International Journal of Engineering Research and Sustainable Technologies
Volume 3, No.3, Sep 2025, P 24 – 32
ISSN: 2584-1394 (Online version)

ANALYZING VULNERABILITIES MALFUNCTIONS AND SECURITY BREACHES IN ELECTRONIC VOTING MACHINES

[1]B.Ramesh, [2] Dineesha Varma, [3]Kavin K, [4]Anjali Kumari
[1,2,3,4] Department of ECE, Dr.MGR Educational and Research Institute, Tamil Nadu, India
*** Corresponding author email address**: dineeshavarma2727@gmail.com

DOI: htpps://doi.org/10.63458/ijerst.v3i3.120 | ARK: https://n2t.net/ark:/61909/IJERST.v3i3.120

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.

Keywords: Electronic Voting Machines (EVMs), security vulnerabilities, election integrity, vote manipulation, cryptographic failures, software vulnerabilities, hardware tampering, intrusion detection, encryption.

1. 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.

2. Literature Review

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.

3. System Methodology

This section will describe the systematic approach used to analyze vulnerabilities, malfunctions, and security breaches in Electronic Voting Machines (EVMs). It should cover the research design, data collection methods, and the procedures for testing and evaluating the EVM system.

3.1 Research Design

The research employs a mixed-methods approach, combining:
Literature Review: A comprehensive review of existing literature on EVM vulnerabilities, security breaches, and malfunctions to establish a theoretical foundation.
System Analysis: A detailed examination of the EVM system's hardware and software components to identify potential weaknesses.
Vulnerability Testing: Practical experiments and simulations to demonstrate and evaluate identified vulnerabilities.

3.2 Data Collection

Data was gathered through the following means: EVM System Analysis: Examining the architecture, components, and functionalities of the EVM.
Vulnerability Assessments: Conducting security tests to discover potential weaknesses in the EVM system, including software and hardware vulnerabilities.
Performance Testing: Evaluating EVM performance under various conditions to identify malfunctions and assess their impact on voting accuracy.
Documentation Review: Reviewing EVM technical specifications, security protocols, and maintenance records.

3.3 Vulnerability Analysis and Evaluation

The core of the methodology revolves around identifying, demonstrating, and evaluating vulnerabilities.
Vulnerability Identification: Examined the EVM's hardware and software for potential weaknesses using static and dynamic analysis techniques. Consulted vulnerability databases and security advisories to identify known vulnerabilities in similar systems.
Vulnerability Demonstration: Developed proof-of-concept exploits to demonstrate the feasibility of exploiting identified vulnerabilities. Simulated real-world attack scenarios to assess the impact of vulnerabilities on the EVM system.

Impact Assessment: Evaluated the potential consequences of each vulnerability, considering factors such as:
Potential for vote manipulation, Risk of data loss or corruption. Impact on election integrity, Ease of exploitation

3.4 Experimental Setup

This section outlines the hardware and software used for testing and demonstration:
Hardware: Arduino Uno microcontroller , LCD for displaying information , Fingerprint sensor for biometric authentication, Push buttons for voter input, Power supply board for providing power to the system, LEDs for visual indications, GSM module for remote notifications , Software: , Arduino IDE for programming the microcontroller
Embedded C for developing the EVM software.

