IRO Journal on Sustainable Wireless Systems (ISSN: 2582-3167)
www.irojournals.com/irosws/

A Digitalized Voting System using Fingerprint Authentication

Ayisha P[1], Karishma V S[2], Renuka T[3], Shruthi Dileepkumar[4], Akhila E[5]

[1,2,3,4] Student, Department of Computer Science and Engineering, Jawaharlal College of Engineering and Technology, Palakkad, Kerala, India.

[5]Assistant Professor, Department of Computer Science and Engineering, Jawaharlal College of Engineering and Technology, Palakkad, Kerala, India

E-mail: [1]ayishaaliotp02@gmail.com, [2]karishmavs2001@gmail.com, [3]renukaraviotp@gmail.com
[4]shruthidileep2001@gmail.com, [5]mailtoakhilasathish@gmail.com

Abstract

Electronic voting, also referred to as "e-voting," has been used since the 1970s and has several benefits over paper-based systems, including increased efficiency and reduced mistake rates. However, there are still obstacles to the widespread adoption of these systems, particularly when it comes to enhancing their susceptibility to potential defects. To promote error-free, quick, and secure voting in elections, the study proposes an authentication system and a digitalized version of the current voting system in this research and suggests a fingerprint authentication method because fingerprints serve as a user's unique and crucial form of identification. Aadhar database is stored in the system, and when a voter enters the polling booth, authentication and verification are done through a fingerprint scanner with the help of this. The voter can cast their vote digitally once the authentication and verification processes have been completed. If the voter has already voted, an error occurs and the 'voter has already voted' message is displayed. Since the system already has the entire voter's information, if there is a problem with the authentication procedure, the voter won't be able to cast their vote. The proposed design has an easy-to-understand architecture and responds quickly. It makes trouble-free, easy, and accurate counting possible. This approach allows qualified voters to cast their ballots from anywhere in India.

Keywords: Biometric, fingerprint voting, NodeMCU, Security, Authentication and Verification.

DOI: https://doi.org/10.36548/jsws.2023.2.006
Received: 03.05.2023, received in revised form: 03.06.2023, accepted: 18.06.2023, published: 28.06.2023

1. Introduction

A population selects a person or people to hold public office through a formal process of collective decision-making called an election. Elections have served as the main tool for representative democracy in modern times since the 17th century. On occasion, elections may be held to fill legislative, executive, judicial, regional, and municipal seats. The greatest democracy in the world, India, is based on the principle that each citizen elects their own officials. However, in the modern period, there are many issues that the fair election process must deal with, such as booth capture, tampering, voting fraud, interference with the "electronic voting machines (EVMs)", etc. It is the responsibility of a responsible engineer to take action to stop this threat. The voting process is conducted electronically with the most prevalent EVMs, which eliminates the need for paper ballots because they are time-consuming and subject to purposeful or accidental inaccuracy. The validity of the voter is a main issue today, as it is important to confirm that the same voter cannot cast two votes. By implementing a voting system based on biometrics, this problem can be solved. Biometrics is the study of biological data through measurement and analysis. Technology that analyses and measures physical traits of the human body, such as fingerprints, voice patterns, facial patterns, hand measurements, DNA, and eye retinas, is known as biometrics. Due to the great variety of physical identifying methods, the field of biometrics has expanded. A well-known identifier and kind of biometric that can be used by law enforcement is the human fingerprint.

The human fingerprint can also be used as a human biometric system because each individual's fingerprint is unique and different, proving that it cannot be copied or altered. The fingerprint is utilised for user identification and authentication. The system will check to see if the voter's finger matches the pre-stored impression in the database while they are voting if they keep their finger in the scanner. If they match, the system will permit the voter to cast his vote; if not, it will deny it. The rest of the voter's fingers will become disabled once they have cast the vote using a certain finger.

The proposed model consists of a R307 fingerprint reader, a Node MCU microcontroller plus Wi-Fi, a keypad, an LCD matrix display, and a 12 volt/1 A dc power supply. An alarm is used to signal that the fingerprints do not match.

