication. Since the voting system is accurate in terms of authentication, it could not offer the facility of remote notifications [6].

Poduval et al. developed a modern and improved electronic voting system emphasizing secure voting and rapid vote processing. It increased user-friendliness. At that time, it did not use biometric verification. This is because the system could not effectively resist impersonation attacks [7].

Syed et al. designed a hybrid biometric electronic voting system that combined fingerprint and facial verification. As a result, it possessed enhanced verification accuracy. This increased the processing and hardware requirements of the system [8].

Kale et al. designed an electronic voting machine based on biometrics using fingerprint sensors to prevent unauthorized usage. The design improved election security, although it did not incorporate reporting modules for monitoring processes [9].

A literature study performed by Khasawneh et al. assessed diverse systems of e-voting, pointing out that systems with biometric capabilities are far more secure than other systems, but that scalability and costs are still some concern [10].

Gurav et al. developed an IoT-based fingerprint voting system that allows remote monitoring of the voting process. Though the proposed method was more accessible, the approach was deficient in the prevention of multiple voting in disparate polling units for both candidates in the election process through polling units [11].

Simts issued a survey on the secured voting system constructed through fingerprint scanning devices, highlighting the effectiveness of biometrics but noting the difficulties in the management of fingerprint data [12].

Karthikeyan et al. designed a secured electronic voting machine with biometric authentication to eliminate human intervention. The result was increased security in elections, but it lacks alert systems using GSM and/or IoT technology [13].

Arinze et al. designed an RFID process automation for a voting process with transparency, and it improved the process speed for voter recognition. The lack of biometric authentication affects safety [14].

A smart voting system was designed using Arduino for distance voting control. The project made voting easier but was vulnerable to unauthorized access attacks due to the lack of two-factor authentication in the voting system [15].

There was much research on voting systems that used GSM technology for voting confirmation notifications via SMS but were vulnerable to attacks since they applied one-factor authentications [16].

Further study conducted by Sharma et al. showed that fingerprint-based voting systems have been made more secure against impersonation and unauthorized voting, focusing on unique identification of voters, although it utilized single-factor authentication, which made it vulnerable to spoofing attacks [17].

Patel et al. analyzed multi-factor authentication schemes for electronic voting systems. They found that the combination of biometrics and other methods like RFID or smart cards can dramatically improve the security of these systems but increase the system complexity too [18].

A GSM technology-based e-voting system capable of delivering real-time alert notifications as well as the status of the votes to the election authorities has been conceptualized by Kumar et al. The disadvantages in the system are the absence of biometric validation on the voters' side [19].

Rao et al. have created a voting framework using embedded control, targeting the automation process within vote casting and storage. While the work showed stable performance, the framework lacked the incorporation of communication mechanisms and authentication levels [20].

III.PROPOSED SYSTEM

The discussed project introduces a Fingerprint-Based Smart Electronic Voting System, which will help in conducting the voting process in a secured, reliable, accurate, and fraudulent way by using fingerprint verification, RFID verification, and Embedded Control. The prime aim of this project is to avoid impersonation in the election process ensure there are no repeated votes, and make the election process less manual.

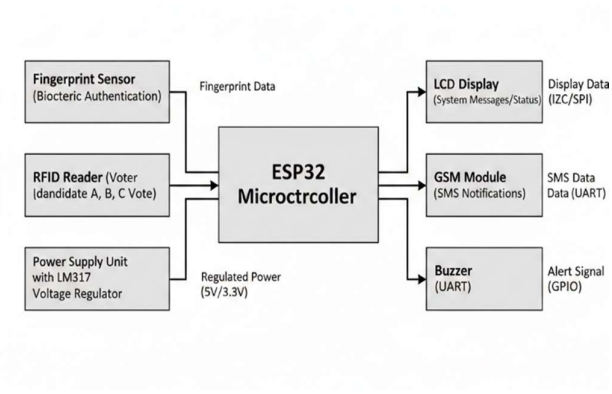

Figure 3.1. System Architecture of the Fingerprint-Based Smart Electronic Voting System

