IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IOT BASED FINGERPRINT VOTING SYSTEM

[1]Mrs Lavanya N, [2]Sneha M, [3]Sariya Tehseem, [4]Shaistha Mehdi, [5]Saikrishna Ghawalkar

[1]Assistant Professor, [2]Student, [3]Student, [4]Student, [5]Student
Department of Computer Science and Engineering,
ATME College of Engineering Mysore, Karnataka, India

Abstract: A new technology that has the potential to improve the security and accuracy of voting is the biometric fingerprint voting system. The state-of-the-art in biometric fingerprint voting systems is thoroughly reviewed in this study. The article begins by giving a general review of the idea of biometric authentication and its several varieties. After that, it talks about the drawbacks of the current voting methods and how biometric voting systems can fix them. The article goes into additional detail about the different hardware and software elements of a biometric fingerprint voting system, as well as the various methods for fingerprint matching. The report also examines the difficulties of deploying biometric fingerprint voting systems, including cost-effectiveness, scalability, and privacy issues. The study thoroughly examines the benefits and drawbacks of biometric fingerprint voting systems vs conventional voting methods. The benefits include increased security, accuracy, and efficiency, while the drawbacks include implementation costs, technological challenges, and potential privacy issues. The study continues with a discussion of potential prospects for biometric fingerprint voting system research, including enhancing the precision of fingerprint-matching algorithms, resolving privacy issues, and creating more scalable and affordable systems.

Index Terms **- Biometric Authentication, Fingerprint Matching, Voting Systems, Security, Accuracy, Efficiency, Privacy Concerns, Scalability**

I. INTRODUCTION

The traditional paper-based voting system has been used for decades, but it has some limitations in terms of accuracy, security, and efficiency. Biometric fingerprint voting systems have emerged as a potential solution to address these limitations. Biometric authentication is a unique method of identifying an individual based on their physiological or behavioural characteristics. Among the various biometric modalities, fingerprints are the most used for identification due to their uniqueness and stability. Biometric fingerprint voting systems utilize this technology to provide a secure, accurate, and efficient voting process. This paper presents a comprehensive survey of state-of-the-art biometric fingerprint voting systems. The paper first provides an overview of biometric authentication and its various types. The different types of biometric authentication include facial recognition, iris recognition, voice recognition, and fingerprint recognition. Among these, fingerprint recognition is the most widely used for its accuracy, ease of use, and cost-effectiveness.

Fig. 1: Paper Ballot Voting System

The paper then discusses the shortcomings of the traditional paper-based voting system and how biometric fingerprint voting systems can address these limitations. The traditional paper-based voting system has several disadvantages, such as the potential for ballot stuffing, impersonation, and tampering. These issues can compromise the accuracy and fairness of the election. Biometric fingerprint voting systems provide a solution to these issues by using fingerprint recognition technology to authenticate voters and ensure that each voter can only vote once. The paper further elaborates on the components of a biometric fingerprint voting system. These components include hardware, software, and algorithms used for fingerprint matching. The hardware used in biometric fingerprint voting systems includes fingerprint scanners and computers that store and process voter data. The software

used in these systems includes voter registration software, database management software, and software used for fingerprint matching.

Fig. 2: EVM Voting Machine

The paper also discusses the challenges faced in the deployment of biometric fingerprint voting systems. These challenges include privacy concerns, scalability, and cost-effectiveness. Privacy concerns arise when personal data, such as fingerprints, are collected and stored. It is important to ensure that this data is protected and not misused. Scalability is another challenge faced in the deployment of biometric fingerprint voting systems. These systems need to be able to handle large numbers of voters during elections, and the system should be able to scale up or down as required. Cost-effectiveness is also a challenge, as biometric fingerprint voting systems can be expensive to implement and maintain. The disadvantages of biometric fingerprint voting systems include the cost of implementation, technical difficulties, and potential privacy concerns. Implementing a biometric fingerprint voting system can be expensive, requiring significant investments in hardware, software, and personnel. Technical difficulties can also arise, such as fingerprint recognition failures, system crashes, and database errors. Privacy concerns are another disadvantage, as personal data, such as fingerprints, are collected and stored, raising concerns about data security and privacy breaches.