2. Related Work

Vote duplication or tampering are prevented by the e-voting system's by the inclusion of Aadhar[1]. Block chain technology and platforms are also used. Blockchain is a distributed, decentralised ledger that is employed to effectively record the transaction. It has an intriguing quality that makes data difficult to modify once it is recorded inside a blockchain. The Aadhar database aids in obtaining voter demographic information, including fingerprint information. The fingerprint is transformed into a digital signature that can be used to guarantee election security.

“EVM authentication based on the biometric information is proposed” [2]. In this case, the biometric data is a finger print. The "PIC16F877A microcontroller and other related peripherals like GSM module, Power supply, Fingerprint module, LCD, etc. are used in the construction of this paper." to confirm the admissibility of the person comparing the current fingerprint with the previous one saved in the database. The PICI6F877A microcontroller is very easy to operate, and it is also simpler to code or program. The fact that it employs FLASH memory technology is one of its key advantages because it allows for unlimited write-erase cycles. For any usable electronic circuit to be tested and put into operation, power supply is necessary. The foundation of the power supply is a full wave bridge rectifier, filter circuit, and voltage regulator. A computer and a GSM-GPRS system's communication are connected by a GSM or GPRS module, and the system sends the voter feedback right after they cast their ballot.

A finger print voting system with Arduino is suggested in a paper titled Advanced voting system using fingerprint [3], which makes voting in elections error-free. This study suggests error-free voting in elections using a system made up of a fingerprint unit, Arduino Uno microcontroller board, power supply system, and LCD screen. An input device called a fingerprint module is used to process fingerprints and take digital images of the fingerprint pattern. In order for the system to create and store a template of the finger based on processing results, the user must enter the finger impression twice throughout the fingerprint enrolling procedure. The system will output all information to the LCD panel. It displays the outcome, whether it was successful or not.

Bhavana, Bhoomika, Bindu, Madhuri and Asha developed a system that uses thumb impression for voter identification [4]. Voters' thumbprints are submitted into the system during elections and compared to the database's records that are currently available. The

proposed model uses an LCD screen, EEPROM, and EVM.EVM is used to speed up and improve the reliability of polling, and EEPROM is used to store data indefinitely. The outcome is displayed on an LCD. The GABOR method is used in this model to compare the fingerprint to the database that has been saved.

A fingerprint sensor is utilised in this Biometric Based Secured Remote EVS [5] system to verify the validity of voters by integrating their biometric. The Delete/Okey, Check Match, Register/Back, Move Up, and Down push buttons have all been utilised. The Match key must be pressed by voters as they approach the voting booth to cast their ballot. When the Match key is hit, a buzzer beeps and an LED illuminate. The user is then instructed to maintain their finger over the fingerprint sensor by an LED. As soon as the module has a picture of the finger, it uses hashing to locate any associated IDs that are stored in the database. As soon as the module has a picture of the finger, it uses hashing to locate any associated IDs that are stored in the database.

When the IDs match, the LCD displays "voter authorized," and the green LED starts to shine, signalling the start of the second voting step. The voter is then able to select their preferred candidate. Pressing the new matrix set of keys accomplishes this.

This proposed framework for a fingerprint-based voting system's [6] goal is to make the current voting process more precise, transparent, and quick while also guaranteeing that each voter only casts one vote. This system is made up of a control unit, an EEPROM, an LCD display, a power supply, a microcontroller, and a ballot unit. A ballot unit is a straightforward voting gadget that lists the candidates. For voter identification, a finger is scanned using a fingerprint sensor. The control unit manages the polling process, including how many votes were cast overall, when the poll was sealed, and when the results were eventually announced. A microcontroller unit is a type of computer that has a lot of input and output options and internal memory. The voting outcome is displayed on the display device. Permanent data storage is accomplished through EEPROM.

