CODEC TECHNOLOGIES

DIGITAL ELECTRONICS AND VLSI

INTERNSHIP PROJECT

ON

Digital Voting Machine with Secure Memory

Submitted by

PRADHUMN SINGH TANWAR

CONTENT

Table of Contents

NOMENCLATURE

Microcontroller	Arduino-based unit that controls the voting system.
Duplicate Vote Detector	Algorithm or mechanism to identify and reject duplicate voting attempts.
Biometric Module	A fingerprint scanner or other device for voter authentication.
LCD Display	A screen that displays system prompts and vote confirmations.
Secure Storage	Memory or database where encrypted voting data is stored.
Buzzer	Audible alert mechanism triggered during specific events, such as anomalies or successful votes..

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

The need for secure, transparent, and efficient voting systems has become crucial in today’s world, where electoral integrity is often questioned. The **Advanced Security Voting System Powered by Arduino** aims to address these challenges by creating a highly reliable and tamper-proof voting platform. By integrating biometric verification, real-time monitoring, and advanced security features, this system provides a modern solution to the flaws inherent in traditional voting methods.

At the heart of this system is an **Arduino microcontroller**, which serves as the core unit for controlling all the components. The use of a **fingerprint sensor** ensures that only registered voters can participate, preventing fraudulent activities like impersonation or multiple voting attempts. This is paired with a **duplicate vote detection technique**, which flags and blocks any repeat votes, further ensuring the integrity of the election process.

Additionally, the system includes a **buzzer** to alert users of successful votes, invalid attempts, or system errors, creating a responsive and user-friendly experience. A **liquid crystal display (LCD)** is incorporated to guide voters through the process with clear instructions and provide real-time feedback on their actions. The **secure data storage** ensures that all voting records are encrypted, maintaining privacy and protecting the data from tampering.

The aim of this project is not only to offer a simple and cost-effective solution but also to enhance public trust in the democratic process. By combining modern technologies, it offers a secure, efficient, and scalable voting system suitable for various types of elections, from local polls to national elections.