II. LITERATURE SURVEY

Table 1: Relevant studies on advantages and disadvantages of approaches to the voting system

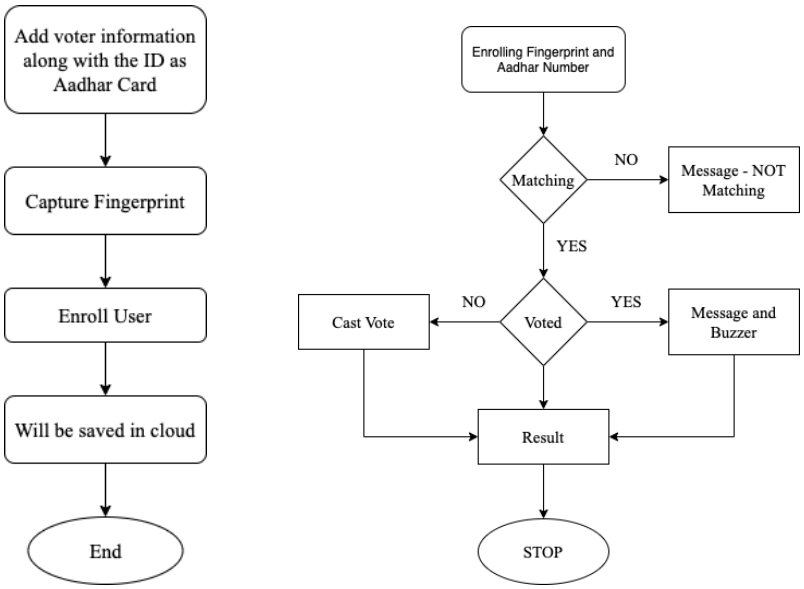
Sl No.	Title	Author	Methodology	Limitation
1	Secured Electronic Voting Machine using Biometric	Anandaraj S, Anish R, Devakumar P V Year: 2015	Uses biometric methods so that more securable and flexible real-time applications can be gained. As this system has automatic counting, we can make the result published faster and better.	Only work when the system is connected to the internet.
2	Smart Wireless Authenticating Voting Machine	Devendra Vijay Naik Year: 2015	The fingerprint of the voter gets converted into an encrypted format code and the output signal is transmitted to AVR via wireless then the data is processed using AVR and the unique encrypted fingerprint is stored in the database.	Only a short distance can be accessed using Zigbee.
3	RFID-Based Biometric Voting Machine Linked to Aadhaar for Safe and Secure Voting	B Madan Mohan Reddy, D Srihari Year: 2015	RFID tag is used which contains the verification data which is already stored in LPC 2148. The Fingerprint scanner is used to check whether the RFID belongs to that person or not.	The system is costlier to implement.
4	Electronic voting with biometric verification Offline and Hybrid EVMS solution	Ansif Arooj, Mohsin Riaz Year: 2016	The hash code is generated using the fingerprints of both hands and the generated hash code have a 13-digit key which can be stored as a barcode.	Internal memory must be increased. It will look at the time to process the data. It can retain the data only for 2 years.
5	Modernized Voting Machine using Fingerprint Recognition	Gomathi B, Veena Priyadarshini S Year: 2013	RFID tag is used. The Fingerprint scanner is used to check whether the RFID belongs to that person or not.	The system is costlier to implement.

6	A Secured Biometric Voting System Using RFID Linked with the Aadhar Database	P M Benson Mansingh, T Joby Titus, V S Sanjana Devi Year: 2020	RFID cards can store all the details about a user. If the RFID card can be scanned by the scanner and put the thumbprint on the fingerprint scanner if it's matched the user can allow the vote or if the fingerprint does not match the user is not allowed to vote.	The system is costlier to implement.
7	Electronic Voting System using Biometrics, Raspberry Pi and TFT module	A M Jagtap Year: 2019	The voter will enter the Aadhar ID on the Touch screen module, and then the fingerprint of the voter will be scanned and matched with a database stored on the cloud. If it matches, then only further processes will start.	Database storage is limited to certain votes.
8	Secured Smart Voting System using Aadhar	Madhuri B, Adarsha M G, Pradhyumna K R, Prajwal B M Year: 2017	Biometric online voting system, which determines whether a particular person is eligible for casting vote by authenticating his/her fingerprint. Voter details are retrieved from the Aadhar Database and verified.	Only works when the system is connected to the internet and this system requires a smartphone with an inbuilt fingerprint scanner.
9	Biometric Voting Machine Based on Fingerprint Scanner and Arduino	Atharva Jamkar, Omkar Kulkarni, Aarti Salunke, Dr Anton Pljonkin Year: 2019	Fingerprint-based biometric voting machines are divided into two parts, in the first part the user needs to register and in the second part the user will vote for the desired candidate.	Users must enrol before voting. Only 99 candidates can enrol and vote because of the limitations of Arduino.
10	Wireless Voting Machine	Soma Bhattacharrya, Dibyangana Roy, Esha Pramanik, Trishita Nath, Snapan Kundu Year: 2019	A biometric scanner functions in two different stages. Initially, the fingerprints of the voters are captured and stored in the database against their respective voter identity card numbers. At the time of voting, once the voter provides his fingerprints on the scanner, the scanner only compares with stored fingerprints in the database system.	Implementing the system is more expensive.

