IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.67

Volume 5, Issue 3, March 2025

Secure IoT-Based Electronic Voting Machine

Mr. Shreejit D. Umale, Mr. Mandar .P. Mandavgane,
Mr. Vedant M. Thakare, Mr. Prajwal D. Bhagat. Prof. N. T. Gadre
Department of ENTC
Sipna College of Engineering & Technology, Amravati, Maharashtra, India.

Abstract*: This paper aims to design and develop a biometric-enabled electronic voting machine. The proposed biometric electoral voting system allows the user to scan so that his or her credentials can be compared to existing fingerprint images which are already stored in the system's database. Counting is going on right away, making the voting process more efficient, faster, and safer. This system requires the identification of the voter's Aadhaar card and the voter's thumb impression. Voter's complete data, including all voter's fingerprint images, is collected and stored in the database. While voting, the voter gives their Aadhaar card details and puts their finger on the fingerprint scanner, the system looks for the seal already provided in the database and then compares it to authenticate the voter's identity. If the data matches, the system commands the voter to vote through the electronic voting machine. If the fingerprints do not match, the voter is not allowed to vote. If any voter tries to vote again then an alert message gets sent to the respective authorities and considered vote rigging*

Keywords: Enhanced EVM security, fingerprint authentication, fraud alert

I. INTRODUCTION

Election is the act of a party casting votes to elect an individual for some type of position. Election may involve a public or private vote depending on the position. Most positions in the local, state, and federal governments are voted on in some type of election. 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 the election period ends, all these boxes are opened and votes are counted manually in the presence of the certified officials. In this process, there can be errors in the 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 election in favor of certain candidates. To avoid these shortcomings, the government of India came up with a direct-recording electronic (DRE) voting system which is usually an Electronic voting machine (EVM). These devices have been praised for their simple design, ease of use, and reliability. However, it has been found that EVMs are not tamper-proof and are easily hacked. Moreover, these attacks, hardware, and software, go without any detection but are quite simple to implement. This made us bring forth a system that is secure, transparent, reliable as well as easy to use for the citizens. Biometric e-voting systems are not a phenomenon anymore they are being actively used in countries like Ghana and Ireland and are spreading in many other developing nations. In this project, we propose an idea to avoid fraudulence in the mechanism to make e-voting in India a reality. It improves security performance and avoids forgery votes because naturally, one human fingerprint is different from another human's.

Many methods have been developed to avoid fraud in voting systems, but we are not able to eradicate it. The objective of this project is to improve the security performance of the voting machine and provide easy access to cast votes by using fingerprint authentication. We use Arduino IDE software and an R307S fingerprint scanner to scan the fingerprint of every individual. The scanned fingerprint is authenticated. If it matches, the individual is allowed to cast the vote.

II. LITERATURE REVIEW

Electronic voting systems that incorporate biometric authentication and Internet of Things technology greatly improve security, effectiveness, and transparency. Studies show that by comparing voter identities to a pre-registered database, fingerprint-based biometric verification effectively prevents voter fraud and multiple voting attempts. In addition to increasing accuracy, this method expedites the voting process.

DOI: 10.48175/IJARSCT-23929

IoT integration makes it easier to transmit data in real time, monitor remotely, and distribute results effectively. Some systems even safeguard data transfer by using cryptographic methods, such as the Diffie-Hellman approach. To improve security and transparency, blockchain technology is also being investigated to offer a decentralized, unchangeable ledger for voting.

Despite these developments, issues with scalability, voter privacy, and the requirement for strong authentication procedures still exist. Researchers recommend ways to improve scalability, such as adding sharding techniques and refining consensus algorithms. In summary, although biometric and Internet of Things-enabled electronic voting systems exhibit considerable potential, further research is required to resolve the outstanding issues and secure broad acceptance.