The ESP32 microcontroller is used as the control unit that interacts with various authentication, input, and output devices. The use of an RFID reader and fingerprint scanner entails a twofold authentication process, which confirms the authenticity of the voters before allowing them to cast their votes. Push buttons are used as the voting channels that allow the voter to pick her/his preferred candidate. The LCD screen displays real-time messages of the system and voting procedures to the user. A GSM module is incorporated to send notifications of the voting process status to the election officials. A buzzer is used in situations where there may be unauthorized access and repeated voting. A power supply made by the voltage regulator LM317 regulates the entire system and promotes the stability of all hardware components.The design is anchored on an ESP32 microcontroller that acts as a central processing unit because of its processing power, low power consumption, and communication capabilities. The ESP32 module is responsible for all the operations performed within the electoral voting platform, such as voting authentication, casting votes, notification generation, and connecting with other components. A two-factor authentication process is integrated for better security. First, authentication is done by identifying a voter through his/her RFID card for verification of a voter's registration information. After a successful RFID verification process, fingerprint authentication is carried out by scanning a fingerprint to match with a stored biometric template.

Only after both stages of authentication are accomplished can the voter cast his vote. Voting is done by the use of push buttons labeled for each candidate. The casting vote is accurately stored in the system memory, and the voter status is updated to avoid any other voting attempts. A 16×2 LCD display is used to display the system messages related to the authentication of the voters and the voting procedure.

For increased transparency and monitoring purposes, there is the addition of the GSM module in the system for real-time alerting or voting status updates to the election authorities. In cases of illegal access attempts or invalid credentials as well as multiple voting attempts, the system automatically declines the process while activating the buzzer alert for early detection of fraudulent activities. Finally, there is the use of the regulated power supply mechanism based on the voltage regulator, LM317, for the supply of stable voltages to the various hardware components of the system for continuous functionality.

The system is ideal, as it is cost-effective with the ability to be scaled up to suit small election processes like those conducted in learning institutions, organizations, or local governing bodies. Biometric security, intelligence embedding, and communications combined offer a viable method to provide secure voting through modern electronics.

IV.METHODOLOGY

The methodical process of the proposed fingerprint-based smart electronic voting system can be divided into a series of operational steps to ensure secure authentication, effective voting process execution, and efficient system monitoring. Every step is designed to contain minimal human intervention to ensure system security.

A.System Initialization

In this first phase, the ESP32 microcontroller is responsible for initializing all hardware components that are connected to the module, such as the fingerprint reader, RFID reader, GSM module, LCD display module, push buttons, and buzzer module. The RFID reader is loaded with a database of registered voters that contains RFID and fingerprint codes for authentication of voters once the voting process is ready and ready to start, as indicated by the display on the LCD module.

B. RFID-Based Voter Identification

When the voter comes to the system, his/her RFID reader is read by the RFID reader. The RFID details scanned

are sent to ESP32. The ESP32 compares those scanned RFID details with the storage database. If those RFID details are correct and weren't previously used, then the voter will proceed to the next authentication process for the voting system. The buzzer alert for invalid RFID details is activated for a voter.

C. Fingerprint Authentication

Upon successful RFID verification, the voter is asked to touch his or her finger onto the fingerprint scanner. The captured image of the fingerprint is processed, and it's compared with the existing fingerprint template for the captured RFID. Upon successful matching, the voter is authenticated. However, any difference will result in the rejection of the vote along with the activation of the alert.

D. Vote-Casting Process

After the two-factor authentication process is over, the system permits the voting interface to be activated. The voter casts a vote by depressing the push button associated with the liked candidate. The ESP32 module records the vote, and the status of the voter is changed to prevent the possibility of the voter casting repeated votes. A message appears on the LCD indicating the successful recording of the vote.

e. Alert and Notification Mechanism

In the event of unauthorized access, duplicate votes, or authentication failure, the buzzer is activated to respond immediately. Moreover, the GSM module has the ability to send alerts or vote update notifications to the election commission to monitor remotely.

F. System Reset and Standby Mode

After casting votes, it resets the authentication session and goes back into standby mode. This makes it possible to have continuous operation during an election.

