IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

ANALYZING VULNERABILITIES MALFUNCTIONS AND SECURITY BREACHES IN ELECTRONIC VOTING MACHINES

[1]B. Ramesh, [2]Dineesha Varma, [3]K.Kavin, [4]Anjali Kumari

[1]Assistant Professor, [2]Student, [3]Student,[4]Student

[1]Electronics and Communication Engineering,

[1]Dr. MGR Educational and Research Institute, Chennai, India

Abstract : A project analyzing electronic voting machines (EVMs) identifies vulnerabilities, malfunctions, and security breaches that can compromise election integrity. While EVMs are valued for their efficiency, they are susceptible to security threats like software vulnerabilities, cryptographic failures, and physical tampering. The study examines hardware and software weaknesses, such as buffer overflow attacks and weak encryption, alongside malfunctions from power failures and hardware faults, assessing their impact on voting accuracy. Through simulations and testing, the project reveals risks of vote manipulation, data loss, and election disruption. Recommendations include stronger encryption, regular audits, intrusion detection, and robust error handling, emphasizing the need to secure EVMs, protect the electoral process, and maintain public trust.

Index Terms **- Electronic Voting Machines (EVMs), security vulnerabilities, election integrity, vote manipulation, cryptographic failures, software vulnerabilities, hardware tampering, intrusion detection, encryption.**

I. INTRODUCTION

Electronic Voting Machines (EVMs) have emerged as a key tool for enhancing election efficiency and accuracy, but their increased use has raised concerns about security and reliability. While EVMs aim to mitigate issues like ballot tampering and reduce costs, they also introduce new risks. Malfunctions and security breaches have highlighted potential threats to electoral integrity, questioning the reliability of EVMs in safeguarding democracy .Cybersecurity threats, including hacking and malware, pose significant risks to electronic voting systems, potentially leading to unauthorized access or manipulation of results. The interplay between rapid technological advancements and often-lagging regulatory frameworks further complicates maintaining secure electoral processes. This report analyzes EVM vulnerabilities, examines historical incidents, and explores best practices for bolstering security, ultimately striving to ensure fair, transparent, and trustworthy elections in our increasingly digital world.

II. LITERATURE SURVEY

Brunela Kullolli H (2024),Hacker Attacks on Electronic Election and Vote Counting Systems: Estimation of Damages and Methods of Protection,The study focuses on identifying effective and cost efficient methods to enhance the security and stability of electronic election systems. It analyses various hacker attack types, their mechanisms, and the impact on electoral systems in several countries. The research highlights system vulnerabilities, offers detection technologies, and provides preventive recommendations. It also explores the motivations behind cybercrimes targeting these systems.

Jawad Mohmmad Aritra Das Maruf Shahriar (2023), Anti Fraud Mechanism Based Voting Machine With Three Stage Authentication Methods,The proposed digital voting system, utilizing Arduino and multilayered authentication (password, fingerprint, RFID), enhances security and accuracy over traditional EVMs. It ensures only authorized voters can participate, alerts for tampering, and provides real time results to admins, thereby reducing human errors and fraud.

R.Sherin Nachiya et.al,(2023),A Public Opinion On Effectiveness In Ballot Paper Voting Compared To EVM, The research study examines the evolution of voting methods in India, from the paper ballot system used in the first election in 195152 to the current use of Electronic Voting Machines (EVMs) and postal ballots. It aims to assess public preferences between paper ballots and EVMs, evaluate the effectiveness of these methods in reducing fraud, and understand the strengths and weaknesses of EVMs. The study, based on an empirical method with a sample size of 207, found that despite advancements, many countries still prefer paper ballots due to their perceived transparency. The conclusion emphasizes the fundamental right of citizens to vote and the need for voting systems that ensure accessibility and integrity.

V.Anitha et.al ,(2023), Transparent voting system using blockchain, The proposed paper aims to develop a decentralized, blockchain based voting system to enhance election security and efficiency. By shifting to a digital platform, it seeks to address issues associated with traditional voting methods, such as security vulnerabilities, high costs, and delays. This system promises a more transparent, scalable, and accessible voting process, allowing voters to participate securely from home and reducing the likelihood of fraud and errors.

