IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Special Issue 3, November 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 11, Special Issue 3, November 2023 ||

Smart Biometric Voting System

V.Sundara Jeyalakshmi[1], M. Dinesh[2], K. Hari Haran [3], P. Kamban[4], J. Kugan [5]

Assistant Professor, Department of Electronics and Communication Engineering, Adhiyamaan College of Engineering, Krishnagiri District, Tamil Nadu, India [1],

U.G Scholars, Department of Electronics and Communication Engineering, Adhiyamaan College of Engineering, Krishnagiri District, Tamil Nadu, India. [2, 3, 4,5]

ABSTRACT: Modernizing the voting process will improve accessibility and convenience for voters while preserving the fairness and security of elections. This abstract provides an innovative strategy to overcome these difficulties by showcasing a “Fingerprint-Based Voting System Using Arduino”. Theresults of traditional paper-based voting systems may not always be reliable and are subject to various types of fraud. This suggested system blends fingerprint identification with an Arduino-based platform to establish a secure and effective voting mechanism, taking use of developments in embedded systemsand biometric technologies. Using their own fingerprint, each voter's identification is confirmed using fingerprint authentication. The risk of fraudulent voting is eliminated by this biometric verification, which guarantees that only eligible voters can cast their ballots. To protect the integrity and confidentiality of the voting data, the system makes use of strong encryption techniques, thwarting any unauthorized access or tampering. The Arduino platform enables election officials to track the voting process in real-time and quickly identify any abnormalities. The system is made to be user-friendly, making it easy for voters to follow the steps and precisely cast their ballots. The system is inexpensiveand easily scalable to fit varied election sizes and budgets thanks to the use of open-source Arduino electronics. An important step has been taken towards enhancing the security and effectiveness of thevoting process with this ground-breaking Fingerprint-Based Voting System Using Arduino. It addresses issues with data integrity, authentication and accessibility, ultimately contributing to more transparent and trustworthy elections.

KEYWORDS: - Fingerprint, voting system, Arduino, Biometric Authentication, Election Security, Cost Efficiency, Electronic Voting, Biometric Verification, Voter identity, Secure Voting.

I. INTRODUCTION

The "SMART BIOMETRIC VOTING SYSTEM" is an innovative project designed to modernize a characteristic of democratic administration is election, which allows citizens to express their preferences on a range of matters, including amending the constitution, passing laws, and selecting the best candidate to lead them. There is an electoral system in place to set out the election'sregulations. While political elections are the most prevalent type, elections are essential to the operations of many other kinds of organizations. For businesses, unofficial organizations, and nonprofits, elections are essential. Elections are the way of the democratic world, but holding fair elections has proven difficult for all electoral bodies, particularly in nations with high rates of corruption, lax laws, and low levels of transparency. Additionally, to that, conducting Billions of dollars were spent on elections. The primary goal of this study report is to design a prototype for a fingerprint voting system that can support safe and reliable election progress. To enable an error-free voting process, the system incorporates a variety of hardware elements, including switches, LEDs, microcontrollers, and fingerprint modules. The R307 fingerprint sensor is utilized in the system's implementation to capture user finger prints, which are then stored in internal memory. Arduino is thenused to process and analyse the captured photos. An LCD panel is utilized to implement the user interface; it is primarily used to print instructions to users while the voting process and results are beingexecuted.

II. RELATED WORKS

Vishal Vilas Natu [1] proposed the voting system is completely depending on paper work and electronics machine. There is more paper work to save the information of voter and the voter must goto ballot box by carrying voter id for authentication. Once authentication is done by election executive then voter donate their vote by using electronic machine. The machine consists of list of candidate and presents multiple buttons in front of their particular name by pushing the button voter can donate their vote to candidate. To overcome this traditional election system there has to study of digital technologyand their security.

Khasawneh, M., et al. said in paper-based elections voters cast their votes by simply depositing their ballots in sealed

boxes distributed across the electoral circuits around a given country. When theelection period ends, all these boxes are opened and votes are counted manually in presence of the certified officials. In this process there can be error in counting of votes or in some cases voters find ways to vote more than once.Sometimes votes are even manipulated to distort the results of an electionin favour of certain candidates [2]. Viredra Kumar, et al. [3] proposed An Electronic Voting System that will automatically perform authentication,validation and counting with the help of UIDAI. The proposed electronic voting system can be implemented along with the traditional election system.The proposed an approach that will use the information provided by UIDAI in electronic votingsystem.

