IoT-Based Smart Electronic Voting Machine for Candidate Selection Using Fingerprint

Rajat Kishor Varshney[1], Brijesh Nishad[1], Ashutosh[2], Aayush Pandey[3]
[1]Assistant Professor, Computer Science and Engineering - IoT, GNIOT, Greater Noida
[1]Scholar, Computer Science and Engineering - IoT, GNIOT, Greater Noida
[2]Scholar, Computer Science and Engineering - IoT, GNIOT, Greater Noida
[3]Scholar, Computer Science and Engineering - IoT, GNIOT, Greater Noida
[1]rajatvarshney1207@gmail.com, [1]bnlv1212@gmail.com, [2]ashuyadavay6397@gmail.com, [3]vipulrai419@gmail.com

***Abstract*—The incorporation of IoT technology in EVMs is a major innovation in voting processes through improved security, transparency, and accessibility. This paper suggests an IoT-based Smart EVM with components like Arduino Uno, ESP32, Fingerprint Sensor modules, push buttons, OLED displays, LED indicators, and a buzzer. The system provides biometric authentication, secure data transmission to a cloud server, real-time tracking of votes, and user-friendly interactions through auditory and visual feedback. The proposed solution addresses the challenges of traditional EVMs, such as tampering, impersonation, and lack of transparency. Thus, the IoT-based Smart EVM enhances security, efficiency, and accuracy. This will lead to better voter confidence in election integrity while pointing out potential risks in cybersecurity, infrastructure needs, and cost.**

***Index Terms*— IoT, Smart EVM, Biometric Authentication, Arduino Uno, ESP32, Fingerprint Sensor, Secure Data Transmission, Cloud Server, Real-time Voting, Transparency, Security, Election Integrity, Cybersecurity, Voting Technology, Push Buttons, OLED Displays, LED Indicators, Buzzer.**

I. Introduction

EVMs have revolutionarily changed the electoral process by providing faster and more dependable alternatives to traditional paper-based voting. This has made them much more efficient, reducing the likelihood of human error in vote counting, making the election much more transparent and trustworthy. The good news, however, is that traditional EVMs are still riddled by critical challenges despite their widespread adoption. [1] There still remains the problem of vulnerability of their use to tampering, unauthorized access, and impersonation, apart from weak real-time monitoring. This has led in turn to increasing skepticism about the integrity of and reliance upon electoral outcomes, hence compelling further innovation on voting technologies.

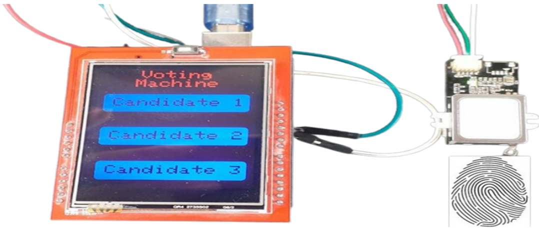


Fig. 1. Smart EVM

The IoT has emerged as a powerful technological framework capable of addressing these challenges. By integrating IoT into EVMs, we can revolutionize the way elections are conducted, ensuring security, transparency, and accessibility at every stage of the voting process. The proposed IoT-based Smart EVM is based on cutting-edge IoT components and methodologies to build a robust system that eliminates traditional shortcomings. It uses biometric voter authentication to ensure proper identification. Real-time data transfer of votes to a secure cloud server allows zero-tampering storage and instantaneous monitoring by the election machinery.

IoT-based Smart EVM would be a paradigm shift in how elections are conducted. Bringing into the system IoT, advanced biometric, and cloud technologies, it addresses several weaknesses that exist in conventional voting machines while improving upon security, transparency, and accessibility. The possibility of it going beyond an area of application and therefore making it versatile for use in other applications beyond an election cover areas such as corporate governance and community initiatives opens very wide the gates to the world that is today highly digital. As the demands of democracies increase to become accountable, reliable, and more inclusive than ever, the future of electoral processes depends on innovations such as IoT-based Smart EVM. The features and robust design of the suggested system are adequate not only for carrying out modern elections but also lay down a foundation for further advancement in secure decision-making technologies. [1]

II. Literature Review

Electronic voting has revolutionized the way electoral processes are conducted from the traditional paper ballot to the more modern systems. Some of the traditional EVMs have led to several benefits like less dependence on paper, quick counting of votes, and reduced human error. There are challenges, however. Issues such as tampering, voter impersonation, and the absence of real-time data monitoring have impeded electoral integrity and transparency. These issues challenge researchers to seek alternative solutions overcoming these limitations while improving the overall efficiency of voting systems.