V.PROPOSED METHOD

The fingerprint-based smart electronic voting system is a combination of all necessary hardware elements, devices, and factors that make voting safe and secure through authentication and real-time monitoring. Each one of them has a distinct and significant role in ensuring the accuracy and stability of the whole system.

1.ESP32 Microcontroller

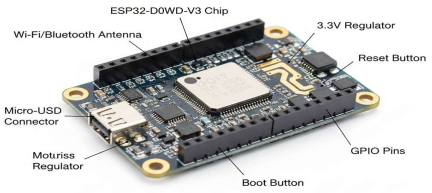

Figure5.1 ESP32 Microcontroller

The ESP32 is the microcontroller that functions as the central processing and controlling circuit within the voting system. ESP32 has all the characteristics of the highly perceptible embedded processor within the context of e-voting systems that are characterized by high processing speed, reduced power consumption, and on-chip communication.

2. Fingerprint Sensor

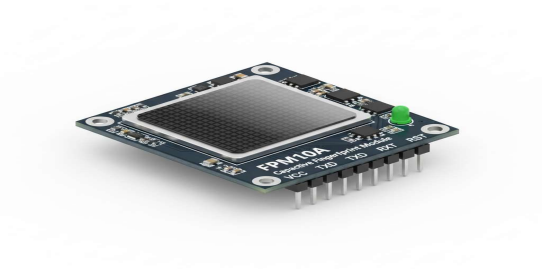

Figure 5.2 Fingerprint Sensor

The fingerprint sensor will be utilized in performing biometric authentication of voters. The sensor takes a snapshot of a voter's fingerprints and then proceeds to match them with existing fingerprints. This is because it has been reported that each person has unique fingerprints. It, therefore, plays a critical role in preventing vote impersonation.

3. RFID Reader & RFID Tags

Figure5.3 RFID Reader & RFID Tags

The RFID reader helps in voter identification by using an RFID card/tag, which has been allotted to registered voters. The RFID tag has a unique identification number, which has to be confirmed before enabling biometric authentication. This provides an extra level of security during the voting process.

4. Push Buttons

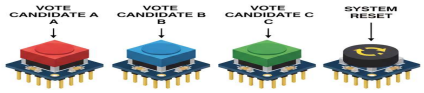

Figure 5.4 Push Buttons

The push buttons serve as the voting interface through which the votecasters can vote by clicking on the name of one of the candidates. Every push button is linked to a particular candidate. After a click, the corresponding vote is registered by the ESP32, and the input is disabled for the votecaster.

5. LCD Display (16×2)

Figure 5.5 LCD Display(16×2) Push Buttons

The LCD module offers a friendly interface for users by displaying system messages, authentication messages, voting instructions, and confirmation messages.

6. GSM Module

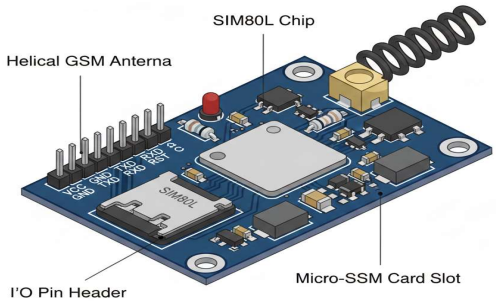

Figure 5.6 GSM Module

The GSM module enables the sending of real-time notification and alert services to the election body or the relevant authority. These include but are not limited to voting success, status alerts, and efforts to prevent unauthorized access.

7. Buzzer

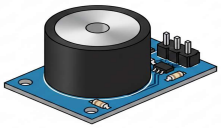

Figure 5.7 Buzzer

The buzzer act as alerting system and to warning and also indicate unauthorized entry, no authentic entry, or frequent voting. It makes an instant sound in case of any suspicious.

8. Power Supply Unit (LM317 Voltage Regulator)

The regulated power supply with the use of the voltage regulator LM317 is meant to ensure that the voltage to all hardware components remains stable and consistent.

