IOT BASED FINGERPRINT FRAUD DETECTION VOTING SYSTEM

Abstract

The fingerprint-based fraud detection voting system is a model that aims to address the inefficiencies and vulnerabilities in the current voting system by introducing an innovative approach to voting authentication and fraud prevention. Traditional voting systems often rely on identification cards, which can be susceptible to duplication and misuse. In this paper, we propose a solution that utilizes biometric fingerprint recognition technology to authenticate voters, ensuring secure and reliable voting processes. The system involves the development of an online voting machine equipped with a fingerprint reader. During the registration process, voters' fingerprints are stored as unique identifiers. On the day of voting, the fingerprint reader acquires the voter's fingerprint and compares it with the pre-stored data to verify their identity. This eliminates the need for physical identification cards and reduces the risk of fraudulent activities. To maintain voter anonymity, the system assigns each user a unique and random ID, ensuring no connection to their personal details. The interface of the voting machine is designed to be user-friendly and intuitive, prioritizing clear visual representation of data and basic functionalities. This enables voters to cast their votes easily and confidently, enhancing the overall voting experience. The fingerprint-based fraud detection voting system offers several advantages over traditional methods. It significantly reduces the risk of voter fraud by relying on the uniqueness of fingerprints, which are difficult to forge or manipulate. Moreover, it eliminates the need for voters to carry identification cards, streamlining the voting process and reducing the chances of lost or stolen cards. Through this paper, we aim to

Authors

Akanksh R V
Department of Information Science Engineering
Dyananda Sagar College of Engineering
Bangalore-78

Hamsa K
Department of Information Science Engineering
Dyananda Sagar College of Engineering
Bangalore-78

Nisarga K
Department of Information Science Engineering
Dyananda Sagar College of Engineering
Bangalore-78

Saijyoti G Meti
Department of Information Science Engineering
Dyananda Sagar College of Engineering
Bangalore-78

Dr.Vaidehi M
Department of Information Science Engineering
Dyananda Sagar College of Engineering
Bangalore-78

contribute to the improvement of voting systems, ensuring fairness, accuracy, and transparency in the electoral process. By leveraging the power of biometric fingerprint technology, we can enhance the security and integrity of voting, fostering trust among voters.

Keywords: IoT, Arduino UNO, Arduino IDE, Fraud Detection, Voting System.

I. INTRODUCTION

Security is of primary concern and in this busy, competitive world, human cannot find ways to provide security to his confidential belongings manually. Instead, he finds an alternative which can provide a full fledged security as well as atomized. In the ubiquitous network society, where individuals can easily access their information anytime and anywhere, people are also faced with the risk that others can easily access the same information anytime and anywhere. Because of this risk, personal identification technology, which can distinguish between registered legitimate users and imposters, is now generating interest. Generally passwords, identification cards and PIN verification techniques are being used but the disadvantage is that the passwords could be hacked and a card may be stolen or lost. The most secured system is fingerprint recognition because a fingerprint of one person never matches the other. Biometrics studies commonly include fingerprint, face, iris, voice, signature, and hand geometry recognition and verification. Many other modalities are in various stages of development and assessment. Among these available biometric traits fingerprint proves to be one of the best traits providing good mismatch ratio, high accurate in terms of security and also reliable.

Biometrics is the science and technology of measuring and analyzing biological data. Biometrics refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, for authentication purposes. The field of biometrics was formed and has since expanded on too many types of physical identification. Among the several human fingerprints remain a very common identifier and the biometric method of choice among law enforcement. These concepts of human identification have led to the development of fingerprint scanners that serve to quickly identify individuals and assign access privileges. The basic point of these devices is also to examine the fingerprint data of an individual and compare it to a database of other fingerprints. In our paper we have used fingerprints for the purpose of voter identification or authentication. As the thumb impression of every individual is unique, it helps in minimizing the error. A database is created containing the fingerprint images of all the voters as required. Illegal votes and repetition of votes is checked for in this system with accurate coding. Hence with the application of this fingerprint based EVM system elections could be made fair and free from rigging. Further that the elections would no longer be a tedious and expensive job.

II. LITERATURE SURVEY

Rudrappa B. et. al., introduces an innovative approach to voting systems using fingerprint biometrics. The primary aim of this research is to develop a secure and efficient electronic voting system that leverages fingerprint authentication to ensure accurate and tamper-resistant voting. By registering eligible voters with their unique fingerprints and relevant details, the system can authenticate voters during the voting process, preventing unauthorized individuals from casting ballots. This biometric-based voting solution enhances security, reduces voter fraud, and ensures the integrity of the electoral process. With automatic vote counting and result generation, the system offers transparency and efficiency, contributing to modernizing and securing electoral processes. However, challenges related to data privacy and technological vulnerabilities require careful consideration for its successful implementation. Overall, the fingerprint-based voting system presents a promising solution to improve voting integrity and accuracy, ultimately bolstering public trust in democratic processes.[1]