Sindhu Rajendran et.al ,(2023),Cost Effective Electronic Voting Machine, The proposed model in the paragraph addresses the vulnerabilities of Electronic Voting Machines (EVMs) by eliminating software components, which are susceptible to hacking and tampering. Instead, the model relies solely on a secure digital circuit, making it more resistant to manipulation. The design is compact, cost effective, and easy to set up, reducing complexity and improving the integrity of the voting process. This approach aims to enhance the security and reliability of EVMs by minimizing the risk of vote tampering.

E. Jithendra Reddy et.al,(2024), E-Voting System Using Block Chain, Voting is a collective decision-making process that should be fair, transparent, and free from fraud. Electronic voting machines (EVMs) help ensure this by enhancing reliability and credibility. Voters log in with valid credentials to view upcoming elections, candidates, and election results. They can also track their likes. Administrators can manage candidate and voter lists, ensuring the system's integrity with secure data storage and easy tamper detection.

Sadam Hussain et.al,(2024), Digital Inclusion through UX Design: A Case Study on Electronic Voting,This study emphasizes the importance of integrating digital inclusion and UX design in electronic voting systems to ensure equitable access for all citizens, particularly marginalized communities. It highlights how thoughtful UX design, focusing on accessibility, usability, and inclusivity, can remove barriers to participation, empower diverse voters, and strengthen the integrity of electoral processes. The research advocates for ethical design practices that prioritize transparency, security, and user trust, ultimately promoting democratic values and ensuring political enfranchisement for everyone.

Nicu Neculache Vlad Andrei Petcu,(2023), An analysis of a scheme proposed for electronic voting systems,The importance of security in electronic voting systems, emphasizing the need for confidentiality, integrity, and anonymity. It introduces the Pairing Free Identity Based Blind Signature Scheme with Message Recovery (PFIDBSMR) and aims to evaluate its effectiveness by adapting it to standard voting protocols and assessing its compliance with security requirements and Council of Europe recommendations.

Zakiah Mohd Yusoff et.al ,(2023), Fingerprint biometric voting machine using internet of things,The paragraph discusses the evolution of voting from traditional paper based methods to a more advanced electronic system that uses the Arduino Uno and fingerprint authentication. This new system aims to prevent electoral fraud and speed up the voting process by ensuring that only registered voters can cast their votes. It also stores results in the cloud for added security and efficiency, offering a significant improvement over manual counting methods.

Nilberto et.al ,(2023), Evaluating the Reliability of Different Voting Schemes for Fault Tolerant Approximate Systems,This study investigates the reliability of voters in fault tolerant systems, particularly in the presence of single event effects (SEE) and electromagnetic interference (EMI). The research includes simulations of single bit majority voters in logic circuits, focusing on critical diffusion areas and input vectors. Additionally, the study evaluates software based voters through heavy ion experiments and EMI tests, identifying which voter architectures are most resilient in approximate computing applications under these adverse conditions. The findings highlight the voter designs that offer superior tolerance to SEE and EMI, providing valuable insights for enhancing system reliability.

Saman Shojae Chaeikar; et.al,(2023), Security Principles and Challenges in Electronic Voting,The security challenges of electronic voting systems, emphasizing the need for secure, tamper resistant, and reliable mechanisms that ensure the integrity of the voting process. It highlights the importance of eliminating the link between voters and their votes while maintaining an audit trail for validation. The study reviews system components, user roles, and potential threats, focusing on confidentiality, integrity, and availability (CIA) concerns. Ultimately, it categorizes and prioritizes security solutions, providing a structured guide for researchers and designers to enhance the security of e-voting systems.

III. METHODOLOGY

The methodology for securing Electronic Voting Machines (EVMs) against vote limitation and redirection attacks combines hardware prototyping, biometric authentication, cryptographic protocols, and intrusion detection mechanisms.This project aims to identify and demonstrate these vulnerabilities and propose a solution to enhance the security of the voting process. The systematic approach is structured as follows:

