Hyderabad Karnataka Education Society's

Poojya Doddappa Appa Engineering College, Kalaburagi

(An Autonomous Institution, affiliated to VTU, Belagavi)

A PROJECT REPORT

ON

"ARDUINO-BASED FINGERPRINT VOTING SYSTEM: ENSURING ACCURATE AND FRAUD-FREE ELECTION"

Submitted in the partial fulfillment of the requirements for the award of the degree of Bachelor of Engineering in Computer Science and Engineering

Submitted by

Mr. ABHAY H.D	**3PD19CS001**
Miss. MADHURI	**3PD19CS037**
Miss. MANSI BENNUR	**3PD19CS043**

Under the Guidance of

Dr. SHARANABASAPPA GANDAGE

Assistant Prof, CSE Dept, PDACEK

Department of Computer Science and Engineering

POOJYA DODDAPPA COLLEGE OF ENGINEERING, KALABURAGI

2022-2023

`

Hyderabad Karnataka Education Society's

Poojya Doddappa Appa Engineering College, Kalaburagi

CERTIFICATE

This is to certify that the Project work entitled **"ARDUINO-BASED FINGERPRINT VOTING SYSTEM: ENSURING ACCURATE AND FRAUD-FREE ELECTION"** carried out by **ABHAY H.D (3PD19CS001), MADHURI (3PD19CS037), MANSI BENNUR (3PD19CS043)** in partial fulfillment for the award of Bachelor of Engineering in Computer Science & Engineering of Poojya Doddappa College of Engineering, Kalaburagi, an Autonomous Institution, affiliated to Visvesvaraya Technological University, Belagavi during the academic year 2022-2023. The project has been approved as it satisfies the academic requirements in respect of project work prescribed for the said degree.

Dr. Sharanabasappa Gandage	Dr. Prakash Pattan	Dr. Sujata Terdal	Dr. S.R.Mise
(Guide name)	(Project Coordinator)	(HOD Dept. of CSE)	(Principal)

Examiners : **Signature with Date**

1.

2.

Acknowledgement

We express our deep sense of gratitude and indebtness to our esteemed instituted "PDA COLLEGE OF ENGINEERING", KALABURAGI which has provided us an opportunity to fulfill the most cherished desire to reach our goal.

We would like to express our sincere thanks to Dr. S.R. MISE Principal P.D.A.C.E.K for his valuable support during the development of this project work.

It's our great pleasure to express our heartiest thankfulness and gratitude to our H.O.D Dr. SUJATA TERDAL who has been the inspiration right from the starting till its completion of the project work successfully

We would like to showcase our gratitude to the project coordinator Dr. PRAKASH PATTAN for his valuable guidance, keen interest, and encouragement at various stages of our project.

Our special gratitude to our guide Dr. SHARANABASAPPA GANDAGE for his inspiration, guidance, constant supervision, direction and discussions in successful completion of the Project Report.

Last but not least we express our deep sense of gratitude to the teaching and non-teaching staff members of the department who have cooperated and supported us in direct or indirect way during the completion of the project work.

ABHAY H.D	**3PD19CS001**
MADHURI	**3PD19CS037**
MANSI BENNUR	**3PD19CS043**

ABSTRACT

The Indian democratic system relies heavily on an efficient and secure voting process. This project aims to enhance the existing Indian voting system by implementing a biometric-based solution using Arduino technology. By incorporating biometric authentication, the proposed system offers increased security and cost-effectiveness compared to the current methods, reducing the likelihood of rigging and malpractice during elections. The system leverages biometric identifiers such as fingerprints to ensure accurate authentication of voters. Every individual possesses a unique fingerprint, making it an ideal biometric characteristic to prevent fraudulent voting practices. The voter data, including fingerprint information and phone numbers, is stored in a registration database, ensuring comprehensive records of eligible voters. To provide real-time feedback to voters, a GSM module is employed to send messages confirming successful vote casting. Furthermore, alert messages are sent to remind voters who haven't cast their votes, while any attempts of re-voting trigger an alert message to the nearest police station, preventing duplicate voting. In terms of data storage, instead of using Wi-Fi modules, the system utilizes Google Spreadsheet as a platform to store polling data securely. This includes the number of votes polled for each respective party and the final results of the winning party. By employing Arduino technology and integrating biometric authentication, this project establishes an Arduino-based biometric voting system that ensures accurate and fraud-free elections. The elimination of fake voters, enhanced security measures, real-time voter feedback, and reliable data storage contribute to a more robust and transparent electoral process, strengthening the democratic foundation of India.

CONTENTS

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION TO THE TOPIC

Voting is an essential right bestowed upon every citizen in a democratic country like India. It allows individuals to express their opinions and choose their leaders. Elections are not only conducted at the national level but also within schools, colleges, banks, societies, and other organizations. However, ensuring the integrity and fairness of the voting process has been a constant challenge. To address this, the integration of biometrics has emerged as a promising solution.

Biometrics refers to the recognition of individuals based on their physical characteristics, such as fingerprints, iris patterns, facial features, and voice. In this project, the focus is on fingerprint recognition as a biometric identifier. Each person possesses a unique fingerprint, making it an ideal marker for signature verification and authentication. Fingerprint matching methods can be categorized into correlation-based matching, minutiae-based matching, and pattern-based (or image-based) matching.

In correlation-based matching, fingerprint images are superimposed, and the correlation between corresponding pixels is computed. Minutiae-based matching involves extracting minutiae from the fingerprints and finding alignments that result in the maximum number of minutiae pairings. Pattern-based matching compares the stored template with the candidate's fingerprint, aligning the images based on orientation.

