Fingerprint-Based Voting System

Conference Paper · September 2023

CITATION
1

READS
3,968

2 authors, including:

Gangadurai Elumalai
Velammal Engineering College
14 PUBLICATIONS **2** CITATIONS

SEE PROFILE

Journal of Telecommunication Study

Volume-8, Issue-2 (May-August, 2023)

www.matjournals.com

Fingerprint-Based Voting System

Gangadurai E [1*], Divakaran R [2], Aruneshwaran U [3]
[1]Assistant Professor, [2,3]Under Graduate Student, Department of Electronics and Communication Engineering, Velammal Engineering College, Chennai, Tamil Nadu, India

[*]Corresponding Author: gangadurai@velammal.edu.in

Received Date: September 16, 2023 *Published Date: September 27, 2023*

ABSTRACT

In the contemporary era, electronic voting machines (EVMs) have emerged as indispensable tools in elections, vital for ensuring the authenticity of the electoral process and curbing the risk of multiple voting instances. This paper introduces a ground-breaking approach to tackle the issue of electoral fraud by harnessing the distinctive fingerprint data contained within an individual's Aadhar card—a widely accepted biometric identity document in various nations. Our novel concept revolves around fingerprint-based voting machines, designed to offer a secure and streamlined voting experience that eliminates the necessity for voters to carry conventional identification documents. This system operates seamlessly by linking every voter's identity to their Aadhar card, facilitating the effortless retrieval of biometric data. The voting process commences when a voter places their finger on a dedicated fingerprint reader, which reads and cross-references the data against the UIDAI's (Unique Identification Authority of India) cloud-based database. In cases where the provided fingerprint aligns with the registered data, the voter is granted access to cast their vote. Conversely, if a discrepancy is detected, an immediate warning message is displayed on an LCD screen, and the voter is precluded from participating in the electoral proceedings. Beyond the commendable boost in security for the voting process, this innovative system promises several advantages, including accelerated result processing when compared to conventional methods. Nevertheless, it is imperative to address a host of crucial considerations encompassing data privacy, cybersecurity, inclusivity, system reliability, and navigating the legal and ethical intricacies before contemplating the large-scale implementation of such a transformative system. This abstract offers a glimpse into the potential benefits and challenges of leveraging Aadhar card fingerprint data to enhance the security and efficiency of the voting process, underscoring the necessity of a thorough and prudent approach to electoral innovation.

Keywords- Aadhar card, Data privacy, Electoral innovation, Electronic voting machines, Fingerprint-based voting, Security, Unique Identification Authority of India (UIDAI)

INTRODUCTION

The Aadhar-based voting system represents a ground-breaking approach revolutionising the electoral process in India, offering numerous advantages. By integrating the unique Aadhar identification number into the voting system, several key benefits can be realized. Firstly, the system significantly enhances the security and integrity of the electoral process [1, 2]. Aadhar's biometric authentication, linking individuals' fingerprints or iris scans to their unique identification numbers, ensures that only eligible voters can cast their ballots. This robust verification process effectively eliminates instances of voter fraud and impersonation, safeguarding the integrity of elections. Secondly, the Aadhar-based system streamlines the voter registration process, making it more efficient and accurate. Citizens with Aadhar cards are automatically eligible to vote, eliminating the need for separate and often cumbersome registration procedures [3-5]. This simplification not only reduces administrative burdens but also increases the accessibility of voting, encouraging more eligible citizens to participate in the democratic process. Moreover, the system addresses the issue of duplicate voting effectively.

By cross-verifying unique identification numbers, the system ensures that each voter can cast only one vote, eliminating the possibility of multiple votes from the same individual, and reinforcing fairness and transparency in elections [6]. Furthermore, the Aadhar-based system can lead to increased voter turnout. The simplified registration process and the introduction of a more secure and accessible system remove barriers that may discourage citizens from participating in elections [7]. By making voting more convenient and inclusive, the system promotes a more representative democracy where the voices of all eligible citizens can be heard. Additionally, the automation of vote collection and tabulation in the Aadhar-based system improves efficiency. Manual counting and tabulation processes are time-consuming and prone to errors. By automating these tasks, the system reduces the time required to declare results, allowing for quicker dissemination of election outcomes [8-10]. This efficiency contributes to public trust and confidence in the electoral process.