David Chaum [4] addressed the concepts of retrieve only the data that is related to the voting process and exclude all their irrelevant in formation.untraceable electronic mail and digital pseudonyms, which can apply for electronic voting for anonymity. Virendra Kumar Yadav et al. [5], an approach that will use the information provided by UIDAI in smart voting system. The proposed system procedure is carried out in mainly few stages: registration, verification and validation.These stages of proposed system are illustrated.

D. Ashok Kumar et al. [6] made a comparative Study on Fingerprint Matching Algorithms forEVM. Then fingerprint is matching voter can vote to candidate by using EVM. Fingerprint is secure method for EVM. Jefferson D., et al. [7] reviewed and computer of critique and security communication in secure voting system. The web-based voting system being built by Accenture and in security the fingerprint technology are uses.

Finger print voting elections mean that people can trust the results because it allows for a processthat is so auditable, transparent and secure. It's also helps reduce human error. Finger print voting andelectronic counting means that people can get official election results within hours, instead of weeks. Again, this builds trust.Technology will be a useful way of improving voter education and registration, to increase engagement and voter turnout. It is very good at making voting more accessible, meaningit's easier for disable people to vote independently [8].

III. EXISTING METHOD

Sri Lanka adopted the past-the-post (PTP) system for the first time, as stated in the 1978 constitution. That is the position where the candidate who, in addition to winning the most votes, is unworthy of anyone, comes in second. There was an activity in the majority of electoral districts in addition to a number of different districts.

People were extremely irritated because Sri Lanka's first-past-the-post (FPTP) system has previously led to bigger impacts. Currently, all 225 parliamentarians in Sri Lanka are chosen by a single ballot, with 29 national seats and 196 members allocated to 22 multi-member constituencies. Each voter may designate as their preferred representatives in their electoral district up to three candidates from their party of choice (without using a rank ranking system). Counting preferences is one of the hardest counting tasks.

In Sri Lanka, the voting method known as "preferential voting" is used instead of the more widely used term "open list." The public's belief that MPs with huge electoral districts are less approachable and less interested in local issues has contributed to the unpopularity of this system. Erroneously, other worries about campaign finance and election violence have also been mistakenly linked to and perceived as drawbacks of the current democratic system.

As of my most current knowledge update in September 2021, there were no well-known or well-established biometric voting systems using Arduino in official government elections. However, the Arduino-based voting systems and biometric identification projects were still in the development and experimentation stages. That's probable that these initiatives have progressed since then.

IV. PROPOSED SYSTEM

The offline version of the suggested system uses an Arduino-based electronic fingerprint voting system. This system uses fingerprint verification. It also accepts the voter's national ID card number, offers a voting interface, and displays error or confirmation notifications. Fingerprints are used for authentication since they process biometric data more quickly and accurately than other biometric data and are widely used in the immigration system worldwide. There might be a team in charge of this system at the electoral departments here. The separators were positioned far away fromthe boll booths. They were accustomed to handling processing tasks including image and fingerprint processing, data transfer between the client and the database, report generation, and voter messaging.Every citizen of Sri Lanka has their biometric and demographic information stored in a single database. Sub-databases with copies of district-level citizen data were placed next to the servers in each district election office in order to lessen the strain on the central database. Only those who fall under its purview can access the data that all of the sub databases retrieve from the central database. The information is updated on a regular basis and is kept in a volatile manner that allows it to be deleted as needed. The databases of SAB will only retrieve information essential to the voting process, eliminating any extraneous information. These datasets will be utilized to provide electoral process reports and results. Voting from any location is made possible by these databases as long as the voteris within electoral circuits. A valid National Identity Card number is a prerequisite for verifying an individual's identity. When the number is located, it will first be verified

in the local database before being searched in the central database. If an individual's number is not located in the central database,they will not be able to participate in the voting process fraudulently, if the number is located in the central database, their data will be cached to a sub database. In order to complete their process for verification, the person's finger print will be scanned at the client site and compared one-to-one with the data derived from the local database at the fixing servers. This entry has been taken out of the localdatabase.