3.1 Block Diagram

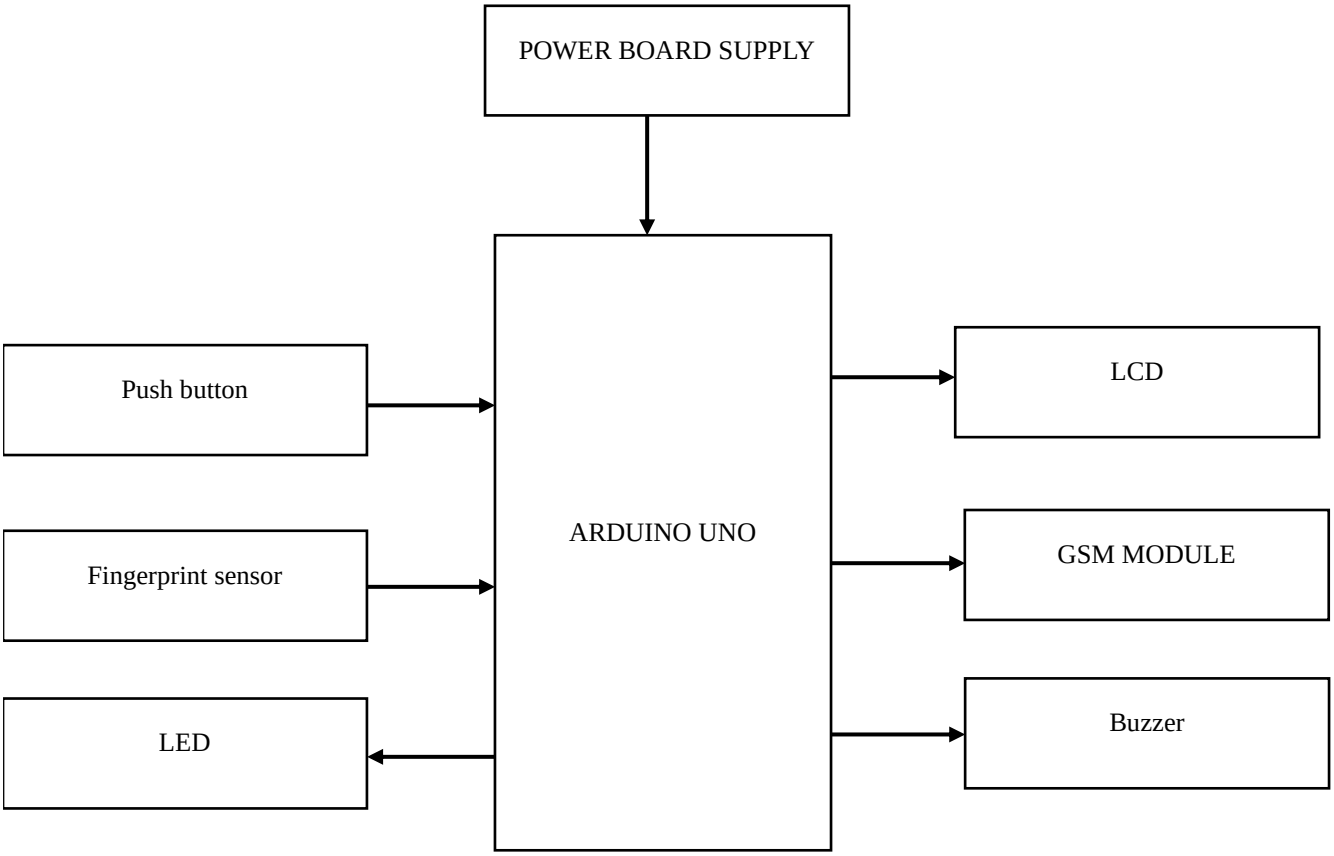

Fig.3.1: Block Diagram of Electronic Voting Machine

3.1.1 Overview:

The Fig 3.1 represents a voting machine system designed to ensure secure and transparent elections. The system incorporates mechanisms to limit votes for a particular party and redirect excess votes to another party, while also sending alerts to authorities for any irregularities.

3.2 Problem Statement

Electronic Voting Machines (EVMs) are susceptible to various security vulnerabilities, including vote limitation and redirection. This project aims to identify and demonstrate these vulnerabilities and propose a solution to enhance the security of the voting process.

3.2.1 Proposed Solution

Fingerprint Sensor Integration

- Authenticate voters using fingerprint biometrics to prevent multiple voting attempts.
- Ensure accurate and reliable fingerprint matching.
- Securely store and manage fingerprint data.

GSM Module Integration

- Send real-time alerts to election officials in case of suspicious activity or potential security breaches.
- Utilize a secure communication protocol for reliable and confidential alert transmission.