The work by Khadija et.al, introduces an innovative and robust approach to enhance the security and integrity of voting systems through the use of fingerprint biometrics. In today's world, traditional voting methods often face challenges related to voter impersonation, ballot tampering, and electoral fraud, which can undermine the credibility and fairness of elections. To address these issues, the authors propose a biometric-based voting solution that leverages individuals' unique fingerprints for authentication and voting.The key components of the "Fingerprint Based Secured Voting" system are as follows: Firstly, the voter enrollment process involves registering eligible voters in the system by capturing their unique fingerprints along with other necessary details, which are then securely stored in a central database. During the voting process, the identity of each voter is verified using their registered fingerprint, ensuring that only authorized individuals can participate in the election. This biometric authentication adds an additional layer of security, mitigating the risk of multiple voting attempts or unauthorized access to the system. Once the voter's identity is authenticated, they can cast their votes electronically through the system. The integration of fingerprint biometrics in the voting process not only enhances security but also facilitates efficient and accurate vote counting.The implementation of the "Fingerprint Based Secured Voting" system offers several advantages. Firstly, it increases voter confidence by ensuring that each eligible citizen's vote is accurately recorded and counted. Secondly, it reduces the risk of electoral fraud and manipulations, safeguarding the integrity of the electoral process. Furthermore, by using electronic vote counting, the system minimizes the chances of manual counting errors and provides timely and reliable election results. This enhances the transparency and efficiency of the voting process, promoting public trust in democratic practices.However, like any voting system, the "Fingerprint Based Secured Voting" approach also comes with challenges that need to be addressed. Ensuring the privacy and security of voter data is of utmost importance, as any compromise in this regard could lead to potential misuse or unauthorized access to sensitive information. Additionally, the system needs to be resilient against potential technological vulnerabilities that could be exploited by malicious actors.In conclusion, the "Fingerprint Based Secured Voting" paper presented at the ICAC3 conference introduces a promising and forward-thinking solution to strengthen the security and reliability of voting systems. By harnessing the power of fingerprint biometrics, the proposed system aims to build trust and confidence in the electoral process, ensuring fair and transparent democratic practices. Addressing the challenges and implementing robust security measures will be crucial in successfully deploying such a system for future elections.[2]

Mohammed Khasawneh in his work has presented an advanced electronic voting (e-voting) solution that addresses the crucial issue of security in modern elections. E-voting has garnered attention for its potential to streamline the voting process, increase voter accessibility, and expedite result tabulation. However, the adoption of electronic voting systems also raises concerns about potential vulnerabilities, such as voter impersonation, ballot manipulation, and cyber threats. This paper tackles these challenges head-on by proposing a novel approach that leverages biometric authentication to enhance the integrity and privacy of election processes. The core innovation of the "biometric-secure e-voting system" lies in its utilization of biometric technology for voter authentication. During the initial enrollment phase, each eligible voter is required to register in the system by providing their unique biometric data, typically their fingerprints, which are then securely stored in a central database. This process ensures that every voter's identity is linked to their biometric signature, establishing a robust one-to-one relationship between the individual and their voting record. During the actual voting process, a voter's identity is verified through their biometric data before granting access to cast their ballot electronically. By using biometric authentication, the system significantly reduces the risk of voter impersonation and unauthorized access, thereby enhancing the overall security and credibility of the electoral process. This added layer of protection ensures that only legitimate voters can participate and that each vote is accurately attributed to its rightful origin. Furthermore, the "biometric-secure e-voting system" implements encryption and other security measures to safeguard the confidentiality and integrity of the cast votes. The use of cryptographic techniques ensures that the votes remain private and tamper-resistant, preventing any unauthorized parties from viewing or modifying the voting data. This aspect is crucial for building trust among voters and stakeholders and upholding the democratic principles of fair and transparent elections. While the paper presents an innovative and promising solution, it likely also addresses some of the potential challenges and considerations associated with implementing such a complex system. For instance, ensuring the proper handling and storage of biometric data to protect against potential data breaches and privacy concerns is of utmost importance. Additionally, the system's robustness against technical issues and potential attacks needs thorough evaluation and testing. In conclusion, the research paper on the "biometric-secure e-voting system for election processes" contributes significantly to the advancement of electronic voting technologies. By incorporating biometric authentication and stringent security measures, the proposed system addresses the crucial issues of voter verification, data privacy, and vote integrity. If effectively implemented, this innovative e-voting solution has the potential to enhance electoral processes, foster public trust, and strengthen the foundation of democratic practices worldwide.[3]

Oluwatosin in his work present that in the traditional voting processes, involving physical ballots and manual vote counting, often encounter various issues such as time-consuming procedures, logistical challenges, and the potential for human errors in tabulating results. Additionally, ensuring the legitimacy of voters and preventing fraudulent activities, such as voter impersonation, are crucial aspects of any credible electoral process. To overcome these challenges and improve the overall election process, the author proposes an online voting system that leverages biometric technology, a cutting-edge approach to individual identification and authentication. The key objective of the research is to design and implement an online voting system that offers convenience, security, and transparency. The system is intended to enable eligible voters associated with the University of Ibadan to cast their votes remotely from their devices, reducing the need for physical presence at polling stations. This enhances accessibility, especially for students who may be studying off-campus or unable to physically attend the elections .Biometric authentication is a central feature of the proposed system.

During the voting process, each voter's identity is verified using their unique biometric data, such as fingerprints or facial features. This ensures that only legitimate and authorized individuals can participate in the elections, effectively preventing voter impersonation and safeguarding the integrity of the electoral process. Biometric authentication adds an extra layer of security compared to traditional password-based systems, as it is difficult to forge or replicate an individual's biometric characteristics. The "Online voting system with biometric authentication for UI elections" is designed with robust security measures to protect the confidentiality and integrity of the votes. The transmission of voting data is likely encrypted to prevent interception and tampering, ensuring that each vote remains anonymous and tamper-resistant. Data security is of paramount importance in any electronic voting system, as the trust and credibility of the process depend on safeguarding sensitive information. Another significant advantage of the proposed system is the swift and accurate tabulation of votes. Once the voting period ends, the system automatically calculates and compiles the results, eliminating the need for manual vote counting. This expedites the declaration of election outcomes, promoting efficiency and reducing delays in announcing winners. While the thesis focuses on the benefits and potentials of the "Online voting system with biometric authentication for UI elections," it is essential to recognize that electronic voting systems also face challenges and considerations.

One crucial aspect is ensuring the privacy and security of biometric data. Safeguarding this sensitive information is vital to protect voters' privacy and prevent any unauthorized access or misuse of biometric records. Additionally, the proposed system must be resilient against potential cyber threats, such as hacking attempts or denial-of-service attacks, which could disrupt the voting process or compromise the integrity of results. In conclusion, Oluwatosin Adesua's thesis on the "Online voting system with biometric authentication for UI elections" presents a forward-thinking and technologically advanced solution to modernize and secure the electoral processes within the University of Ibadan. By introducing an efficient online voting system that incorporates biometric authentication and robust security measures, the proposed system aims to enhance accessibility, credibility, and voter confidence in the election process. However, further research and considerations are essential to ensure the system's privacy, integrity, and resilience against potential cyber threats, enabling a more comprehensive and successful implementation of the proposed system.[4].

