IOSR Journal of Mobile Computing & Application (IOSR-JMCA)
e- ISSN: 2394-0050, P-ISSN: 2394-0042.Volume 12, Issue 2 (Mar. – Apr. 2025), PP 01-09
www.iosrjournals.org

Design And Development Of An Electronic Voting System Incorporating Fingerprint And Radio Frequency Identification-Based Authentication

[1]Olusi Titilayo R. [1] Adeife Oyebola T. [2]Dada Olabisi M.
[3]Bolaji-Adetoro D. Funsho
[1,2,3] Computer Science Department
Institute Of Info. & Comm. Tech.
Kwara State Polytechnic
[1]Networking And Cloud Computing Department
Federal Polytechnic Offa

Abstract
Conducting free and fair elections is a challenging task for the election commission, requiring significant resources to ensure the process is secure and orderly. To address these challenges and offer a cost-effective solution, this research proposes the implementation of biometric technology, specifically fingerprint scanning, along with Radio Frequency Identification (RFID). The goal of this research is to enhance the current voting process by making it more accurate, transparent, and efficient, while ensuring that each individual can cast only one vote. The system relies on thumbprint identification, leveraging the fact that each person's fingerprint is unique. This gives it a significant advantage over traditional voting methods. By ensuring that only authorized voters can access the system, the risk of fraud is minimized. The system grants access to cast a vote only if the scanned fingerprint with Radio Frequency Identification (RFID) matches an entry in the voter database, otherwise, it denies access. Additionally, this method is designed to reduce the overall cost of election management and maintenance.

Keywords: *Voting, Fingerprint module, Radio Frequency Identification, Arduino.*

Date of Submission: 17-12-2024 Date of Acceptance: 27-12-2024

I. Introduction

Advanced democratic societies rely heavily on the foundation of free and fair elections, which have traditionally been conducted using paper-based voting methods. However, with the advent of technology, new possibilities and challenges have emerged in the electoral process. While conventional voting methods face difficulties such as logistical issues, vulnerability to manipulation, fraud, and limited accessibility, electronic voting (e-voting) systems are increasingly being considered as a solution. These systems offer potential benefits, including greater accuracy, efficiency, accessibility, and transparency. By utilizing technology, e-voting can streamline procedures, reduce errors, and enhance election security and integrity (Prasad *et al.*, 2016).

However, the adoption of electronic voting systems is not without its challenges and controversies. Security, reliability, and privacy concerns persist, as vulnerabilities to hacking, tampering, or system malfunctions can undermine the credibility of election results. One of the main hurdles is ensuring secure and reliable voter authentication. Traditional methods, such as ID cards or signatures, are often susceptible to fraud and may not provide the level of security required for electronic voting. As a result, there is growing interest in using biometric authentication technologies, like fingerprint recognition, to more accurately and securely verify voters' identities (Abdulkadir *et al.*, 2019).

Electronic voting has become increasingly popular due to its flexibility and ease of use, enabling more convenient participation compared to traditional voting methods. However, the transition to e-voting introduces several challenges that must be addressed for the system to function effectively. Among these challenges are key factors such as **completeness**, which ensures that all legitimate votes are counted, and **correctness**, which guarantees that the election results accurately reflect the voters' intentions. In addition to these, other important requirements include:

- **Anonymity**: Protecting voter privacy by ensuring that votes cannot be traced back to individuals.
- **Fairness**: Ensuring that no voter has an unfair advantage and that no votes are altered or tampered with during the process.

- **Convenience**: Providing a user-friendly experience that allows all eligible voters to participate with ease.
- **Robustness**: Building a system resilient enough to withstand technical failures or deliberate attacks.
- **Mobility**: Allowing voters to cast their ballots from various locations, thereby increasing voter participation.
- **Uniqueness**: Ensuring that each voter can only cast one vote.
- **Coercion resistance**: Preventing voters from being forced or pressured into voting a certain way.
- **Efficiency**: Designing a system capable of handling large-scale elections without delays or technical issues.

Elections play a vital role in allowing citizens to choose their representatives and voice their preferences in governance. Therefore, the reliability of the voting process is critical for maintaining trust in democratic systems. Any voting system, particularly e-voting, must be resilient against fraudulent activities while remaining transparent and understandable to all stakeholders. Voters and candidates need confidence in the system for the election results to be deemed legitimate. As highlighted by Abdulkadir *et al*. (2019), ongoing enhancements to e-voting technology are essential to address these concerns effectively.

