International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.028 ISSN: 2581-4621

FINGERPRINT BASED VOTING SYSTEM USING IOT

Samba Siva Rao Kopanaty
Dept. of Electronics & Communication Engineering (Associate Professor)
Bapatla Engineering College Bapatla, Guntur, India
sambasivarao.kopanaty@gmail.com

Viswavidyasudha Pudi
Dept. of Electronics & Communication Engineering (UG Student)
Bapatla Engineering College Bapatla, Guntur, India
pudiviswavidyasudha@gmail.com

Gangadhar Yekambaram
Dept. of Electronics & Communication Engineering (UG Student)
Bapatla Engineering College Bapatla, Guntur, India
gangadharyekambaram@gmail.com

Venkata Ramana Amla
Dept. of Electronics & Communication Engineering (UG Student)
Bapatla Engineering College Bapatla, Guntur, India
amlavenkataramana@gmal.com

Mohammed Aasid Shaik
Dept. of Electronics & Communication Engineering (UG Student)
Bapatla Engineering College Bapatla, Guntur, India
skmohammedaasid@gmail.com

Abstract**—** The voting process is the foundation of democracy, and citizens are allowed to exercise their will, vote for representatives, and make decisions that shape their communities and countries. Securing and modernizing the voting process is essential today, as new technologies can drastically enhance the efficiency and integrity of voting systems. This paper discusses an Arduino Uno-based biometric voting system. By using a fingerprint module for authentication and push buttons with LED lights for instant feedback, providing a secure, easy-to-use, and transparent voting process. The system is secure and easy to use.

The admin panel provides immediate access to the voting results, promoting transparency and accountability in the electoral process. Additionally, the system provides provisions for the visually impaired voters, ensuring that the process is inclusive. Since the results are updated in cloud storage, this new solution transforms traditional voting processes ensuring the integrity and reliability of the democratic process.

Keywords—Arduino Uno, Buzzer module, Fingerprint sensor, Internet of things, Led indicators, Wi-fi module.

INTRODUCTION

Fingerprint authentication in electronic voting systems significantly boosts election security and integrity by preventing voter fraud and forgery. This biometric technology ensures that each individual can cast only one vote, eliminating the possibility of duplicate voting. Moreover, the system streamlines the process by automating vote counting, which reduces the time needed for result declaration and minimizes human errors. Compared to traditional paper ballots, fingerprint-based voting is cost-effective, cutting down expenses related to printing, manpower, and logistics. It also improves accessibility, making it easier for individuals with disabilities to participate and enabling remote voting through IoT integration. By providing real-time audit trails and reducing the risk of election tampering, this system promotes public trust and transparency in the electoral process.[1] Electronic voting with fingerprints has far-reaching usage across various spheres. When utilized for government elections, it is accurate and protects against vote manipulation at state, national, and local levels. When utilized in non-political spheres, the system is applied at universities, company boardrooms, and labor unions to perform honest and fair elections. Fingerprint verification is utilized in e-governance schemes to allow for secure and validated decision-making. Firms and schools also apply biometric verification for web surveys and polls to ensure the vote integrity. Even the justice system can use the technology for validated and secure voting in court sessions. Such wide usage indicates the flexibility of the system in diverse decision-making processes.[2] Electronic voting with biometric authentication has been used successfully in most countries, with its potential to enhance the electoral process. Estonia is a pioneer, enabling citizens to vote online using biometric authentication, as nearly 47% of the votes were cast online in the 2019 elections. Brazil has gone fully to an electronic poll, more and more using fingerprint authentication to prevent electoral corruption. The United States has implemented electronic voting in some states, while biometric authentication is yet to be used on a large scale. South Korea also employs biometric voting to offer secure and efficient elections. Worldwide, the technology has boosted voter turnout, reduced election fraud, and generated public confidence. The high implementation cost, cybersecurity risk, and digital literacy of the voter are still significant challenges to its extensive use. India trusts Electronic Voting Machines (EVMs), but biometric authentication is yet to be followed. The Election Commission of India has considered the integration of fingerprint authentication with Aadhaar to strengthen voter identification and prevent fraud. But concerns such as the vast population of the country, rural connectivity, and data privacy issues have delayed progress. Pilot projects in individual constituencies can experiment with the viability of biometric voting. It will take strong policy mechanisms, technology advancements, and extensive public awareness drives. The Internet of Things (IoT) refers to a network of devices that share information and communicate with each other using the internet. In fingerprint voting, IoT plays a crucial role as it enables data transmission in real-time, remote access, and security. IoT enables the storage of voters' data and its analysis on scalable databases like the cloud, which encourages transparency and accountability through monitoring logs. IoT also increases the effectiveness of the voting process by making the process efficient and providing instant feedback, while guaranteeing the security of the system.This paper is organized as follows. In chapter 2 the paper follows the Literature Review.