VI.RESULT AND DISCUSSION

The fingerprint-based smart e-voting system designed using fingerprinting was experimented with in various settings to test its functionality and security capabilities. The experimental setting included a small election scenario with various voters and candidates. The system's performance was analyzed on various parameters such as accuracy in authentication, speed of response, system stability, and ability to resist fraud.

During the testing process, the method accuracy of the dual-authentication process that used the RFID method coupled with fingerprinting was high in determining the identity of the voters. Genuine voters were authenticated, while others who were not authorized and unregistered RFID cards were barred from access. The fingerprint reader exhibited correct matching features with low rejection rates. Duplicate voting was eliminated through the change of status of the voters whenever votes were cast.

The voting procedure was observed to be simple to use. The voters were able to perform the authentication process and cast their vote within a short period of time. The push-button voting system responded well to the input commands given to the system, and the votes were registered correctly without loss of information. The messages displayed on the LCD were very helpful to the voters.

The alert and notification systems are functioning as expected. Every time there was an invalid authentication and repeated vote attempts, the buzzer was switched on instantaneously, giving an instant response. Conversely, the GSM module was very effective in sending alert notification messages and vote status messages to the election authority.

As far as the stability of the system and the performance of the ESP32 microcontroller are concerned, there were neither pauses nor crashes in the processings related to the authentication as well as the voting. This became possible due to the stable voltage supply provided by the LM317 voltage regulator.

On the whole, the experimental outcome confirms that the proposed system is efficient in maintaining voting security, minimizing human interventions, and providing secure vote records. Since the above explanation puts forward the necessity of incorporating biometric verification along with embedded control and communication modules, this leads to an efficient method for secure e-voting systems in small-scale settings.

VII.CONCLUSION

The project successfully demonstrate the fingerprint based smart electronic voting system is design and developed to improve security ,reliability and transparency associate with overall election process. The implementation of fingerprint scan identify techniques coupled with the RFID recognition process makes the proposed system free from impersonation as well as repeated voting. The microcontroller ESP - 32 work as main processing system controlling unit in this entire process to handle the entire authentication process, vote registration, alert activation, and communication process effectively.

The voting interface is very simple and user-friendly and designed with the help of push buttons and LCD displays, and it will allow the voters to vote in a very confident manner. The addition of the GSM module for notifications and alerts will improve the voting monitoring process since the authorities will get notifications instantly about the voting and unauthorized attempt events. The power supply part will ensure that the system works properly during the whole voting process with the help of the voltage regulator LM317.

Experimentation has shown that the designed system produces effective results with a high degree of authentication accuracy, short response time, and reliable vote recording performance. It also detects fraud and prevents it, and the entire system reduces manual interference and human error. The cost-effective nature of its design and a modular architecture further make it very apt for small-scale elections conducted in educational institutions, organizations, and local governing bodies.

Although the proposed system achieves its intended objectives, a number of enhancements could be considered for future development: cloud-based storage for data enables vote management from a central location and provides access to data of elections from a distance. Also, the system can be extended to face recognition or other additional biometric modalities to further strengthen multi-factor authentication, while mobile or web-based applications may be developed to enable real-time monitoring dashboards of election authorities.

The integrity and transparency required for large-scale election data could be improved using encrypting methods and blockchain systems. In addition to these improvements, future improvements to the system include scalability using several election terminals located in connected secure networks. This will improve system robustness and usability in a large-scale election setting.

The fingerprint-based smart e-voting system designed using fingerprinting was experimented with in various settings to test its functionality and security capabilities. The experimental setting included a small election scenario with various voters and candidates. The system's performance was analyzed on various parameters such as accuracy in authentication, speed of response, system stability, and ability to resist fraud.

VIII.REFERNCES

[1] M. Satyanarayana, K. S. Reddy, and S. V. Rao, "Biometric based electronic voting system using fingerprint recognition," *International Journal of Research in Engineering and Technology*, vol. 6, no. 4, pp. 210–214, Apr. 2020.

[2] P. Bhargavi, R. S. Reddy, and M. S. Kumar, "Design and implementation of secure electronic voting system using fingerprint authentication and GSM," *International Journal of Engineering Science and Computing*, vol. 7, no. 6, pp. 13345–13349, Jun. 2021.