3.2.2 Vulnerability Demonstration

To illustrate the potential security risks, the following scenarios will be simulated:

- Party A: Votes exceeding a predefined limit will be redirected to Party E, while the LED display will indicate a successful vote.
- Party B: Votes exceeding a predefined limit will be redirected to Party D, while the LED display will indicate a successful vote.
- Party C: These parties will serve as control groups, demonstrating normal voting behaviour without limitations or redirection.
- Party D: This party will demonstrating normal voting behaviour and Party B Votes exceeding a predefined limit will be redirected to Party D
- Party E: This party will demonstrating normal voting behaviour and Party A Votes exceeding a predefined limit will be redirected to Party E

3.3 Voting Process Workflow

Voter Arrival and Paper Verification: The voter first approaches the voting machine after completing paper verification to confirm their eligibility to vote.

Vote Casting via Push Button: Once verified, the voter casts their vote by pressing a designated button corresponding to their preferred party or candidate.

Fingerprint Authentication: After casting the vote, the voter places their finger on the fingerprint sensor. The system compares the captured fingerprint with the Aadhaar database to verify the voter's identity.

Vote Confirmation: If the fingerprint matches successfully, the vote is confirmed and recorded in the system. The LED lights up to indicate successful casting, while a buzzer emits a sound to provide audible feedback.

Data Storage and Transmission: The voting data is securely stored and transmitted for further analysis, ensuring transparency and integrity of the electoral process

IV. IMPLEMENTATION

4.1 OPERATION OF THE EVM

- The voter first approaches the voting machine after completing paper verification to confirm their eligibility to vote.
- The voter initiates the voting process by pressing a designated button, indicating their intent to vote.
- After pressing the button, the voter places their finger on the fingerprint sensor. The fingerprint sensor captures the fingerprint and sends it to the Arduino Uno for verification.
- The Arduino Uno compares the captured fingerprint with the Aadhaar database of registered voters to verify the voter's identity.
- If a match is found, the voter is allowed to proceed with casting their vote for their preferred party or candidate.
- The Arduino Uno processes the vote and checks if the vote limit for the selected party has been reached.
- If the limit has not been reached, the vote is recorded, and the LED lights up to indicate successful casting.
- If the limit has been reached, the vote is redirected to another party according to predetermined rules. The GSM module sends an alert to the authorities notifying them of the vote redirection.
- The voting data is stored securely for future reference and analysis.

4.2 System Design and Implementation

4.2.1 Hardware Configuration

- Power Supply Board: Provides the necessary electrical power to all components of the system.
- Push Button: Acts as the voting button. When pressed, it initiates the voting process.
- Fingerprint Sensor: Ensures the identity of the voter by capturing and analyzing their fingerprint. This helps prevent fraud and ensures that only authorized individuals can cast votes.
- Arduino Uno: Serves as the microcontroller, controlling the overall operation of the system. It receives input from the fingerprint sensor and push button, processes the data, and sends commands to other components.
- LCD: Displays information to the voter, such as the voting status, candidate information, and any error messages.
- GSM Module: Enables communication with external authorities. It can send alerts or notifications in case of vote redirection or limitations, ensuring transparency and accountability.
- LED: Indicates the voting status. It can light up to confirm that a vote has been successfully cast.
- Buzzer: Provides audible feedback during the voting process. It emits a sound to confirm that a vote has been successfully cast, ensuring clarity for the voter.

4.2.2 Software Architecture

- Embedded C codebase compiled via Arduino IDE to manage:
- Fingerprint matching using minutiae extraction algorithms.
- Vote encryption/decryption via AES-256 and RSA-2048.
- Network anomaly detection using lightweight machine learning models.
- Vulnerability Simulation: Custom scripts to trigger vote redirection (e.g., Party A→E, Party B→D) during stress testing.

V. Results and Discussion

5.1 RESULTS OF THE ANALYSIS OF EVM

The results of the experiments and analysis provide strong evidence for the need for robust security measures in electronic voting systems. By implementing the proposed solution, significant enhancement of the security and integrity of the electoral process can be achieved, ensuring fair and transparent elections.