III. HARDWARE COMPONENTS:

Arduino UNO

The Arduino Uno is a popular microcontroller board based on the ATmega328P, commonly used for prototyping and educational projects. It features 14 digital input/output pins (6 of which can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. The board is easy to program using the Arduino IDE, which utilizes a simplified version of C/C++.

Fig. 1. Arduino UNO

Fingerprint Sensor

A fingerprint sensor is a biometric device that scans and identifies an individual's unique fingerprint pattern to authenticate their identity. These sensors use advanced imaging techniques to capture the ridges and valleys of a fingerprint, converting them into a digital template. There are different types of fingerprint sensors, including optical, capacitive, ultrasonic, and thermal sensors. Optical sensors use light to capture an image, while capacitive sensors detect electrical charge differences to map the fingerprint. Ultrasonic sensors use sound waves to create a detailed 3D image, and thermal sensors capture heat patterns.

Fig. 2. Fingerprint sensor

GSM Module:-

The GSM (Global System for Mobile Communications) module is a crucial component in modern wireless communication systems, primarily used for mobile communication and data transfer. It operates on the GSM network, allowing devices to send and receive SMS (Short Message Service), make voice calls, and access the internet. The module typically connects to microcontrollers and other electronic devices, enabling them to communicate over the cellular network.

DOI: 10.48175/IJARSCT-23929

Fig. 3. GSM module

SD Card Module

An SD card module is a hardware component designed to enable microcontrollers, development boards (such as Arduino or Raspberry Pi), or other electronic systems to read from and write to Secure Digital (SD) memory cards. It acts as an interface between the SD card and the microcontroller, making it easier to store and retrieve data. These modules are equipped with a voltage level shifter that converts the 3.3V signals used by SD cards to the logic level required by the microcontroller, which is often 5V in the case of Arduino boards. Most SD card modules communicate using the Serial Peripheral Interface (SPI) protocol, which is widely supported by microcontrollers.

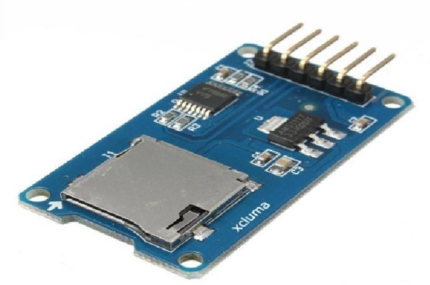

Fig. 4. SD card module

IV. METHODOLOGY

The proposed work seeks to develop a sophisticated electronic voting machine (EVM) that integrates biometric fingerprint verification and GSM-based real-time fraud detection to significantly improve the security, transparency, and reliability of the voting process. In contrast to traditional voting systems, which are prone to manipulation, impersonation, and double voting, this system ensures that only eligible and authenticated voters can cast their ballots. The integration of a fingerprint sensor serves as the first layer of security, where each voter’s identity is verified against a pre-registered database. This biometric verification eliminates the risk of voter impersonation, ensuring that no unregistered or unauthorized individual can participate in the voting process.

Once the voter is successfully authenticated, they are presented with a simple and user-friendly voting interface where they can select their preferred candidate using a panel of buttons. To further increase transparency and trust, the chosen vote is immediately displayed on an LCD screen, allowing the voter to confirm their selection before the vote is finalized. This visual confirmation ensures voter satisfaction and prevents any confusion regarding the vote cast. The system’s transparency in displaying the selected vote adds a crucial layer of accountability, reinforcing the integrity of the election process.

A particularly innovative aspect of the proposed system is the incorporation of a GSM module, which adds a layer of security. If a voter attempts to cast a vote more than once, the system will automatically detect this fraudulent activity and immediately send a real-time alert to the relevant electoral authorities via the GSM network. This alert will include key information such as the voter’s identity and the time of the second attempt, allowing authorities to intervene quickly and prevent any fraudulent activity from affecting the election results. The real-time communication feature ensures that any anomalies are addressed promptly, safeguarding the election's integrity.