II. LITERATURE REVIEW

Mr.Sharathchandra N R [3] aims to enhance election security and efficiency by integrating biometric fingerprint authentication with embedded systems. It eliminates rigging through fingerprint registration before elections and real-time verification during voting. Using a fingerprint module, Arduino Uno microcontroller, Wi-Fi module, LCD, and buzzers, the system authenticates voter identity and enables vote casting only for verified individuals. Advanced algorithms, like the Gabor filter, ensure accuracy by minimizing fingerprint noise and improving matching efficiency. This technology reduces election fraud, speeds up vote counting, minimizes costs, and provides better accessibility, making the voting process secure, practical, and effective for diverse applications. CH Srilatha [4] to ensure secure and efficient elections. By using fingerprint sensors for voter authentication and IoT technology for real-time data processing, the system prevents identity fraud and electoral malpractices. Advanced cryptographic protocols and blockchain ensure data confidentiality, making the voting process secure, user-friendly, and reliable. It represents a significant step toward modernizing election systems and fostering trust in democratic processes. Prof. Prabhakara B. K [5] proposes a biometric smart voting system using Aadhaar-linked fingerprint and facial recognition to enhance election security and efficiency. It employs advanced LBPH algorithms for voter authentication, reducing fraud and ensuring transparency. By integrating

Aadhaar data, the system offers a user-friendly, tamper-proof, and efficient voting process while addressing privacy concerns and data protection challenges. Dhanush S J [6] proposes this biometric voting system enhances election security and transparency using fingerprint authentication. It replaces ID cards with a fingerprint-based database, preventing duplicate voting and unauthorized access. The system also notifies voters and simplifies the process, fostering trust in modern electoral systems. Nandhakumar J [7] presents a secure and efficient voting system leveraging biometric and IoT technologies. It uses fingerprint authentication to verify voter identity, ensuring only authorized individuals can cast their votes. The system integrates Aadhaar verification and prevents multiple voting attempts by alerting malpractices through a buzzer. Votes are cast via a keypad and stored in the cloud using ThingSpeak, enabling real-time results and remote voting. The system aims to modernize elections by reducing fraud, enhancing accessibility, and ensuring transparency. Awsan A.H.Othman[8] proposes an online voting system that combines IoT and Ethereum blockchain technologies to ensure security, transparency, and efficiency. It encrypts votes on the blockchain for tamper-proof records, uses IoT devices like fingerprint sensors and OTP verification to prevent fraud, and eliminates the need for physical ballot boxes, making voting more accessible and cost-effective. The system is versatile, suitable for governmental elections, referendums, and private organizational polls, fostering trust and modernizing the democratic process. M G Gurubasavanna[9] introduces a secure voting kiosk using Raspberry Pi, integrating fingerprint, face, and iris recognition for multimodal authentication. It ensures cross-constituency voting, fraud prevention, and real-time voter verification. This approach enhances election security and fosters trust in democratic processes.