EXISTING SYSTEM

Figure 1: *EVM machine.*

The Electronic Voting Machines (EVMs) used in India were developed in collaboration with government-owned companies (Fig.1), the Electronics Corporation of India (ECIL) and Bharat Electronics Limited (BEL) [6]. These machines have evolved, with the first-generation EVMs introduced in the early 1980s [6]. These first-generation machines used microcontrollers and external storage for firmware and vote data [6]. Subsequent generations incorporated improvements, eventually leading to the third-generation design [6, 8]. As of July 2009, there were approximately 1,378,352 EVMs in use in India [6]. Among them, 448,000 were third-generation machines manufactured from 2006 to 2009, with 253,400 from BEL and 194,600 from ECIL [6]. The remaining 930,352 were second-generation models produced from 2000 to 2005, with 440,146 from BEL and 490,206 from ECIL [6]. The first-generation machines, whose service life had expired, were not used in national elections [6]. The existing EVMs have their limitations and vulnerabilities, which have led to concerns about their security [5, 9, 11]. Research has been conducted to analyze these vulnerabilities and suggest improvements [5]. The Aadhar-based voting system presents a transformative solution to the challenges faced by traditional voting methods [1]. Through enhanced security, streamlined registration, prevention of duplicate voting, increased voter turnout, and efficient result tabulation, the system promotes a fair, transparent, and inclusive democratic process in India [1]. By leveraging Aadhar's capabilities, this innovative approach strengthens the electoral system, ensuring that elections accurately reflect the will of the people [1, 4, 10].

LITERATURE SURVEY:

The field of Aadhar-based voting systems has seen significant research and technological advancements. Notable studies and works in this domain include which explores the integration of Aadhar-based voting with blockchain technology for enhanced security and transparency [1, 2]. Focusing on the design of a blockchain-based electronic voting system to ensure the integrity and immutability of voting records [3]. The researchers investigate the implementation of end-to-end verifiability in voting systems, addressing theoretical and practical aspects [4]. Presenting a secure electronic voting machine that incorporates biometric authentication to enhance voter identification and prevent fraud [5] which analyses the security vulnerabilities of India's electronic voting machines, highlighting potential weaknesses and suggesting improvements [6]. Providing an expert committee's evaluation of the upgraded electronic voting machine, along with recommendations for enhancements [7]. This article discusses the financial aspects of India's elections, highlighting the significant costs involved in conducting elections.

PROPOSED SYSTEM

The proposed Aadhar-based voting system's working process can be summarized as follows:

Verification: The voter approaches the Aadhar-based voting machine and provides their Aadhar card or Aadhar number.

Aadhar Authentication: The machine authenticates the provided Aadhar details by verifying biometric information, such as fingerprints or iris scans, ensuring the person is a legitimate voter and preventing impersonation.

Voter Registration: Upon successful Aadhar authentication, the machine registers the voter as eligible to cast their vote.

Candidate Selection: The machine displays the list of candidates and their respective symbols on the screen. The voter selects their preferred candidate by pressing the corresponding button or symbol on the machine.

Vote Casting: After candidate selection, the machine records the voter's choice securely and ensures it is associated with the correct candidate.

Confirmation: The machine displays a confirmation message to the voter, indicating that their vote has been successfully cast.

Vote Counting: At the end of the voting process, the Aadhar-based voting machine securely stores the cast votes, which can be retrieved later for counting and result declaration.

It's important to note that the specific technical implementation of an Aadhar-based voting machine may vary, but the general working process outlined above provides a simplified overview of how such a system functions (Fig. 2).