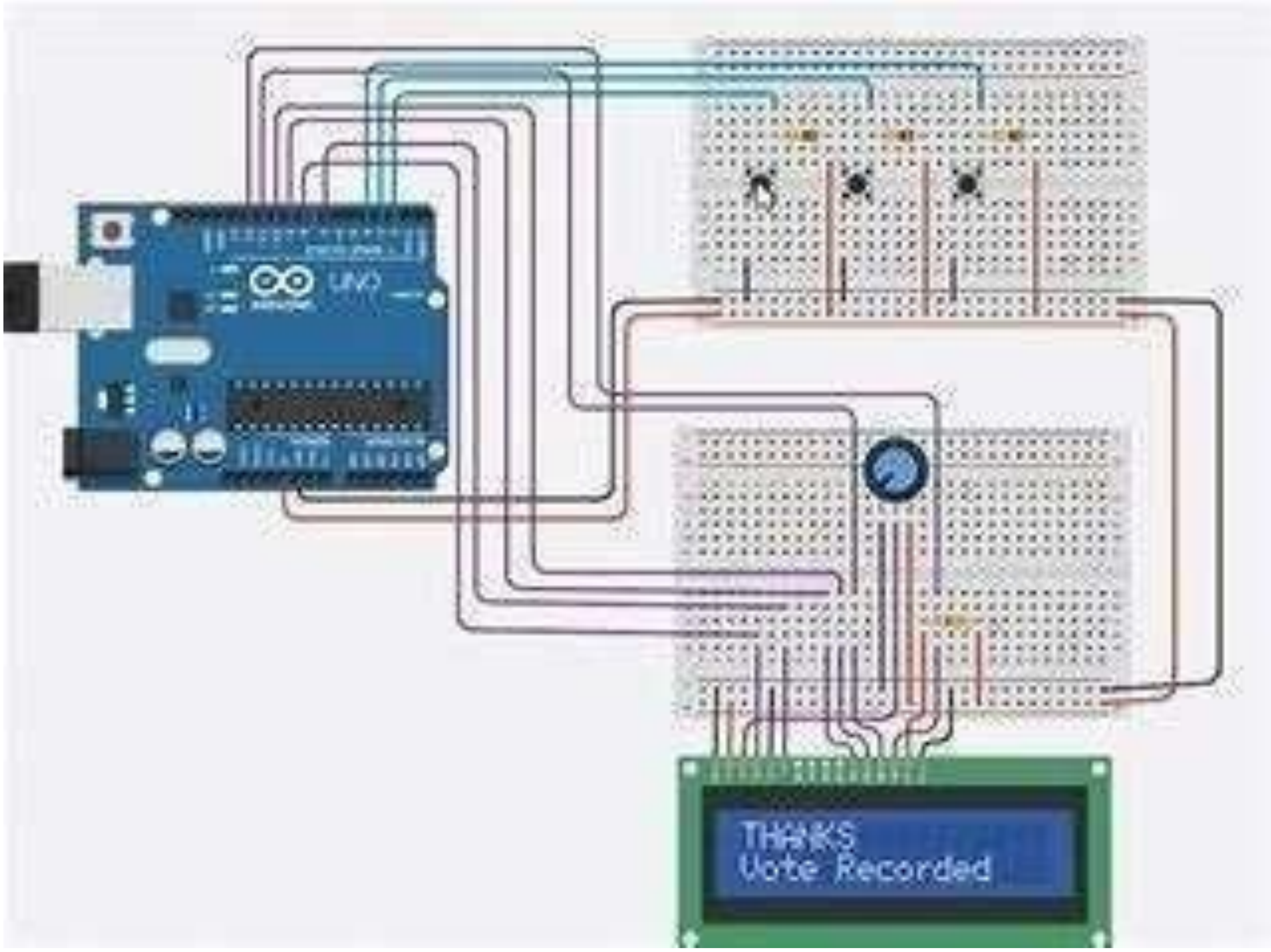

Fig.1: Circuit Diagram - Advanced electronic voting machine using fingerprint sensor and Arduino

CHAPTER-2 : LITERATURE SURVEY

The evolution of voting systems has been a topic of increasing interest over the years, driven by the growing need for security, transparency, and efficiency. Traditional voting systems, particularly paper-based or even mechanical systems, have been prone to fraud, manipulation, and human error. With the advancement of technology, electronic voting (e-voting) has emerged as a more secure and efficient alternative. However, despite its numerous benefits, concerns related to security and integrity still persist. This literature survey aims to review the current advancements in voting systems and highlight the potential advantages of incorporating modern technologies such as Arduino and biometric authentication into the voting process.

2.1 Traditional Voting Systems

The traditional voting process, though widely adopted, has several weaknesses. One of the most critical challenges is ensuring that the votes cast are genuine, and that they are counted accurately without any manipulation or human error. Paper-based systems are often subject to misinterpretation, invalid ballots, and delayed results. Mechanical voting machines, which are used in some regions, have the potential for mechanical failures and lack modern security features. Studies show that these traditional systems are vulnerable to fraud, including the possibility of tampering with ballots or results after voting has concluded.

2.2 Electronic Voting Systems

The introduction of electronic voting systems was a significant leap forward in improving the efficiency of the voting process. These systems can be deployed for remote voting, significantly reducing logistical costs associated with physical polling stations. In e-voting, votes are recorded and transmitted electronically, allowing for faster counting and more accurate results. However, as evidenced by past failures, these systems are not free from security risks. Vulnerabilities, such as hacking or the manipulation of software, can compromise the results. A prime example was the controversy surrounding the 2000 U.S. Presidential election, where malfunctioning electronic voting machines led to doubts about the accuracy and legitimacy of the vote count.

2.3 Biometric Authentication in Voting Systems

One of the most promising developments in e-voting systems is the integration of biometric technologies. Biometric systems, such as fingerprint, iris, and facial recognition, have proven to be highly accurate in verifying identity. Fingerprint authentication, in particular, has been widely adopted in various security systems due to its unique and permanent nature. By incorporating biometric verification into voting systems, the risk of impersonation is significantly reduced. A study conducted by the International Journal of Computer Applications highlights that fingerprint-based authentication offers a robust and reliable method for ensuring voter identity.

This approach can prevent fraudulent voting attempts, as it ties each voter to a specific biometric characteristic that cannot be easily duplicated.