Biometrics involves the automated identification of individuals based on their unique biological and behavioral traits. In biometric recognition, an individual's characteristics are measured and compared to previously stored biometric data to verify their identity. Fingerprints, which are impressions of the friction ridges on a fingertip, have long been used for identification. More recently, fingerprint recognition has become one of the most widely adopted biometric technologies due to its ease of capture, the availability of multiple data points (ten fingers), and its longstanding use by law enforcement agencies.

Automatic fingerprint identification is recognized as one of the most reliable biometric methods. This is largely due to the distinctiveness and permanence of fingerprints, which remain unchanged throughout a person's life. Fingerprints are unique to each individual, and even identical twins do not share the same fingerprint patterns. The simplicity of fingerprint collection and the high accuracy of matching also contribute to the technology's widespread use (Ashok & Ummal, 2011).

In a democratic society, elections and voting are fundamental pillars. However, traditional election methods face numerous challenges, including inconvenience, lack of fairness, limited mobility, and insufficient anonymity. Additionally, the high cost of conducting traditional elections can strain societal resources. To address these issues, the concept of **electronic voting** (e-voting) was introduced, enabling people to cast their votes over the Internet or intranet, thereby reducing the overall cost for governments, organizations, and associations.

The key advantages of e-voting, particularly its **mobility** and **convenience**, make it an appealing option for future elections. Despite technological advancements in electronic voting over the past two decades, certain challenges such as coercion resistance and ensuring completeness remain unresolved. However, the proposed e-voting mechanism aims to meet many essential requirements of traditional e-voting systems while offering greater efficiency, making it a practical solution for modern electoral processes (Ashok & Ummal, 2011).

The systems perspective involves examining how interconnected components work together to achieve a specific outcome. By taking this "big picture" approach, analysts can understand how each part contributes to the overall system, often revealing multiple solutions to a problem rather than a single correct answer. In the case of electronic voting (e-voting), the process involves gathering significant amounts of input, processing the data using various technologies, and producing a singular output. These technologies, which will be explained in more detail later, enable e-voting to be a potentially cost-effective and time-efficient method, provided that a secure and reliable system is in place.

II. Related Works

Vinayachandra *et al*. (2020) introduced an Arduino-based Authentication Voting Machine (AVM) that utilizes both Radio Frequency Identification (RFID) and fingerprint technology for student elections. One of the key focuses of their system is addressing the challenge faced by visually impaired individuals, who often lack the ability to vote independently and confidentially due to their disability. The proposed system is designed to be user-friendly, allowing visually impaired voters to cast their votes independently through the use of audio guidance.

The system is built on an Arduino Mega 2560 microcontroller and incorporates several components, including an SD card module, an LCD display, buttons, a buzzer, GSM SIM 900A, and a headset. Pre-recorded audio, stored on the SD card, guides the voters by announcing the names of the candidates through the headset to ensure privacy. To prevent double voting, the system is designed to trigger a buzzer once a vote is cast, locking the system from further input. A control button, managed by polling officials, can deactivate the buzzer and allow the system to accept the next vote. Additionally, a result button is included to display the final vote count for each candidate, with the results stored on the SD card and shared via the GSM SIM900A module.

By offering this system, the authors aim to foster greater inclusion in democratic processes, allowing visually impaired individuals to participate equally and independently in elections.

Abdulkadir *et al*. (2019) developed an electronic voting system aimed at streamlining the election process, ensuring it is fast, free, and fair. The system was designed using an Arduino Mega microcontroller and interfaced with a fingerprint sensor, keypad, GSM module, real-time clock, LCD, and a personal computer. The development of the system involved creating an algorithm and programming it through the Arduino IDE.

Voter data, including biometric information, is stored during the registration phase, and each registered voter is assigned a random voting PIN sent to their mobile number. Before voting, the system authenticates the voter by verifying both their biometric data and PIN against the stored information. Once authentication is successful, the voter is allowed to cast their vote, which can be done in either open or closed ballot mode. The system also records the time of each vote and tallies the results to determine the winner based on the majority of votes. This electronic voting system is designed to enhance the efficiency and integrity of the election process.