This project utilizes fingerprint authentication to ensure the integrity of the voting process. The fingerprints of eligible candidates are enrolled and stored in the system. During voting, the stored fingerprints are matched with the database, along with the corresponding Unique numbers, to verify the identity of the voter. The system also checks for any attempts at multiple voting, preventing malpractices.

To enhance accessibility and efficiency, the voting system is designed to operate online using platforms like Google Spreadsheet. This allows voters to cast their votes from anywhere in the world and enables real-time result computation. By leveraging cloud technology, the system provides a faster and more streamlined approach to conducting elections.

The traditional method of voting, involving paper-based ballots and manual counting, was time-consuming and prone to errors. The introduction of electronic voting machines brought some improvements, but concerns about security and accuracy persist. This project aims to address these issues by implementing an Arduino-based biometric voting system that ensures a secure and fraud-free electoral process.

The system's functionalities include fingerprint-based voter authentication, prevention of duplicate voting, real-time result storage in the cloud, and alert generation in case of malpractices. By combining biometrics, cloud technology, and Arduino programming, the project aims to create an efficient and reliable voting system.

The subsequent sections of this report will deliver into the design, implementation, and evaluation of the Arduino-based biometric voting system. The system's effectiveness in preventing malpractices and ensuring accurate election results will be assessed. Through this project, it is hoped that the Indian voting system can be strengthened, promoting transparency, trust, and the democratic values of the nation.

1.2 PROBLEM STATEMENT

During elections, two major issues commonly arise, causing problems for the voting population. Firstly, disputes often arise regarding the eligibility of elderly voters. This issue stems from variations in staff levels within the academic ladder and the time difference between promotions to the next level. These discrepancies create confusion and uncertainty about who is eligible to vote. Secondly, elderly voters often face long queues, leading to fatigue and potential voter coercion by candidates and their campaign teams taking advantage of the situation.

These factors contribute to a lack of credibility and fairness in staff elections. There is a clear need for a system that addresses the inefficiencies of the current voting process and provides features to overcome these challenges. By implementing an improved voting system, these issues can be solved, ensuring a more credible and fair election process.

1.3 OBJECTIVES

The aim of the project is to develop an application that enhances the election process for staff elections through the implementation of various stages of security authentication. The case study focuses on creating an efficient platform that allows eligible voters to exercise their right to vote from a specific location during the election period.

The objectives of the project are as follows:

- To establish a secure platform that ensures the authenticity of votes and voters by implementing mechanisms such as fingerprint registration. This aims to prevent unauthorized access and ensure that only eligible voters can participate in the election.
- To enhance the identification of voters by utilizing biometric features that are unique to each individual. By relying on biometric authentication, the project aims to eliminate the possibility of sharing voter credentials and enhance the accuracy and integrity of the election process.
- To address the issue of long queues during the voting period. By enabling voters to cast their votes from a specific location, the project aims to streamline the voting process, reduce waiting times, and enhance the overall efficiency of the elections.

By achieving these objectives, the project aims to provide a secure, convenient, and efficient platform for staff elections, ultimately improving the overall electioneering process.

1.4 SCOPE

The scope of the project is centered around the development of a biometric voting system that utilizes fingerprint registration to enable voters to participate in elections from their respective physical locations. The key components of the scope include:

- Biometric Voting System: The project aims to design and implement a comprehensive biometric voting system that ensures the authenticity and integrity of votes through fingerprint registration. By leveraging biometric technology, the system will enhance the accuracy and security of the voting process.

- Fingerprint Registration: The system will include a mechanism for registering the fingerprints of eligible voters. This registration process will establish a unique biometric identity for each voter, which will be used for authentication during the voting process.
- Remote Participation: The system will enable voters to participate in the elections from their physical location, eliminating the need for them to be present at a specific polling station. This remote participation feature will provide convenience and accessibility to voters, allowing them to exercise their democratic rights from anywhere.
- Authentication and Verification: The project will incorporate robust authentication and verification mechanisms to ensure that only eligible voters can cast their votes. The fingerprint registration data will be used to authenticate voters and verify their identity during the voting process.
- Security and Integrity: The scope includes implementing stringent security measures to safeguard the voting system from unauthorized access, tampering, or manipulation. Data encryption, secure communication channels, and other security protocols will be employed to maintain the integrity of the voting process.
- Scalability and Flexibility: The project will consider the scalability and flexibility aspects, allowing the system to handle a large number of voters and adapt to future technological advancements. The architecture and design will be scalable to accommodate the growing needs of the electoral process.

By focusing on these aspects, the project aims to contribute to the improvement of the election process by providing a secure, efficient, and accessible voting system based on biometric authentication using fingerprint registration.

1.5 EXISTING SYSTEM

The current voting system utilizes Electronic Voting Machines (EVMs) consisting of a control unit and a balloting unit. However, several issues persist within this system, prompting the need for an improved solution like the Arduino-Based Biometric Voting System, which ensures accurate and fraud-free elections.

In the existing system, voters are required to carry their ID cards for verification. The presiding officer manually checks the list and ID card to verify the voter's eligibility, which is time-consuming and prone to errors. The Arduino-Based Biometric Voting System addresses this problem by incorporating biometric authentication, such as fingerprint recognition. Each voter's fingerprint data is securely stored in the system, and upon verification, the voter can cast their vote. This eliminates the need for manual ID checks and streamlines the verification process, saving time and improving efficiency.

Security concerns also plague the existing system. It is possible for unauthorized individuals to tamper with the program installed in the EVMs, compromising the integrity of the election. The Arduino-Based Biometric Voting System provides enhanced security measures, ensuring the integrity of the voting process. By utilizing the unique fingerprint of each individual, the system establishes a secure and tamper-proof means of identification and authentication. This significantly reduces the risk of unauthorized access and manipulation.