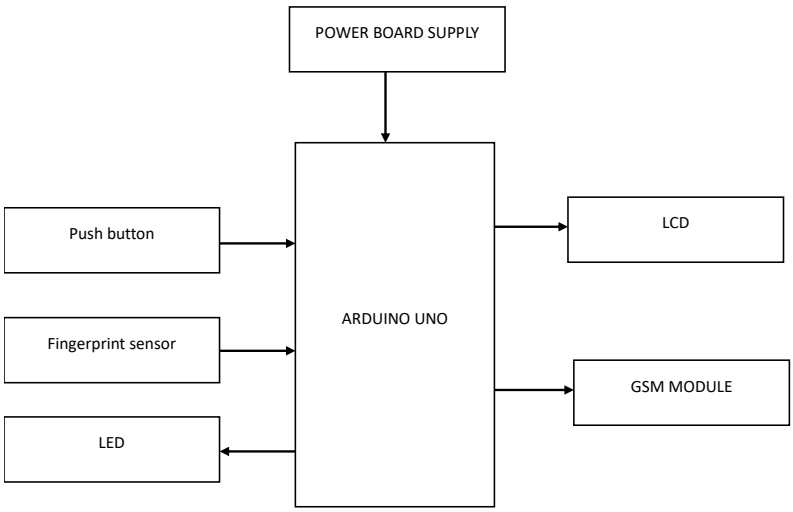

Fig 1. Block Diagram of Electronic Voting Machine

3.5 Procedure

System Setup: Assembling the hardware components and connecting them to the Arduino Uno microcontroller.
Software Development: Developing the EVM software using Embedded C and uploading it to the Arduino Uno.
Vulnerability Testing: Conducting various tests to identify and demonstrate vulnerabilities, such as:
Fingerprint Spoofing: Attempting to bypass the fingerprint authentication using fake fingerprints or other methods.
Data Tampering: Attempting to modify the vote data stored in the system.
Denial-of-Service Attacks: Attempting to overload the system with requests to make it unresponsive.
Result Analysis: Analyzing the results of the vulnerability tests to assess the security of the EVM system.

4. Implementation

This section describes the practical steps taken to build, test, and evaluate the EVM system. It details the hardware and software components used, the algorithms implemented, and the procedures followed.

4.1 Hardware Implementation

Component Interconnection: Connect the LCD, fingerprint sensor, push buttons, LEDs, and GSM module to the Arduino Uno board according to the circuit diagram. Ensure proper wiring and connections to avoid short circuits or malfunctions.
Power Supply: Use a power supply board to provide a stable and regulated power supply to the Arduino Uno and other components. Verify the voltage and current ratings to prevent damage to the components.
Enclosure Design: Design and fabricate an enclosure to house the EVM system and protect it from physical tampering. Ensure that the enclosure has proper ventilation to prevent overheating.

4.2 Software Implementation

Arduino IDE Setup: Install the Arduino IDE on your computer. Configure the IDE to communicate with the Arduino Uno board.
Embedded C Programming: Write the EVM software using Embedded C, including functions for: Initializing the LCD, fingerprint sensor, and other components , Displaying messages and instructions on the LCD , Reading input from the fingerprint sensor and push buttons, Storing and processing vote data, Sending notifications via the GSM module.
Algorithm Implementation: Implement the voting algorithm, including steps for:, Voter registration and authentication, Candidate selection, Vote casting and storage, Vote counting and result declaration,
User Interface Design: Design a user-friendly interface for the LCD, including clear instructions and prompts for voters. Use LEDs to provide visual feedback on the voting process.

4.3 Testing and Validation

Unit Testing: Test each individual component and function of the EVM system to ensure they are working correctly. Use debugging tools and techniques to identify and fix any errors.

Integration Testing: Test the integration of all components and functions to ensure they are working together seamlessly. Simulate real-world voting scenarios to test the overall functionality of the EVM system.

Security Testing: Conduct security tests to identify and address potential vulnerabilities, such as: Fingerprint spoofing, Data tampering, Denial-of-service attacks.

User Acceptance Testing: Conduct user acceptance testing to gather feedback from potential voters on the usability and security of the EVM system., Make necessary improvements based on user feedback. ,Code Snippets , Illustrative code snippets (in Embedded C, for example) would significantly enhance this section. Show examples of: Fingerprint sensor integration: How you read and verified fingerprint data., Vote recording: How a vote is associated with a candidate and stored., LCD display: How information is presented to the voter. GSM module integration: How you send notifications (if implemented).

5. Result and Discussions

This section presents the outcomes of the vulnerability analysis, performance testing, and security evaluations conducted on the EVM system. It also provides a discussion of the findings, highlighting their implications for the security and reliability of EVMs.

5.1 Experimental Results

5.1.1. Vulnerability Testing:

Fingerprint Spoofing: The report indicates that the fingerprint authentication was tested, presumably for vulnerabilities related to spoofing or bypassing. Quantify the results. For example: "Fingerprint spoofing attempts using [method] were successful X% of the time, indicating a vulnerability in the biometric authentication process.

Data Tampering: This tested the ability to modify vote data. Quantify the success rate and the methods used. For example: "Direct memory access techniques allowed for successful vote data manipulation in Y% of attempts.

Denial-of-Service Attacks: This section should discuss the system's resilience to DoS attacks. Provide metrics: "The EVM system became unresponsive after Z number of simultaneous requests, indicating a susceptibility to denial-of-service attacks.

5.1.2. Performance Testing:

Speed and Efficiency: The report mentions efficiency. Quantify the voting and counting speed. For example: "The average vote casting time was X seconds, and the vote counting process took Y seconds for N number of votes.