BLOCK DIAGRAM OF THE PROPOSED SYSTEM

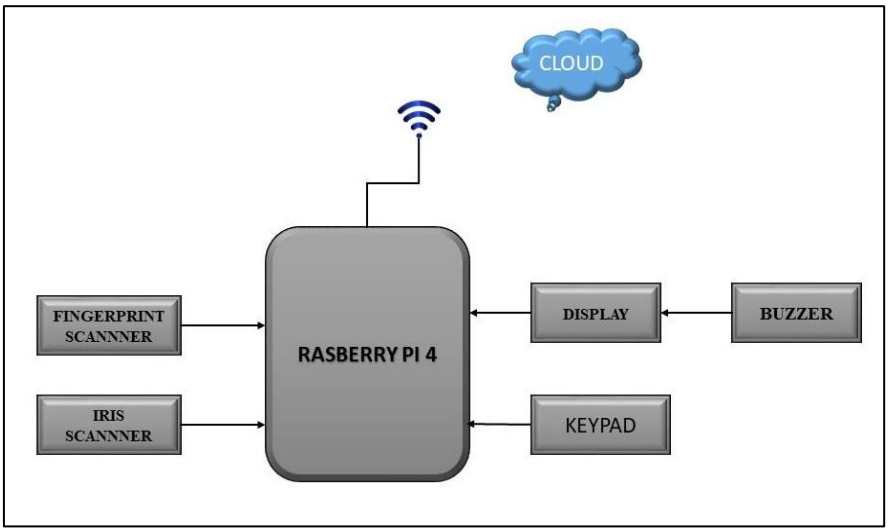
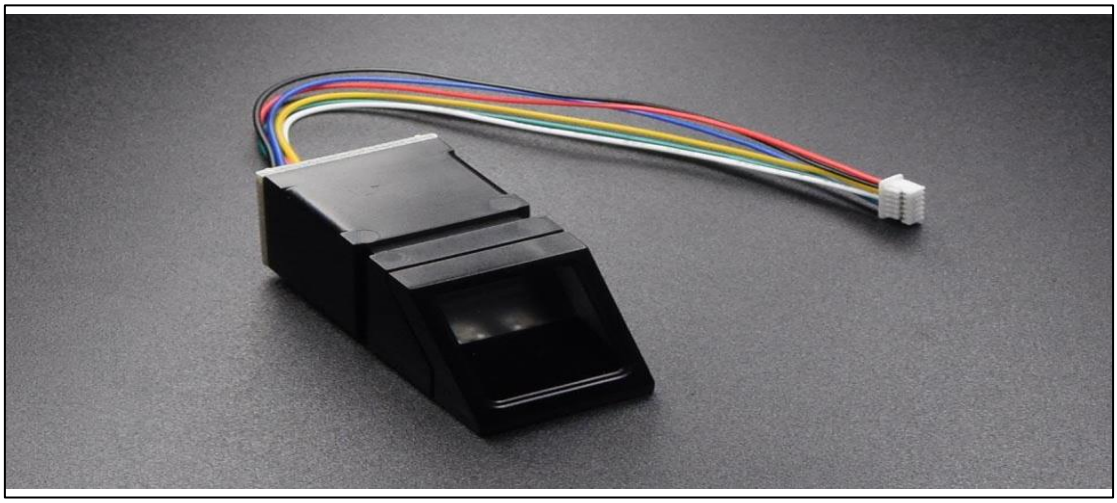


Figure 2: *Block diagram of the proposed system.*

HARDWARE COMPONENTS:

Fingerprint Module

Dactyloscopy is another term for identifying fingerprints. Comparison of two friction ridge skin impressions made by human fingers, palms, or toes is the process of fingerprint identification. Here, a biometrics system is utilised [11]. The goal of biometric identification for this study is to read user fingerprints so that each image can be defined and saved in the system's internal memory in an individually unique manner. The numerical values that are assigned to these distinctive fingerprint images are distinctive and simple to retrieve (Fig. 3).



(Source: Optical-Light-Imaging-Photon: Fingerprint Sensor R307 for ... (circuit.rocks))

Figure 3: *Finger scanner.*

Iris Scanner

An iris scanner can be used as an alternative or complementary method to fingerprint-based systems. It verifies voters' identities using unique patterns in their irises (Fig. 4).