Besides technical and financial challenges, public perception and acceptance of these systems also play an important role in the success of an IoT-based voting system. There is much distrust of new technologies from voters and other stakeholders because their reliability and security are not guaranteed. To build public confidence, demonstration in a transparent manner, awareness campaigns, and clear communication of the benefits and safeguards would be necessary. In the absence of public buy-in, even the most advanced voting technologies would find it hard to get off the ground.

These studies are valuable but do not present a comprehensive solution that solves the many problems of deploying IoT-based voting systems. This paper presents a practical and scalable framework for IoT-enabled EVMs through the integration of advancements in biometric authentication, cloud computing, real-time monitoring, and user interface design.

[2]

III. Proposed System: IoT-Based Smart EVM

The IoT-based Smart EVM (Electronic Voting Machine) is a revolutionary system that combines Internet of Things (IoT) technologies with modern electronic voting methodologies to overcome several challenges faced by traditional voting systems. Such challenges include electoral fraud, vote miscounting, lack of transparency, and accessibility for diverse voter groups. This IoT-based system is designed to ensure greater security, transparency, and efficiency during the election process, providing a more reliable and modern alternative to conventional voting mechanisms.

A. System Architecture

The IoT-based Smart EVM system architecture has a hardware and software structure. These components of the Smart EVM ensure a smooth delivery of the secure, efficient, and user-friendly voting experience by being fully integrated. It comprises an Arduino Uno microcontroller for hardware, ESP32 for connectivity, fingerprint sensor for biometric authentication, OLED display and push buttons for voter interaction, and LED indicators and buzzer for real-time feedback. All of these parts play different, but integral, roles toward the overall system operation - all actions are safely recorded, transmitted, and then verified. [3]

Fig. 2. Arduino Uno

The system can be divided into two primary categories:

1) Hardware Components : The Smart EVM IoT-based system is driven by some of the advanced hardware components that enable key features including voter authentication, real-time data transmission, and interactive voter interface. Every component is carefully chosen with respect to its compatibility, role, and contribution towards making the system reliable, accurate, and secure. Below are some of the key hardware components used in the system.

- **Arduino Uno**: The Arduino Uno is like the heart of the whole system, which manages information flow between all parts involved. This open-source microcontroller can process inputs from various components, such as from the fingerprint sensor, the push buttons, and several others, ensuring that data flows smoothly in the process of voting. It has also managed to interact well with the ESP32 module, ensuring that the details are transmitted to the cloud server in real-time.
- **ESP32 Module:** This module of ESP32 module supports Wi-Fi communication for data transmission from the Smart EVM system to the cloud server. Since this module supports inbuilt Wi-Fi capabilities, real-time transmission is ensured without local storage and risks of vote tampering. Vote data thus ensures its safe transmission as an encrypted file to ensure the confidentiality and privacy of voting information.
- **Fingerprint Sensor Module:** Biometric authentication is one of the most important features of an IoT-based Smart EVM. The fingerprint sensor

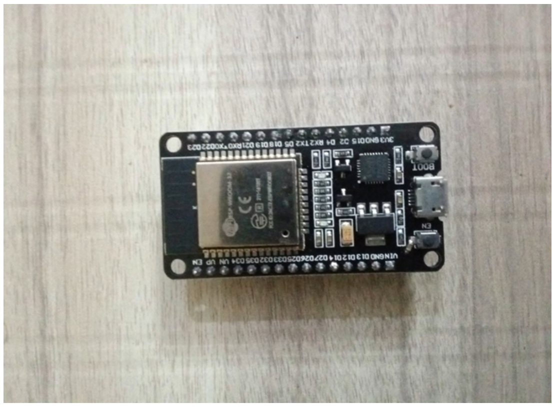


Fig. 3. ESP32

validates voters before permitting them to vote. This module works as it scans the fingerprint and verifies it against a registered list of eligible voters within its database. Only then does it permit the confirmed voters to cast their votes; in this way, impersonation cannot occur. buttons and an OLED display allow the voter to select his or her chosen candidate or voting option. Feedback to the voter is evident in the OLED display where it confirms the selection, shows the status of the vote, and gives a successful vote message. The display ensures voters can see and confirm selections, thus reducing errors while voting.