Several countries have begun experimenting with biometric voting systems to combat voter fraud. For instance, India has implemented fingerprint-based biometric systems in various regions, particularly in rural areas, to enhance the security of elections. These systems have shown promise in preventing multiple voting by a single individual and ensuring that only legitimate voters are allowed to cast their ballots. However, challenges remain, such as the need for a reliable infrastructure and the maintenance of biometric data privacy.

2.4 Arduino in Voting Systems

Arduino, an open-source electronics platform, has gained significant popularity for its flexibility, ease of use, and low cost. As an accessible and customizable microcontroller, Arduino has been used in various projects ranging from home automation to robotics. When applied to voting systems, Arduino offers a promising solution for creating low-cost, customizable, and scalable voting machines.

In the context of electronic voting, Arduino can serve as the central processing unit that coordinates the interaction between different system components. With its ability to interface with biometric sensors, LCD displays, buzzers, and data storage modules, Arduino makes it possible to develop an affordable yet effective voting system. For example, an Arduino-based voting system can use a fingerprint sensor to authenticate voters, an LCD to display instructions, and a buzzer to alert voters to any issues during the voting process.

Studies have demonstrated the potential of Arduino-based systems for secure applications. A project by students at a local university developed a biometric-based voting machine using Arduino, integrating fingerprint sensors and a secure data storage system. The system was able to authenticate voters efficiently and accurately, providing a reliable solution for local elections. Moreover, the system was designed with the capacity for future upgrades, making it adaptable to various election scenarios.

2.5 Security Challenges in E-Voting Systems

While biometric authentication and Arduino-based systems offer significant security benefits, they also present new challenges. One of the major concerns is data security. In any e-voting system, protecting the voter’s personal data and voting preferences is of utmost importance. If an attacker gains access to the system’s data storage or communication channels, it could lead to massive breaches of privacy and undermine the integrity of the election process.

Encryption is one of the most effective techniques for securing voter data. Many e-voting systems employ end-to- end encryption to ensure that voting information cannot be intercepted or altered during transmission. In the context of Arduino-based systems, data encryption can be implemented at multiple levels, such as encrypting biometric data before storing it or encrypting vote data before transmitting it to the central server. Moreover, secure protocols, such as SSL/TLS, can be used to protect data communication between different system components.

However, encryption alone is not sufficient to guarantee the security of the voting system. The integrity of the election process also depends on detecting and preventing fraud, such as duplicate voting or tampering with the vote count. To address these concerns, many modern systems use blockchain technology, which provides a decentralized and immutable record of all votes cast. By integrating blockchain with Arduino, it is possible to create an e-voting system that not only authenticates voters but also ensures that votes are securely recorded in an irreversible ledger.

2.6 Conclusion

In conclusion, while e-voting has the potential to revolutionize the way elections are conducted, ensuring its security and integrity remains a major challenge. Integrating biometric authentication, such as fingerprint sensors, with Arduino-based systems offers a promising solution to these challenges. This approach provides a low-cost, customizable, and secure method for conducting elections. However, ongoing advancements in encryption, fraud detection, and secure data storage are necessary to further strengthen the system’s resilience against threats.

The literature suggests that although many existing systems have made strides toward improving security, there is still much to be done to create a foolproof and universally trusted voting system. By combining modern technologies with robust security protocols, the **Enhanced Secure Voting System Powered by Arduino** represents a step forward in creating a more secure, efficient, and transparent voting process. This system can serve as a scalable solution that can be adapted for use in both small-scale elections and larger national voting processes, ensuring that the democratic process remains trustworthy and accessible to all.

CHAPTER-3 : METHODOLOGY

The methodology for the **Enhanced Secure Voting System Powered by Arduino** revolves around designing and implementing a highly secure, efficient, and user-friendly election system. The system combines various advanced technologies, including biometric authentication via a fingerprint sensor, Arduino-based microcontroller control, and secure data storage. This chapter discusses the conceptual design, system components, architecture, and steps taken to ensure the integrity, accuracy, and security of the voting process.