(Source: BMT-20 Dual Iris Scanner (radiumbox.com))

Figure 4: *Iris scanner.*

Extraction Algorithm

A specialized algorithm processes fingerprint images to enhance their accuracy and extract minutiae data for identification (Fig. 5).

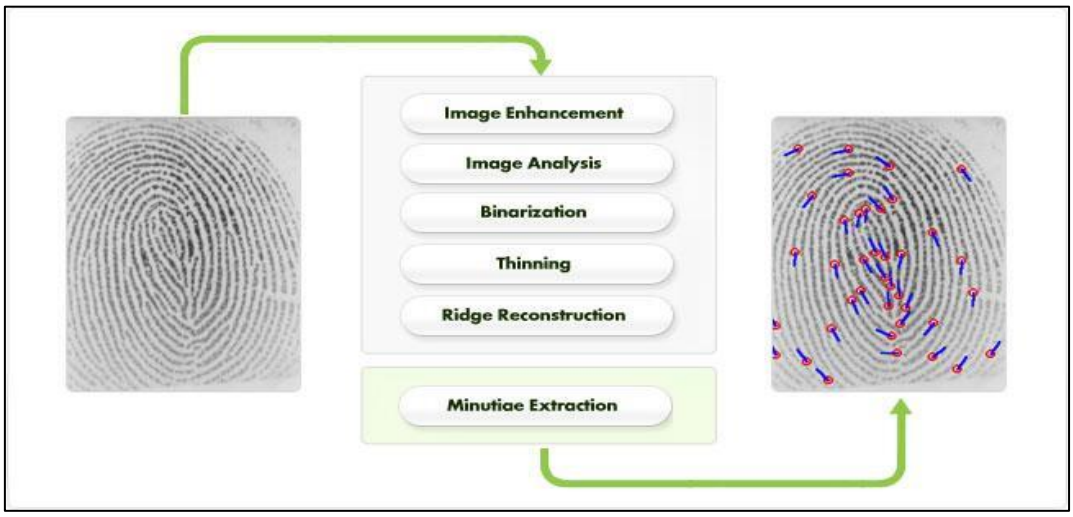


Figure 5: *Minutiae extraction.*

When given a fingerprint image, the extraction method enhances the image, analyses the fingerprint's features, and then executes binarization utilising the analysed data. It thins the work while taking temporal performance into account, extracts characteristics following post-processing, and saves as a template made up of characteristic points [12, 13].

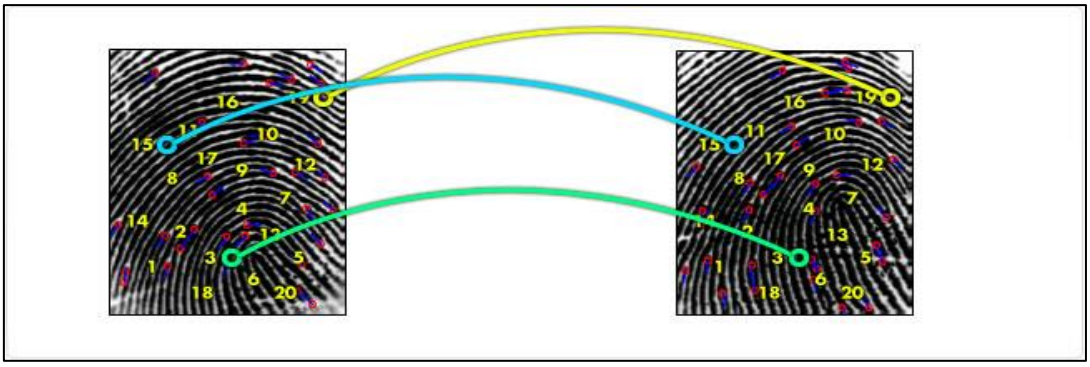
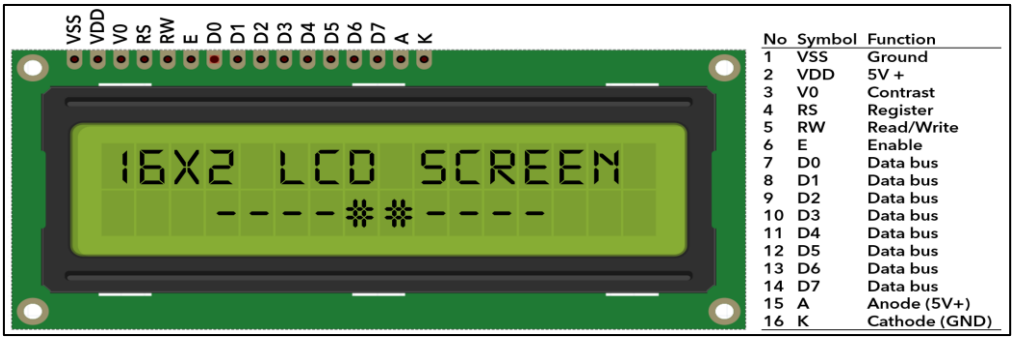