Based on an electronic voting system, the suggested Biometrically Secured Electronic Voting system [7] is proposed. Each voter can be recognized by this system by providing a fingerprint. Every time a fingerprint is received, the system compares it to the fingerprint in the database. The system is set up so that if a vote is accidentally cast for a candidate, the voter can change their vote, but only once. Another benefit of this technology is that it operates

entirely offline, making data un hackable. The suggested system includes an LCD display, an EVM, an Arduino, and a fingerprint scanner.

3. Proposed Work

This method intends to build a fingerprint-based voting system in which the voter is authenticated by scanning his or her fingerprint on the fingerprint reader, which aids in the conduct of free and fair elections in a democratic country like India. The proposed model is more secure in that the voter is authenticated by scanning their fingerprint on the fingerprint reader. Another advantage of the approach is that it prevents fake voters. In this system, a person can also vote from outside his or her allotted location or from his or her preferred location. The system comprises the following components: a power source, a Node MCU microcontroller with Wi-Fi, an LCD display, a fingerprint scanner, and an alarm. Voters are well guided by the LCD display. Initially, the voter places his fingerprint on the fingerprint reader, which verifies the user's identity. If the voter is verified, he or she will be able to vote via a web interface. If a problem occurs when scanning the fingerprint or if a disabled person votes, their Aadhar number can be used to verify their identity. The system architecture of the system is shown in Figure 1.

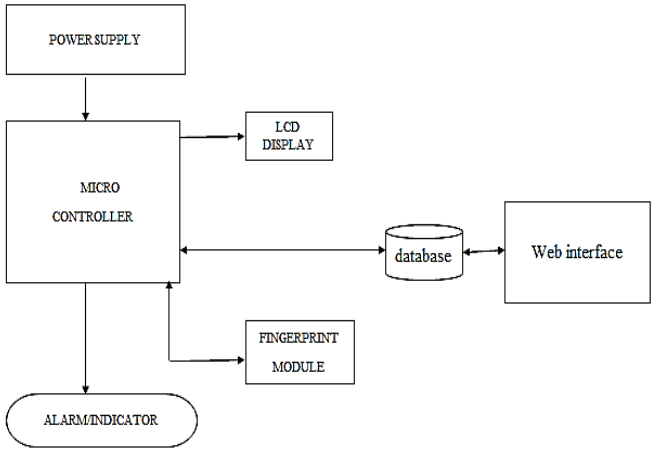

Figure 1. System Architecture of Biometric Authentication System

The voter's fingerprint impression is entered into the system as input, which is then compared to the entries in the database. The fingerprint authentication system is in charge of the voter's authentication and verification. Once the authentication and verification processes are completed, the system will allow the voter to vote. The fingerprint authentication system is

in charge of managing eligibility, voting permission, and the verification procedure. The voter can then cast their vote via the web interface.