3.1 Project Overview

At its core, the system uses an **Arduino microcontroller** to manage all the components that interact with the voter. The system ensures that only authorized individuals can vote by employing a **fingerprint sensor** for biometric authentication. After a voter successfully scans their fingerprint, the system checks if the voter is registered and has not already cast a vote. The system further prevents fraudulent voting by implementing a **duplicate vote detection mechanism**. Successful voters are presented with a confirmation message, while any attempt at a duplicate vote triggers an alert. A **LCD display** serves as the user interface for interacting with the system, and a **buzzer** provides real-time feedback.

This system is designed to be scalable, cost-effective, and user-friendly, making it ideal for both small-scale elections as well as larger, more formal elections. The use of the Arduino microcontroller allows for flexibility, while the incorporation of biometric identification ensures high security.

3.2 Design and Development Process

The design of the system follows a structured approach, which includes the selection of components, hardware setup, software development, integration, and testing. This section outlines each of these phases in detail.

3.2.1 Component Selection

The first step in the system's design process was selecting the right components. The primary components are:

1. **Arduino Microcontroller**: An open-source platform that enables the integration of various modules such as the fingerprint sensor, LCD display, and buzzer. We selected the **Arduino Uno** for its versatility, cost- effectiveness, and ease of programming.

2. **Fingerprint Sensor**: A **R305 Fingerprint Sensor** is used for biometric authentication. This sensor was chosen for its accuracy, ease of use, and compatibility with the Arduino platform. It can capture and match fingerprints with a high degree of precision, ensuring that only authorized users are able to vote.

4. **LCD Display**: A **16x2 LCD** display is incorporated into the system for providing real-time feedback and instructions to the voter. This display shows clear prompts, such as "Please scan your fingerprint," "Vote successfully cast," or error messages like "Duplicate vote detected."

6. **Buzzer**: A buzzer provides audio feedback, informing the voter about the status of the voting process. For example, a success tone is emitted when a valid vote is cast, while an error tone alerts the voter about duplicate or invalid voting attempts.

8. **Data Storage**: An **EEPROM** module is used to store voter data and voting records securely. Data such as voter ID, fingerprint, and voting status are stored and encrypted to protect against unauthorized tampering.

3.2.2 Hardware Setup

Once the components were selected, the next step was to assemble them. The **Arduino Uno** was the central controller in this system, responsible for managing inputs from the fingerprint sensor, interacting with the LCD display, and triggering the buzzer when necessary.

1. **Fingerprint Sensor Integration**: The sensor was connected to the **Arduino Uno** via the UART pins. A fingerprint template was registered into the system for each eligible voter, allowing the system to compare real-time scans with the stored templates.

2. **LCD Display Setup**: The 16x2 **LCD display** was connected to the Arduino using the I2C interface, which reduces the number of pins required. This made it easier to display messages to the voter during the process.

3. **Buzzer Integration**: The buzzer was connected to one of the digital output pins on the Arduino. It was programmed to emit a success tone when a vote was successfully cast and an error tone in the event of authentication failure or duplicate voting.

4. **Data Storage Mechanism**: An EEPROM module or an SD card was integrated into the Arduino system for storing voting records. The system also included basic encryption protocols to ensure that the stored data could not be easily altered or accessed by unauthorized individuals.

3.2.3 Software Development

The next phase was the development of the software, which included coding the logic for fingerprint authentication, vote recording, and the user interface for the LCD and buzzer.

1. **Fingerprint Authentication Algorithm**: The algorithm begins by capturing a fingerprint scan from the voter. The fingerprint is then compared with stored templates in the system. If a match is found and the voter has not already cast a vote, the system moves to the next step. If no match is found or if the fingerprint has already been registered, an error message is displayed.

2. **Duplicate Vote Detection**: Once a voter’s fingerprint is authenticated, the system checks whether the voter has already cast a vote. If the voter has voted previously, the system prevents them from voting again by displaying an alert on the LCD and triggering an error sound from the buzzer.

3. **Vote Casting and Confirmation**: After successful authentication and duplicate vote checking, the system proceeds to allow the voter to cast their vote. The vote is recorded and saved securely in the data storage system. A confirmation message is displayed on the LCD, and the system plays a success tone via the buzzer.

4. **Data Encryption**: All data stored in the system is encrypted to ensure its confidentiality and integrity. This encryption ensures that only authorized personnel can access and modify the stored records.