Figure 6: *Matching algorithm.*

By comparing two templates obtained by the characteristic point extraction technique—more particularly, by comparing the positions of each characteristic point and the structure—the matching algorithm determines whether there is a match (Fig. 6).

LCD

A liquid crystal display (LCD) provides an interface for users to interact with the voting machine, displaying instructions, messages, and vote confirmation (Fig. 7).

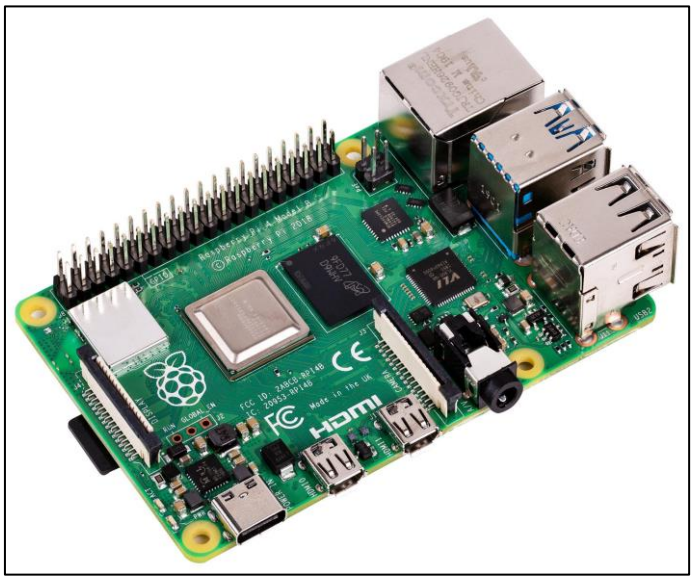


(Source: Interface LCD 16x2 with Raspberry Pi 4 - The Engineering Projects)

Figure 7: *LCD.*

Raspberry Pi Module

The Raspberry Pi serves as the central processing unit, enabling Aadhar authentication, user interface, vote recording, data transmission, result compilation, and system management (Fig. 8).



(RASPBERRY PI B+ | Raspberry Pi 1 - Model B+ 512MB RAM | Distrelec International)