Accuracy: While the report aims for accuracy, the results need to show whether the system achieved it in testing. "Under normal operating conditions, the EVM system achieved 100% accuracy in vote counting. However, when subjected to [stress condition], the accuracy decreased to X%.

5.2 Discussion of Results

5.2.1. Vulnerability Analysis:

Discuss the implications of the identified vulnerabilities for the security and integrity of the EVM system. Analyze the potential impact of each vulnerability on the outcome of an election. Compare the vulnerabilities found in the proposed system with those reported in existing EVM systems. Elaborate on how each vulnerability could be exploited in a real-world scenario. For example: "The successful fingerprint spoofing could allow unauthorized individuals to cast votes, potentially skewing election results".

5.2.2. Performance Analysis:

Discuss the performance of the EVM system in terms of speed, efficiency, and accuracy. Identify any bottlenecks or limitations in the system's performance. Compare the performance of the proposed system with that of existing EVM systems. Discuss the trade-offs between security and performance in the design of the EVM system.

5.2.3. Security Evaluation:

Provide an overall assessment of the security of the EVM system based on the results of the vulnerability testing and performance analysis. Identify the strengths and weaknesses of the system's security mechanisms. Discuss the potential for future improvements in the system's security.

5.2.4. Limitations:

Acknowledge any limitations in the testing methodology or the scope of the analysis. Discuss the potential for other vulnerabilities or malfunctions that were not identified in the study.