[3] R. Ismail, Z. A. Othman, and M. H. Selamat, "A smart card (MyKad) and fingerprint authentication for e-voting system," *International Journal of Engineering & Technology*, vol. 7, no. 3, pp. 45–50, 2019.

[4] A. Poudel, S. A. Hasan, and S. Nepal, "Secure electronic voting using blockchain technology," *IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 150–157, 2020.

[5] W. A. Wibowo and E. I. Ujianto, "IoT-based electronic voting system using fingerprint biometrics and ESP32," *Journal of Information Systems and Informatics*, vol. 4, no. 2, pp. 112–120, 2022.

[6] P. Sandeep, R. Karthik, and V. Kumar, "EVM through ID and fingerprint verification using RFID," *International Journal of Engineering Research & Technology (IJERT)*, vol. 10, no. 5, pp. 430–435, May 2021.

[7] P. Poduval, A. Nair, and S. Menon, "Advanced electronic voting system," *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, vol. 8, no. 6, pp. 1881–1886, Jun. 2020.

[8] S. N. Syed, A. R. Ahmed, and M. H. Rahman, "A novel hybrid biometric electronic voting system integrating fingerprint and face recognition," *arXiv preprint arXiv:1801.02430*, 2018.

[9] K. Kale, P. Patil, and A. Deshmukh, "Biometric based electronic voting machine," *International Journal of Innovative Research in Engineering and Technology*, vol. 9, no. 3, pp. 98–102, 2020.

[10] M. Khasawneh, M. Alsharaeh, and A. Alazzam, "A review of electronic voting systems: Security and usability issues," *International Journal of Information Engineering and Electronic Business*, vol. 12, no. 1, pp. 23–31, 2020.

[11] S. Gurav, A. Patil, and R. Jadhav, "Fingerprint based voting system using IoT," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 6, no. 3, pp. 214–219, 2021.

[12] B. H. Simts, "A survey on secured voting system using fingerprint scanner," *International Journal of Psychosocial Rehabilitation*, vol. 24, no. 6, pp. 5605–5612, 2020.

[13] S. Karthikeyan and J. Nithya, "Secured electronic voting machine using biometric authentication," *International Journal of Advanced Research in Electronics and Communication Engineering*, vol. 8, no. 5, pp. 312–316, 2019.

[14] S. N. Arinze, I. C. Nwogu, and C. C. Okafor, "RFID-based process automation for transparent voting systems," *International Journal of Computer Applications*, vol. 178, no. 22, pp. 12–17, 2021.

[15] S. H. P., R. Prakash, and M. Kumar, "Arduino based smart and remote voting system," *International Journal of Engineering Research & Technology (IJERT)*, vol. 9, no. 4, pp. 115–119, 2020.

[16] A. Verma and S. Mishra, "GSM based electronic voting system," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 6, no. 2, pp. 1324–1329, 2022.

[17] R. Sharma, A. Gupta, and S. Mehta, "Fingerprint based secure electronic voting system," *International Journal of Computer Science and Mobile Computing*, vol. 7, no. 3, pp. 45–51, 2018.

[18] D. Patel, H. Shah, and N. Joshi, "Analysis of multi-factor authentication techniques for electronic voting systems," *International Journal of Information Security Science*, vol. 9, no. 2, pp. 89–96, 2020.

[19] A. Kumar, R. Singh, and P. Verma, "GSM technology based secure electronic voting system," *International Journal of Engineering and Advanced Technology*, vol. 8, no. 5, pp. 221–226, 2021.

[20] K. Rao, S. Reddy, and P. Chandra, "Embedded system based electronic voting framework," *International Journal of Embedded Systems and Applications*, vol. 6, no. 1, pp. 1–8, 2022.

[21] A. Mohankumar, K. Suresh Kumar, and R. Gowtham, "*Enhancing Electoral Integrity: A Fingerprint-Verified Voting System for Fair and Secure Elections,"* Asian Journal of Applied Science and Technology, vol. 08, no. 01, pp. 33–46, Feb. 2024.