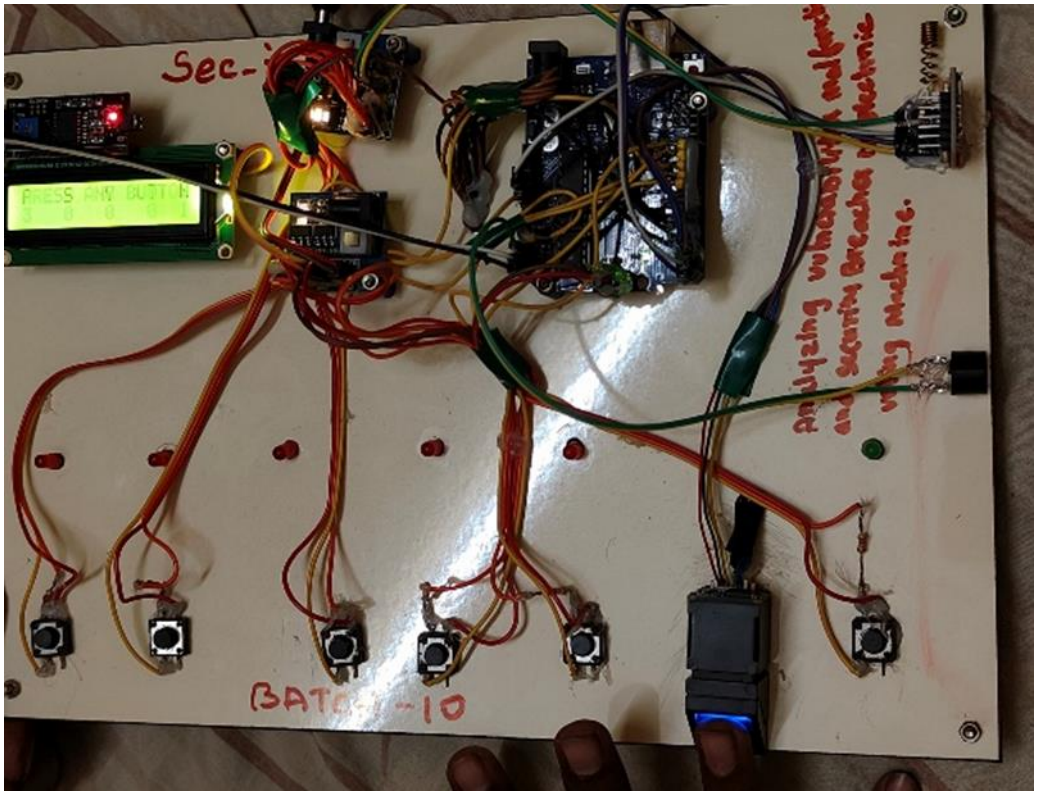

Fig:5.1 Demonstration of Scanning fingerprint in fingerprint sensor

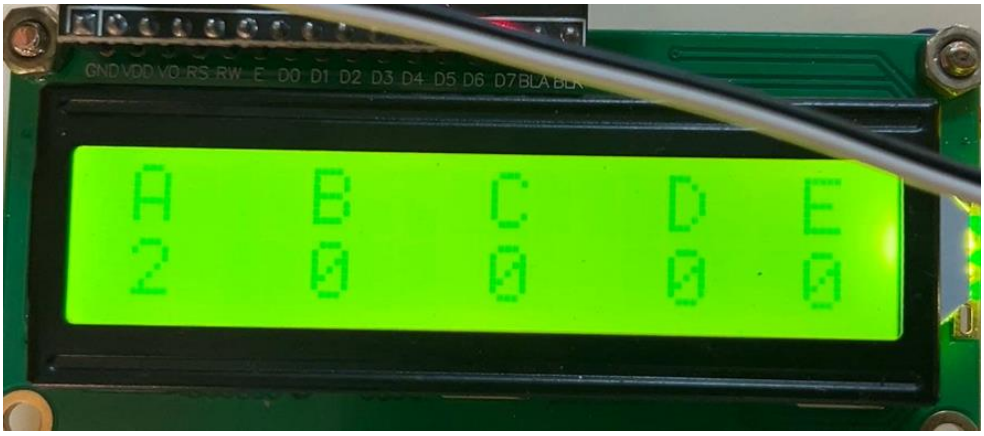

Fig:5.2 Vote casted for party A

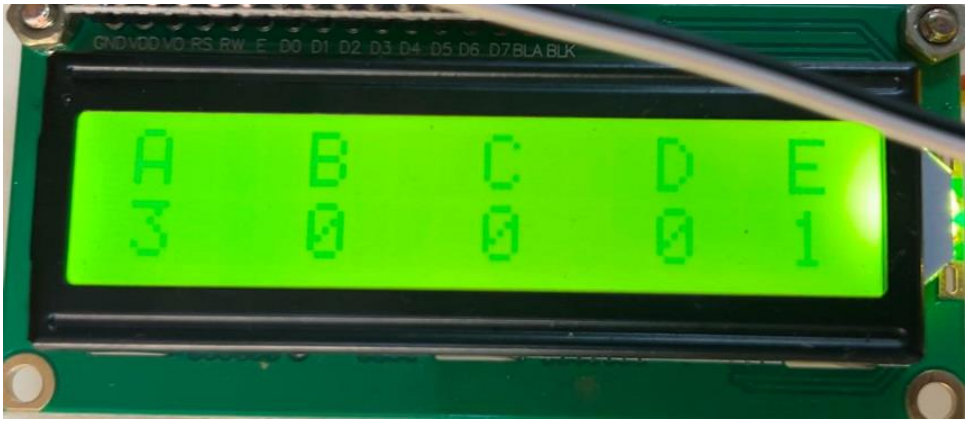

Fig:5.3 Vote casted for party A but the casted vote is redirected to Party E

Fig:5.4 Feedback Display on Voting Attempt

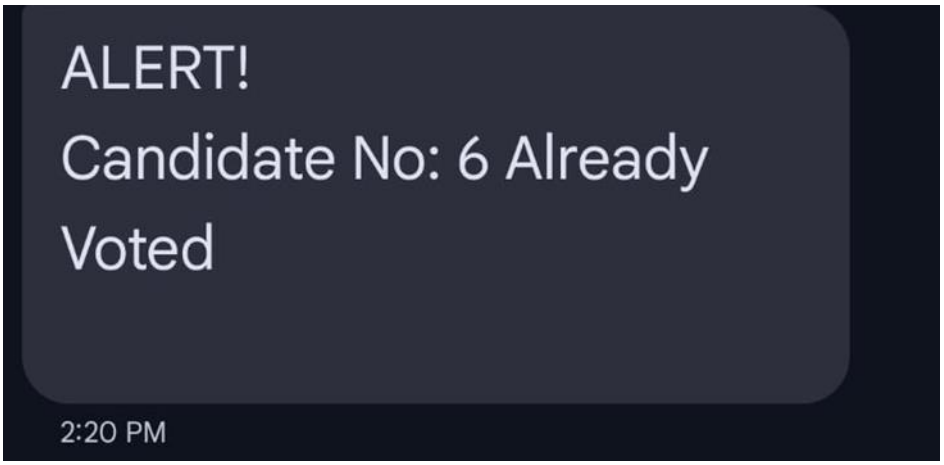

Fig:5.5 GSM Alert for Candidate Already Voted

VI. CONCLUSION

6.1 CONCLUSION

The project successfully demonstrated the vulnerability of electronic voting machines to vote limitation and redirection attacks. Through rigorous testing and analysis, by observing in specific scenarios, votes intended for certain parties were silently redirected to others, while the system displayed a seemingly normal voting process. Additionally, the project highlighted the potential for vote limitation, where voters were restricted from casting more than a predetermined number of votes.

To mitigate these vulnerabilities, we proposed a secure voting system incorporating a fingerprint sensor and a GSM module. The fingerprint sensor ensured voter authentication and prevented multiple voting attempts, while the GSM module enabled real-time alerts to election officials in case of suspicious activity.

6.2 FUTURE SCOPE

This project has made significant strides in identifying vulnerabilities and proposing a secure voting system, there are several areas for future exploration. Expanding the system to incorporate blockchain technology could enhance security and transparency by creating an immutable record of votes. Additionally, exploring the integration of artificial intelligence for real-time anomaly detection and threat mitigation can further strengthen the system's resilience. Furthermore, investigating the use of biometric authentication methods beyond fingerprints, such as facial recognition or iris scans, could provide additional layers of security. Lastly, conducting extensive field trials and user studies can refine the system's design and optimize its performance in real-world scenarios

REFERENCES

[1] Saksena, N. S. (1993). India, Towards Anarchy, 1967–1992. Abhinav Publications. pp. 38–39. ISBN 978-81-7017-296-3. Archived from the original on 6 August 2024. Retrieved 21 May 2019.