III.PROPOSED SYSTEM

Block diagram:

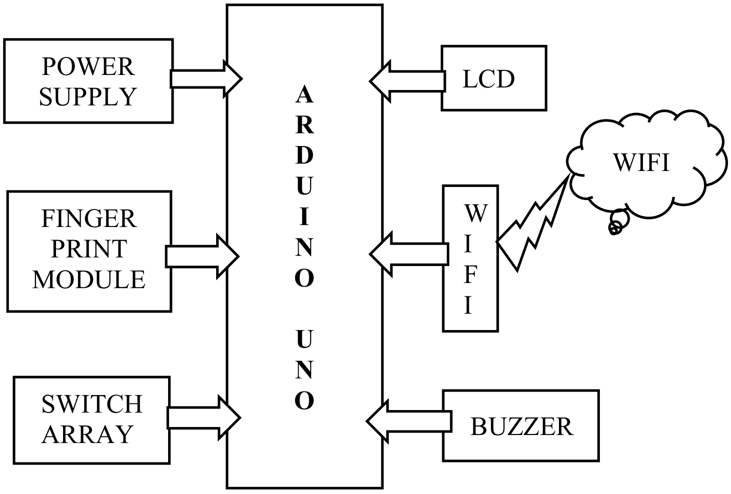


Fig 1: block diagram

HARDWARE IMPLEMENTATION

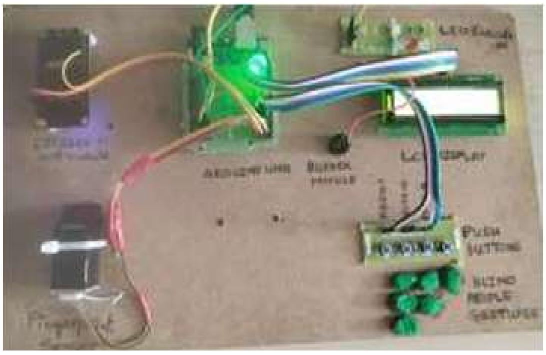


Fig 2: kit implementation

COMPONENTS

ARDUINO

In an IoT-based fingerprint-based voting system, the Arduino Uno acts as the central microcontroller, ensuring that all of the system's components work together seamlessly. It serves as the central processing unit of the system, coordinating inputs from the fingerprint sensor, which takes voter fingerprints and compares them to templates stored in the database for authentication. A voting system which is made with Arduino uno acts as tamper-proof, which records the vote after verification and makes sure related data is accurately processed and sent. Arduino Uno can connect to a range of peripherals in addition to the fingerprint scanner, including an LCD display for real-time feedback to the users, push buttons for user-voter communication, and a Wi-Fi module for access to a central server. The ease of programming the device.

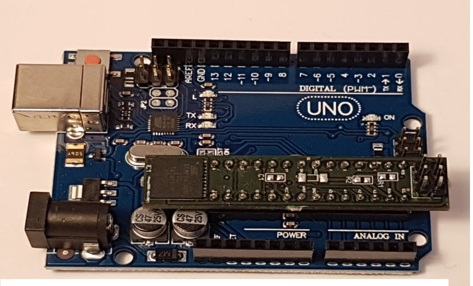


Fig 3: Arduino Uno

Fingerprint Sensor

The inclusion of a fingerprint reader in electronic voting machines offers security and guarantees the proper authentication of voters. Before a voter can cast their vote, the reader reads their unique fingerprint patterns and matches them against a database to verify their identity. It offers an added layer of security against illegal use and tampering with votes. It also simplifies it for the voters by not using identification documents or cards, offering higher convenience and efficiency in voting.

Fig 4: fingerprint scanner

Buzzer Module

A buzzer module can play a crucial role in providing audible feedback or alerts during the voting process. It can notify voters once their vote is successfully recorded, signal the opening and closing of polling stations, or alert election officials to system errors or irregularities. Controlled remotely via an IoT network, the module enables real-time updates and notifications. Moreover, it can be seamlessly integrated with other system components to enhance accessibility and ensure a smooth and user-friendly voting experience for everyone involved.

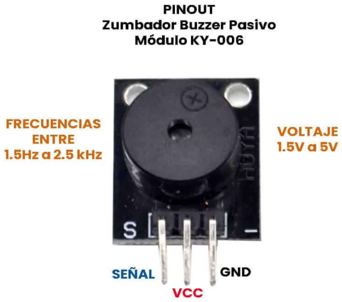


Fig 5: Buzzer module

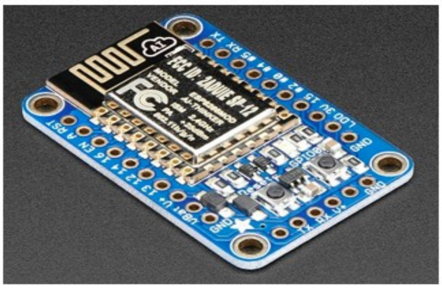
LCD Display

An LCD (Liquid Crystal Display) serves as an essential user interface, offering crucial information to both voters and election officials. It can display step-by-step instructions for voters on how to cast their votes, present the names and parties of candidates, and provide confirmation messages once a vote has been successfully recorded. This ensures a clear and efficient voting experience for all users.