The research work by Anil K. Jain etal., in their work likely delves into the algorithms and methodologies utilized in fingerprint matching for the purposes of identification and verification, with a particular focus on the work conducted by the authors from the Department of Computer Science and Engineering at Michigan State University. Fingerprint matching is a crucial area of research within the field of biometrics, which involves the use of unique physical or behavioral characteristics for individual identification and authentication. Fingerprint biometrics, in particular, have gained widespread adoption due to the high distinctiveness and permanence of fingerprint patterns, making them highly suitable for accurate and reliable identification. The paper is likely to start by providing a brief introduction to fingerprint biometrics, highlighting the significance of fingerprints as a biometric trait for personal identification. It may discuss the advantages of using fingerprints in various applications, such as law enforcement, border control, access control systems, and mobile devices. Following the introduction, the paper is likely to delve into the technical details of fingerprint matching algorithms. These algorithms aim to compare and match an input fingerprint with a reference database to establish a person's identity.

The authors are well-known experts in this area, and their contributions to fingerprint matching research are likely to be highlighted throughout the paper. One of the fundamental components of fingerprint matching is the extraction of distinctive features from the fingerprint image. These features are known as minutiae points, which include ridge endings and bifurcations. The paper may explore different techniques for minutiae extraction and representation, highlighting their advantages and limitations. Another essential aspect of fingerprint matching is the matching algorithm itself. The paper is likely to cover various matching techniques, such as pattern-based matching, minutiae-based matching, and correlation-based matching. Each method may be discussed in detail, along with its effectiveness in different scenarios. Furthermore, the paper may address the challenges encountered in fingerprint matching, such as the presence of noise and distortions in fingerprint images, partial or incomplete fingerprints, and the impact of skin conditions on fingerprint quality. The authors may present solutions and advancements made to address these challenges and enhance the accuracy of fingerprint matching. In addition to fingerprint identification, the paper may explore fingerprint verification techniques. Verification aims to determine whether a provided fingerprint matches the claimed identity of an individual. The authors may discuss the development of fingerprint verification systems and their applications in user authentication and access control. Throughout the paper, the authors may cite relevant studies and research papers, providing an extensive literature review of fingerprint matching in biometrics. The paper is likely to be well-supported with experimental results, demonstrating the performance and effectiveness of different fingerprint matching techniques. In conclusion, "Fingerprint Matching" by Anil K. Jain, Jianjiang Feng, and Karthik Nandakumar serves as a comprehensive and authoritative reference for researchers and practitioners in the field of biometrics and fingerprint matching. By exploring various fingerprint matching algorithms and methodologies, the paper contributes to advancements in biometric technology and its applications in identification and verification systems. The authors' expertise from the Department of Computer Science and Engineering at Michigan State University adds credibility to the research and reinforces its significance in the ongoing efforts to enhance the accuracy and reliability of fingerprint matching techniques.

III. SYSTEM ARCHITECTURE

The system architecture of a fingerprint-based fraud detection voting system is designed to ensure a secure and reliable voting process, mitigating potential fraudulent activities and enhancing the integrity of elections. Each key component plays a crucial role in achieving these objectives.

Fingerprint Capture Devices, these devices serve as the initial point of contact with voters. During the registration and voting phases, specialized fingerprint scanners or integrated sensors within electronic voting machines capture and record the unique fingerprints of eligible voters. These devices ensure accurate enrollment and authentication, as each individual's fingerprint is distinct, reducing the risk of duplicate or unauthorized voting .Database, the central database acts as the backbone of the system, storing the enrolled fingerprints of eligible voters along with their corresponding voter information, such as name, identification number, and voting eligibility status. The database allows for efficient retrieval and matching of fingerprints during the voting process, ensuring that only legitimate voters can cast their ballots. Voting Interface the voting interface provides voters with a user-friendly and intuitive platform to interact with the system and cast their votes securely.

This component may utilize touch screen interfaces or a combination of physical buttons and displays, accommodating voters of diverse backgrounds and preferences. Fraud Detection System, the fraud detection system is a critical component that monitors and analyzes voting data and fingerprint patterns in real-time. Its primary purpose is to detect any suspicious activities or anomalies that may indicate fraudulent behavior. For example, it can identify cases of multiple votes from the same individual or mismatches between enrolled fingerprints and the ones presented during voting. Security Measures, robust security measures are implemented to safeguard the system from potential threats and ensure the confidentiality and integrity of voting data. Sensitive information, such as fingerprints and voter data, is encrypted to prevent unauthorized access. Secure communication protocols establish secure connections between different system components, reducing the risk of data interception or tampering. Access control mechanisms restrict unauthorized access to sensitive areas of the system, enhancing its overall resilience against external threats. Additionally, an audit trail is maintained, recording system activities and changes, enabling administrators to monitor and track potential suspicious behavior. Reporting and Result Generation, once the voting process is complete, the system generates accurate and tamper-proof voting results based on the authenticated and verified votes.

This component ensures that the election outcome is reliable and free from manipulation. Moreover, detailed reports and statistics can be generated for auditing and transparency purposes, providing stakeholders with insights into the election process and results .In conclusion, the system architecture of a fingerprint-based fraud detection voting system combines various components to ensure a secure, efficient, and transparent electoral process. The integration of fingerprint capture devices, a centralized database, a user-friendly voting interface, a fraud detection system, robust security measures, and result generation mechanisms collectively contribute to the system's ability to prevent fraud and uphold the integrity of democratic elections**.**

IV. HARDWARE REQUIREMENT

For the Fingerprint based Fraud detection Voting system to operate effectively, seamless integration of the following hardware components is essential**:**

- Micro controller : Arduino
- Finger print reader
- Power Supply : 12V DC
- DC Motor
- 16x2 LCD Display

Software Requirement In addition to the hardware components, the following software requirements must be met:

- Arduino IDE (1.8.13)
- C programming language.