III. METHODOLOGY

The IoT-based voting machine with fingerprint verification has a functional block diagram that includes a controller, a fingerprint module, a Wi-Fi module, a keypad, a power supply, and a cloud. This system's controller is an Arduino Uno. The laptop provides the system with power. The vote is polled using a keypad. On the serial monitor, messages pertaining to system guidelines and any errors will be visible. The voter's fingerprint database is stored in the fingerprint module, which is also where the voter's finger is placed. Each user's fingerprint is matched up by the fingerprint database in the fingerprint module, and if the fingerprint corresponds to an authenticated person, a message is displayed. The matched outcome will be displayed on the serial monitor. The database contains a copy of the voting ballot. Each candidate's final score is recorded in various cloud fields. When someone casts a ballot for the second time, a buzzer sounds as an alert. The voting unit and the fingerprint unit are separated into two groups here. The block diagram of the verification unit is displayed in Figure 3(a). Mostly, enrolling and matching are covered. It comprises of the fingerprint module, which stores the voter's fingerprint and compares it to the database to see if they match. The voter's Aadhar number is also saved here. The system additionally validates each user's saved Aadhar number. The voting system checks to see whether someone tries to vote more than once. The voting process is shown in Figure 3(b). When a message appears in the fingerprint unit, that person becomes eligible to vote and can use this unit to do so. A register will be increased following the vote. Voters have a choice in where they choose to cast their ballots.

Fig. 3 (a) Proposed Admin Architecture **(b)** Proposed Voter Architecture



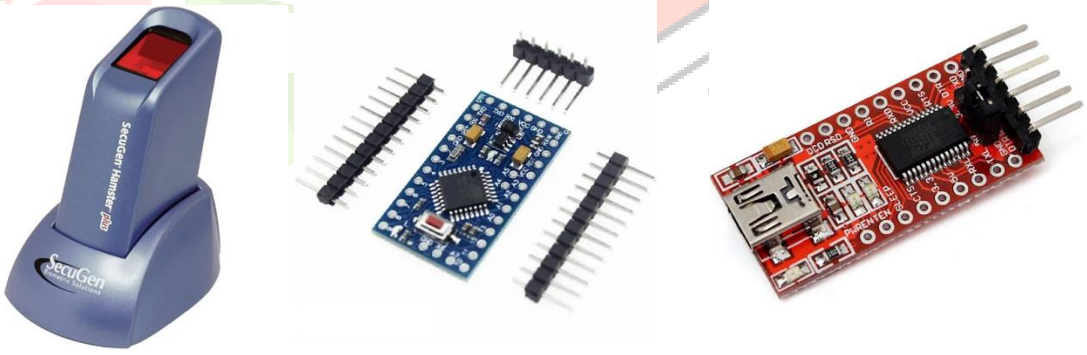
(a) (b)

IV. REQUIREMENTS

Fingerprint Sensor

Fingerprint Module consists of the optical fingerprint sensor, a high-speed DSP processor, a high-performance fingerprint alignment algorithm, high-capacity FLASH chips and other hardware and software composition, stable performance, simple structure, with fingerprint entry, image processing, fingerprint matching, search and template storage and other functions. The fingerprint module has two interfaces TTL UART and USB2.0, USB2.0 interface is often connected to the computer; the RS232 interface may be a TTL level, the default baud is 57600, can be changed, ask for a communication protocol, microcontroller, like ARM, DSP, and other serial devices with a connection, 3.3V- 5V microcontroller are often connected directly.

Fig. 4 Hardware Requirements



Arduino IDE

The Arduino Integrated Development Environment - or Arduino Software (IDE) - contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions and a series of menus. It connects to the Arduino and Genuine hardware to upload programs and communicate with them. Programs written using Arduino Software (IDE) are called sketches. These sketches are written in the text editor and are saved with the file extension .ino. The editor has features for cutting/pasting and searching/replacing text. The message area gives feedback while saving and exporting and displays errors. The console displays text output by the Arduino Software (IDE), including complete error messages and other information. The bottom right-hand corner of the window displays the configured board and serial port. The toolbar buttons allow verifying and uploading programs, creating, opening, and saving sketches, and opening the serial monitor.

V. RESULTS

The Biometric Fingerprint Voting System is a technology-based solution that aims to improve the integrity and security of the voting process. Some of the potential benefits of using such a system are:

- Accurate Identification: Biometric Fingerprint Voting System provides accurate identification of voters, eliminating any chances of impersonation and ensuring that only eligible voters can vote.
- Increased Efficiency: This system helps in making the voting process more efficient and less time-consuming, reducing the chances of errors and delays.
- Enhanced Security: The use of biometric fingerprints ensures that the voting process is secure and tamper-proof, making it difficult for anyone to manipulate or alter the results.
- Reduced Fraud: The system can help to reduce the incidence of fraudulent voting, which is a major concern in many countries.
- Improved Transparency: The use of this system promotes transparency in the voting process by providing a clear record of who voted and when they voted, which can be used to audit the election results.