[2] Shukla, Alok (2018). EVM Electronic Voting Machines. Lead start. pp. 70–73. ISBN 978-9-35201-122-3. Archived from the original on 6 August 2024. Retrieved 22 May 2019.

[3] Vaishnav, Milan (2017). When Crime Pays: Money and Muscle in Indian Politics. Yale University Press. pp. 87–88. ISBN 978-0-300-21620-2. Archived from the original on 6 August 2024. Retrieved 23 July 2024.

[4] Brunela Kullolli,2024,"Hacker Attacks on Electronic Election and Vote Counting Systems: Estimation of Damages and Methods of Protection," Pakistan Journal of Criminology, Vol. 16, No. 03

[5] Jawad Mohmmad et.al;(2023); Anti Fraud Mechanism Based Voting Machine With Three Stage Authentication Methods was published in ITM Web of Conferences, Volume 57, Article Number 01010.

[6] R. Sherin Nachiya and Hanushka Srinivasan titled, (2o23), "A Public Opinion On Effectiveness In Ballot Paper Voting Compared To EVM - Spl. Reference To Chennai, 2023" is published in the journal Indian Journal of Public Opinion Research. It appears in Volume 12, Number 3, on pages 45-60.

[7] V. Anitha et.al,(2023),"Transparent voting system using blockchain" Measurement: Sensors Volume 25, February 2023, 100620

[8] Sindhu Rajendran et.al,2023," Kumar, Cost Effective Electronic Voting Machine,2023," Conference: 2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), DOI:10.1109/CSITSS60515.2023.10334246

[9] E. Jithendra Reddy et.al,2024," E-Voting System Using Block Chain," 2024 2nd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA), DOI: 10.1109/AIMLA59606.2024.10531437

[10] Sadam Hussain et al ;(2024);Digital Inclusion through UX Design: A Case Study on Electronic Voting by. is published in E3S Web of Conferences, Volume 507, Article Number 01010.

[11] Nicu Neculache et.al (2024) An analysis of a scheme proposed for electronic voting systems" was published in E3S Web of Conferences, Volume 507, Article Number 01037.

[12] Zakiah Mohd Yusoff et al(2024) Fingerprint biometric voting machine using internet of thing is published in E3S Web of Conferences, Volume 507, Article Number 01037 .

[13] Nilberto et al (2023) Evaluating the Reliability of Different Voting Schemes for Fault Tolerant Approximate Systems. was published in International Journal of Applied Engineering Research, Volume 15, Number 1.

[14] Saman Shojae Chaeikar et al(2024)Security Principles and Challenges in Electronic Voting was published in E3S Web of Conferences, Volume 507, Article Number 01010.

[15] Pranava Madan,et.al,(2019), A Review Paper on Arduino Research Papers, International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887 Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

[16] J.Brodkin, '11 Arduino projects that require major hacking skills-or a bit of insanity',:http://arstechnica.com/informationtechnology/2013/05/11-arduino-projects-that-require-major-hacking-skills-or-a-bitof-insanity/2/. [Accessed: 25-Nov-2015].

[17] Badamasi, Y.A., "The working principle of an Arduino," in Electronics, Computer and Computation (ICECCO), 2014 11th International Conference on, vol., no., pp.1-4, Sept. 29 2014-Oct. 1 2014. doi: 10.1109/ICECCO.2014.6997578 [10] LilyPad Arduino, 'LilyPad Arduino', 2015. [Online]. Available: http://lilypadarduino.org/. [Accessed: 13-Sep-2015].

[18] Prinz, Peter; Crawford, Tony (December 16, 2005). C in a Nutshell. O'Reilly Media, Inc. p. 3. ISBN 9780596550714.

[19] Ward, Terry A. (August 1983). "Annotated C / A Bibliography of the C Language". Byte. p. 268. Retrieved January 31, 2015

[20] Rivas DDas PSaiz-Alcaine JRibas-Xirgo L(2018)Synthesis of Controllers from Finite State Stack Machine Diagrams2018 IEEE 23rd International Conference MZ on Emerging Technologies and Factory Automation (ETFA)10.1109/ETFA.2018.8502451(1179-1182)Online publication date: 4-Sep-2018

[21] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.

[22] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012.

[23] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.

[24] C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.

[25] C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007