The smooth and accurate operation of the fingerprint-based fraud detection Voting System relies heavily on the correct installation and configuration of both hardware and software components. Any deviations or misconfigurations from the specified requirements may lead to system malfunction and inaccurate fraud detection, which could potentially result in substantial losses and compromise the integrity of the entire voting process. Ensuring meticulous attention to detail during the setup and implementation of the system is imperative to achieve its optimal performance and maintain the trust and reliability in the election process. The figure 1, depicts the entire operation of the proposed system. Figure 2, presents the circuit diagram comprising of Arduino IDE and other components like the sensors and the display.

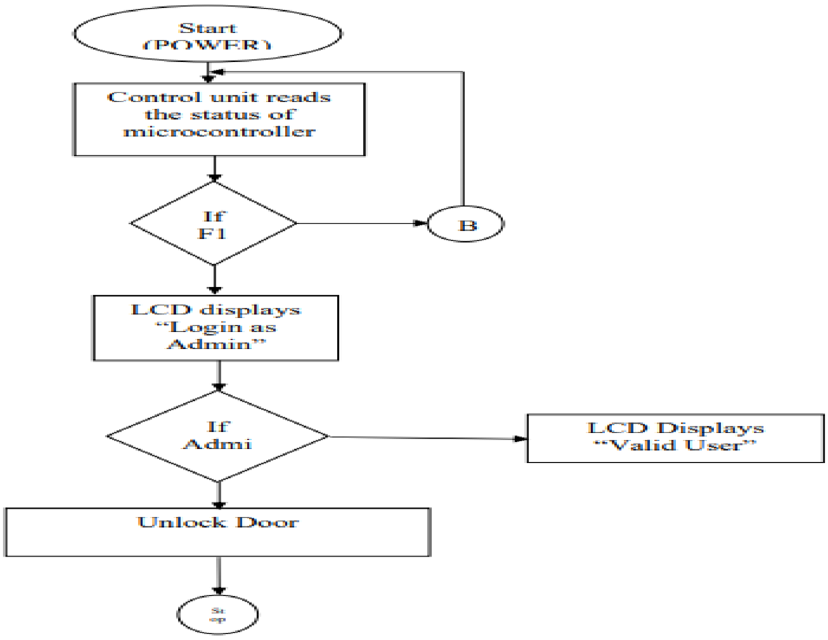

Start (POWER)
Control unit reads the status of microcontroller
If F1
B
LCD displays "Login as Admin"
If Admi
LCD Displays "Valid User"
Unlock Door
St op

Figure 1: Operational Flow Chart depicting the working of the

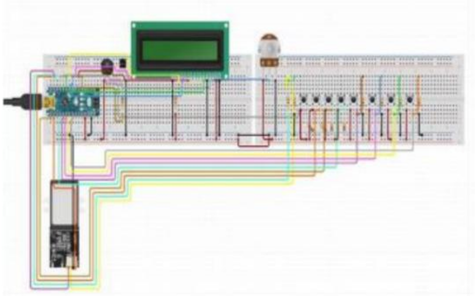


Figure 2: The Circuit Diagram

V. PROPOSED METHODOLOGY

The proposed methodology for the fingerprint-based fraud detection voting system is centered around leveraging biometric technology and advanced algorithms to enhance the security and accuracy of the voting process.

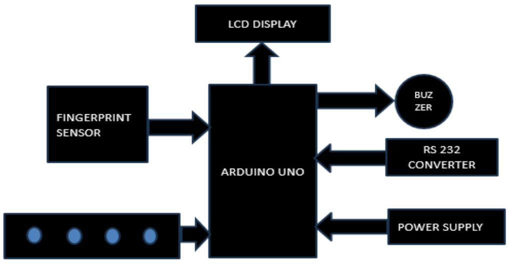


Figure 3: Block Diagram

Firstly, during the initial registration phase, eligible voters' unique fingerprints are enrolled and securely stored in a centralized database. This database acts as the repository for all enrolled fingerprints and corresponding voter information, ensuring a reliable reference for future authentication. During the voting phase, voters' fingerprints are captured using specialized fingerprint scanners or integrated sensors within electronic voting machines. The captured fingerprints are then compared in real-time with the enrolled templates in the database to verify the identity of each voter. This biometric authentication process ensures that only legitimate voters can participate in the election, significantly reducing the risk of fraudulent activities like multiple voting attempts or voter impersonation. The fraud detection system is a crucial component of the proposed methodology. It continuously monitors and analyzes voting data, fingerprint patterns, and user behaviors to identify any suspicious activities or anomalies. Advanced algorithms are employed to detect patterns that may indicate fraudulent behavior, such as irregular voting patterns or attempts to manipulate the system. The system promptly alerts the election administrators to any potential fraud, allowing them to take appropriate actions and ensure the integrity of the voting process. Security measures are embedded throughout the system to protect against potential threats and maintain data confidentiality. Sensitive information, such as fingerprints and voter data, is encrypted to prevent unauthorized access. Robust access control mechanisms restrict entry to authorized personnel only, reducing the risk of internal tampering. Additionally, the system maintains an audit trail to track and log all system activities, enabling administrators to review and investigate any security incidents or suspicious behavior. Regular system maintenance, updates, and performance evaluation are crucial aspects of the proposed methodology. Continuous monitoring and evaluation help identify and address potential vulnerabilities, ensuring that the system remains up-to-date and effective against emerging security threats. Overall, the proposed methodology for the fingerprint-based fraud detection voting system combines biometric technology, advanced algorithms, and stringent security measures to create a robust and reliable electoral system. By leveraging the unique characteristics of individuals' fingerprints for authentication and implementing proactive fraud detection mechanisms, the proposed methodology aims to instill trust, transparency, and fairness in the electoral process, reinforcing the foundation of democratic principles.