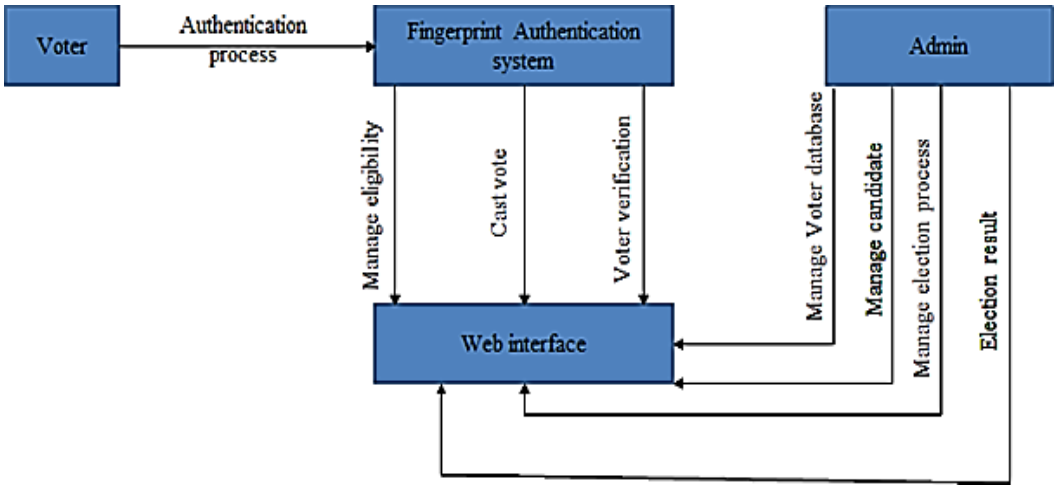

Figure 2. Dataflow Diagram of Biometric Authentication System

Data flow diagram of the authentication system for secure voting is shown in Figure 2. The fingerprint impression or Aadhar number of a voter is given as input to the system and matched with the records already existing. The registered voter's data (in a real-life scenario, the Aadhar database) in the present prototype is stored in a database. If the particular pattern of the fingerprint matches the record, then access to vote is granted. If the pattern does not match the record stored in the database, access to cast a vote is denied. Once the voter casts their vote using a particular finger, the rest of the fingers will be disabled. After verification, the ballot unit will be enabled within a particular time limit, and voters can cast their vote. Figure .2 depicts a level 1 data flow diagram. The polling station login interface allows voters to interact with the system. Voters can select whether to use Aadhar or biometric data. When the voter selects the biometric information, the online interface displays a waiting message on the screen.

The voter can then scan their fingerprint using the fingerprint scanner for authentication and verification. Once authentication and verification are complete, the web interface will display the voter's name and data, as well as a cast vote message for the appropriate candidates based on their area. They can vote for their favourite candidate, and the results will be presented on the screen and saved in the database. These data are accessible to the administrator, and the administrator can access the system using their credentials. They may control the candidates, voters, and quantity of votes. When a voter uses Aadhar on the web interface, they can

authenticate and verify themselves using their Aadhar number, and they can vote in the same way. If the authentication and verification fail, an alarm will ring.

4. Hardware & Software

4.1 Node MCU Microcontroller Plus Wi-Fi

Figure 3. Node MCU Microcontroller Plus Wi-Fi

"The NodeMCU (Node Microcontroller Unit) is an open-source platform" for creating hardware and software that is based on the ESP8266, a low-cost System-on-a-Chip (SoC). All basic computer parts, including "CPU, RAM, networking (Wi-Fi), and even a modern operating system and SDK", are included in the Espressif Systems ESP8266. It is therefore an excellent option for all types of "Internet of Things (IoT) projects".

4.2 Fingerprint Reader

Figure 4. R305-Fingerprint Reader

This fingerprint sensor module, model number "R305-TTLUART, has a TTL UART interface. The user can save the finger print data in the module and set it to identify the person

in 1:1 or 1:N mode". The fingerprint module may communicate directly with a 3v3 or 5v microcontroller. Interfacing with a PC necessitates the use of a level converter (such as the MAX232).

4.3 Languages C# and PHP

The C# programming language is used to implement connections in physical components, while the PHP programming language is used to create web interfaces.

"PHP is a server-side scripting language that is embedded in HTML. It is used to manage dynamic content, databases, session tracking, even build entire e-commerce sites".

5. Results and Discussion

The system is implemented with the biometric authentication. There are mainly two units in the system. The first unit is the authentication and verification unit, and the other is the voting unit. In the voter verification unit, the voter is verified by scanning his or her fingerprint on the fingerprint reader. Three scenarios are presented in this section: the first-time voter, the multiple-voter, and the fingerprint and Aadhar number mismatch. When a voter casts a ballot for the first time, his or her fingerprint is compared to fingerprints that have already been saved; if a match occurs, the voter is allowed to vote, and the message "Matched" appears on the LCD display screen. A beep sound will be made and an "already voted" message will appear on the monitor if an authenticated voter attempts to cast a vote more than once. He or she is unable to vote if the fingerprint or Aadhar number is not present in the database. In the voting unit, the voter can cast their vote on a web page provided. He or she can choose their candidate and cast their vote. Finally, the authorised officer gets the summary of votes.