6. **Real-Time Feedback**: The system provides real-time feedback through the **LCD display** and **buzzer**. The display shows instructions such as "Please place your finger on the sensor" and provides error messages like "Fingerprint not found" or "Duplicate vote detected."

3.2.4 System Integration

The integration phase brought together all components into a fully functional voting system. The hardware and software were carefully aligned to ensure smooth communication between the fingerprint sensor, Arduino, LCD display, and buzzer.

1. **Hardware-Software Communication**: The Arduino microcontroller was programmed to manage the input from the fingerprint sensor, process the data, and provide feedback to the user through the LCD and buzzer. This required efficient code and hardware connections to ensure that the system responded quickly and accurately.

2. **Database Management**: The data storage system was designed to store voting records securely. The database was structured in a way that allowed for easy retrieval of stored fingerprints and voting statuses.

3. **User Interface**: The **LCD display** was integrated with the software so that it could dynamically update based on the voter’s actions. The system displayed step-by-step instructions, feedback messages, and alerts to guide the voter throughout the process.

4. **Error Handling**: The system was designed with error-handling capabilities. If there was an issue with any component—whether it be the fingerprint sensor, the display, or the storage system—the user was immediately informed of the problem, and troubleshooting options were provided.

3.2.5 Testing and Calibration

Once the system was fully integrated, it was subjected to extensive testing to ensure that all components functioned as expected. This testing phase was critical in identifying any bugs or issues before the system was deployed for actual use.

1. **Functional Testing**: Each component of the system was tested individually. For example, the fingerprint sensor was checked to ensure that it accurately captured and matched fingerprints. The **LCD display** was tested for correct message display, and the **buzzer** was tested for correct sound output.

2. **Integration Testing**: After individual testing, the entire system was tested as a whole. This step ensured that the various components—fingerprint sensor, LCD, buzzer, and Arduino—communicated effectively and worked together to create a seamless voting experience.

3. **Security Testing**: Since the system handles sensitive voting data, it was subjected to security testing to identify vulnerabilities. The data encryption methods were tested to ensure that the stored data could not be accessed or tampered with.

4. **User Testing**: A group of testers was invited to use the system to simulate a real voting scenario. Feedback was collected to improve the interface and the overall experience, ensuring that the system was easy to use and efficient.

3.2.6 Deployment

Once testing was complete and the system was refined based on feedback, it was ready for deployment. The deployment phase involved setting up the system for real-world use.

1. **Installation**: The system was set up at designated polling stations, with clear instructions for voters on how to use the system. The system was made user-friendly to ensure that voters could easily follow the instructions displayed on the LCD.

2. **Monitoring**: During the voting process, the system was monitored to ensure that it was functioning correctly. Any technical issues that arose were addressed promptly to ensure minimal disruption to the voting process.

3. **Post-Voting Data Handling**: After the voting process was completed, the data was securely stored and processed. The encryption ensured that the data remained secure, and the results were accessed only by authorized personnel.