Fig 6: LCD Display

Wifi module

In an IoT-driven fingerprint-based voting system, the Wi-Fi module is key component to ensure easy communication between the voting machine and the central database. It enables the transmission of voter identification information, such as fingerprint images, to a central database for authentication. Once authenticated, the module updates real-time voting records with minor chance to tampering or duplication. The Wi-Fi module also provides remote monitoring and control of the



voting process, maximizing transparency and efficiency. By utilizing IoT advancements, this system guarantees a secure, dependable, and user-friendly voting experience.

Fig 7: Wifi module

SOFTWARE

Arduino IDE:

The Arduino Integrated Development Environment (IDE) is an open-source, cross-platform computer application for Windows, macOS, and Linux. It is written in terms of C and C++ functions, allowing users to write and upload code to Arduino-compatible boards. Moreover, through the use of third-party cores, the IDE can communicate with other firms' development boards. The source code of the Arduino IDE is published under the GNU General Public License, version 2. The IDE accommodates C and C++ programming with special rules for structuring the code. The IDE has a software library based on the Wiring project, which makes input and output operations easier. The code written by the user needs only two main functions—one to start the sketch and one for the main program loop. The functions are compiled and linked with a standard program stub (main()) to form an executable program, which acts as a cyclic executive. The process uses the GNU toolchain, which comes with the IDE. The Arduino IDE also translates the compiled code into a text file in hexadecimal format. The file is then loaded to the Arduino board by a loader program contained in the board's firmware. In default scenarios, the IDE is the main utility for uploading user code to official Arduino boards. Historically a descendant of the Processing IDE, the Arduino IDE started using a Visual Studio Code-based Eclipse Theia IDE framework from version 2.0. As the popularity of Arduino as a software platform has grown, other firms have created proprietary open-source compilers and tools (referred to as cores). The tools enable users to write and upload sketches to a number of different microcontrollers other than those supported by Arduino

Fig 8: Arduino symbol

THINGSPEAK

The Arduino IDE software is employed for programming the Arduino microcontroller, which is the system control unit of the voting system. With the in-built Wi-Fi module, data is communicated from the fingerprint sensor to the ThingSpeak cloud platform through the Arduino board. The wireless integration ensures effective and efficient communication ThingSpeak plays a critical role in a fingerprint-based voting system using IoT by offering the cloud platform for data analysis and management. In the voting system, ThingSpeak is employed to store and analyze data collected from fingerprint sensors and other hardware components. Upon scanning the fingerprint by the voter, data is locally authenticated and then relayed to ThingSpeak for secure storage and further analysis through Wi-Fi connectivity. Real-time updates and secure storage allow voting records to be centrally stored and tamper-proof. ThingSpeak, when integrated with Wi-Fi connectivity and Arduino IDE software, enhances the functionality and efficiency of the system between the cloud and the hardware. Wi-Fi connectivity also provides ThingSpeak the ability to facilitate real-time monitoring of the electoral process. The dashboards of the platform can be accessed by the election officials for monitoring voter turnout, system performance, and spotting irregularities from remote locations. The integration of ThingSpeak with cloud-based functionalities, Wi-Fi connectivity, and the versatility of the Arduino IDE software offers an efficient and secure fingerprint-based voting system that can be scaled up. Together, they offer an efficient and advanced solution for election conduct.