Figure 8: *Microcontroller.*

FLOWCHART

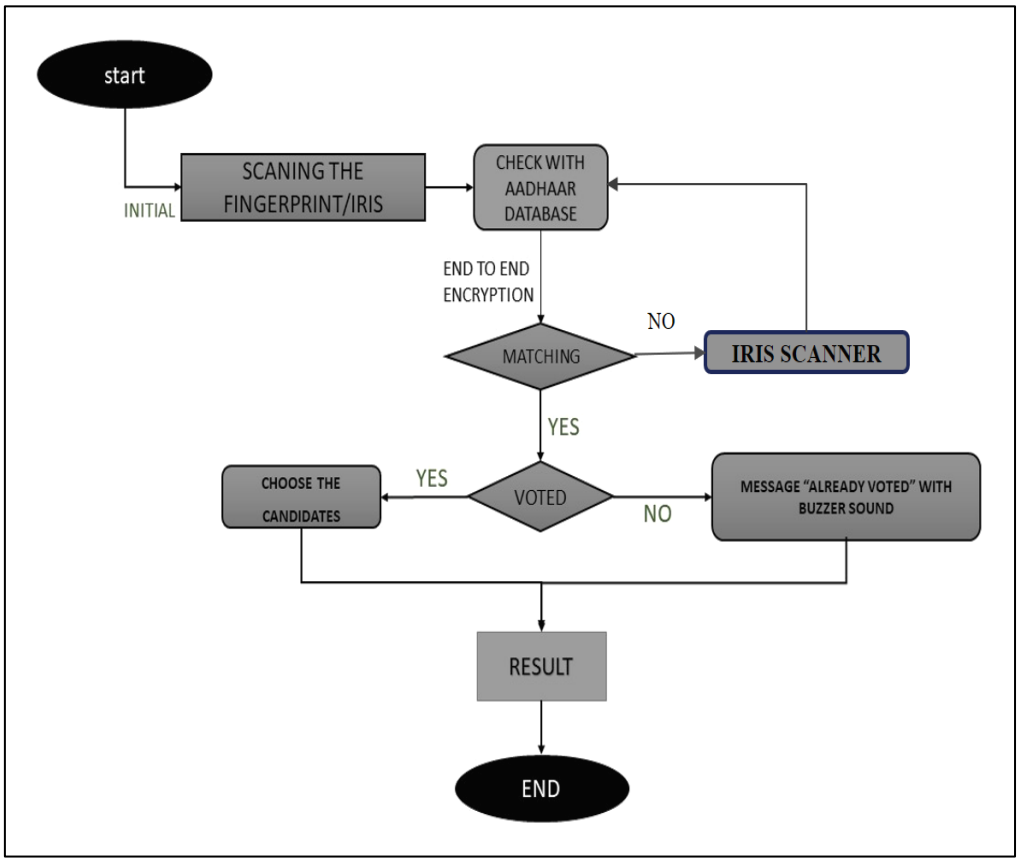


Figure 9: *Flowchart of the algorithm.*

SOFTWARE COMPONENTS

Raspberry Pi OS

The official operating system optimized for Raspberry Pi, based on Debian, provides the foundation for the voting system's software.

Fingerprint Module Software

The software package includes an SDK with libraries, APIs, and documentation for integrating the fingerprint module. It also offers drivers for host system communication, configuration tools, demo applications, and comprehensive documentation for developers (Fig. 9).

RESULT AND DISCUSSION

The proposed Fingerprint-based voting system represents a significant improvement over previous systems. This new system enhances security, expedites the voting process, increases transparency, and upholds the integrity of the voting process. It effectively prevents illegal voting, ensures ease of use, and provides real-time feedback to voters. Moreover, it prevents multiple votes by the same person and rigorously verifies voters' eligibility. These advancements contribute to a safer and more efficient voting method, essential for the growth of a developing nation (Fig. 10 and 11).