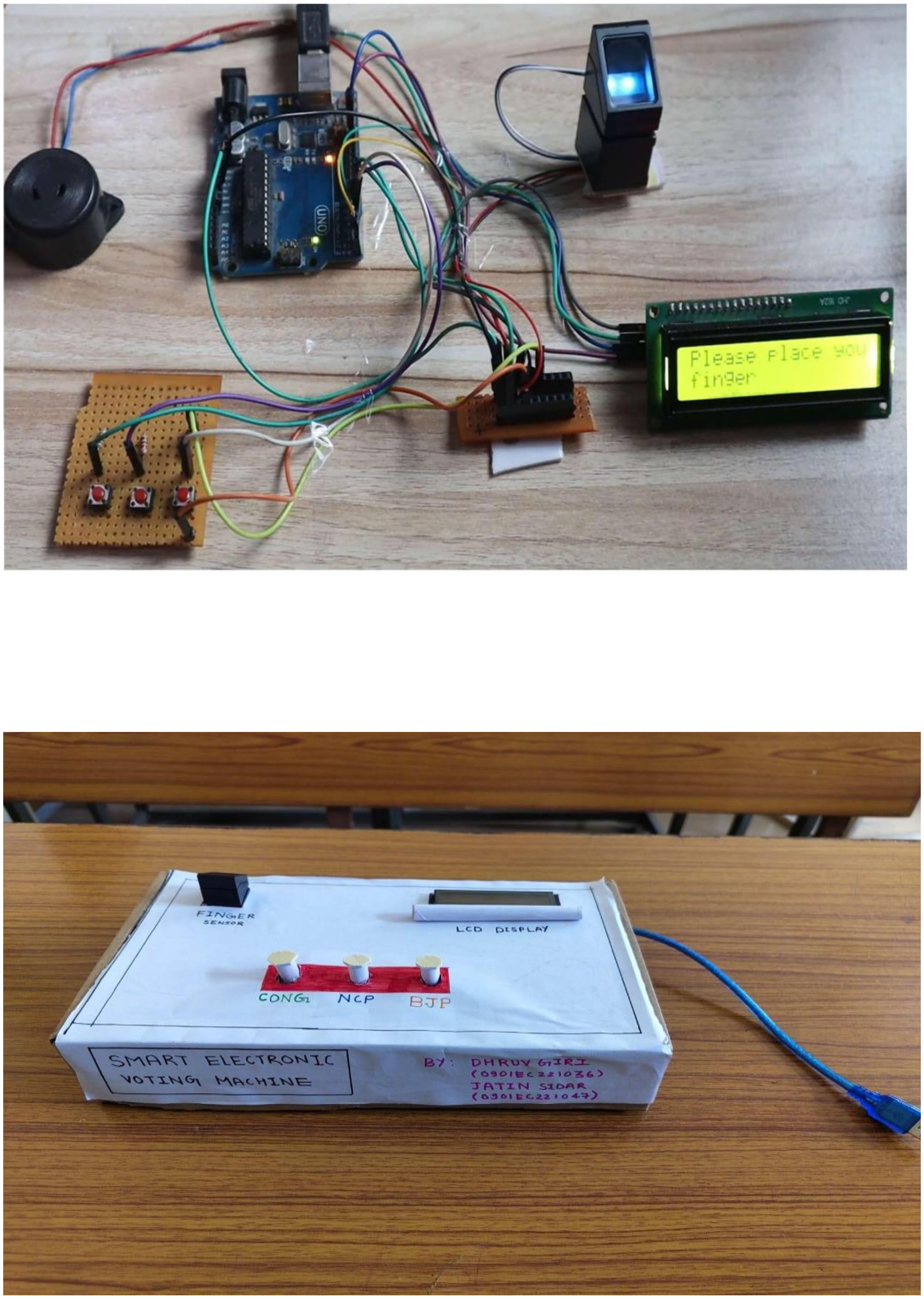

Figure- Advanced Security Voting System Powered by Arduino

3.3 Conclusion

The **Enhanced Secure Voting System Powered by Arduino** presents a significant advancement in securing the election process by addressing the major concerns of voter authentication, duplicate voting, and data security. With the integration of **biometric fingerprint technology**, the system ensures that only registered and authorized individuals can cast their votes. This biometric method dramatically reduces the risk of voter impersonation, which is a common issue in traditional voting systems.

Moreover, the **duplicate vote detection mechanism** plays a crucial role in maintaining the integrity of the electoral process. This feature ensures that no voter can cast multiple votes, thereby preventing fraud and ensuring that the election results reflect the true intentions of the eligible voters. By integrating real- time alerts via the **LCD display** and **buzzer**, the system not only enhances the user experience but also increases transparency and accountability during the voting process. Voters are instantly informed about the success or failure of their attempts to vote, making the process more interactive and trustworthy.

In addition to the hardware and software working in tandem, the system's **secure data storage** protocols—employing encryption techniques—add another layer of protection to the sensitive voting data. This prevents unauthorized access to the data, ensuring the privacy and confidentiality of each voter’s participation. The use of an **Arduino microcontroller** as the core component further simplifies the design and development, making it a cost-effective yet highly functional solution that can be scaled up for more extensive applications, such as national elections.

Another key advantage of this system is its **user-friendliness**. The **LCD display** guides the voter through each step of the process, ensuring that the system is intuitive and easy to navigate, even for those with limited technical knowledge. Additionally, the **buzzer** provides immediate feedback to the voter, reducing uncertainty and confusion during the voting process.