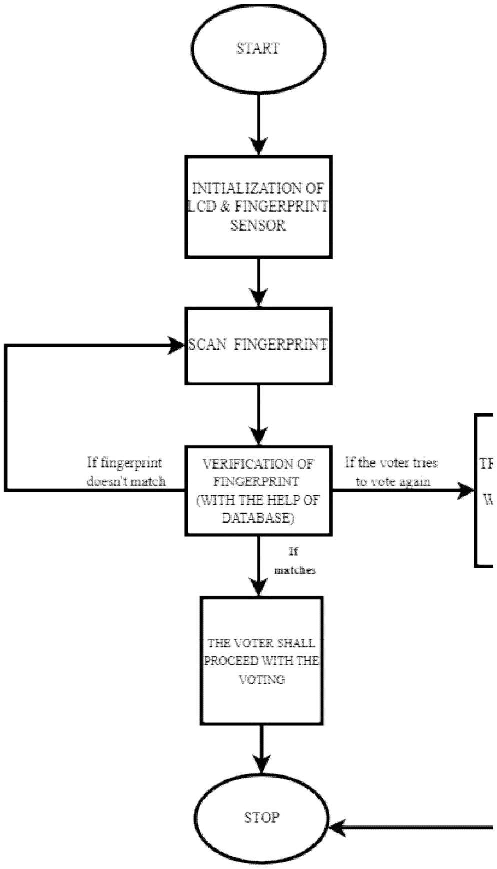
START
INITIALIZATION OF LCD & FINGERPRINT SENSOR
SCAN FINGERPRINT
If fingerprint doesn't match
VERIFICATION OF FINGERPRINT (WITH THE HELP OF DATABASE)
If the voter tries to vote again
TH
W
If matches
THE VOTER SHALL PROCEED WITH THE VOTING
STOP

Fig. 5. Flow Chart of work process.

Moreover, the system is designed to operate autonomously once initialized. This reduces the need for human intervention during the voting process, minimizing the chances of tampering or human error. The EVM is also equipped with tamper-resistant hardware and a backup power supply, ensuring uninterrupted operation and protection from physical manipulation. By combining biometric verification, transparent voting, and real-time fraud detection, the proposed EVM offers a secure, efficient, and trustworthy solution for conducting elections, ultimately enhancing voter confidence and upholding the principles of a fair and democratic process.

V. RESULT

The project's comprehensive setup featuring a fingerprint sensor, GSM module, and LCD screen, all seamlessly integrated with the Arduino UNO microcontroller is shown in Fig. 6. This configuration is designed to ensure secure and efficient voter authentication. Specifically, the image (shown in Fig. 6) portrays a scenario where a voter's biometric authentication, captured by the fingerprint sensor, is considered valid and successfully matches the data stored within the system's database. Upon this successful match, the system strictly crosschecks the database against the voter's fingerprint input, and only upon complete verification will the voter be granted authorization to proceed with the voting process.

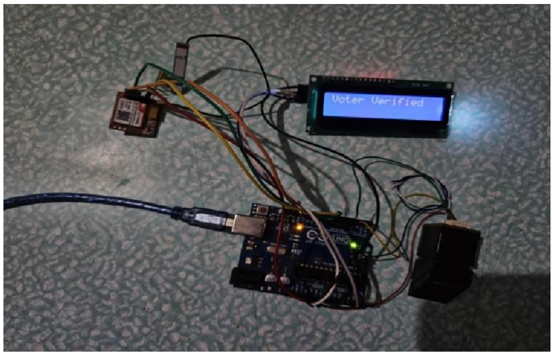

Fig. 6. Overall hardware setup and successful authentication

The image shown in Fig. 7. illustrates a contrasting scenario where a voter's authentication attempt is unsuccessful. Specifically, this portrays a situation where the system, upon processing the voter's fingerprint, discovers either that the individual has already cast their vote or that the provided fingerprint does not correspond to any record within the established database. Consequently, the system rejects the voter's attempt to participate in the election, denying them the ability to submit a vote. Furthermore, in response to this failed authentication, the system automatically generates and transmits an "alert message" to the designated authority, notifying them of the contradiction.