Verifiability is another crucial aspect of a reliable voting system. In the existing system, it is difficult to independently verify whether all votes have been counted correctly. The Arduino-Based Biometric Voting System addresses this concern by providing real-time result calculation and transparency. The system can display the voting results instantly, allowing for immediate verification by stakeholders and preventing any discrepancies or manipulation in the counting process.

Additionally, the availability of the existing system is a concern, as it only operates during the polling period. In contrast, the Arduino-Based Biometric Voting System ensures availability throughout the voting process. Voters can cast their votes from anywhere, and the system can handle a larger volume of voters simultaneously. This accessibility and scalability promote inclusivity and efficiency in the electoral process.

Lastly, the existing system is susceptible to fraudulent practices, such as one candidate casting votes illegally for multiple members. The Arduino-Based Biometric Voting System provides a robust solution to this problem. Each voter's unique biometric data ensures that only eligible individuals can cast their votes, eliminating the possibility of unauthorized voting or proxy voting.

In conclusion, the Arduino-Based Biometric Voting System offers a comprehensive solution to the issues present in the current voting system. By incorporating biometric authentication, enhancing security, providing verifiability, ensuring availability, and preventing fraudulent practices, this system guarantees accurate and fraud-free elections, instilling trust and confidence in the democratic process.

1.6 PROPOSED SYSTEM

The proposed Arduino-Based Biometric Voting System aims to ensure accurate and fraud-free elections by utilizing the fingerprint as a biometric method of verification and implementing an online version of the system. The system operates by enrolling and storing the unique fingerprint of each voter in a database.

During the voting process, the system prompts the voter to enter their unique ID. If the entered ID matches the stored number in the database, the system proceeds to verify the fingerprint. If the fingerprint matches the enrolled data, the system checks whether the person has already voted for the same election. If no previous vote is found, the system displays a "Fingerprint and ID match. Cast vote" message, allowing the voter to proceed.

Voting is facilitated using a keypad. Once the message to cast a vote is displayed, the voter is granted the opportunity to input an OTP (One-Time Password) using the keypad. This additional security measure ensures that only authorized voters can participate. After successfully entering the OTP, the voter can proceed to vote for their preferred candidate.

The system records the voter's choice and the timestamp of their vote in a Google Spreadsheet, ensuring real-time data storage. Additionally, the system maintains a vote register that increments with each cast vote, preventing multiple voting by the same individual.

At the end of the voting process, the system generates the election result. This result can be obtained from the Google Spreadsheet, providing transparency and facilitating efficient result calculation.

By implementing this proposed methodology, the Arduino-Based Biometric Voting System ensures the integrity of the election process. It verifies the unique ID and fingerprint of each voter, prevents multiple voting attempts, and securely stores the voting data. Moreover, the system enhances accuracy by utilizing online voting and facilitates result calculation, thereby contributing to an accurate and fraud-free election.

1.7 LIMITATIONS

The Arduino-Based Biometric Voting System offers several advantages in terms of accuracy and fraud prevention, there are certain limitations that need to be considered. These limitations include:

- Scalability: The project's scalability may be a challenge when it comes to handling a large number of voters. As the number of registered voters increases, the system may face difficulties in efficiently managing and processing the data, potentially leading to delays or performance issues.
- Connectivity and Reliability: The system relies on internet connectivity for communication and data storage. In areas with unreliable or limited internet access, the system's functionality may be compromised. Power outages or network disruptions can also disrupt the voting process, affecting the system's reliability.
- User Familiarity and Accessibility: The project assumes a certain level of technological familiarity among voters. However, not all individuals may be comfortable or familiar with using biometric authentication or electronic devices, potentially causing usability challenges. Ensuring inclusivity and accessibility for all voters, including those with limited technological literacy, may be a concern.
- Cost and Infrastructure: Implementing the Arduino-Based Biometric Voting System may require significant initial investment and infrastructure setup. Procuring and maintaining the necessary hardware, such as fingerprint modules, Arduino boards, and connectivity devices, could pose financial constraints, particularly in resource-constrained regions.
- Data Security and Privacy: As the system relies on the collection and storage of sensitive personal data, such as fingerprints and Unique numbers, ensuring robust data security and privacy protection is crucial. Adequate measures must be implemented to safeguard against data breaches or unauthorized access, protecting voters' privacy and preventing misuse of their information.

- Legal and Regulatory Compliance: The project needs to adhere to legal and regulatory frameworks related to elections and data protection. Compliance with existing electoral laws and ensuring the system meets the necessary standards and certifications can present additional challenges and may require collaboration with relevant authorities.

Addressing these limitations through comprehensive planning, testing, and continuous improvement can help mitigate potential issues and enhance the effectiveness and reliability of the Arduino-Based Biometric Voting System.

CHAPTER 2

LITERATURE SURVEY

[1] Rahil Rezwan, "Biometrically secured electronic voting machine", To ensure a lot of security, finger prints of the citizen is employed because the main authentication resource. Arduino Uno R3 with ATmega 32 microcontroller and fingerprint module and alphanumeric display area unit employed in mechanical device. For dominant the controller unit, that is Arduino UNO R3 with ATMEGA 32 microcontroller, the code from Arduino developer is employed. The Arduino board may be programmed with this code.

[2] A.M. Jagtap, "Electronic voting system using biometrics, raspberry pi and TFT module", In this system, we tend to are exploitation combination of hardware and software system. Raspberry Pi 3B+ (RPI) may be a hardware device connected to the Fingerprint Scanner, bit show. It stores the data on the cloud. This report describes the workability of assorted techniques of web and defines an enquiry schedule to prosecute if web vote is capable of development within the future.

