Ramya M, 2024, 12:5
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Smart Voting System Using Fingerprint Module

Ramya M, Veni Vijayan
Department of Computer Technology

Abstract- The design and development of a biometric information-based electronic voting machine authentication system is the subject of this article. Fingerprint devices are used in electronic voting systems to verify votes cast. The finger print based electronic voting system offers several benefits, such as eliminating the need for ID cards and simplifying the process by simply placing your finger on the sensor. Data is sent to the controlling unit of verification when a finger is put on the finger-print sensor. The controller retrieves the information from the storage device and compares it with the data of the current user. Users are permitted to cast ballots if their finger prints match those that have already been saved. You can cast your votes by simply following the directions that are all provided on the LCD.

Keywords- Arudino Uno, Power Supply, Keypad, LCD Display, Buzzer, Fingerprint Module

I. INTRODUCTION

In the past, casting a ballot involved stamping a paper with the candidate of one's choice and putting it in a ballot box. Each vote must be counted in each ballot box to ascertain the total number of votes cast. The votes for each candidate must then be totaled together to identify the winner, who will be the one with the most votes. Because the results of this manual voting are subject to manipulation, it is unfair to the parties in the race because the results are fabricated. Every person is entitled to vote and use that right to select their leader. Every citizen in Malaysia has the freedom to vote and voice their opinions because it is a democratic nation. The most crucial duty for every citizen is to prevent electoral fraud. In the next election, voters have the option to select a candidate in order to alter the ruling party. Voting is used not just to choose leaders of the government but also of schools, universities, and other organizations. A person can be identified via biometrics, which uses his physical attributes. A person's fingerprint, iris, face, voice, and other biometrics are frequently used to identify them. One-to-one matching is the primary goal of biometrics, followed by one-to-one multiple matchings. One-to-many matching is used to compare the biometric sample to samples that have already been saved. It does a one-to-one matching comparison with the previously stored sample. The biometric method offers a more practical and safe way to verify the identity of the user.

Password security is inferior than biometric security. The distinctiveness of each person's fingerprint makes them useful for authenticity, verification, and signature purposes. A systematic approach is essential to a process at all stages. This is to stop software from breaking down while the system is being simulated. The vote counting procedure has to be accelerated next. Votes were routinely counted by hand in the past, requiring human energy. Because of this, it took a very long time to proclaim the winner, and occasionally the results were revealed the next day. The results may be reported more quickly with this voting technique since it uses an automated mechanism to count the votes. As a result, there is no longer a need to pay employees to manually tally the ballots. Staff compensation consumes a lot of funds, and there are occasions when that sum is insufficient. The funds may be utilized to really purchase a more

efficient voting system, such a biometric voting system that relies on fingerprints.

II. LITERATURE REVIEW

Voting is an essential instrument in a democratic system because it gives people the ability to choose from among eligible candidates the one they think is best. By removing problems like multiple voting, fraudulent voting, and inaccurate ballot paper counting, electronic voting systems offer a smooth and transparent electoral process. By using the voter's fingerprint for authentication, a smart voting system built on an IoT platform solves these problems. Only one party may be chosen by legitimate users using this secure method, and all statistics are transferred to a web server.

The voter data is retrieved by the system via a fingerprint reader and is compared to data that has already been saved. The user can cast a ballot or vote if their information is in the database. A notice shows up on the LCD screen otherwise. In Bangladesh and other nations where electronic voting machines are the norm, the suggested approach will be used.

Voters' fingerprints are stored in a database using electronic voting machines, and the database is then searched for matches. If a voter is not registered but has cast many ballots, the technology can detect this. The user can cast a vote if they match the database. The voting is then totaled and the result is displayed by the system after some time.

The disadvantages of electronic voting devices are covered in this article, including the requirement for human vote counting. In its place, a rapid and secure biometric voting system is suggested, with the goal of shortening the time required to announce the results and increasing the model's flexibility, security, dependability, and scalability.