Figure: proposed system

ALGORITHM:

In order to verify and identify people, biometrics, especially fingerprint recognition, frequently uses minutiae matching and pattern matching techniques. These methods are essential for guaranteeing the precision and dependability of biometric systems. Below is a summary of each:

Matching minutiae: A popular technique in fingerprint identification systems is minutiae matching. It entails identifying and contrasting particular minute details present in a fingerprint. Minutiae are unique features of ridges, usually found near bifurcations and terminals (ridge splits). The following steps are involved in minutiae matching:

- Fingerprint Enrollment: When a person first registers or enrolls in a biometric system, the system takes a fingerprint sample and extracts all of the little details from it.
- Template Creation: These gleaned details are used to generate a template. The enrolled fingerprint might be referred to this template.
- Matching: The system takes a fingerprint and extracts minute points once more from the person attempting to authenticate themselves.
- Comparison: The system makes a comparison between the minute details recorded in the template and the minutiae points derived from the collected fingerprint. In the comparison, the spatial relationships and similarity between minutiae are evaluated.
- Calculation of Score: The number of identical details and their degree of similarity are used to calculate a matching score. The technology confirms the person's identification if the score rises beyond a set level.

Pattern Recognition: Contrarily, pattern matching compares the general features or pattern of the complete fingerprint as opposed to individual details. The fingerprint's overall characteristics are of greater importance to the process. These are the essential phases in matching patterns:

- Enrollment via Fingerprint: Enrollment involves the system capturing and creating a templatefrom the whole fingerprint pattern, similar to minutiae matching.
- Template Creation: The general properties of the fingerprint pattern are used to create atemplate. This could involve the fingerprint's overall form, orientation, and ridge patterns.
- Matching: The system takes another picture of the fingerprint during authentication.
- Comparison: The fingerprint pattern obtained from the collected fingerprint is compared by thesystem to the template that was made during enrolment. It evaluates how comparable the globalproperties.
- Calculation of Score: Based on how similar the collected fingerprint is to the template that hasbeen stored, a matching score is calculated. A predefined threshold must be exceeded for the person's identification to be verified.

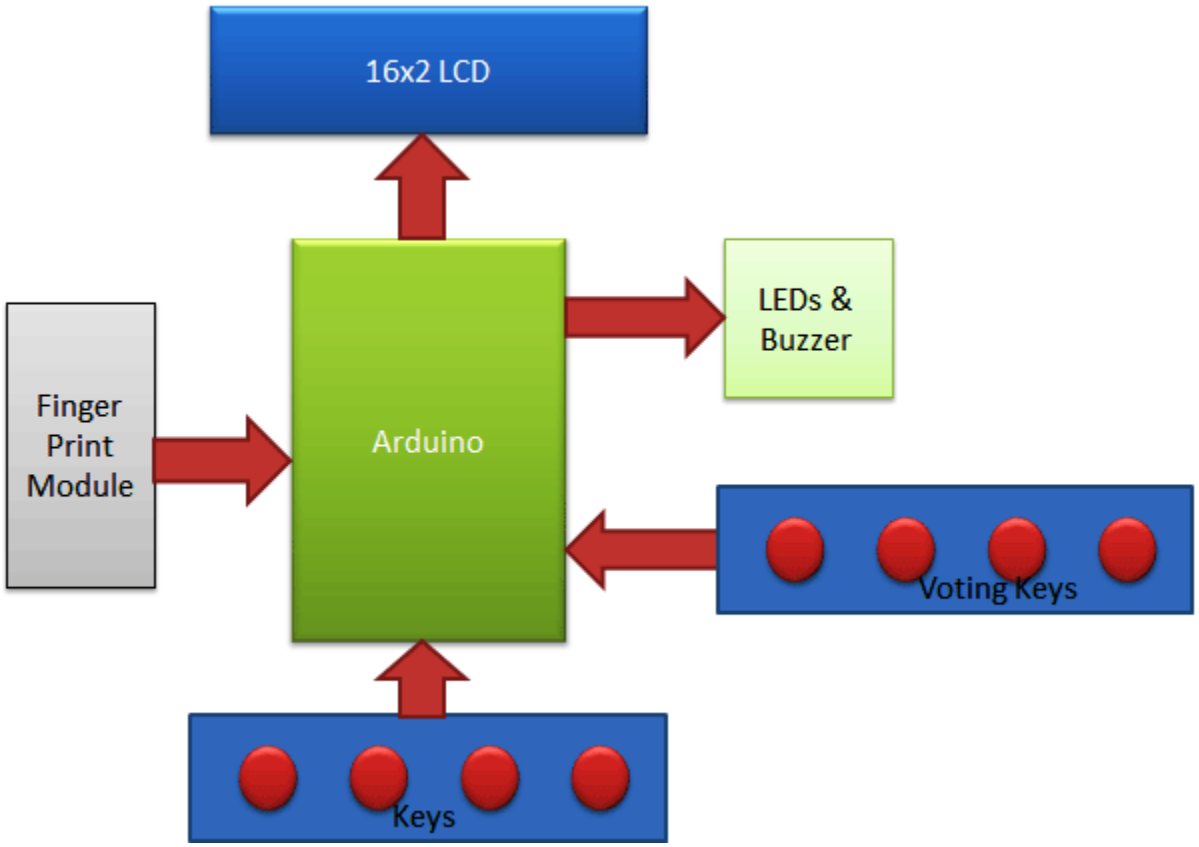
For an automatic fingerprint identification system to function properly, the fingerprint image must be accurately