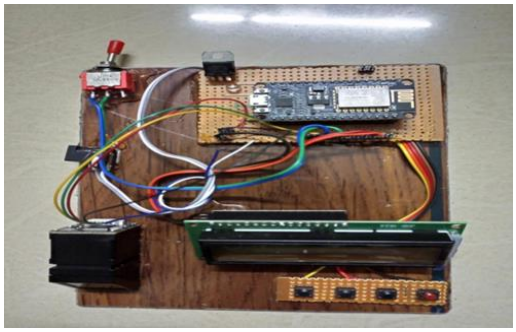

Figure 5. Verification and Authentication Unit

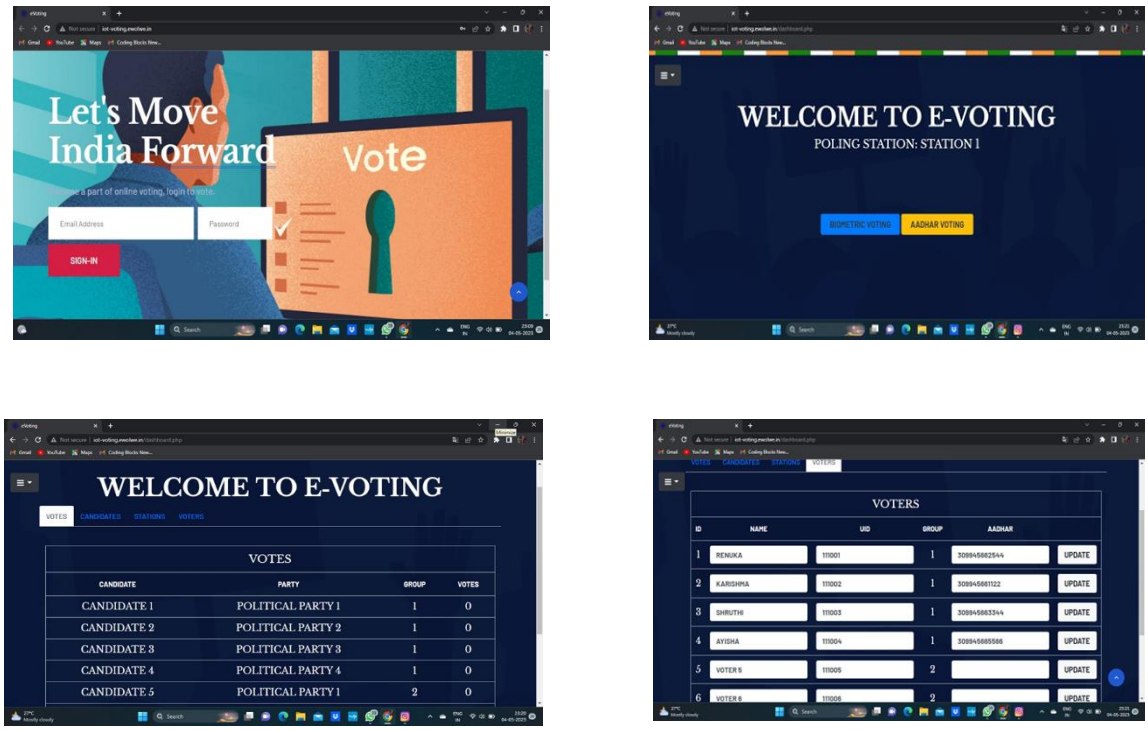

Figure 6. Different Stages of Voting System

6. Conclusion and Future Scope

One of the most commonly used biometric techniques for identifying people is the analysis of their fingerprints. Every identification in the world has a unique fingerprint, and even twins are born with completely different fingerprints that are naturally unchanging throughout their lives. As a result, a fingerprint voting system has been developed. This will prevent illicit practises such as tampering. Citizens can be certain that they alone can choose their leaders, thereby exercising their democratic prerogative. By implementing fingerprint authentication, users of the Fingerprint Voting System can cast their votes for the candidate of their choice. As previously indicated, the major goal is to increase security to prevent duplication and to create a system that lessens the load on those who administer elections.