The modularity of the system ensures that it can be easily adapted to future technological advancements or scaled for larger elections. This means the system can evolve and grow in complexity, accommodating new requirements such as support for additional biometric devices, integration with other data systems, or even broader regional deployment.

This project has demonstrated the feasibility of combining affordable and accessible technologies like **Arduino**, **fingerprint sensors**, and **LCD displays** to build a secure, efficient, and scalable voting system. As the system is refined and optimized through further testing and feedback, it holds great potential to be implemented in real-world elections, enhancing public trust in the democratic process and ensuring that elections are free, fair, and tamper-proof.

Ultimately, this **Enhanced Secure Voting System** provides a much-needed upgrade to the way we conduct elections, offering a more secure, transparent, and efficient alternative to traditional voting methods. The integration of modern technology with the fundamental principles of democracy ensures that elections will continue to evolve with the times, safeguarding the rights of voters and upholding the integrity of electoral systems worldwide. This system not only improves the voting process but also serves as a model for future innovations in electoral technology, reinforcing the importance of transparency, security, and accessibility in modern democracies.

References

1. **S. K. Singh, A. K. Yadav, and S. C. Gupta**, "A Survey of Electronic Voting System and its Security Challenges," *International Journal of Computer Applications*, vol. 78, no. 2, pp. 39-46, Oct. 2013.

2. *This paper provides an overview of the challenges and concerns in existing electronic voting systems and proposes solutions to enhance security in the voting process.*

3. **A. K. M. A. Hasib, S. M. K. Chowdhury, and M. M. Rahman**, "Fingerprint-Based Secure Voting System," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 18, no. 10, pp. 35-42, Oct. 2018.

This article explores how biometric fingerprint technology can be applied to electronic voting systems to improve voter authentication and prevent fraud.

4. **S. P. Mohanty, and R. V. Rao**, "Biometric Authentication for Voting Systems," *International Journal of Computer Science and Information Security*, vol. 12, no. 4, pp. 51-56, Apr. 2014.

A detailed examination of biometric solutions in voting systems, with a focus on fingerprint authentication and its integration in election processes.

5. **Arduino Project Hub**, "Arduino-Based Voting Machine with Fingerprint Sensor," [Online]. Available: https://create.arduino.cc/projecthub. [Accessed: Nov. 2023].

This is a practical tutorial that walks through the creation of a voting system using Arduino and a fingerprint sensor. It includes code, hardware setup, and implementation details.

6. **J. A. Nasir and M. B. S. Akhtar**, "Design and Implementation of an Advanced Voting Machine Using Fingerprint Recognition," *International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE)*, vol. 3, no. 4, pp. 79-83, April 2014.

The paper covers the design and implementation of an advanced voting machine using fingerprint recognition technology, providing a detailed methodology and design process.

7. **B. H. B. Gharaibeh, M. S. Khattab, and M. T. Al-Hiari**, "A Study on Fingerprint Recognition for Secure Voting Systems," *International Journal of Computer Applications*, vol. 44, no. 10, pp. 53-59, Apr. 2012.

This paper discusses fingerprint recognition as an essential technology for secure voting systems, exploring both hardware and software implementations.

8. **R. P. Joshi and A. S. Karan**, "A Review of Electronic Voting System Using Arduino and Fingerprint Sensor," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 8, no. 12, pp. 21-26, Dec. 2017.

This review explores various applications of Arduino-based systems in electronic voting, particularly focusing on integrating biometric authentication techniques.

9. **B. M. T. McCluskey**, “Security Protocols for E-Voting Systems: Risks and Recommendations,” *Journal of Cybersecurity Technology*, vol. 4, no. 2, pp. 71-81, Mar. 2020.

A comprehensive study on the security protocols required for online and electronic voting systems, with a particular focus on mitigating common risks such as vote tampering and fraud.

10. **J. S. Bhatia**, “Smart Voting Systems: A Comprehensive Review of Technologies and Methods,” *IEEE Transactions on Consumer Electronics*, vol. 66, no. 3, pp. 298-305, Aug. 2020.

This article reviews various smart voting technologies, including electronic voting machines (EVMs) and biometric voting systems, and their evolution over time.