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 11, Special Issue 3, November 2023 ||

represented. Thus, before the details are recovered, a fingerprint image undergoes a number of operations such as augmentation, analysis, binarizing, thinning,and ridge construction elevated.

V. BLOCK DIAGRAM



- The voter registration procedure is the first step in the system, where eligible voters input their fingerprint data and personal information. This information is then securely kept in a central database. When a voter shows up at the polls, a biometric scanner scans their fingerprint. The scanner converts the fingerprint into a digital representation.

- The information contained in the voter registration database is compared with the fingerprint data gathered to verify the voter's identity. In the event of a match, the voter may proceed.

- Following validation, the voter can use the voting machine to express their preference. A digitalinterface that shows the candidate's name or platform can be used by the voter to select a candidate.

- The vote data is gathered and tallied to establish the election results once the voting session ends. • The voting machine securely records the vote and may encrypt it to ensure its integrity.This procedure might be dispersed among several sites or consolidated.

- To ensure accountability and transparency, the final vote results are shown in real-time, enabling interested parties to keep tabs on the election's development. An audit and security module keeps an eye on every step of the process to preserve the security and integrity of the system. It ensures a fair election by creating audit trails for accountability and verification.

- Redundancy and backup procedures are in place to guard against system breaches and failures, guaranteeing that the voting process proceeds according to schedule even in the event that • A fingerprint-based voting system increases security and reduces the chance of voter fraud by linking every vote to a unique biometric identification.

Nonetheless, these systems need to ensure the security of the biometric data and address privacy concerns.

VI. EXPERIMENTAL RESULTS

SIMULATED RESULTS:
First enrol the voter's finger and save the fingerprint by given id.

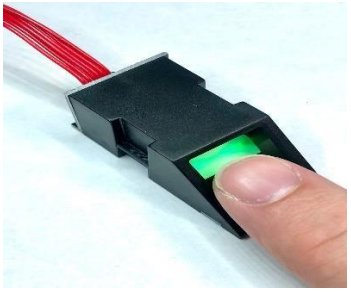


Figure: Place the finger in fingerprint module

In this time voter ask to user to get an id to save their fingerprint. After given id voter place theirfinger on fingerprint module to scan, during the enrolling voter place their finger in two times, in first time image take and convert, then second time check the fingerprint with first scan, if fingerprint matched save the fingerprint in given id. Otherwise "Fingerprint did not match" message displayed onLCD.

In this step voter scan their finger if fingerprint matched, LCD displayed a message "Did Not Match" , then matched "Found Match", "Found Id" (messages were displayed on LCD. In this step display the Id of saved fingerprint.

Fig. 14: Result of finger scanning

After select party, voters cast their three preferential votes to the candidates from the selectedparty. If press party list button more the one time, it's not allowed to poll vote and cannot select morethan 3 candidates from the candidate list.