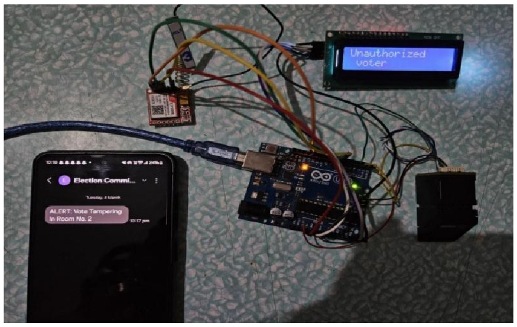

Fig. 7. Fraud alert for unauthorized vote.

VI. CONCLUSION

The proposed Secure IoT-based Electronic Voting Machine (EVM) enhances the traditional voting process by integrating biometric fingerprint verification and GSM-based real-time fraud detection. This system significantly improves the security, transparency, and efficiency of elections, ensuring that only authenticated voters can participate. By eliminating impersonation risks, preventing multiple voting attempts, and offering real-time alerts for fraudulent activities, the system upholds the integrity of the electoral process. Its user-friendly interface and autonomous operation enhance voter confidence and support a fair, democratic voting environment.

REFERENCES

[1] S. S. Das, S. K. Mishra, and S. Dehuri, "Biometric Based Secured Remote Electronic Voting System," 2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9202212/.

[2] T. Haripriya, V. B. G., M. Babu, G. Aswini, and M. S. Rekha, "Biometric System Based Electronic Voting Machine," ResearchGate, May 2024. [Online]. Available: https://www.researchgate.net/publication/381137551_Biometric_System_Based_Electronic_Voting_Machine.

[3] S. Kumar A.J. and H. P., "Biometric-Enhanced Voting Machine: Ensuring Identity Verification and Election Integrity," International Journal of Computer Applications, vol. 186, no. 35, Aug. 2024. [Online]. Available: https://ijcaonline.org/archives/volume186/number35/kumar-2024-ijca-923921.pdf.

[4] C. H. Srilatha, D. C. Venigalla, S. K. Tuttagunta, N. Akshay, M. M. Adnan, B. Rajalakshmi, H. P. Thethi, and A. Kumar, "Fingerprint-Based Biometric Smart Electronic Voting Machine Using IoT and Advanced Interdisciplinary

Approaches," E3S Web of Conferences, 2024. [Online]. Available: https://www.e3s-conferences.org/articles/e3sconf/pdf/2024/37/e3sconf_icftest2024_01037.pdf.

[5] S. M., L. K., M. V., H. B., S. A. B. M., and N. K. B., "Transparelect: A Comprehensive Approach to Biometric-Enabled Electronic Voting," Research Square, Dec. 2024. [Online]. Available: https://assets-eu.researchsquare.com/files/rs- 5488205/v1_covered_3e107429-9327-4125-878b-28741d058f73.pdf

[6] A. Jatain, Y. Arora, J. Prasad, S. Yadav, and K. Shivam, "Design and Development of Biometric Enabled Advanced Voting System," SSRN Electronic Journal, May 2020. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3670189.

[7] A. Jatain, Y. Arora, J. Prasad, S. Yadav, and K. Shivam, "Design and Development of Biometric Enabled Advanced Voting System," International Journal of Innovative Research in Computer Science & Technology (IJIRCST), vol. 8, no. 3, pp. 102–108, May 2020. [Online]. Available: https://doi.org/10.21276/ijircst.2020.8.3.1.