IMPLEMENTATION:

Working Principle

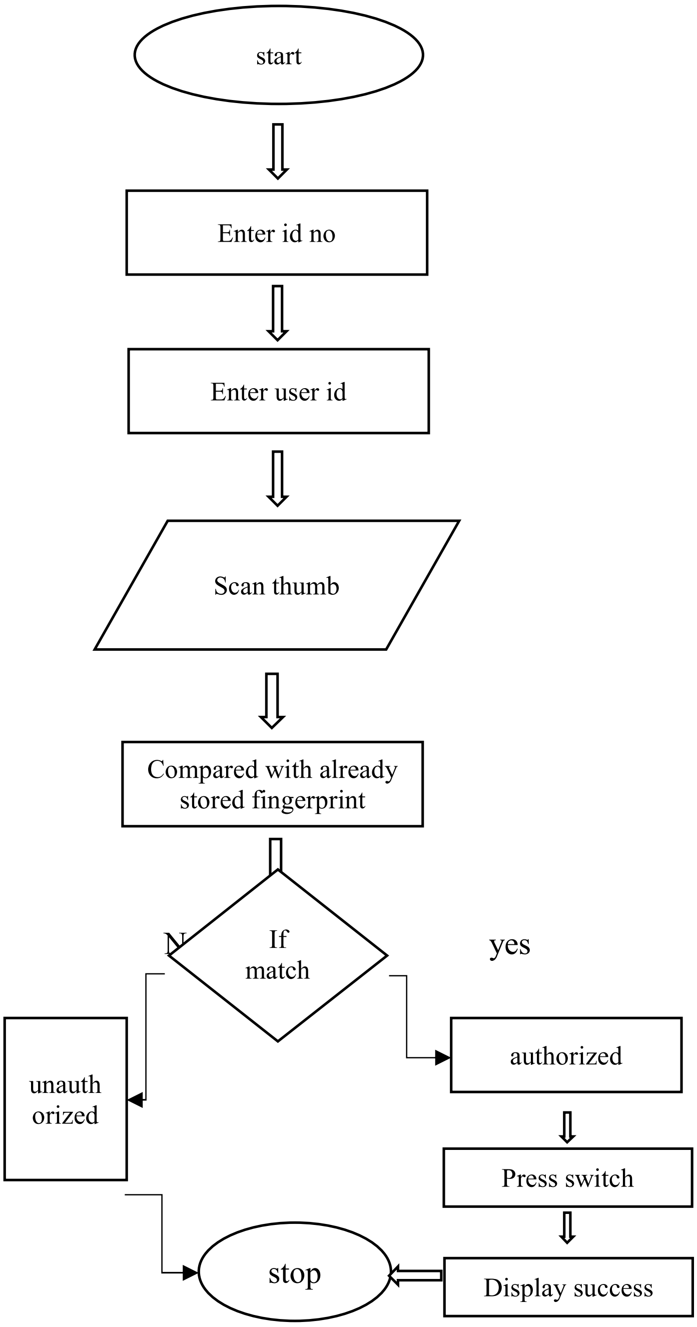


Fig 9: working flow diagram

Prior to the voting process, fingerprints of all possible voters are required to be registered. to the system to give them access to cast their votes during the voting process. Once the fingerprints are registered, the voting process can be started where voters cast their votes to desired candidate. Before scanning the finger, a numerical equivalent value needs to be assigned to the possible fingerprint so that the fingerprint can be saved in a fixed unique integer value location and can be easily accessed during the voting process.

Enrollment

To scan and store fingerprint of the possible voters, first the enroll switch connected to A0 pin of Arduino needs to be pressed, once pressed a red LED lights up followed by the Enter Id message in LCD. Therefore, the unique numerical identification location to the fingerprint can be given in monitor which is connected with system, then scan thumb message is displayed in LCD after placing finger twice on fingerprint sensor, finger enrollment is successful and displays a success message in monitor. After each Start End Set Number for Template Scan Fingerprint Store template in DY50 Flash Memory.