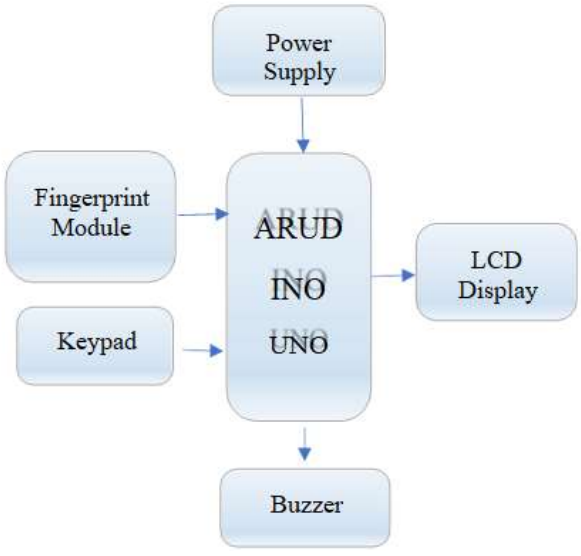
To sum up, voting is an essential instrument in a democracy, and a smart voting system that makes use of IoT and fingerprint authentication may increase security, shorten voting times, and strengthen the democratic process.

III. METHODOLOGY

1. System Diagram

One idea that uses the Internet of Things is the biometric voting system based on fingerprints. The goal of this project is to create a voting procedure that is faster than the current one while also preventing electoral misconduct. The matrix keypad and push buttons serve as the project's inputs, and the buzzer, liquid crystal display, and light emitting diode (LCD) serve as its outputs. when the voter uses the matrix keypad to enter their identity card (IC) number. After that, the Arduino Uno microcontroller will receive the data from the matrix keypad and use it to compare it with the database that has been recorded. The voter can go to the following step, which is the voting stage, if the IC number is confirmed.

There is a chance of ties with this voting mechanism or possibly no votes being cast. The LCD is set to show "TIE NO RESULTS" and "NO VOTES CASTED" in that scenario. The admin may be alerted via the Internet of Things right once and take appropriate action. All of the data will be sent to the monitoring system unit via the IoT platform.



A block diagram of the project is displayed in Figure 1

An Arduino Uno will be connected to an ESP8266 Wi-Fi module in order to transmit the data to the internet, allowing the authorized admin to monitor the data remotely. This project made use of TINKERCAD as it can show simulation in real time and offer lucid insight throughout the simulation process.

We have used an Arduino and fingerprint module to develop a sophisticated system. A fingerprint ID must be registered with the system in order to use this biometric voting machine; the fingerprint ID will be centrally kept in Arduino. A voter may cast a ballot throughout the election process if they insert their finger and it matches information that has been stored. The name of the candidate for whom the voter has cast a vote will appear on LCD to verify the voter. It's conveniently accessible and features a straightforward hardware design.

Summary

Hardware Requirements

- Because this device relies on voters' biometric identities, it needs the following components.
- Biometric identification via fingerprint sensor R305
- 16*2 LCD - To display results
- Arduino Uno - To store information
- Wire connectors - To make connections
- Resistors: To regulate the amount of current

IV. WORKING PRINCIPLE

A controller board based on the ATMEGA328P is called an Arduino Uno. Six of its fourteen digital input and output pins may be utilized as pwm outputs. a 16 MHz ceramic resonator and six analog inputs. An USB port. a reset button, an ICP header, and a power jack. An Arduino Uno together with a few input and output devices make up this setup. The keyboard and rps are among the input devices on the left side of the figure. The input power required to drive the circuit is supplied by the regulated power supply, or RPS. Since each individual has a distinct fingerprint, we may quickly identify them by utilizing the finger print module. By using the fingerprint. With this module, we can manage invalid votes and set up an alarm that sounds when someone tries to rig the results.

V. METHODOLOGY

The methodology of choice is Rapid Application Development (RAD) is the preferred technique because it aims to achieve three key goals: increased speed, improved quality, and reduced cost. RAD places a strong emphasis on utilizing unique methods and digital technologies to expedite the processes of analysis, design, and implementation. Fourth generation programming languages, Joint Application Design (JAD), and Computer Assisted Software Engineering (CASE) tools are examples of tools. Those are all pertinent to and necessary for the suggested met

The stage of the RDA approach are as follow: Phase 1: Conditions Planning is the process of examining the areas directly related to the system that is being suggested. The following areas are related to the proposed system:

- User voting mode
- Voter authentication mode
- Data collection and verification mode
- Data communication mode 2. Voter

Authentication: This satisfies our goal of guaranteeing a safe means of verifying voters prior to their being permitted to cast ballots. Voters would be verified based on the distinct identification information that they held.