Damahoki *et al.* (2022) developed an electronic voting system specifically designed for visually impaired individuals, using the Arduino Mega 2560 microcontroller. The system includes several components, such as an SD card module, LCD display, buttons, buzzer, GSM SIM 900A, and a headset. A key feature of the system is its audio guidance, with candidate names stored on the SD card and relayed through a headset to ensure voter privacy.

To ensure smooth election procedures, the system is divided into two units: a control unit for polling officials and a voting unit for users. After a vote is cast, a buzzer sounds, and the system becomes temporarily disabled to prevent multiple votes. Polling officials can reactivate the system by pressing a control button. Additionally, a result button allows the final votes for each candidate to be displayed and stored on the SD card. The GSM SIM900A module is used to transmit the final voting results.

Ritwik *et al.* (2020) present a study on creating a low-cost, real-time Arduino-based electronic voting machine (EVM). This paper focuses on developing an EVM with an integrated fingerprint scanner for authentication to address issues like wired electronic voting challenges and impersonation. Elections are essential for enabling citizens to select their representatives and voice their preferences on governance. Ensuring the election process's integrity is crucial to maintaining democracy. Therefore, the voting system must be resilient against various types of fraud while remaining transparent and understandable, so that voters and candidates can confidently accept the results.

Poornima *et al.* (2020) developed an Arduino-based authentication voting machine (AVM) utilizing Radio Frequency Identification (RFID) and fingerprint scanning for student elections. The primary goal of this project is to simplify the voting process and enhance transparency. This paper introduces a secure and intelligent voting system that incorporates Arduino IoT technology to provide authenticated voting specifically for college elections.

III. Methodology

Workflow:

1. **Voter Registration**: Eligible voters are enrolled into the system, with their biometric information, such as fingerprints and Radio Frequency Identification, captured and securely stored in the database.
2. **Biometric Verification**: On Election Day, voters visit polling stations where their fingerprints and Radio Frequency Identification are scanned for biometric verification. The system matches the data against stored records to confirm their eligibility.
3. **Voting Procedure**: After successful verification, voters access the voting interface to select their preferred candidates or ballot options. Each vote is securely recorded and anonymized, linked to the voter's biometric identifier for integrity.
4. **Vote Counting**: Once voting ends, the system counts all votes accurately and transparently. The results are securely transmitted to central election authorities for consolidation and public announcement.

The flowchart in Figure 1is representing the voter’s registration while Figure 2 represent voter’s verification and voting procedure respectfully. Figure 3 is the System Architecture Typically, EVM development employs Unified Modeling Language (UML), utilizing use case diagrams, activity diagrams, and sequence diagrams to analyze the system. The use case diagram illustrates interactions between the system and external elements, specifying the roles of each actor.