By establishing this method, people can vote without worrying about security by using their fingerprint instead of paper. Overall, the most of the problems associated with the conventional voting system are resolved by this system. The usability of the web interface determines how effective this solution is. This would undoubtedly provide a safer voting

process, which is crucial for the steady development of a developing country. The suggested fingerprint-based voting method outperforms the current approach in both speed and accuracy. The new system restricts access to unregistered voters, offers user-friendliness and transparency, and upholds the fairness of the electoral process. The system also solves the problem of modifications , which means it does not allow a user to vote multiple times since his fingerprint is recorded once in an election. The system prohibits a voter from casting more than one ballot in a single election. The fingerprint-based voting technology has reduced polling hours and staff requirements while also giving voters the opportunity to avoid casting erroneous ballots. It provides easy and accurate cutting without any trouble.

References

[1] Roopak T M, Dr. R Sumathi.”Electronic voting based on Virtual ID of Aadhar using Blockchain Technology”. Proceedings of the Second International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2020). IEEE Xplore Part Number: CFP20K58-ART; ISBN: 978-1-7281-4167-1, 2020.

[2] Abeesh A I, Amal Prakash P, Arun R Pillai, Ashams H S, Dhanya M, Seena R ”Electronic voting machine authentication using Biometric information”. International Journal of Engineering Research & Technology (IJERT). ISSN: 2278-0181, 2017.

[3] TuerxunWaili, Amir NurIman Bin Mohd Zaid, Mohammed Hazim Alkawaz “Advanced voting system using fingerprint”. International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 6, Issue 2 (2020)

[4] Bhavana.CL , Bhumika.N , Baindhu. HS , Maduri. R , Asha. A "An advanced and secured biometric voting system“. International Journal of Engineering Research & Technology (IJERT). ISSN: 2278-0181, 2018.

[5] Samarth Agarwal , Afreen Haider , Abhishek Jamwal , Param Dev , Rjeevan Chandel "Biometric based secured remote electronic voting system". IEEE 7th International Conference on Smart Structures and Systems ICSSS 2020.

[6] Nahida Nigar , Mohan Lal Nath , MD . Toufil Islam. "A proposed framework for fingerprint based voting system in Bangladesh". International Journal On Informatics Visualization, VOL 4 (2020) NO 1, e-ISSN : 2549-9904, ISSN : 2549-9610, 2020.

[7] Rahil Rezwan , Huzaifa Ahmed , M.R. Biplob , S.M.Shuvo , Md . Abdur Rahman "Biometrically secured electronic voting machine". 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC). 21 - 23 Dec 2017.

[8] Rudrappa B. Gujanatti , Shivaram N. Tolanur , Murughendra S.Nemagoud , Shanta S. Reddy , Sangameshwar Neelagund "AFingerprint based voting system". International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 4 Issue 05, May-2015.

[9] Sarker, M. Mesbahuddin, et al. "An approach of automated electronic voting management system for bangladesh using biometric fingerprint." International Journal of Advanced Engineering Research and Science 3.11 (2016).

[10] R.Murali Prasad, et al, "AADHAR based Electronic Voting Machine using Arduino", International Journal of Computer Applications, vol. 145, no. 12, July 2016.

[11] Desna Sebastian, et al, "Aadhar Based Electronic Voting System and Providing Authentication", International Journal of Science and Engineering Research (IJ0SER), no. 3, March 2015.

[12] M. Yinyeh and K. Gbolagade, “Overview of biometric electronic voting system in ghana,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 7, 2013.

[13] Raj, Rakesh S., et al. "An online voting system using biometric fingerprint and Aadhaar card." IJCAT International Journal of Computing and Technology 1.4 , 87-92, 2014.

[14] Ashok Kumar D., Ummal Sariba Begum T., “A Novel design of Electronic Voting System Using Fingerprint”,International Journal of Innovative Technology & Creative Engineering, ISSN:2045-8711, Vol.1, No.1. pp: 12 19, January 2011.

[15] A. Indapwar, M. Chandak, and A. Jain, “E-voting system using blockchain technology”. Int. J.Adv. Trends Comput. Sci. Eng., vol. 9, no.3, pp. 2775–2779, 2020.