[3] R.Prabha, "E-voting system using Arduino software", Arduino mega because the main unit of system, the sub unit interface to the Arduino embody the finger print module. It utilized a twin authentication technique victimization citizen's fingerprint and distinctive vote pin sent to the voter.

[4] Talib divan, "A finger print matching technique using minute-based algorithm for voting system", Matching method three finger print matching techniques area unit compared to pick out applicable methodology. Security of overall procedure will be protected and therefore the votes area unit assisted with right data.

[5] Ahammad J Biswas, "A secure and automated platform for fingerprint based electronic voting machine", In this EVM system, presently there area unit 2 push switches for characteristic 2 political parties or candidates. once the elector presses a specific switch (A/B) to vote for his candidate, EVM stores the vote for that candidate.

[6] Vinayachandra, K Geetha Poornima, M Rajeshwari and K Krishna Prasad, “Arduino Based Authenticated Voting Machine (AVM) using RFID and Fingerprint for the Student Elections”, The key elements of the machinedriven voting machine conferred during this paper are the two-one AVM unit and another computer program (UI). AVM consists of IoT-component like AN Arduino Mega Board, Fingerprint Scanner, RFID Reader, wireless local area network Interface, Buzzer, mini digital display Monitor, and momentaneous push buttons integrated victimization bread board and programming victimization Python programing language.

[7] Trupti umakant pavshere,, s.v mare, “Secure E- voting system using biometric”, It is supported homographic property and blind signature arrange the recommend system is executed on embedded system that function a mechanical device. Propose a biometric-bodied designed that establish such challenges and pre serves transparency, secure and obscurity at the side of alternative necessary services, victimization techniques.

[8] Khasawneh, M.M. Malkawi, O.AL.Jarseh, “A biometric secure e-voting system for election process”, The basics of any electoral system is one person-one vote. It stands to reason that has to verify votes. the method is enrollment, verification, identification. The potency of the system depends 4 upon the computer programs its usability. this may for sure guarantee a safer choice technique.

[9] Mouad M.W.Alim, Vivek K, T.Gaikwad, “Fingerprint recognition for person identification and verification based on minutia matching”, Minutia based mostly fingerprint matching is delineated hybrid methodology is employed for improvement. The planned system can execute an electronic mechanical device with security and privacy.

[10] Vijay Lakshmi Gupta, Shreya Gupta. Divya Srinivasbasra, “Electronic voting machine using microcontroller”, To develop an electronic voting machine fingerprint detector using microcontroller. Microcontroller forms the management unit of the complete project. Verification is simpler and a lot of convenient. it's easier and safer. Verification is simpler and a lot of convenient. it's easier and safer.

[11] Abdulkadsh, Alkali,Emmumies, “Biometric based fingerprint electronic voting machine”, It provides an inexpensive, regionally assembled simply reproduceable and extremely secure method. Biometric fingerprint recognition device can be used for storing and comparison fingerprint pattern.

CHAPTER 3

SYSTEM REQUIREMENTS

3.1 SOFTWARE REQUIREMENTS

- Language : C Language(used in Arduino IDE)
- Database : Google Spreadsheets(for storing the votes)

3.2 HARDWARE REQUIREMENTS

- RAM : 8 GB
- Processor : Intel Core i5
- Operating System : Windows 10
- System Type : 64-bit operating system