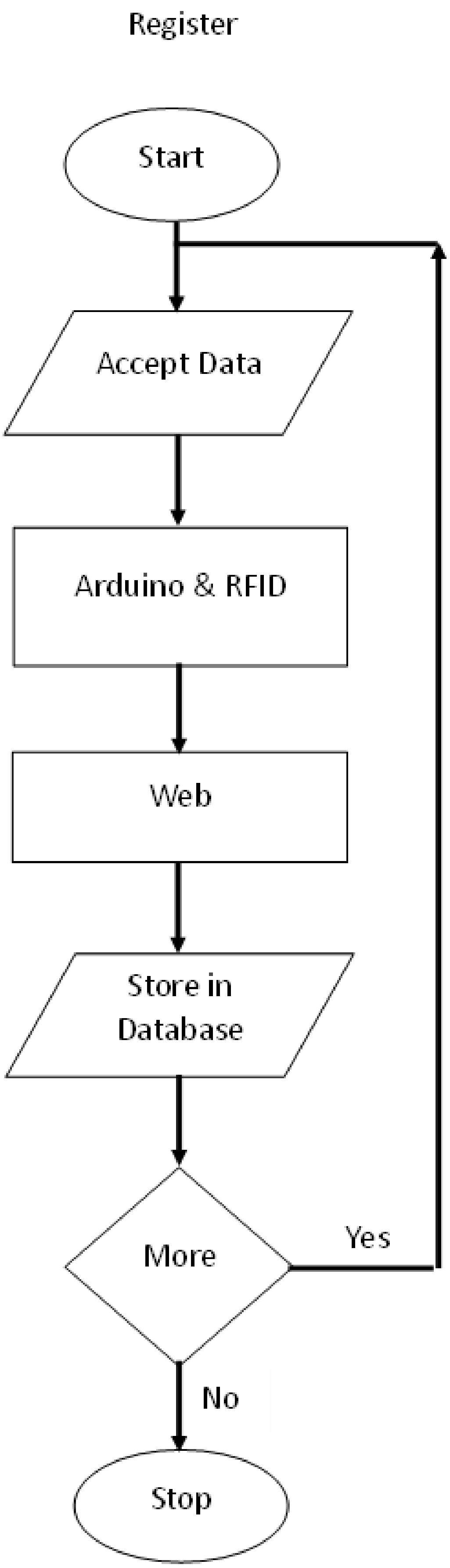

Figure 1: Registration Flowchart

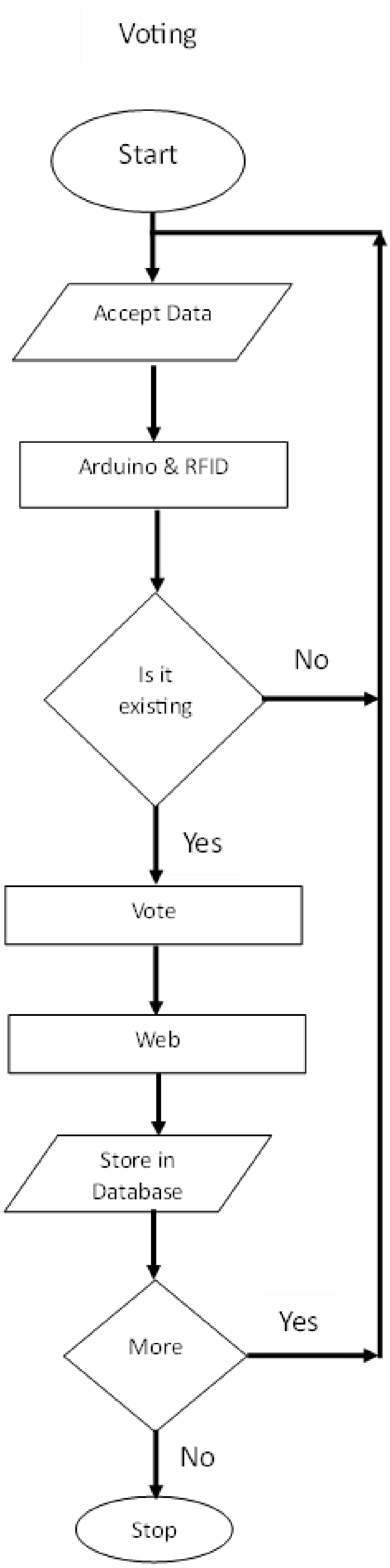

Figure 2: Voting Flowchart

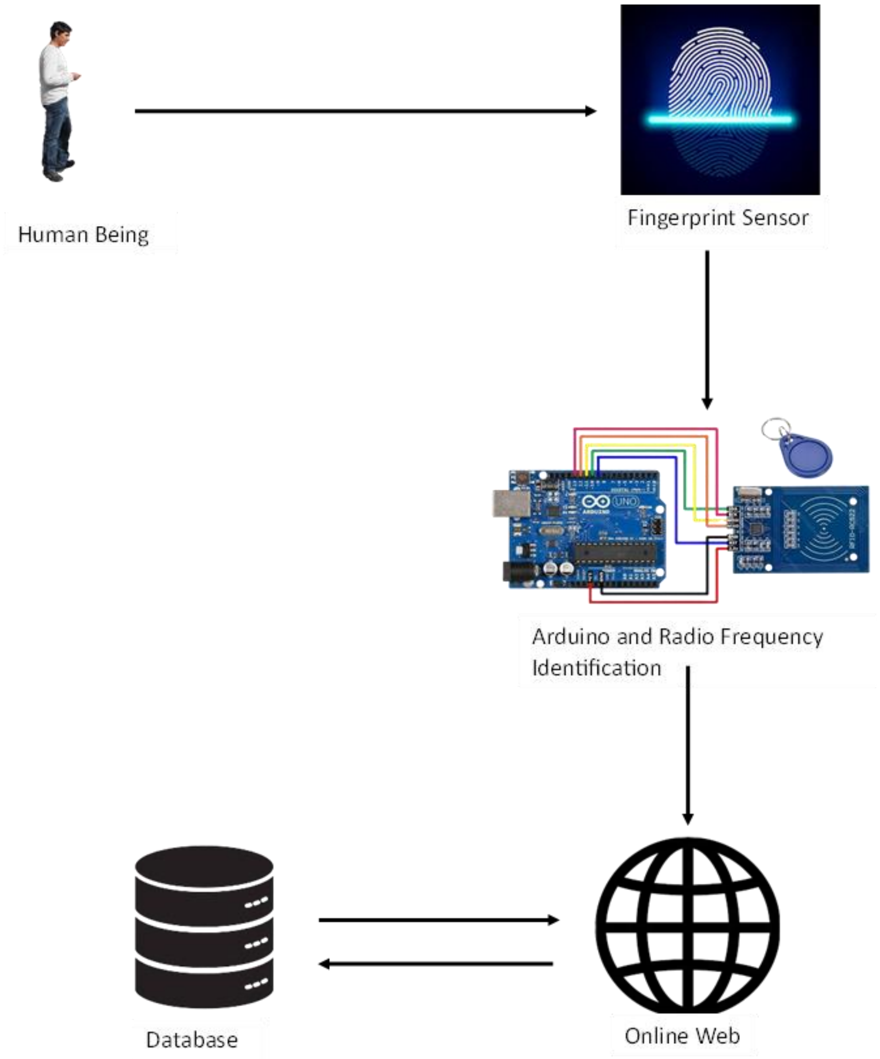

Figure 3: System Architecture

This study employed Arduino and Radio-Frequency Identification (RFID) technology, which uses electromagnetic fields for the automatic identification and tracking of tagged objects. An RFID system consists of a tag—a small radio transponder—as well as a radio receiver and transmitter as represented in Figure 4.

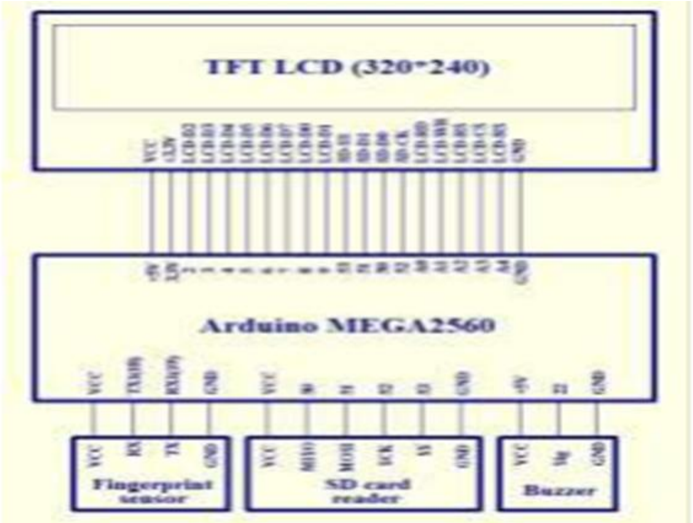

Figure 4: Radio receiver and Transmitter **for voting system.**
Source: (http://main.tu-jo.com/ojs/index.php/TJPS/index)

ARDUINO MEGA 2560

The Mega 2560 is a microcontroller board based on the ATmega2560, offering 54 digital input/output pins (with 15 supporting PWM output), 16 analog inputs, 4 UARTs (hardware serial ports), a 16 MHz crystal oscillator, a USB interface, a power jack, an ICSP header, and a reset button. As shown in Figure 3, the Arduino Mega 2560 is designed for convenience and can be connected to a computer via a USB cable or powered using a battery or an AC-to-DC adapter. Its compatibility with a wide range of shields and robust support for microcontroller applications makes it ideal for rapid prototyping and versatile use as presented in Figure 5.