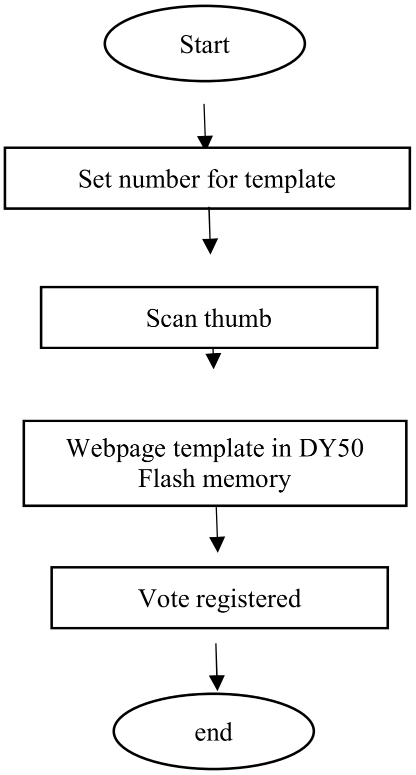


Fig 10: Enrollment flow diagram

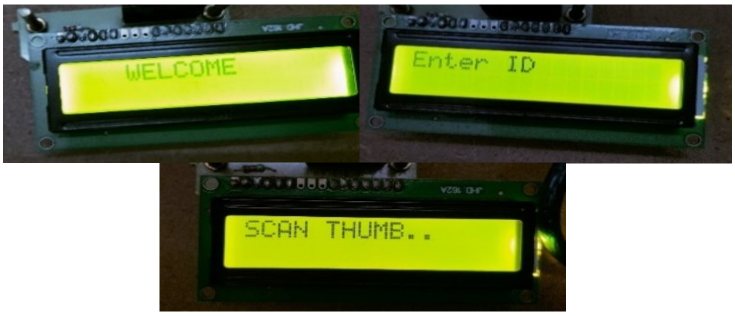


Fig 11: enrollment LCD figures

Voting procedure

The fingerprint of voters will be securely stored on the device. When a person arrives to vote, their fingerprint is scanned using a fingerprint scanner, and the verification process begins. If the fingerprint matches the stored data, the individual is allowed to proceed with the voting process. However, if the fingerprint does not match, the person will be marked as an invalid voter, and an alerting tone will be triggered. Once the voting process is completed, the voter's account is closed, preventing them from voting again. If someone attempts to vote multiple times using their ID, the system displays a message indicating that they have already voted, ensuring that votes are not duplicated. After the successful completion of voting, the individual’s vote is added to the total count.

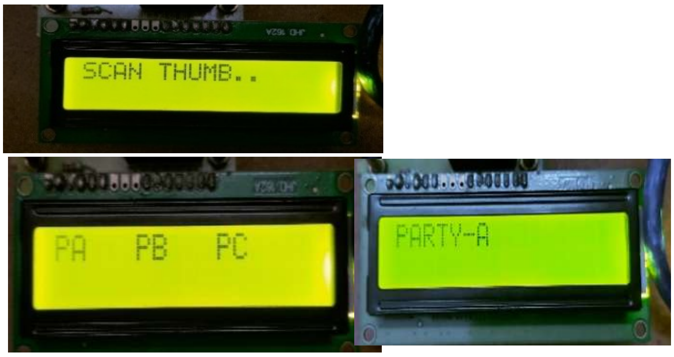


Fig 12: vote casting LCD figures

Authentication

A voter can only cast their vote once during a voting session. The system prevents multiple voting by using a flag register to check if the voter has already voted. This check happens within the code's void loop. When a voter casts their vote, the flag is set to 0. If the same voter tries to vote again, the flag is checked, and since its value is now 0, the system denies access to vote and

displays “Already done ” message on the LCD screen. If the flag is 1, voting is allowed; otherwise, the process is aborted to ensure the system's security.

Fig 13: authentication LCD figure

Additionally, if a person whose fingerprint is not registered in the system attempts to vote, the message "UNAUTHORIZED" is displayed on the LCD screen, and the individual is not allowed to vote.

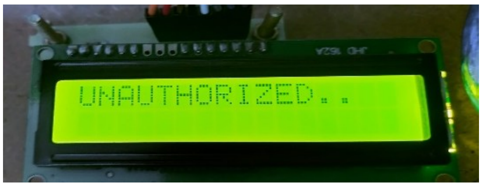


Fig 14: Unauthorized LCD figure

This process helps maintain the system's authenticity and prevents unauthorized voting.