CHAPTER 4

DESIGN OF THE PROPOSED SYSTEM

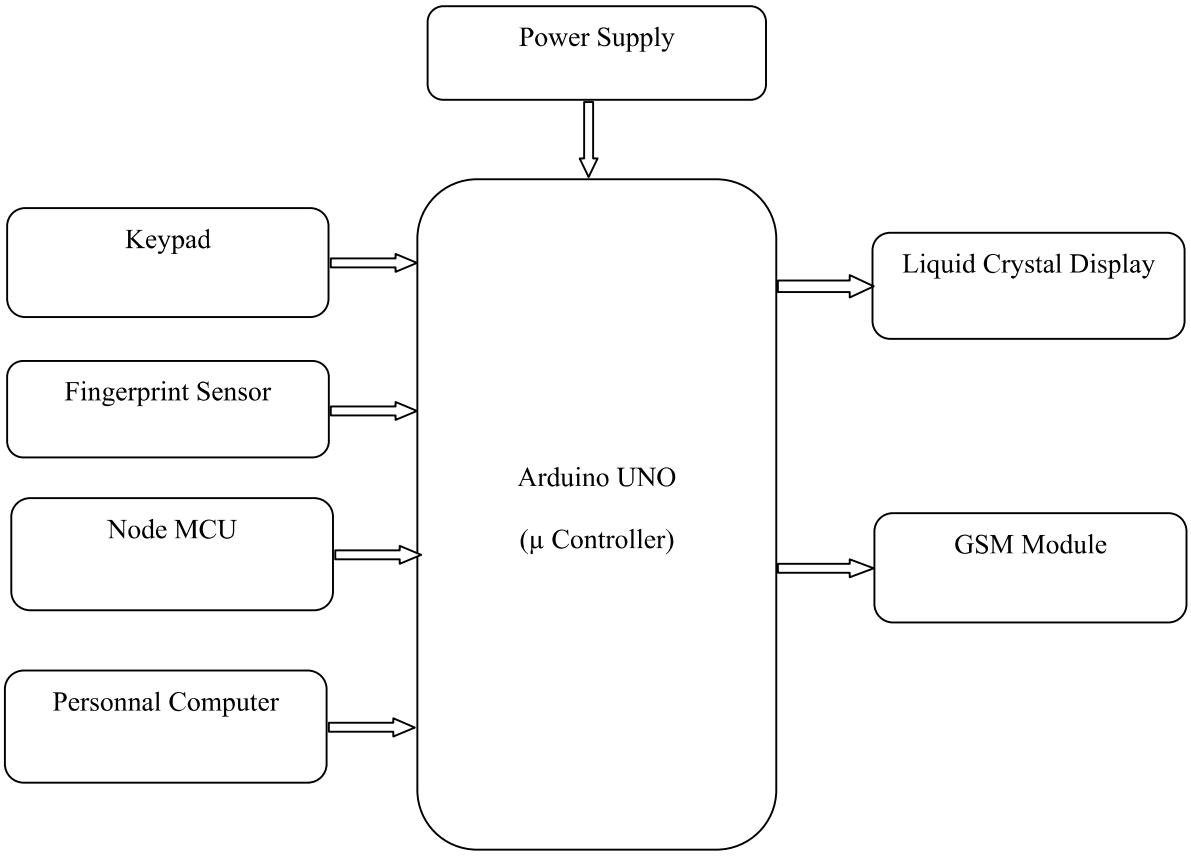

Figure 1: Proposed Block Diagram

The proposed system utilizes an Arduino UNO as the central component, acting as the main unit of the system. It serves as the control hub and interface for various sub-units. These sub-units include a keypad, fingerprint sensor, personal computer, liquid crystal display (LCD), and a GSM module.

The system's software aspect was developed using the Arduino sketch programming language on a personal computer. Once the code was completed, it was uploaded to the Arduino board via a USB port, enabling the board to execute the programmed instructions.

To power the system, an external power supply is employed, ensuring a stable and reliable source of electricity. This power supply supports the Arduino UNO and all the connected sub-units, allowing them to function seamlessly together.

The block diagram illustrates the interconnections and interactions between these components. The keypad and fingerprint sensor serve as input devices, allowing users to provide necessary information and authenticate their identity. The Arduino UNO processes this input, communicates with the personal computer for data storage and analysis, and controls the display and communication functions through the LCD and GSM module, respectively.

Overall, this system design facilitates efficient and effective operation by leveraging the capabilities of the Arduino UNO and its integration with the various sub-units. It offers a comprehensive and interconnected solution for data capture, processing, and communication in a user-friendly and accessible manner.