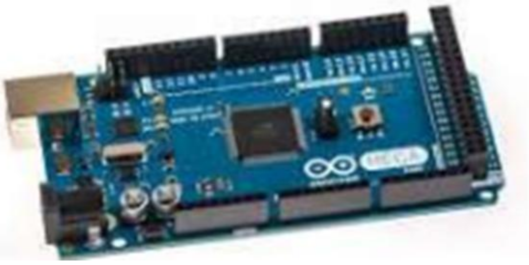

Figure 5: Arduino Mega 2560.
Source: (http://main.tu-jo.com/ojs/index.php/TJPS/index)

Fingerprint Sensor

One of the most effective and straightforward methods to secure information and authenticate users is through fingerprint recognition, eliminating the need for users to create and protect passwords. Fingerprints can be captured using an optical fingerprint sensor, which allows for easy detection and verification. This type of sensor is commonly applied in devices such as safes and includes a powerful DSP chip that handles image rendering, feature extraction, searching, and matching. The sensor can connect to any microcontroller via Serial Tel, sending data packets for imaging, hashing, searching, and recognition. It can store up to 162 fingerprints in its onboard FLASH memory. A red LED within the lens signals when the sensor is active and ready to capture a fingerprint. Figure 6 shows the fingerprint sensor.

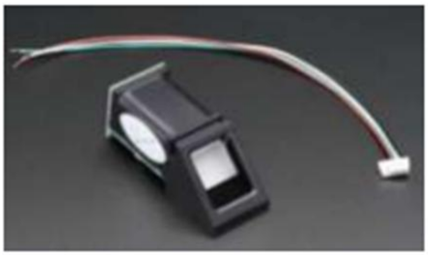

Figure 6: Fingerprint sensor
Source:(http://main.tu-jo.com/ojs/index.php/TJPS/index)

Buzzer

Buzzers are categorized into two types: active and passive. An active buzzer generates a single tone when connected to Vcc and ground, while a passive buzzer functions like a loudspeaker and requires an external signal to operate. Various types of active buzzers are utilized in different applications. The YL-44 is one such model, a compact buzzer that operates within the audible frequency range of around 2 kHz. This buzzer does not require an external frequency generator to sound an alarm. To activate the YL-44, the I/O pin must be set to LOW, and to deactivate it, the pin should be set to HIGH. Additionally, this buzzer can be controlled using PWM. Figure 7 illustrates the active buzzer."

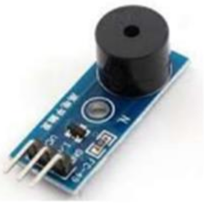

Figure 7: Active buzzer
Source: (http://main.tu-jo.com/ojs/index.php/TJPS/index)

IV. Result And Discussion

When the program was initiated, the output of the Electronic Voting Machine (EVM) is designed to focus on how information is presented to users for data capturing and how the data was authenticated with stored data and how the results are recorded and displayed. This section covers the design of user interfaces, output formats, and data storage structures. The primary outputs of the EVM system include user prompts, confirmation messages, and vote records. Things taken into consideration in determining the output are presented below:

Vote Records Vote records are stored securely in the SD card module. Each vote record includes the following information:

Voter ID: A unique identifier for the voter (not directly tied to personal data to maintain anonymity).

Candidate ID: The identifier of the selected candidate.

Timestamp: The date and time when the vote was cast. The results are presented in Figure 8 through Figure 10.