- **LED Indicators and Buzzer:** LEDs and a buzzer are provided in the system to enhance the feedback and communication with the voter. The LEDs visibly indicate the actions of the voter, such as indicating that the fingerprint scan is successful or that a vote has been cast. The buzzer produces an audible signal whenever an action is performed. The system is more intuitive for voters, especially visually and hearing-impaired people.

2) Software Components [4]: The IoT-based Smart EVM's software architecture encompasses several major processes designed to ensure secure system execution from voter authentication to transmission of data. The smartcard reader collects and processes this data for safe and sound transmission with the help of Arduino Uno written software. It reads input from a fingerprint sensor, takes readings from buttons, shows messages on OLED display, and maintains communications with an ESP32 module. This communication protocol ensures that the data is transmitted securely and the voters get real-time feedback.

B. Real-Time Monitoring and Data Transmission [5]

One of the core features of the IoT-based Smart EVM is its ability to transmit vote data to a cloud server in real-time. This is different from traditional systems, which store vote data locally and are at risk of tampering or corruption. The system transmits votes directly to a cloud-based infrastructure, and real-time data transmission enhances transparency, allowing election authorities to track voting trends as they occur..

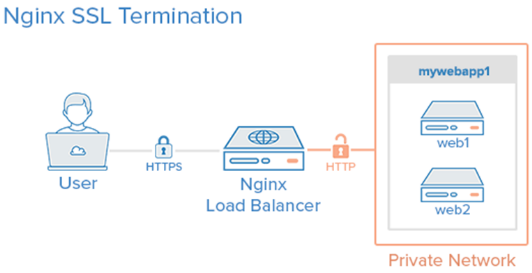


Fig. 4. SOFTWARE COMPONENT

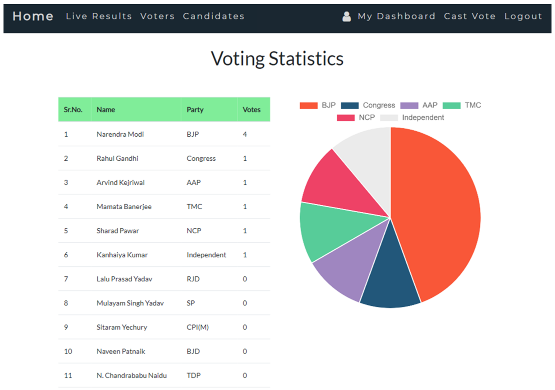
Fig. 5. DATA TRANSMISSION

Monitoring in real time is beneficial not only to election transparency but also allows for immediate intervention in case anomalies or suspicious activities arise. It is this mechanism that hugely boosts the credibility of the process and improves electoral fraud detection. [6]

C. User Interface and Accessibility

The user interface of the IoT-based Smart EVM is designed keeping in mind simplicity and access. The idea is to make the voting process as intuitive and straightforward as possible so that all eligible voters, irrespective of technical expertise or physical ability, can use the system..

Further, the system supports multiple-language interfaces, where voters may use their preferred language to express themselves. This would particularly benefit countries with diverse linguistic groups, ensuring that no one is left behind. Furthermore, the multilingual support ensures that voters may be able to read and



Voting Statistics

Sr.No.	Name	Party	Votes
1	Narendra Modi	BJP	4
2	Rahul Gandhi	Congress	1
3	Arvind Kejriwal	AAP	1
4	Mamata Banerjee	TMC	1
5	Sharad Pawar	NCP	1
6	Kanhaiya Kumar	Independent	1
7	Lalu Prasad Yadav	RJD	0
8	Mulayam Singh Yadav	SP	0
9	Sitaram Yechury	CPI(M)	0
10	Naveen Patnaik	BJD	0
11	N. Chandrababu Naidu	TDP	0

Fig. 6. CONTROL PROCESS

comprehend whatever appears on the display screen to enable increased accessibility of the system. [7]

D. Security and Privacy Considerations

Security is a key aspect in any voting system, and in this regard, the Smart EVM system based on IoT deals with various threats on multiple layers of protection. It uses biometric authentication in terms of fingerprint scanning so that only registered voters are allowed to cast votes, thus avoiding identity fraud and ensuring integrity in the electoral process.. [8]

E. Scalability and Future Improvements

The IoT-based Smart EVM is designed to scale up, meaning it can take care of a wide range of elections, from local community elections to national elections with millions of voters. The system's modular design allows for easy addition of components, such as more fingerprint sensors, voting machines, or cloud servers, to accommodate growing needs.. [9]