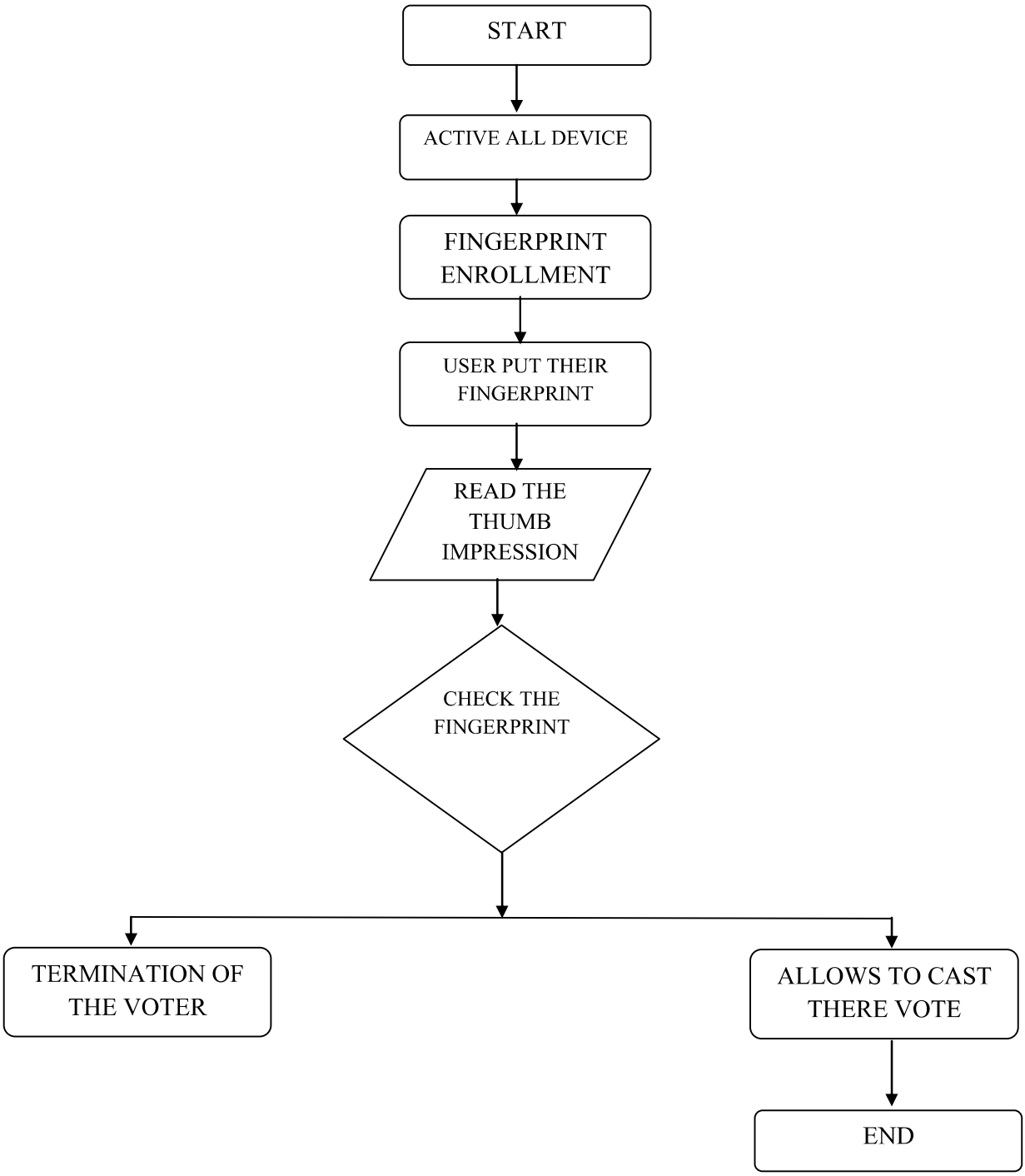

Figure 2: Flowchart of fingerprint based EVM

In the proposed system, the voter begins by enrolling their ID number and fingerprint. This data is stored for verification purposes during the voting process. When a voter approaches the system to cast their vote, the system checks if their ID number and fingerprint match any enrolled data. If there is a match, the system then checks if the voter has already cast a vote in the current election. If they have, the system displays a message indicating that they have already voted.

However, if the voter has not cast a vote before, they are allowed to proceed. Using the keypad, the voter enters an OTP (One-Time Password) provided to them. Once the OTP is validated, the voter can cast their vote by selecting their preferred candidate through the keypad. Each vote is recorded and tallied by incrementing a register.

At the end of the voting process, the system provides the ability to obtain the result. This can be done by analyzing the recorded votes and generating a report or displaying the winner on an output device such as a display screen or personal computer.

Overall, this system ensures that each voter can only cast one vote by verifying their identity through ID number and fingerprint. The use of OTP adds an extra layer of security to prevent unauthorized voting. The system maintains a record of votes, ensuring transparency and accuracy in the election process.

CHAPTER 5

IMPLEMENTATION

The proposed methodology for the IoT-based voting machine with fingerprint verification involves the use of several components, including a controller (Arduino Uno), a fingerprint module, a Wi-Fi module, a keypad, a power supply, and a spreadsheet (Google Spreadsheet). The functional block diagram illustrates the flow and interaction between these components.

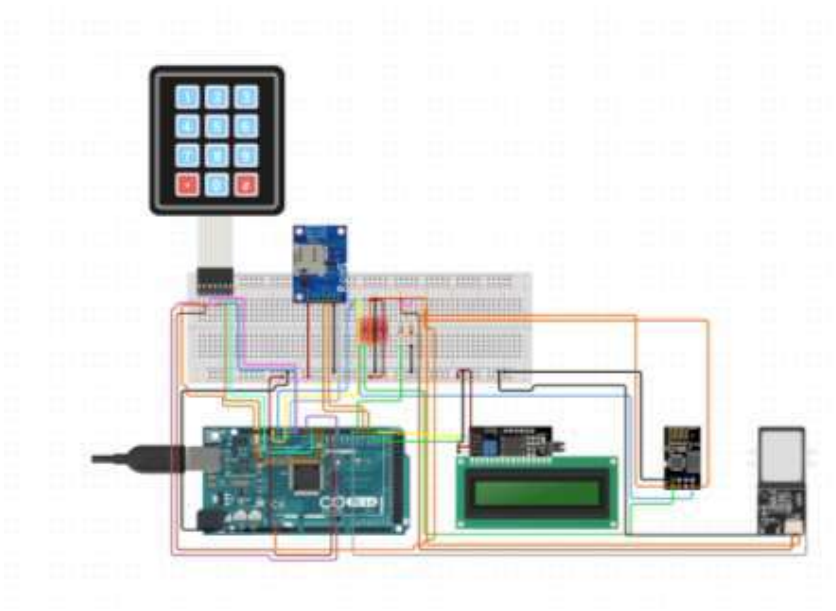

Figure 3: Circuit Diagram of the proposed system

The system is powered by a laptop, providing the necessary power supply. The keypad allows voters to input their votes, and instructions and alerts are displayed on the serial monitor. The fingerprint module is responsible for storing the database of voters' fingerprints. When a user places their finger on the module, it compares the fingerprint with the stored database and displays a message indicating if the person is authenticated.

The ballot paper and final vote count are stored on the cloud, with Google Spreadsheet used for storing the final count obtained by each candidate. The Wi-Fi module (ESP8266) provides internet connectivity to the controller, allowing seamless communication with the cloud-based spreadsheet.

The system is divided into two units: the fingerprint unit and the voting unit. The fingerprint unit handles the enrollment and matching process. It stores the fingerprints of voters and checks for matches in the database. Additionally, the unique number of each voter is stored and verified during the voting process to prevent multiple voting attempts.

The message appears in the fingerprint unit indicating that a person is eligible to vote, they proceed to cast their vote through the unit. After voting, a register is incremented to keep track of the number of votes cast. The voting process is facilitated through the keypad.

Finally, the result can be obtained in the Google Spreadsheet, where the final vote count for each candidate is stored. This allows for easy tabulation and analysis of the voting outcome.

The methodology ensures accurate and secure voting by employing biometric verification, cloud storage for data integrity, and a decentralized approach to voting. By leveraging the Arduino Uno controller and the various components, the system provides a reliable and fraud-resistant voting mechanism.

It is important to note that while the methodology described above provides a general overview of the system, implementation details and specific code implementation will vary depending on the project requirements and the chosen technologies

5.1 TOOLS USED

GSM Module: In this project GSM module is used to send messages to every citizen to successful casting of vote, send alert massages to people who left to cast their vote and also send alert message to nearest police station.