To elaborate on the normal execution of the system, the following steps are taken:

1. **Voter Registration:** Initially, voters need to register their fingerprints with the voting system. This is a one-time process where each voter places their finger on the fingerprint reader, and the system records and stores their unique fingerprint data along with their personal details in a secure database.

2. **Voting Process:** On election day, registered voters enter the ballot room to cast their votes. The voter places their fingerprint on the fingerprint module again to initiate the voting process. The fingerprint reader compares the live fingerprint with the stored registered fingerprints in the database.

3. **Fingerprint Verification:** If the fingerprint matches with one of the registered fingerprints in the database, the system proceeds to the next step. Otherwise, the voter is not authorized to cast a vote. The LCD display will show that the voter is authorized, and the voting process continues.

4. **Voting Authorization**: After successful fingerprint verification, the voter is presented with a list of candidate options. The voter can select the candidate they wish to vote for by making the appropriate selection using the voting interface.

5. **Anti-Double Voting Mechanism:** The system ensures that each voter can cast only one vote. If a voter attempts to vote for the second time, the buzzer will be activated to signal an alert, indicating that the voter has already cast their vote.

6. **Voting Results:** As voters cast their votes, the system counts and stores the votes for each candidate. The voting process continues until all registered voters have cast their votes. Once the voting is complete, the system generates the voting results based on the tallied votes for each candidate.

7. **Admin Access**: Only authorized administrators have access to view the voting results. The administrator can access the system and view the results, which typically include the total number of votes cast, the number of votes received by each candidate, and the overall outcome of the election.

System Analysis Here shows the target environment (hardware and software) for which the system is being developed.

1. **Arduino UNO**: Figure 4 shows the the Arduino Uno , it is a microcontroller board based on the ATmega328. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started. The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega8U2 programmed as a USB-to serial converter. "Uno" means one in Italian and is named to mark the upcoming release of Arduino 1.0. The Uno and version1.0 will be the reference versions of Arduino, moving forward. The Uno is the latest in a series of USB Arduino boards, and the reference model for the Arduino platform.

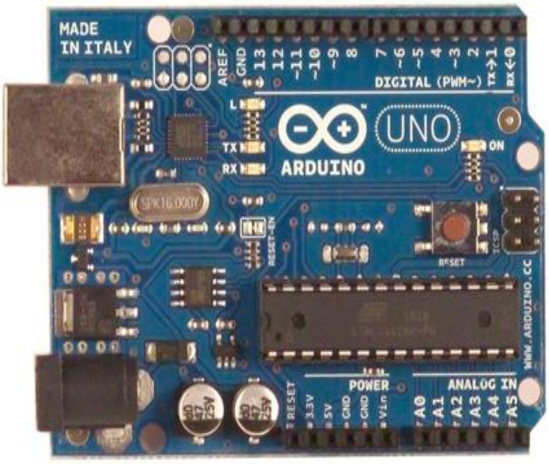


Figure 4.: Arduino UNO

2. **Fingerprint Reader:** A Fingerprint Reader in figure 5, is a biometric device used to capture and verify the unique fingerprint patterns of voters. It plays a critical role in the voting process by ensuring that only authorized and registered voters are allowed to cast their votes. Fingerprint processing includes two parts: fingerprint enrollment and fingerprint matching (the matching can be 1:1 or 1:N). When enrolling, user needs to enter the finger two times. The system will process the two time finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library. For 1:1 matching, system will compare the live finger with specific template designated in the Module; for 1:N matching, or searching, system will search the whole finger library for the matching finger. In both circumstances, system will return the matching result, success or failure.

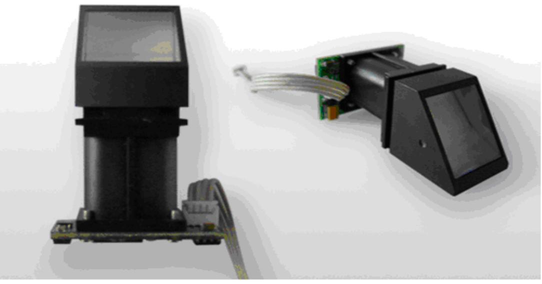


Figure 5: Fingerprint Reader

3. **Power Supply:** Figure 6 shows the voltage regulator, the circuit needs two different voltages, +5V & +12V, to work. These dual voltages are supplied by this specially designed power supply. The power supply, unsung hero of every electronic circuit, plays very important role in smooth running of the connected circuit. The main object of this ‘power supply’ is, as the name itself implies, to deliver the required amount of stabilized and pure power to the circuit. The stabilization of DC output is achieved by using the three terminal voltage regulator IC. This regulator IC comes in two flavors: 78xx for positive voltage output and 79xx for negative voltage output.

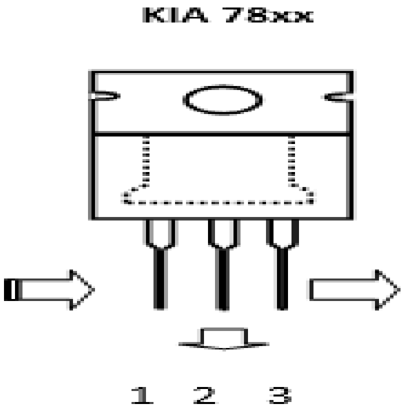


Figure 6: Voltage Regulator

4. **DC Motor:** A DC motor in figure 7, is an electric motor that runs on direct current power. In any electric motor, operation is dependent upon simple electromagnetism. A current carrying conductor generates a magnetic field, when this is then placed in an external magnetic field, it will encounter a force proportional to the current in the conductor and to the strength of the external magnetic field. A DC motor is any of a class of rotary electrical machines that converts direct current electrical energy into mechanical energy. It works on the fact that a current carrying conductor placed in a magnetic field experiences a force which causes it to rotate with respect to its original position. Nearly all types of DC motors have some internal mechanism, either electromechanical or electronic, to periodically change the direction of current flow in part of the motor. DC motors were the first form of motor widely used, as they could be powered from existing direct-current lighting power distribution systems. A DC motor's speed can be controlled over a wide range, using either a variable supply voltage or by changing the strength of current in its field windings. Small DC motors are used in tools, toys, and appliances.