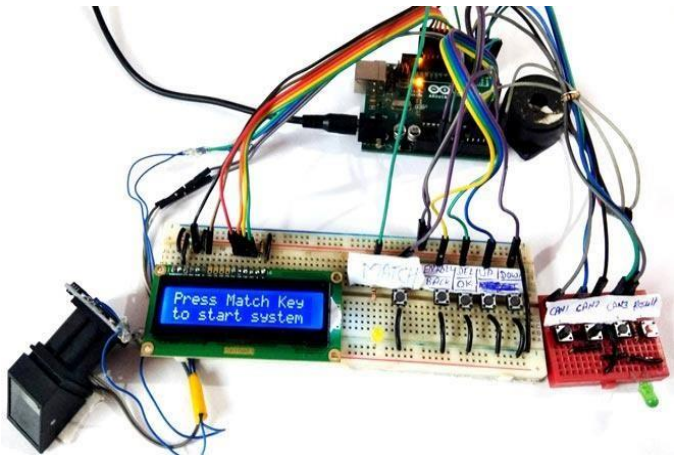


Figure: Experimental Result

VII. FUTURE SCOPE

This voting technique contributes to increased vote security. IoT-based voting also makes postal voting more secure. Voting on this method is possible from any location in the globe. When compared to the existing methodologies, this technology yields results faster. More memory on the controller facilitates the storing of more data. Increasing the number of biometrics such as face, iris, and so on can increase security. We can achieve complete automation of the system by improving internet security. In order to enable voters to cast ballots from any location with an analogous state, our future effort will involve connecting all of the surveying booths inside a state with suitable online security. This explains why the Internet of Things-based fingerprint voting machine will be beneficial to rigging. The project's main goal was to create a fingerprint-based voting system that eliminates voting fraud and streamlines the voting process. Given that the system created for this project is merelya rudimentary prototype, there are undoubtedly a ton of opportunities for improvement with increased money and investigation. We'll talk about a few methods to improve this project below this system canhave a WIFI module added to it. The host server can then be securely connected to a large number of voting machines via a LAN. This will make it possible to store data in real time on a host server that is situated in a safe area. Since the data are now sent to the host server in real time, physically destroying the device won't result in data loss.

VIII. CONCLUSION

The goal of this “Smart Biometric Voting System” was to create a working prototype fingerprint voting system that guarantees a quick and secure voting process. An Arduino Nano fingerprint voting system prototype was created for this purpose, utilizing a R307 fingerprint module, an LED (16x2), and an EEPROM internal memory storage method. The culmination of several effective hardware and software integrations is the finished system. Review and analysis, system and algorithm design, hardwiring, hardware and software integration, testing and debugging, and result analysis are all steps in the process. In conclusion, the prototype device successfully registered voters' fingerprints in the R307 fingerprint module flash memory, confirmed voters' statuses (registration and multiple voting), compared newly input fingerprints with a stored fingerprint template, and authorized voters. to vote and was successful in producing a result. In conclusion, the gadget is a fantastic substitute for other drawn-out election procedures, particularly the ballot paper voting technique. At a later stage of development, the prototype device could be improved even further. For example, adding an additional memory space might help store any amount of fingerprint data, and adding a WIFI module could help deliver results wirelessly to the host computer.

REFERENCES

[1]..Vishal Vilas Natu,2014. Smart-Voting using Biometric “International Journal of EmergingTechnology and Advanced Engineering [1].

[2]..Khasawneh, M., M. Malkawi and O. Al-Jarrah, 2008. A Biometric-Secure e-Voting System for Election Process, Proceeding of the 5th International Symposium on Mechatronics and its Applications(ISMA08), Amman, Jordan[2].

[3]. Virendra Kumar Yadav, SaumyaBatham, Mradul Jain, Shivani Sharma, 2014. An Approach to Electronic Voting

System using UIDAI, International Conference on Electronics and Communication Systems[3].
[4]. Chaum, D.L., 1981. Untraceable Electronic Mail,Return Addresses and Digital Pseudonyms, Communications of the ACM[4].
[5]. 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[5].
[6]. Ashok, Kumar D. and T. Ummal Begum, 2011. A Novel design of Electronic Voting System Using Fingerprint[6].
[7]. 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[7].
[8].[Mohamed S. Sulaiman, M. Anto Bennet, A.A.Aravind, S.K. Rajvel and G. Janakiraman, 2016.A Design of E-Voting Using Fingerprint RecognitionSystem for Secured Voting, Middle-East Journal of Scientific Research, 24(Techniques and Algorithms in Emerging Technologies)[8].

BIOGRAPHY

Mrs.V.Sundara Jeyalakshmi,M.E,Assistant Professor,
Electronics and Communication Engineering Department,
Adhiyamaan college of Engineering,Hosur

Dinesh.M,
Electronics and Communication Engineering Department, Adhiyamaan college of Engineering, Hosur

Hari Haran.K,
Electronics and Communication Engineering Department, Adhiyamaan college of Engineering, Hosur

Kamban.P,
Electronics and Communication Engineering Department, Adhiyamaan college of Engineering, Hosur

Kugan.J,
Electronics and Communication Engineering Department, Adhiyamaan college of Engineering, Hosur

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details