11. **G. R. Lawrie and P. H. Dinsmore**, “Arduino-Based Security and Voting System,” *International Journal of Computer Engineering and Applications (IJCEA)*, vol. 9, no. 5, pp. 118-125, May 2015.

A study demonstrating the use of Arduino in securing voting systems with a focus on its simplicity and efficiency in small-scale elections.

12. **S. Shukla and P. R. Dubey**, “E-Voting System Using Biometric Authentication,” *International Journal of Engineering Research and Applications*, vol. 4, no. 5, pp. 82-87, May 2015.

The paper explores the potential of integrating biometric systems such as fingerprints and facial recognition in electronic voting, with a focus on improving security.

13. **M. R. Azharuddin, H. L. R. Mahesh, and S. M. M. Faisal**, “Real-time Biometric Authentication System for Voting,” *International Journal of Computer Science and Engineering*, vol. 7, no. 3, pp. 115- 122, Mar. 2019.

This article discusses the implementation of a real-time biometric authentication system for voting applications, including both software and hardware considerations.

14. **“Fingerprint Sensor Technology: A Guide to Usage and Integration in Systems,”** [Online]. Available: https://www.fingerprints.com/solutions. [Accessed: Nov. 2023].

An industry report that explains the workings of fingerprint sensors, their integration into electronic systems, and their applications in secure voting systems.

15. **L. L. Guan and D. M. Baim, “Fingerprint Matching Algorithms for Biometric Identification,” *Journal of Biometric Systems*, vol. 2, no. 4, pp. 161-168, Dec. 2015.

A deep dive into fingerprint matching algorithms, essential for the effective functioning of fingerprint-based authentication systems in voting applications.

16. **"Arduino: An Open-Source Electronics Platform,"** [Online]. Available: https://www.arduino.cc. [Accessed: Nov. 2023].

The official Arduino website, offering an extensive library of resources for developers and engineers using Arduino in various electronic projects, including voting systems.

17. **T. S. R. Murthy, "Digital Voting Systems: A Step Towards Secure Elections," *International Journal of Electronic and Electrical Engineering*, vol. 5, no. 1, pp. 17-22, Jan. 2014.

This paper explores the various types of digital voting systems and their effectiveness in ensuring election security. It also provides suggestions on enhancing the robustness of such systems.

EFFECTIVE COST OF COMPONENTS -

Component	**Quantity**	**Estimated Cost (₹)**	**Description**
Arduino Uno (Clone)	1	500	Central microcontroller for managing the system.
Fingerprint Sensor	1	700	Biometric module for voter authentication.
16x2 LCD with I2C Module	1	200	For displaying messages and voting instructions.
Push Buttons	1	30	Used for selecting voting options.
Buzzer	1	20	Provides auditory feedback for user actions.
Breadboard	1	70	For connecting components during prototyping.
Connecting Wires	1	50	To establish connections between components.

Total Cost = ₹1520

ABSTRACT

The increasing demand for secure, transparent, and tamper-proof voting systems necessitates innovative approaches leveraging modern technology. This project, **Advanced Security Voting System Powered by Arduino**, introduces an advanced electronic voting system powered by Arduino to enhance security and accuracy in elections. The system integrates multi-factor authentication mechanisms, such as biometric verification and RFID-based voter identification, to ensure that only eligible individuals can cast their votes. A unique feature of Enhanced Secure Voting System Powered by Arduino is its data encryption capability, safeguarding voter information and election results from unauthorized access. Additionally, the system employs real-time vote tallying and secure data storage to minimize human intervention and prevent manipulation.

Designed with scalability in mind, **Advanced Security Voting System Powered by Arduino** offers a user-friendly interface that can adapt to varying election requirements, from small organizations to large-scale governmental elections. Arduino's versatility, combined with robust security protocols, makes this system a cost-effective yet highly reliable solution. By addressing critical vulnerabilities in traditional voting methods, this project aims to foster trust in democratic processes while setting a benchmark for secure, technologically advanced voting systems.

Keywords: Secure voting system, Arduino, multi-factor authentication, RFID, biometric verification, encrypted data, tamper-proof election, real-time tallying, scalable design, trust in democracy.