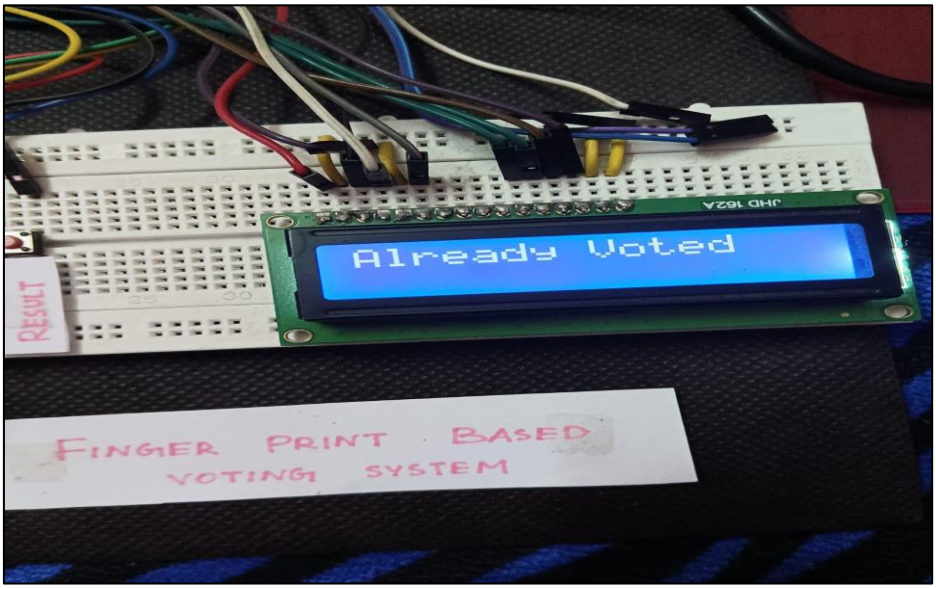


Figure 10: *False vote alert.*

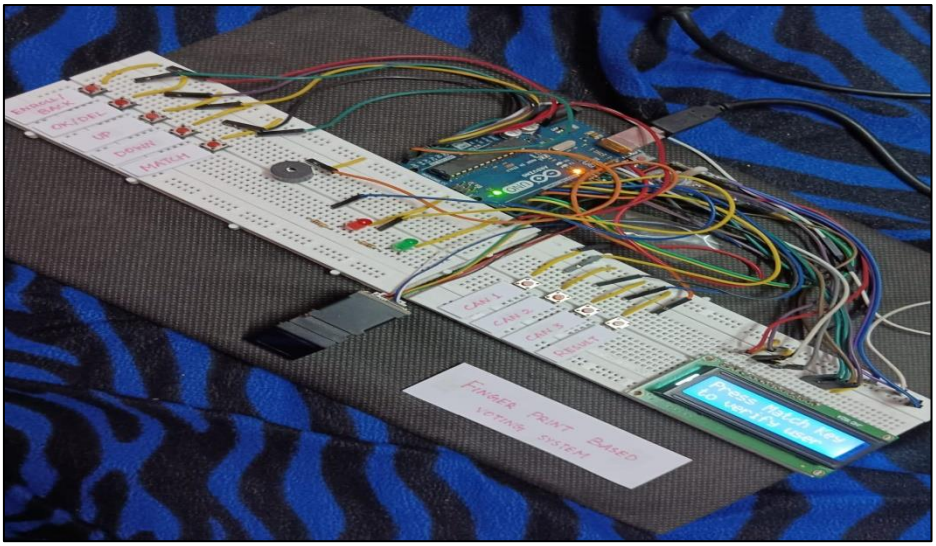


Figure 11: *Prototype of the project.*

CONCLUSION AND FUTURE WORK

The Aadhar-based voting system presents a comprehensive and transformative solution to the contemporary challenges faced by democracies worldwide in modernizing and reinforcing the electoral process. It adeptly addresses the imperative of securing elections while concurrently fostering inclusivity and efficiency. A pivotal element of this system is its adept utilization of Aadhar's distinctive identification capabilities, leveraging biometric authentication to provide an unprecedented level of security. This multifaceted approach not only serves as a deterrent to fraudulent voting but also elevates public confidence in the electoral mechanism. By eradicating the potential for duplicate voting, this system fundamentally enhances transparency and overall integrity. Moreover, the Aadhar-based voting system simplifies the process of voter registration, thereby enhancing accessibility and convenience for citizens. This streamlined approach, combined with the robust security measures in place, holds the promise of elevating voter turnout rates, ensuring a more comprehensive representation of the populace in the democratic process. Furthermore, the system's automation of vote collection and tabulation not only reduces the likelihood of errors but also expedites the release of election results. Timely result announcements contribute significantly to reinforcing public trust in the electoral process and mitigate the potential for disputes or controversies. In essence, the Aadhar-based voting system represents a monumental stride toward fortifying democracy. By championing principles of fairness, transparency, and accessibility in the electoral process, it accurately mirrors the collective will of the citizenry, thereby reaffirming the foundations of democratic governance. As nations adapt to the evolving digital landscape, embracing innovative solutions such as this emerges as a pivotal strategy in securing the future of democratic principles and practices on a global scale.