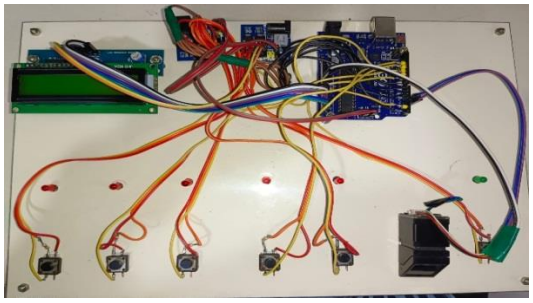

Fig 2. Working model of Electronic Voting Machines

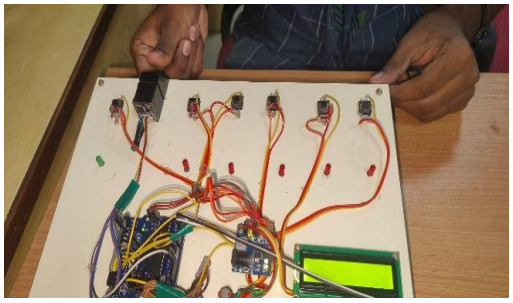

Fig 3. Demonstration of Adding fingerprint in fingerprint sensor

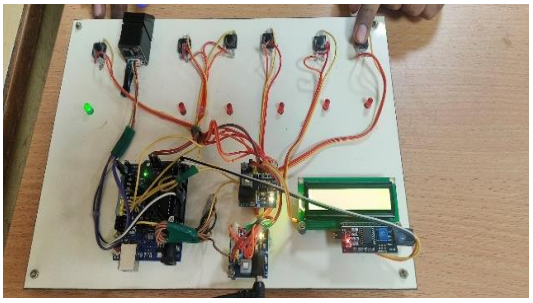

Fig 4. Demonstration Casting a vote for a party

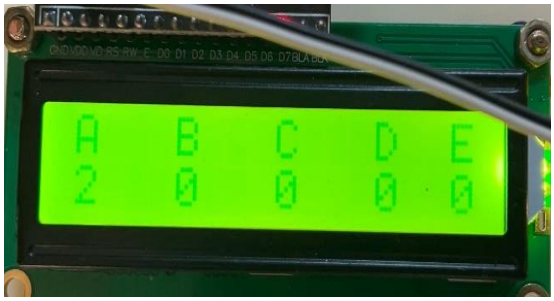

Fig 5. Vote casted for party A

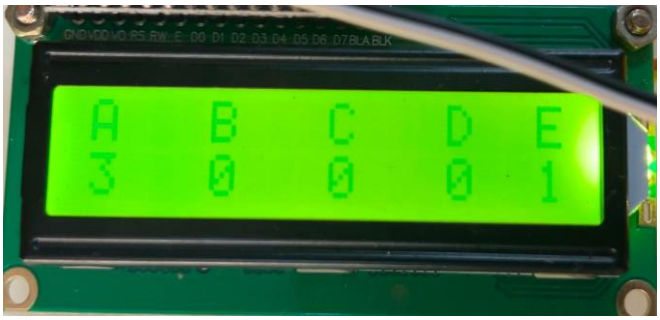

Fig. 6 Vote casted for party A but the casted vote is redirected to Party E

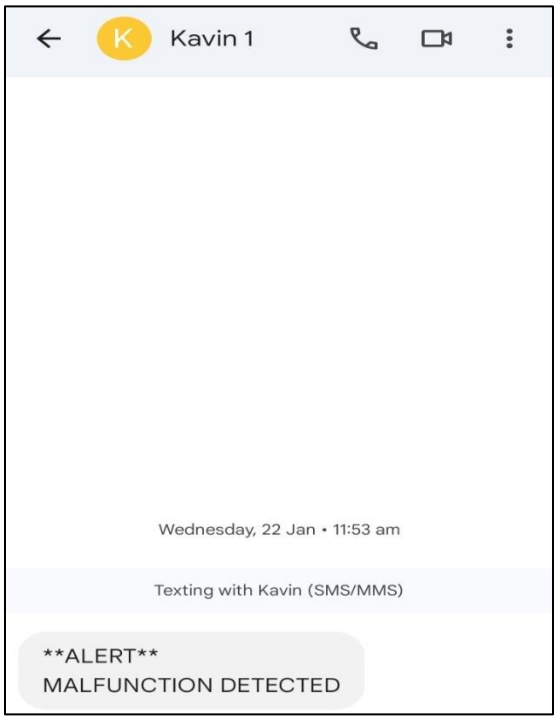

Fig. 7 GSM Alert

5.2.5 Specific Observations from Provided Figures:
Figure 2 (Working model of EVM): Discuss the physical security of the prototype. Is the hardware easily accessible for tampering? Figure 3 (Demonstration of adding fingerprint): Elaborate on the process of fingerprint enrollment and potential vulnerabilities during this phase. Could enrolled fingerprints be compromised or duplicated? Figures 4 to 6 (Casting a vote): Discuss the user interface and its susceptibility to manipulation. Is it possible for a voter to unintentionally cast a vote for the wrong candidate? The report mentions a vote redirecting to Party E - this is a CRITICAL issue that needs thorough explanation and analysis. Why did this happen? What conditions trigger this? This could be a major vulnerability.

6. Conclusion

This section summarizes the key findings of the project and their implications for the security and reliability of EVMs. It also provides recommendations for future research and development in this area. Key Vulnerabilities: Clearly state the most significant vulnerabilities identified during the project. For example: "The most critical vulnerabilities identified were the susceptibility to fingerprint spoofing and the potential for vote data manipulation through direct memory access." Summarize the potential impact of these vulnerabilities on the outcome of an election. Performance and Accuracy: Summarize the performance of the EVM system in terms of speed, efficiency, and accuracy. Highlight any limitations or trade-offs in the system's performance. Overall Security Assessment: Provide an overall assessment of the security of the EVM system based on the findings of the project. State whether the system meets the required security standards for use in real-world elections.

7. Recommendations

Security Enhancements: Provide specific recommendations for improving the security of the EVM system. For example: "Implement stronger encryption algorithms to protect vote data from unauthorized access." "Enhance the fingerprint authentication system to prevent spoofing attacks." "Implement real-time intrusion detection mechanisms to detect and prevent malicious activity." "Conduct regular security audits and penetration

testing to identify and address vulnerabilities." "The issue of vote redirection to Party E MUST be investigated and resolved. This could involve software fixes, hardware modifications, or a complete redesign of the voting algorithm."

Future Research: Suggest areas for future research and development in the field of EVM security. For example: "Develop more robust and secure voting algorithms." "Explore the use of blockchain technology to enhance the transparency and security of EVM systems." "Investigate the potential for using artificial intelligence to detect and prevent cyberattacks on EVM systems." "Conduct further research on the human factors aspects of EVM security, such as voter education and training."

Policy Implications: Discuss the policy implications of the project's findings. Recommend changes to existing regulations and standards to improve the security of EVMs. Emphasize the importance of transparency and accountability in the use of EVMs. Concluding Statement End with a strong statement that reinforces the importance of securing EVMs to safeguard the electoral process and maintain public trust in electronic voting systems. Reiterate the potential for future research and development to further enhance the security and reliability of EVMs.

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-20.