Data Collection and Verification:

Prerecorded data in the system's memory, or database, is required before voters (or staff) may be confirmed. Thus, the information of each potential voter (staff) data must be gathered in order to enable verification. This contains all the information required to properly generate an election ID for them and allow the suggested method to ascertain if they qualify for different elections.

Data Communication

The internet would be used by the suggested system to function. This makes voting possible for all voters, wherever they may be, and makes it

possible for them to utilize a wider variety of devices. This is a network that is exclusive to participants in that specific organization. In this instance, information about the institution would be relayed from the hallway across this network. This information is only a list of students who are allowed to leave the school through the hallway; it is not very complicated. It is possible to send important extra data about the student. It is not necessary to send any more information about the host's destination name. Since this is the current criteria to take a leave of absence, this information is just needed in the hall. At departure locations, namely the school gate, Whether you have been given the all-clear to leave school at your residential hall is the information that is needed.

Phase 2: User Design: During this phase, key system components would be visually represented and the data and operations of the system would be illustrated using a variety of software modeling tools. The programming tools selected to put the suggested strategy into practice were also mentioned. Making this proposed system far more user-friendly and simple to use is a major accomplishment.

VI. CONCLUSION

All things considered, this device resolves the majority of the problems encountered during the paper ballot casting time. This machine's usability and net interface are what determine its performance. This will genuinely guarantee a more safe voting process, which may be crucial for a growing country's healthy growth. This study proposes a fingerprint-based voting mechanism that is faster and more accurate than previous methods. The new device maintains voting process integrity, simplicity of use, transparency, and prohibits access for unregistered voters. In addition, the voting system verifies the voter's eligibility and stops multiple votes using the same character. Additionally, as long as the voter is inside the electoral boundaries, they can vote from anywhere.
Voting machines that use fingerprints have created a danger to prevent erroneous votes. It shortens the time for voting, Simple to transport from the polling place to the polling place, Cut down on the balloting center staff, It provides trouble-free, accurate counting that is seamless. provision of preventative measures for voting.

REFERENCES

1. Vishal Vilas Natu, 2014. Smart-Voting using Biometric “International Journal of Emerging Technology and Advanced Engineering, 4(6).
2. Khasawneh, M., M. Malkawi and O. AlJarrah, 2008. A Biometric-Secure eVotingSystem for Election Process, Proceeding of the 5th International SymposiumonMechatronics and its Applications (ISMA08), Amman, Jordan
3. R. Murali, P. Bojja, and M. Nakirekanti, “AADHAR based electronic voting machine using Arduino,” International Journal of Computer Applications, vol. 145, no. 12, pp. 39–42, Jul. 2016, doi: 10.5120/ijca2016910786.
4. R. Rezwan, H. Ahmed, M. R. N. Biplob, S. M. Shuvo, and M. A. Rahman, “Biometrically secured electronic voting machine,” in 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Dec. 2017, pp. 510– 512, doi: 10.1109/R10- HTC.2017.8289010.
5. S. Anandaraj, R. Anish, and P.V. Devakumar, “Secured electronic voting machine using biometric,” in 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Mar. 2015, pp. 1–5, doi: 10.1109/ICIIECS.2015.7192976.
6. B. U. Umar, O. M. Olaniyi, A. B. Olatunde, A. A. Isah, A. K. Haq, and I. T. Ajayi, “A bifactor biometric authentication system for secure electronic voting system,” in 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON), Apr. 2022, pp. 1–5, doi:10.1109/NIGERCON54645.2022.9803174.
7. N. B. Kintu and I. Z. Mohamed, “A secure evoting system using biometric fingerprint and crypt-watermark methodology,” in ASCENT International Conference Proceedings – Information Systems and Engineering, 2018, pp. 1–18.

8. Virendra Kumar Yadav, SaumyaBatham, Mradul Jain, Shivani Sharma, 2014. An Approach to Electronic Voting System using UIDAI, 2014 International Conference on Electronics and Communication Systems.
9. Ashok, Kumar D. and T. Ummal Begum, 2011. A Novel design of Electronic Voting System Using Fingerprint.
10. Jefferson, D., A. Rubin, B. Simons and D. Wagner, 2009. A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), Technical Report,available at: http://www.servesecurityreport.org, last visited 2009.
11. Virendra Kumar Yadav, Saumya Batham, Mradul Jain, Shivani Sharma, 2014. AnApproach to Electronic Voting System using UIDAI, 2014 International Conferenceon Electronics and Communication Systems.