Figure 4: GSM module

Fingerprint Module: We are using R305 fingerprint module to enrol biometric data and verification of authorised voter to allow to vote.

Figure 5: Fingerprint module (R305)

Arduino Uno: Arduino Uno (ATMEGA328) microcontroller is used for processing the data. It is heart of project and used to control all external peripherals. Fig.3

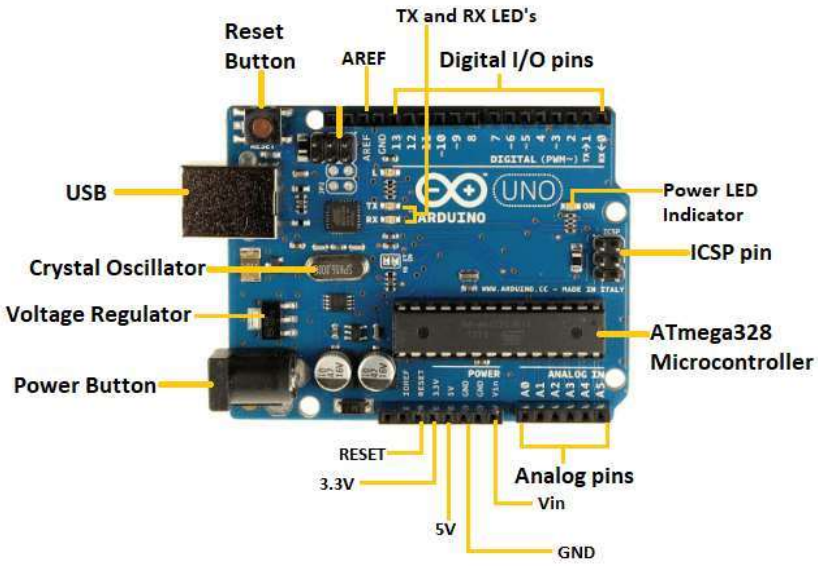

Figure 6: Arduino UNO

ESP8266-01 WiFi Module: This module is used to sending polling votes to respective party automatically when citizens cast their votes and results to firebase Real time Database.

Figure 7: ESP8266-01 WiFi Module

LCD Display: It is used to display instructions of controller and results.

Figure 8: LCD Display

5.2 LIBRARIES DEVELOPED

The Arduino Uno, a popular microcontroller board, relies on a serial software library to enable communication between the board and other devices. The library provides functions and tools to establish serial communication via the UART (Universal Asynchronous Receiver-Transmitter) interface on the Arduino Uno. It allows for the transmission and reception of serial data, enabling the Arduino to communicate with sensors, actuators, displays, and other peripherals. The library supports various communication protocols, such as Serial, Serial1, and Serial2, providing flexibility for multiple serial devices. With the serial software library, developers can easily implement robust and efficient serial communication in their Arduino Uno projects

The Arduino Uno utilizes an I2C (Inter-Integrated Circuit) library to facilitate communication with I2C devices. This library provides functions and tools for establishing and managing I2C connections on the Arduino Uno board. It enables the Uno to act as both a master and a slave device on an I2C bus, allowing for seamless communication with various I2C peripherals, such as sensors, LCD displays, and EEPROMs. The I2C library simplifies the process of sending and receiving data over the I2C protocol, making it easier for developers to integrate I2C devices into their Arduino Uno projects and create complex interactions between multiple devices.

The Arduino Uno makes use of a fingerprint sensor library to interface with fingerprint sensors. This library provides functions and tools to easily integrate fingerprint sensors into Arduino Uno projects. It allows for capturing and processing fingerprint data, as well as verifying or identifying fingerprints against stored templates. The fingerprint sensor library supports various fingerprint sensor models and simplifies the implementation of fingerprint recognition capabilities in Arduino Uno applications. With this library, developers can create secure access control systems, biometric attendance systems, or any other application that requires fingerprint authentication, leveraging the power of fingerprint sensor technology with the Arduino Uno.

The keypad library for Arduino Uno simplifies the integration of keypad input into projects. It provides functions and tools to interface with various types of keypads, allowing users to easily read and interpret key presses. The library supports both matrix and single-button keypad configurations, enabling the Arduino Uno to detect and handle key events effectively. With the keypad library, developers can create interactive systems that utilize keypads for user input, such as security systems, menu navigation interfaces, or password entry systems. It offers a straightforward and efficient solution for incorporating keypad functionality into Arduino Uno projects, enhancing user interaction and control.

CHAPTER 6

RESULT AND DISCUSSION

The implemented system of the Arduino-Based Biometric Voting System has shown promising results in ensuring accurate and fraud-free elections. The system consists of two units: the verification unit and the voting unit, both controlled by the Arduino UNO.

In the verification unit, three scenarios are considered to maintain the integrity of the voting process. Firstly, for voters casting their vote for the first time, their fingerprint and unique number are compared with the data stored in the database. If a match occurs, the voter is authenticated, and a message displaying "Authenticated. Proceed" is shown on the serial monitor. This step ensures that only authorized voters are allowed to cast their votes.

Secondly, the system detects if an authenticated user attempts to vote more than once. If such an attempt is made, a buzzer sound is produced, indicating that the voter has already cast their vote. Simultaneously, a message stating "Already voted" is displayed on the serial monitor. This feature prevents individuals from attempting to manipulate the system by casting multiple votes.

Lastly, if the fingerprint and unique number of a person are not available in the database, they are not allowed to cast their vote. This ensures that only registered voters are eligible to In the voting unit, voters can cast their votes using the keypad interface. The votes are recorded and transmitted to Google Spreadsheet, a cloud-based platform. This approach allows for secure and efficient storage of voting data. At the end of the voting process, the authorized officer can access the summary of the voting through the Google Spreadsheet platform. This enables quick and accurate tabulation of the votes and ensures transparency in the election results.