Figure 7: DC Motor

5. **16x2 LCD Display:** LCD stands for Liquid Crystal Display. The most commonly used LCDs found in the market today are 1 Line, 2 Line or 4 Line LCDs which have only 1 controller and support at most of 80 characters. Display data RAM (DDRAM) stores display data represented in 8-bit character codes. Its extended capacity is 80 X 8 bits, or 80 characters. The area in display data RAM (DDRAM) that is not used for display can be used as general data RAM. So whatever you send on the DDRAM is actually displayed on the LCD.

Figure 8: 16x2 LCD Display

VI. NOVELTY

This paper describes a forest fire detection system using IoT. The system incorporates several features to ensure efficient detection and timely response to forest fires.

1. **Voter Registration:** During the voter registration phase, each voter's fingerprint is captured using a fingerprint reader and associated with their personal details in a local database. This database will be stored securely within the voting system's hardware.

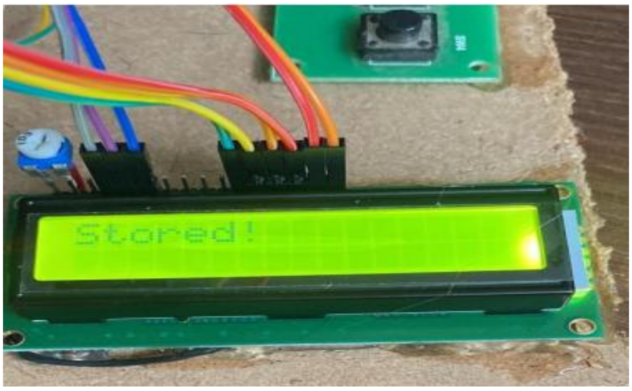


Figure 9: Fingerprint Registered

2. **Voting Process:** On election day, registered voters enter the ballot room to cast their votes. The voter places their fingerprint on the fingerprint module again to initiate the voting process. The fingerprint reader compares the live fingerprint with the stored registered fingerprints in the database.

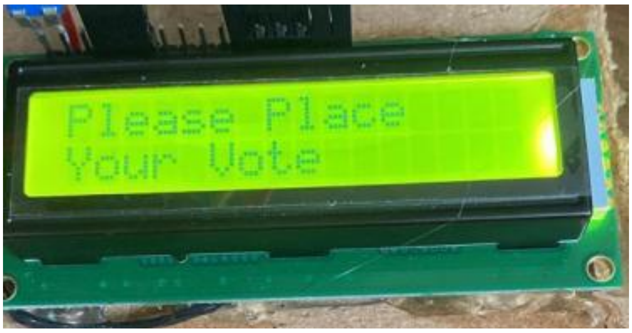
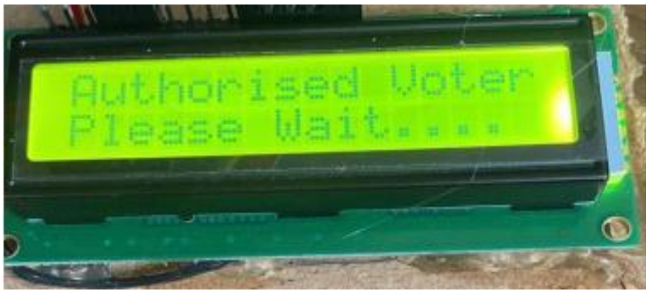


Figure 10: Voting Process

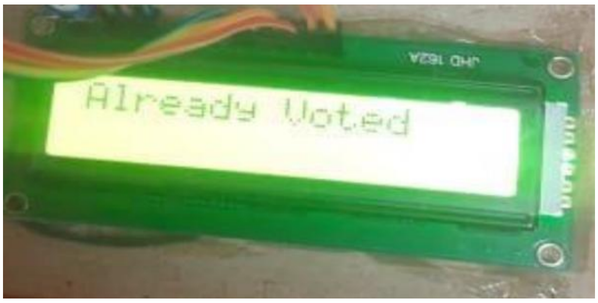
3. **Voter Authorization:** When a registered voter approaches the voting system to cast their vote, they must place their finger on the fingerprint reader once again. The reader captures the live fingerprint of the voter and converts it into a biometric template. If the fingerprint matches with one of the registered fingerprints, the voter is authorized to proceed with the voting process. This authorization ensures that only legitimate voters can cast their votes and prevents impersonation or double voting attempts.



```
Authorised Voter
Please Wait....
```

Figure 11: Voter Authorization

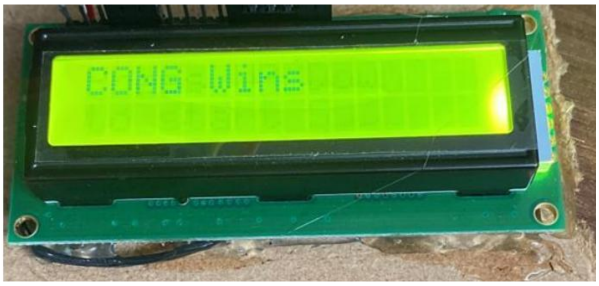
4. **Anti-Double Voting Mechanism:** To prevent double voting, the system keeps track of which voters have already cast their votes. If a voter attempts to vote for the second time, the system will display an alert indicating that the voter has already cast their vote. If the voter is trying to cast vote for second time then buzzer will give signal.



```
Already Voted
```

Figure 12: Fraud Detection

5. **Voting Results:** At the end of the election, the system in figure 13 displays the local voting results, indicating the number of votes received by each candidate. This approach ensures data integrity and security, as the results are kept within the voting system's hardware, reducing the risk of external tampering or unauthorized access.



```
CONG Wins
```

Figure 13: Sample result

VII. CHALLENGES AND LIMITATIONS

Fingerprint-based fraud detection voting systems offer several advantages, but they also come with certain challenges and limitations:

1. **Biometric Accuracy:** Fingerprint recognition may not be 100% accurate due to factors like worn-out or damaged fingers, poor image quality, or errors in the biometric algorithm, leading to false positives or false negatives.