VI. CONCLUSION

In conclusion, this study has shown that voting by biometric fingerprint offers several advantages over voting by traditional paper ballot. The voting process is made more efficient and secure using biometric authentication, particularly fingerprint recognition. The various parts of biometric fingerprint voting systems, including the hardware, software, and algorithms for fingerprint matching, have all been examined in this work. The research has also looked at the difficulties in deploying these systems, such as cost-effectiveness, scalability, and privacy issues. The introduction of biometric fingerprint voting systems still faces difficulties despite the potential benefits. The collection and storage of personal data, such as fingerprints, must be done securely, therefore privacy concerns must be considered carefully and addressed. Particularly about large-scale elections, scalability and cost-effectiveness must also be considered.

Since biometric fingerprint voting systems are still a relatively new topic, more research and development are required to address any outstanding issues and raise the general level of these systems' quality. Future work will concentrate on increasing the precision of algorithms for matching fingerprints. Although modern algorithms are largely reliable, mistakes and false positives can still happen. To increase the algorithms' precision and lower the likelihood of mistakes during the matching process, more research is required. Future research will also address privacy issues raised by biometric voting systems using fingerprints. Personal data collection and storage, such as the storage of fingerprints, poses serious privacy concerns that must be addressed with the right security measures. Future studies should concentrate on creating innovative methods for protecting personal information and making sure it is gathered and maintained safely. In conclusion, future studies around biometric fingerprint voting systems ought to concentrate on enhancing the precision of fingerprint-matching algorithms, addressing privacy issues, creating more scalable and affordable systems, and resolving technical issues related to the implementation of these systems.

VII. ACKNOWLEDGMENT

We are thankful to Dr. Basavaraj L, Principal, ATME College of Engineering, Mysuru for having supported us in our academic endeavors by granting us permission and extended full use of the college facilities to carry out this project successfully. We are extremely thankful to Dr. Puttegowda D, Head of the Department, Department of Computer Science and Engineering, for his valuable support and his timely inquiries into the progress of the work.

We are greatly indebted to my Project coordinator Lakshmi Durga, Associate Professor, Department of Computer Science and Engineering, for her timely inquiries into the progress of the project work. We express our earnest gratitude towards our guide Mrs. Lavanya N, Assistant Professor, Department of Computer Science and Engineering, for her consistent cooperation and support in getting things done.

We are obliged to all teaching and non-teaching staff members of Department of Computer Science and Engineering for the valuable information provided by them in their respective fields. Lastly, we thank almighty, our parents and friends for their constant encouragement and courage, for helping us in completing the project report successfully.

REFERENCES

[1] Anandaraj, S., 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), pp. 1-5. IEEE, 2015.

[2] Naik, Devendra Vijay. "Smart wireless authenticating voting machine." In 2015 International Conference on Communications and Signal Processing (ICCSP), pp. 0785-0788. IEEE, 2015.

[3] Reddy, B. Madan Mohan, and D. Srihari. "RFID based biometric voting machine linked to aadhaar for safe and secure voting." International Journal of Science, Engineering and Technology Research (IJSETR) 4, no. 4 (2015): 995-1001.

[4] Arooj, Ansif, and Mohsin Riaz. "Electronic voting with biometric verification offline and hybrid evms solution." In 2016 Sixth International Conference on Innovative Computing Technology (INTECH), pp. 332-337. IEEE, 2016.

[5] Gomathi, B., and S. Veena Priyadharshini. "Modernized voting machine using fingerprint recognition." International Journal of Scientific & Engineering Research 4, no. 5 (2013): 156-161.

[6] Mansingh, PM Benson, T. Joby Titus, and VS Sanjana Devi. "A secured biometric voting system using RFID linked with the Aadhar database." In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1116-1119. IEEE, 2020.

[7] Jagtap, A. M., Vishakha Kesarkar, and Anagha Supekar. "Electronic voting system using biometrics, raspberry pi and TFT module." In 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), pp. 977-982. IEEE, 2019.

[8] Madhuri, B., M. G. Adarsha, K. R. Pradhyumna, and B. M. Prajwal. "Secured smart voting system using aadhar." In 2017 2nd international conference on emerging computation and information technologies (ICECIT), pp. 1-3. IEEE, 2017.

[9] Chicco, Davide, Christopher A. Lovejoy, and Luca Oneto. "A machine learning analysis of health records of patients with chronic kidney disease at risk of cardiovascular disease." IEEE Access 9 (2021): 165132-165144.

[10] Bhattacharrya, Soma, Dibyangana Roy, Esha Pramanik, Trishita Nath, and Snapan Kundu. "Wireless voting machine." In 2019 International Conference on Opto-Electronics and Applied Optics (Optronix), pp. 1-3. IEEE, 2019.