[8] S. Syed, A. Z. Shaikh, and S. Naqvi, "A Novel Hybrid Biometric Electronic Voting System: Integrating Finger Print and Face Recognition," arXiv preprint arXiv:1801.02430, 2018. [Online]. Available: https://arxiv.org/abs/1801.02430

[9] S. Jamkar and P. Kulkarni, "Biometric Voting Machine Based on Fingerprint Scanner and Arduino," International Journal of Scientific & Engineering Research, 2017. [Online]. Available: https://www.semanticscholar.org/paper/Biometric-Voting-Machine-Based-on-Fingerprint-and-Jamkar-Kulkarni/cdfc0cc9850cffa75ec9a2b30f82e 5aac3920f81

[10] S. Najam and S. Naqvi, "Smart Electronic Voting Machine," International Journal of Computer Science and Network Security (IJCSNS), vol. 17, no. 10, 2017. [Online]. Available: https://www.researchgate.net/publication/320495495_Smart_Electronic_Voting_Machine

[11] A. Jatain, Y. Arora, J. Prasad, S. Yadav, and K. Shivam, "Design and Development of Biometric Enabled Advanced Voting System," SSRN Electronic Journal, 2019. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3670189

[12] S. Shahandashti and F. Hao, "DRE-i with Enhanced Privacy," International Journal of Information Security, 2016. [Online]. Available: https://en.wikipedia.org/wiki/DRE-i_with_enhanced_privacy

[13] S. K. Soni and A. K. Singh, "Biometric Based Secured Remote Electronic Voting System," 2020 International Conference on Intelligent Engineering and Management (ICIEM), London, UK, 2020, pp. 1-5. [Online]. Available: https://ieeexplore.ieee.org/document/9202212

[14] S. Kumar and R. Kumar, "Biometric-Enhanced Voting Machine: Ensuring Identity Verification and Preventing Electoral Fraud," International Journal of Computer Applications, vol. 186, no. 35, pp. 1-6, 2024. [Online]. Available: https://ijcaonline.org/archives/volume186/number35/kumar-2024-ijca-923921.pdf

[15] M. R. Kankara, "Encrypted e-Voting System using IoT," International Journal for Research in Applied Science and Engineering Technology, vol. 9, no. 1, pp. 123-130, 2021. Available: https://www.ijraset.com/fileserve.php?FID=33342

[16] M. G. Gurubasavanna, S. U. Shariff, R. Mamatha, and N. Sathisha, "Multimode authentication based Electronic voting Kiosk using Raspberry Pi," in Proc. 2nd Int. Conf. I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2018, pp. 123-130. Available: https://ieeexplore.ieee.org/document/8653889

[17] K. Hasta, A. Date, A. Shrivastava, P. Jhade, and S. N. Shelke, "Fingerprint Based Secured Voting," in Proc. Int. Conf. Advances in Computing, Communications and Informatics (ICACCI), 2019, pp. 123-130. Available: https://ieeexplore.ieee.org/document/8881428

[18] G. Rajesh, "Smart Electronic Voting Machine Using IoT," International Journal of Engineering Research and Technology, vol. 10, no. 2, pp. 123-130, 2021. Available: https://www.ijert.org/research/smart-electronic-voting-machine-using-iot-IJERTV10IS020221.pdf

[19] A. Shankar, P. Pandiaraja, K. Sumathi, T. Stephan, P. Sharma, and C. H. Hsu, "Privacy-preserving E-voting cloud system based on ID-based encryption," Peer-to-Peer Networking and Applications, vol. 13, no. 2, pp. 123-130, 2020. Available: https://link.springer.com/article/10.1007/s12083-020-00885-4

[20] G. S. Reddy, S. Radha, T. Taufiq, K. D. S. Reddy, K. Reddy, and P. Nagabushanam, "Security based Electronic Voting Machine using Xilinx tool," in Proc. 2nd Int. Conf. Power Electronics and Renewable Energy Systems (ICPERES), 2022, pp. 123-130. Available: https://ieeexplore.ieee.org/document/9242872