2. **Cost and Infrastructure**: Implementing and maintaining a fingerprint-based system can be costly, especially for large-scale elections. It requires investing in reliable hardware, software, and database management.

3. **Voter Enrollment:** Registering and enrolling voters' fingerprints can be time-consuming, particularly in regions with a large voter population or limited access to technology.

4. **Privacy Concerns**: Storing and managing biometric data raises privacy concerns. Ensuring the security and confidentiality of fingerprint data is crucial to prevent potential misuse or data breaches.

5. **Accessibility and Inclusivity:** Some voters, particularly the elderly or disabled, may face challenges using fingerprint readers, limiting their accessibility to the voting process.

6. **Duplication Attempts:** Determined fraudsters may attempt to replicate fingerprints to impersonate legitimate voters. This necessitates robust anti-spoofing measures in the biometric system.

7. **Maintenance and Reliability**: Fingerprint readers require regular maintenance and calibration to maintain their accuracy and reliability, and technical failures during elections can disrupt the voting process.

8. **System Complexity:** Introducing a new and complex voting system requires voter education and training for both administrators and voters to ensure its smooth operation.

9. **Laws and Regulations:** Compliance with data protection laws and regulations is essential to safeguard voter privacy and prevent misuse of biometric data.

10. **Fallback Mechanisms:** The system needs to have fallback mechanisms in case of fingerprint recognition failures, allowing voters to use alternative identification methods if necessary.

Despite these challenges, fingerprint-based fraud detection voting systems can significantly enhance the security and integrity of elections. Addressing these limitations through continuous improvement and careful implementation can lead to a more robust and trustworthy voting system.

VIII. FUTURE SCOPE

The fingerprint-based fraud detection voting system holds promising future prospects due to its inherent advantages in ensuring secure and tamper-resistant elections. Some potential future scopes for this system include:

1. **Enhanced Security:** Advancements in biometric technology can lead to even more secure and accurate fingerprint recognition, making the system more robust against potential fraud attempts.

2. **Integration with Blockchain:** Combining fingerprint-based voting with blockchain technology can further enhance transparency and immutability, ensuring a verifiable and tamper-proof record of votes.

3. **Mobile Voting**: As mobile devices become more sophisticated in biometric capabilities, the system could be adapted for secure and convenient voting using smartphones.

4. **Wider Adoption:** Governments and organizations worldwide might adopt the system to conduct secure elections, thereby enhancing voter confidence and participation.

5. **Accessibility and Inclusivity:** Research on accommodating individuals with disabilities through biometric technology can lead to more inclusive voting systems.

6. **Data Privacy Advancements**: Ongoing research can focus on refining privacy measures, ensuring that biometric data remains secure and protected.

7. **Interoperability**: Future developments could work towards creating standardized biometric systems that can be seamlessly integrated into different voting infrastructures.

8. **Real-time Monitoring:** Incorporating real-time monitoring features would allow administrators to detect and respond promptly to any anomalies during the voting process.

9. **Machine Learning for Fraud Detection:** Implementing machine learning algorithms can continuously analyze voting patterns and detect unusual behaviors or fraudulent activities.

10. **International Use:** With advancements, the system may gain recognition as a secure and reliable voting method, encouraging its adoption in international elections and improving election integrity globally.

Overall, the future of the fingerprint-based fraud detection voting system looks promising, with ongoing technological advancements aimed at enhancing security, accuracy, and accessibility in the electoral process.

IX. CONCLUSION

In conclusion, the implementation of a fingerprint-based fraud detection voting system offers significant advancements in the security and integrity of the voting process. By leveraging the unique biometric characteristics of fingerprints, this system ensures accurate identification of voters and effectively detects fraudulent activities. Through the development and integration of fingerprint enrolment, real-time matching, fraud detection mechanisms, and a user-friendly interface, the voting system provides a robust solution. It enables authorized voters to cast their vote seamlessly while preventing unauthorized individuals from participating multiple times. The system's ability to integrate with existing voter registration databases further enhances its effectiveness and reliability. The administrator's access to comprehensive result analysis and reporting facilitates informed decision-making and ensures transparency in the electoral process. Through rigorous testing and evaluation, the system's functionality, accuracy, and security are validated, instilling confidence in its performance. Once deployed, ongoing maintenance and support are essential to ensure the system's continuous operation and adaptability to evolving needs. Overall, the fingerprint-based fraud detection voting system addresses the critical challenges of voter authentication and fraud prevention. Its successful implementation significantly contributes to fair and trustworthy elections, safeguarding the democratic principles of transparency, accuracy, and inclusivity.