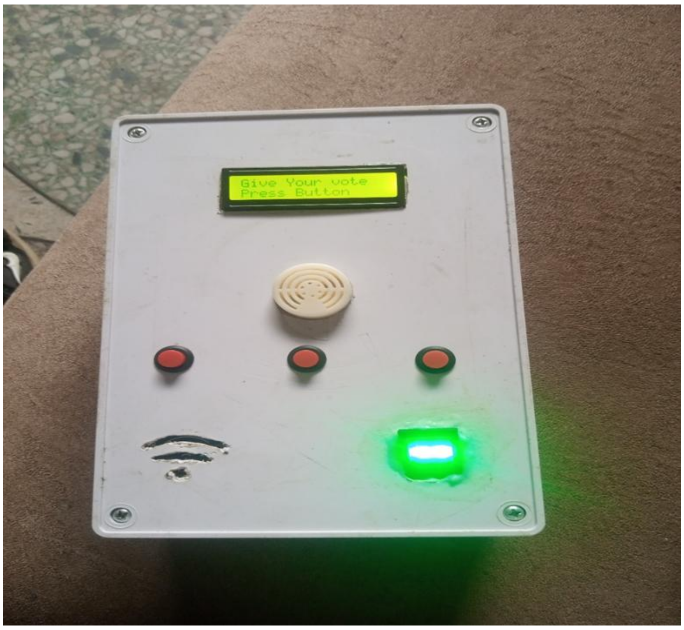

Figure 8: Constructed Voting System

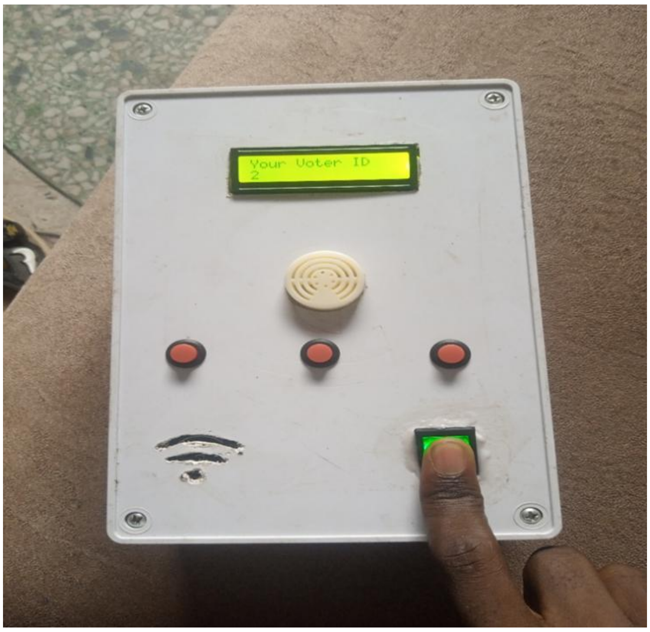

Figure 9: Constructed Voting Process System

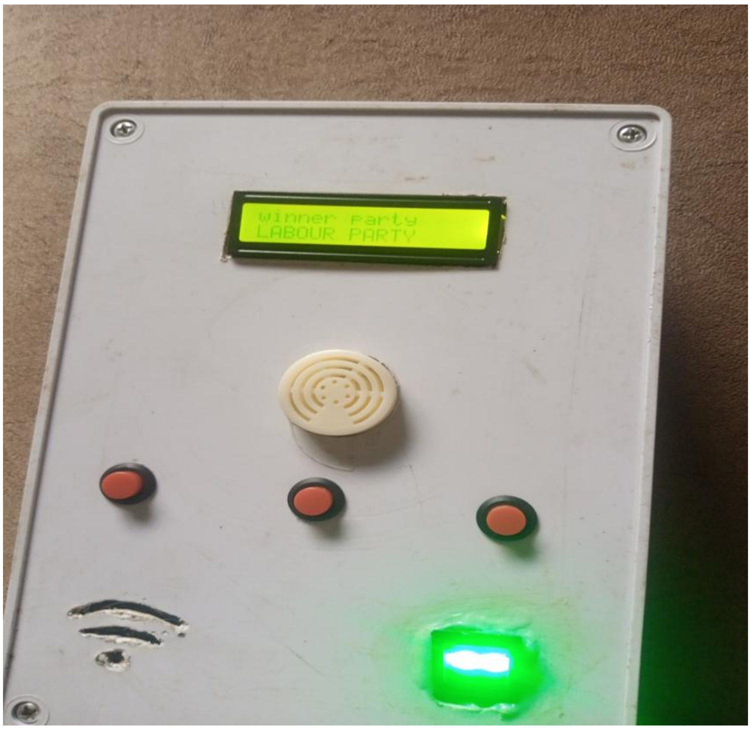

Figure 10: Constructed Result Display System

V. Conclusion

The EVM system incorporating fingerprint and RFID authentication developed in this research addresses critical challenges in traditional voting systems, such as security, efficiency, and data integrity. The successful integration of hardware and software demonstrates the practicality and effectiveness of leveraging advanced technologies to enhance the voting process.