RESULT

The Results can be viewed on Thingview app and the results as follows:

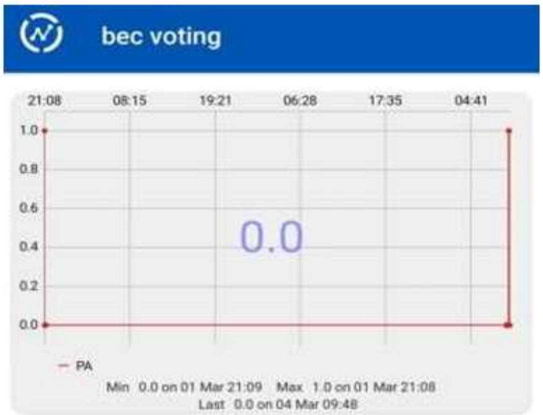


Fig 15: Party A voting results

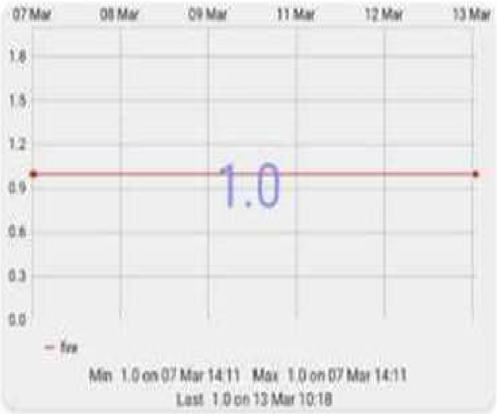


Fig 16: Party B voting results

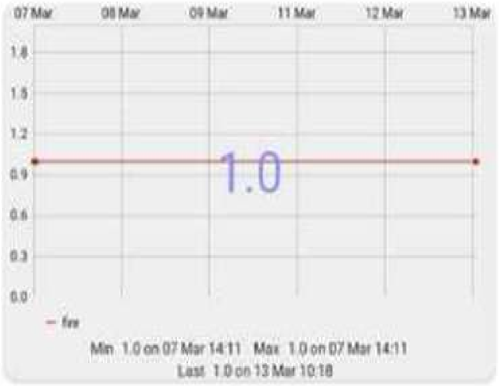


Fig 17: Party C voting results

CONCLUSION

The Arduino Uno-based biometric voting system marks a major step forward in the modernization of electoral processes. By combining biometric authentication, real-time feedback, and cloud-based result updates, this system enhances security, transparency, and efficiency in voting. Its inclusive design supports visually impaired voters, emphasizing accessibility and diversity. This innovative solution not only protects the integrity of elections but also establishes a new benchmark for reliability and user-friendliness in democratic systems.

Reference

[1]Abeesh A. I., Amal Prakash P., Arun R. Pillai, Ashams H. S., Dhanya M., and Seena R., published in the International Journal of Engineering T), Special Issue, 2017.
[2] Debojyoti Ghosh et al., published in the International Journal of Novel Research and Development (IJNRD), Volume 3, Issue 5, May 2018.
[3] Sharathchandra N R, Dr. Jose Alex Mathew, and Dr. B C Prem Kumar, published in the International Journal of Creative Research Thoughts (IJCRT), Volume 10, Issue 8, August 2022.
[4] CH Srilatha et al., published in the E3S Web of Conferences, Volume 507, 2024.
[5] Prof. Prabhakara B. K., Adhya Shetty P., Anushree, Ashwitha, and Mayoori P., published in the International Journal of Creative Research Thoughts (IJCRT), Volume 12, Issue 4, April 2024.
[6] Dhanush S J, Kishore B, Sanketh B G, Madhu D, and Dr. M J Chandrashekar, published in the International Journal of Research and Analytical Reviews (IJRAR), Volume 9, Issue 3, July 2022.
[7] Nandhakumar J., published in the International Journal for Research in Applied Science and Engineering Technology (IJRASET), Volume 10, Issue 5, May 2022.
[8] Awsan A. H. Othman, Emarn A. A. Muhammed, Hamzah A. A. Muhammed, Prof. Mogeeb A. A. Mosleh, and Haneen K. M. Mujahid, published in the 2021 International Conference of Technology, Science and Administration (ICTSA).
[9] M.G. Gurubasavanna, Mamatha R., Saleem Ulla Shariff, and Dr. N. Sathisha, presented at the Second International Conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud), 2018.