FUTURE WORK

The Fingerprint-based voting system opens the door for various enhancements and future developments. Some potential areas for future work include:

- Enabling remote voting within electoral boundaries, further increasing accessibility.
- Enhancing security measures to protect voter data and system integrity.
- Exploring the integration of advanced biometric authentication methods for even greater accuracy.
- Implementing blockchain technology to ensure the immutability of voting records.
- Conducting extensive field trials and refining the system based on real-world usage.
- Addressing scalability and infrastructure challenges to accommodate a large number of voters.
- By continuously improving and expanding the Fingerprint-based voting system, we can contribute to the advancement of secure and efficient democratic processes.

REFERENCES

1. T.M. Roopak and R Sumathi (2020). Electronic voting based on virtual ID of aadhar using blockchain technology. *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*. IEEE, Available at: https://doi.org/10.1109/ICIMIA48430.2020.9074942
2. R Hanifatunnisa and B Rahardjo (2017). Blockchain based e-voting recording system design. *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*. IEEE, Available at: https://doi.org/10.1109/TSSA.2017.8272896
3. P Y.A. Ryan, S Schneider and V Teague (2015). End-to-end verifiability in voting systems, from theory to practice, *IEEE Security & Privacy*, 13(3), 59-62, Available at: https://doi.org/10.1109/MSP.2015.54
4. S Anandaraj, R Anish and P V Devakumar (2015). Secured electronic voting machine using biometric. *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*. IEEE, Available at: https://doi.org/10.1109/ICIIECS.2015.7192976
5. S Wolchok, E Wustrow, J. Alex Halderman, et al (2010). Security analysis of India's electronic voting machines.

Proceedings of the 17th ACM conference on Computer and Communications Security, (pp. 1-14). ACM, Available at: https://doi.org/10.1145/1866307.1866309

6. Scribd, "Expert Committee Report On EVM", [Online] Available at: https://www.scribd.com/document/6794194/Expert-Committee-Report-on-EVM
7. Bloomberg (2019), "Why India's election is among the world's most expensive", [Online] Available at: https://economictimes.indiatimes.com/news/elections/lok-sabha/india/why-indias-election-is-among-the-worlds-most-expensive/articleshow/68367262.cms [Accessed on March 2019].
8. S. Abimanyu, R. Anbarasan and S. Dhinakaran (2021). Iris detection based authentication for secure voting system, *International Journal of Engineering Research & Technology*, 9(5), 404-406, Available at: https://www.ijert.org/research/iris-detection-based-authentication-for-secure-voting-system.IJERTCONV9IS05085.pdf
9. Md Khasawneh, Md Malkawi, O Al-Jarrah, et al (2008). A biometric-secure e-voting system for election processes. *2008 5th International Symposium on Mechatronics and Its Applications*. IEEE, Available at: https://doi.org/10.1109/ISMA.2008.4648818
10. V Kumar Yadav, S Batham, M Jain and S Sharma (2014). An approach to electronic voting system using UIDAI. *2014 International Conference on Electronics and Communication Systems (ICECS)*. IEEE, Available at: https://doi.org/10.1109/ECS.2014.6892510
11. D L Chaum (1981). Untraceable electronic mail, return addresses, and digital pseudonyms, *Communications of the ACM*, 24(2), 84-90, Available at: https://doi.org/10.1145/358549.358563
12. Q Zhao, L Zhang, D Zhang, et al (2008). Adaptive pore model for fingerprint pore extraction. *2008 19th International Conference on Pattern Recognition*. IEEE, Available at: https://doi.org/10.1109/ICPR.2008.4761458
13. M R. Girgis, T M. Mahmoud and T Abd-El-Hafeez (2007). An approach to image extraction and accurate skin detection from web pages, *World Academy of Science, Engineering and Technology*, 367-375, Available at: https://www.researchgate.net/publication/238782112_An_Approach_to_Image_Extraction_and_Accurate_Skin_Detection_from_Web_Pages

CITE THIS ARTICLE

Gangadurai E, et al. (2023). Fingerprint-Based Voting System, *Journal of Telecommunication Study*, 8(2), 30-38.