Overall, the implemented Arduino-Based Biometric Voting System has demonstrated several benefits. Firstly, it enhances the accuracy of the election process by verifying the identity of voters through fingerprint and unique number authentication. This prevents unauthorized individuals from casting votes and ensures that each vote is attributed to the rightful voter.

Secondly, the system effectively eliminates the possibility of voter fraud by detecting and alerting attempts to cast multiple votes. The inclusion of a buzzer sound and the "already voted" message serves as a deterrent to potential fraudulent activities.

Additionally, the use of Google Spreadsheet as a cloud-based platform for vote storage and retrieval ensures the security and accessibility of voting data. Authorized personnel can easily access and analyze the voting summary, simplifying the counting and reporting process.

CHAPTER 7

CONCLUSION

In conclusion, the implemented Arduino-Based Biometric Voting System has successfully addressed the challenges of accuracy and fraud in elections. By combining biometric verification, secure cloud storage, and real-time monitoring, the system provides a robust and transparent framework for conducting credible and fraud-free elections. This system can be a valuable tool in promoting democracy and ensuring the integrity of electoral processes. participate in the election, maintaining the integrity of the voting process.

In conclusion, the proposed IoT-based voting system presents a significant step towards the digitization of the electoral process, enhancing efficiency, security, and accuracy. By incorporating biometric and Unique number verification, the system ensures that only authorized individuals can cast their votes, eliminating the possibility of multiple voting and safeguarding the integrity of the election.

One of the key advantages of this system is the reduction in the time required to announce the election results. With real-time data processing and secure cloud storage, the system enables quick tabulation and analysis of votes, expediting the result announcement process and providing timely information to the public.

Moreover, the introduction of biometric verification adds an extra layer of security to the voting process. By authenticating voters based on their unique fingerprints, the system prevents impersonation and unauthorized access, making it highly reliable and trustworthy.

Furthermore, the integration of Unique number verification strengthens the identification process, ensuring that only eligible voters participate in the election. This feature eliminates the possibility of fraudulent voting and reinforces the democratic principles of fair representation and equal opportunity.

Additionally, the flexibility of the system allows for the implementation of postal voting, extending the convenience of casting votes to individuals who are unable to visit polling stations physically. This inclusion promotes inclusivity and accessibility, enabling broader participation in the democratic process.

Overall, the IoT-based voting system not only streamlines the electoral process but also enhances its security and transparency. By leveraging advanced technologies, such as biometric verification and secure cloud storage, the system offers a robust framework for conducting accurate, fraud-free, and efficient elections. This solution paves the way for the advancement of democracy in the digital age, ensuring that citizens' voices are heard and their votes are counted accurately.

REFERENCES

[1] Mr.kalash Srivastava, M.P.S Chawla " Fingerprint based Electronic VotingMachine with Inbuilt Identification and Verification System(2018)", journal ofAdvances in electronic devices, vol.3, no.3,pp.3-13.

[2] A.M.jagtap, Vishakha kesarkar, Anagha supekar" Electronic Voting System usingBiometrics, Raspberry Pi and TFT module(2018)", IEEE Xplore, vol-3, no-4,pp5386-9439.

[3] Ifthekhar Ahammad, Pradip lal biswas, juwel Chowdhury, obaedur Rahim rizbhi,Sanjana sirah and ashraful isla, "Towards a secure and automated platform forfingerprint-based electronic voting machine (2019)", IEEE Xplore, vol.1,no.1,pp.34-41.

[4] Rahil rezwa, Huzaifa ahmed, M.R.N.Biplob, S.M.shuvo, MD.Abdur Rahman," Biometrically secured electronic voting machine (2017)", IEEE Region,vol.4,no.5,pp.21-23.

[5] R.Prabha, X.Trini, V.Deeika and C.Iswarya," A Survey on E-Voting SystemArduino software (2016)", International Journal of Advanced Research inElectrical,vol.5,no.2,pp.36-47.

[6] Vinayachandra, K Geetha Poornima,M Rajeshwari1,and K Krishna Prasad,"Arduino Based Authenticated Voting Machine (AVM) using RFID and Fingerprint for the Student Elections", Journal of physics, vol 5, no-3, pp.12-16.

[7] A. Tirupathi Rao; N. Pattabhi Ramaiah; V. Raghavendra Reddy; C. Krishna Mohan, "Nearest Neighbor Minutia Quadruplets Based Fingerprint Matching with Reduced Time and Space Complexity" IEEE 14th International Conference on Machine Learning and Applications (ICMLA), 9-11 Dec. 2015.

[8] Dibya Dahal, "Electronic Fingerprint Voting System", Metropolia applied university, vol.6,no.7, pp.289-445

[9] Bhuvanapriya.R, Rozil banu.S, Sivapriya.P, Kalaiselvi.V.K.G, "Smartvoting", IEEE, vol.10,no.9,pp.143-159.

[10] Scott Wolchok, Eric Wustrow, "Security Analysis of India's Electronic Voting Machines", IEEE,vol-4,no.8,pp.140-114.58.

[11] Vipul Awasthi; MPS Chawla, “Fingerprint analysis using minutiae extraction” School of Electronics, Devi Ahilya Vishwavidyalaya, Indore (M.P), 7 June. 2012.

[12] M. Adhiyaman; D. Ezhilmaran, "Fingerprint matching and similarity checking system using minutiae based technique”, IEEE International Conference on Engineering and Technology (ICETECH), 20-20 March 2015.