i. **Security**: The dual-layer authentication system ensures that only authorized voters can cast ballots, effectively preventing unauthorized access and reducing the risk of electoral fraud, thereby increasing the credibility of election outcomes.

ii. **Efficiency**: The streamlined voter authentication and voting process minimizes the time required per voter, which is particularly advantageous in high-turnout elections by reducing delays and improving overall throughput.

iii. **Data Integrity**: Reliable data management techniques, including secure storage and regular backups, safeguard voting records, ensuring their accuracy and availability for post-election audits and dispute resolution.

iv. **User Experience**: An intuitive and user-friendly interface simplifies navigation, reducing errors and enhancing voter confidence and satisfaction with the system.

References

[1] Abdulkadir, H. A., Emmanuel, G. D., Dauda, E., Mshelia., & Sadiq O. O. (2019). “Design And Development Of An Arduino Based Electronic Voting System”: International Refereed Journal Of Engineering And Science (IRJES) 8(1), PP. 48-57.

[2] Barrett, S. F., & Pack, D. J. (2019). "Microcontrollers: Fundamentals And Applications With PIC." Synthesis Lectures On Digital Circuits And Systems, 7(1), 1-227. DOI: 10.2200/S00326ED1V01Y201205DCS039

[3] Damahoki, W. (2022). "Cryptography And Network Security: Principles And Practice." Pearson Education. ISBN: 978-0134444284.

[4] Drabha, K., & Want, R. (2021). "Advanced Electronic Voting Machine Using Arduino." IEEE Pervasive Computing, 5(1), 25-33. DOI: 10.1109/MPRV.2006.2

[5] Jain, A. K., Ross, A., & Prabhakar, S. (2020). "An Introduction To Biometric Recognition." IEEE Transactions On Circuits And Systems For Video Technology, 14(1), 4-20. DOI: 10.1109/TCSVT.2003.818349

[6] Lakshmi, M, K., Prathyusha, V., Lakshmi, T, N., Vijyalakshmi, K., & Lavnaya. (2017): “An Electronic Voting Machine By Using Arduino”: INTERNATIONAL JOURNAL FOR RESEARCH & DEVELOPMENT IN TECHNOLOGY 7(3), 2349-3585.

[7] Li, S. Z., & Jain, A. K. (Eds.). (2018). "Handbook Of Face Recognition." Springer. ISBN: 978

[8] Marwa, A. (2018) “Arduino – Based Electronic Voting Machine”: Software Engineering Department, College Of Computer Science And Mathematics, University Of Mosul, Mosul, Iraq: Tikrit Journal Of Pure Science 23 (10), ISSN: 1813 – 166.

[9] Myers, G. J., Sandler, C., & Badgett, T. (2021). "The Art Of Software Testing." John

[10] Poornima, G. J., Sandler, C., & Badgett, T. (2020). "The Art Of Software Testing." John

[11] Ritwik, S. F., & Pack, D. J. (2020). "Microcontrollers: Fundamentals And Applications With PIC." Synthesis Lectures On Digital Circuits And Systems, 7(1), 1-227. DOI: 10.2200/S00326ED1V01Y201205DCS039

[12] Sercan Et Al., (2017): Arduino And Php Based Electronic Voting System Design And Implementation; IEEE Transactions On Circuits And Systems For Video Technology, 14(1), 4-20. DOI: 10.1109/TCSVT.2003.818349

[13] Shneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., & Elmqvist, N. (2019). "Designing The User Interface: Strategies For Effective Human-Computer Interaction." Pearson. ISBN: 978-0134380384.

[14] Stallings, W. (2022). "Cryptography And Network Security: Principles And Practice." Pearson Education. ISBN: 978-0134444284.

[15] Vinayachandra, K., Geetha Poornima, M., Rajeshwari., & Krishna P., (2020) "Arduino Based Authenticated Voting Machine (AVM) Using RFID And Fingerprint For The Student Elections": Journal Of Physics: Conference Series 1712 (2020) 012004 Doi:10.1088/1742-6596/1712/1/012004

[16] Want, R. (2021). "An Introduction To RFID Technology." IEEE Pervasive Computing, 5(1), 25-33. DOI: 10.1109/MPRV.2006.2