REFERENCES

[1] Signals, Systems and Computers, 2004 Conference Record of the Thirty-Eighth Asilomar Conference on Publication 7-Nov-2004 Volume: 1, on page(s): 577-581 Vol.1.
[2] International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012.
[3] International Journals of Biometric and Bioinformatics, Volume (3): Issue (1).
[4] Mukesh Kumar Thakur, Ravi Shankar Kumar, Mohit Kumar, Raju Kumar "Wireless Fingerprint Based Security System using Zigbee" , International Journal of Inventive Engineering and Sciences (IJIES) ISSN: 2319–9598, Volume-1, Issue-5, April 2013.
[5] Mary Lourde R and Dushyant Khosla, "Fingerprint Identification in Biometric Security Systems", International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010.
[6] "Fingerprint Matching" by Anil K. Jain, Jianjiang Feng and Karthik Nandakumar, Department of Computer Science and Engineering, Michign State University. About Authors: A .Aditya Shankar is a final year undergraduate student, Dept. Of Electronics and Communication Engineering from Dadi Institute of Engineering and Technology, Visakhapatnam, Andhra Pradesh. His main areas of interest are Sensor Technology, Analog and Digital Circuits, Embedded Systems and Wireless Communication & Networking.
[7] Fingerprint Based Secured Voting Khadija Hasta; Aditya Date; parna Shrivastava; Prajakta Jhade; S. N. Shelke 2019 International Conference on Advances in Computing, Communication and Control (ICAC3)
[8] Year: 2019 | Conference Paper | Publisher: IEEE
[9] Fingerprint-Based Vote Marking System for Elector Identification G John Baptist; K Vishnu; S Sneha;
[10] Kg Arya; L R Silpa Sangeeth 2023 International Conference on Signal Processing, Computation, Electronics, Power and Telecommunication (IConSCEPT) Year: 2023 | Conference Paper | Publisher: IEEE
[11] Online Smart Voting System Using Biometrics Based Facial and Fingerprint Detection on Image Processing and CNN S.JEHOVAH JIREH ARPUTHAMONI; A.GNANA SARAVANAN 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) Year: 2021 | Conference Paper | Publisher: IEEE
[12] Arduino based Electronic Voting System with Biometric and GSM Features Venkateswara Rao Ch;
[13] M V Pathi A; B S Sailesh A 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT) Year: 2022 | Conference Paper | Publisher: IEEE
[14] A fingerprint matching technique using minutiae based algorithm for voting system: A survey Talib Divan;
[15] Veena Gulhane 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT) Year: 2015 | Conference Paper | Publisher: IEEE
[16] EVMFFR: Electronic Voting Machine with Fingerprint and Facial Recognition Thirumal R.; Rahul B. R.; Rahulpriyesh B.; Konguvel E.; Sumathi G. 2022 Second International Conference on Next Generation Intelligent Systems (ICNGIS) Year: 2022 | Conference Paper | Publisher: IEEE
[17] Smart electronic voting system based on biometric identification-survey J. Deepika; S. Kalaiselvi; S. Mahalakshmi; S. Agnes Shifani 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM) Year: 2017 | Conference Paper | Publisher: IEEE
[18] Development of Fingerprint Voting Application using Aadhar card Kalaimathi. B; Rajasekar. T; Kowsalya. M; Pooja.J. M; Priya. T 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) Year: 2023 | Conference Paper | Publisher: IEEE
[19] Location-free Voting System with the help of IOT Technology Qasim Abbas; Tariq Ali; Hussnain Abass;
[20] Sarah Javaid; Tanzeela Hussain 2018 12th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS) Year: 2018 | Conference Paper | Publisher: IEEE

[21] Development of a credible and integrated electronic voting machine based on contactless IC cards, biometrie fingerprint credentials and POS printer Syed Mahmud Hasan; Md. Tahmid Rashid; Md. Shadman Sakib Chowdhury; Md. Khalilur Rhaman 2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE) Year: 2016 | Conference Paper | Publisher: IEEE

[22] Voting System based on BlockChain and using Iris Recognition Subha P; Padmasree P; Sowndharya Lakshmi R 2021 4th International Conference on Computing and Communications Technologies (ICCCT) Year: 2021 | Conference Paper | Publisher: IEEE

[23] Biometric Based Secured Remote Electronic Voting System Samarth Agarwal; Afreen Haider; Abhishek Jamwal; Param Dev; Rajeevan Chandel 2020 7th International Conference on Smart Structures and Systems (ICSSS) Year: 2020 | Conference Paper | Publisher: IEEE

[24] Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract Syada Tasmia Alvi; Mohammed Nasir Uddin; Linta Islam 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT) Year: 2020 | Conference Paper | Publisher: IEEE

[25] Arduino Based Secure Electronic Voting System with IoT and PubNub for Universities K C Arun; Shahbaz Ahmad; Saba Noor; Iqra Mumtaz; Mubashir Ali 2022 Second International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE) Year: 2022 | Conference Paper | Publisher: IEEE

[26] Secured Smart Voting System using Aadhar B Madhuri; M G Adarsha; K R Pradhyumna; B M Prajwal

[27] 2017 2nd International Conference On Emerging Computation and Information Technologies (ICECIT) Year: 2017 | Conference Paper | Publisher: IEEE

[28] Design and implementation of convenient and compulsory voting system using finger print sensor and GSM technologies Pradeep Kumara V.H.; Ravindra P. Rajput 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA) Year: 2020 | Conference Paper | Publisher: IEEE

[29] Electronic Voting Machine Using Fingerprint Scanner with Image Enhancement Technique Sai Deepak Alapati; Chandana Chennamsetty; Pujitha Dantam; Anusha Dabbara; Muthukumar Arunachalam 2023 International Conference on Computer Communication and Informatics (ICCCI) Year: 2023 | Conference Paper | Publisher: IEEE

[30] Enhancing the Security of Online Voting System Using Defined Biometrics Devanshi Malik; Kritika Tripathi; Jyotsna 2023 IEEE 3rd International Conference on Technology, Engineering, Management for Societal impact using Marketing, Entrepreneurship and Talent (TEMSMET) Year: 2023 | Conference Paper | Publisher: IEEE

[31] Biometrically secured electronic voting machine Rahil Rezwan; Huzaifa Ahmed; M. R. N. Biplob; S. M. Shuvo; Md. Abdur Rahman 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC) Year: 2017 | Conference Paper | Publisher: IEEE

[32] Biometric Voting Machine Based on Fingerprint Scanner and Arduino Atharva Jamkar; Omkar Kulkarni;

[33] Aarti Salunke; Anton Pljonkin 2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT) Year: 2019 | Conference Paper | Publisher: IEEE