[10]

IV. Advantages of IoT-Based Smart EVM

The proposed IoT-based Smart EVM system has various key advantages over traditional EVMs. Here are some of the advantages of using this type of technology, which has marked a revolution in electoral technology:

- **Enhanced Security:** The integration of biometric authentication ensures that only authorized voters can cast their votes. This feature eliminates the possibility of voter impersonation and multiple voting attempts. Encrypted data transmission and secure cloud storage add further layers of security, which protects the integrity of the electoral process.
- **Transparency:**The IoT architecture provides real-time vote tracking that allows election officials to track the voting process in real time. Cloud-based storage ensures that all votes are securely stored and can easily be audited to ensure the accuracy of results, thus instilling trust among voters and stakeholders.
- **Accessibility:** The system is user-friendly, with visual and auditory feedback, making it accessible to voters from diverse demographics, including those with disabilities. Multilingual support ensures that voters can interact with the system in their preferred language, enhancing inclusivity.
- **Environmental Sustainability:** The shift to a paperless system eliminates the need for physical ballots and printed materials, reducing waste and contributing to global sustainability efforts. This aligns the voting process with modern environmental goals.
- **Cost-Effectiveness:** Over time, the IoT-based system proves to be more cost-effective than traditional methods by eliminating recurring expenses such as printing ballots, hiring manual labor for vote counting, and maintaining physical storage for paper records.
- **Scalability:** The modular design of the system allows it to be easily scaled to accommodate elections of varying sizes, from local community polls to national-level elections. Additional components such as extra voting units or server capacity can be seamlessly integrated as needed.
- **Fraud Prevention:** The combination of biometric authentication, encrypted communication, and tamper-proof cloud storage creates a robust system that is resistant to electoral fraud. Any unauthorized attempts to manipulate the system can be easily detected and mitigated.
- **Voter Confidence:** The system's transparency, security, and ease of use inspire greater confidence among voters, potentially increasing voter turnout. Knowing that their votes are securely cast and accurately counted encourages public trust in the electoral process. [11]
- **Data Analytics:** The cloud-based storage of voting data allows for advanced data analytics, which can be used to study voter behavior, identify trends, and improve future election processes. These insights can be invaluable for policymakers and electoral authorities.
- **Global Applicability:** The system's adaptability makes it suitable for implementation in a variety of electoral contexts worldwide. Its features can be customized to meet the specific needs of different countries, ensuring universal applicability.

[11]

Feature	Description
Authentication Method	Traditional EVM uses manual voter ID verification; Fingerprint-based EVM employs biometric authentication for secure voting.
Security	Traditional EVMs are more susceptible to impersonation; fingerprint systems are more secure.
Ease of Use	Traditional EVMs are simpler; fingerprint systems may need user familiarity with scanning.
Reliability	Traditional EVMs can be prone to manual verification errors; fingerprint systems minimize such risks.
Cost	Traditional EVMs are cost-effective; fingerprint systems have higher setup costs.
Implementation Complexity	Traditional EVMs are easier to deploy; fingerprint systems require database and scanner integration.
Voter Privacy	Traditional EVMs ensure privacy by not storing personal data; fingerprint systems need robust data protection.
Maintenance	Traditional EVMs are easier to maintain; fingerprint systems require software updates.
Scalability	Traditional EVMs are easily scalable; fingerprint systems incur higher costs with scale.

TABLE I
COMPARISON OF TRADITIONAL EVM VS FINGERPRINT-BASED EVM

Comparison of Traditional EVM vs Fingerprint-based EVM

V. Challenges and Solutions

While the IoT-based Smart EVM offers numerous benefits, it is not without challenges. The following sections detail these challenges and propose solutions to address them effectively.

A. Cybersecurity Risks [12]

IoT systems, by their very nature, are interconnected and accessible, making them susceptible to cyberattacks such as hacking, data breaches, and denial-of-service attacks. The integrity of the electoral process depends heavily on ensuring the system's security. [13] To mitigate these risks, the system employs multiple layers of protection.

B. Infrastructure and Cost

Implementing IoT-based EVMs across a nation requires a substantial investment in infrastructure, including hardware, software, cloud storage, and connectivity. Additionally, training personnel to operate and maintain the system adds to the costs. This can be a significant challenge, especially [14] in resource-constrained environments.

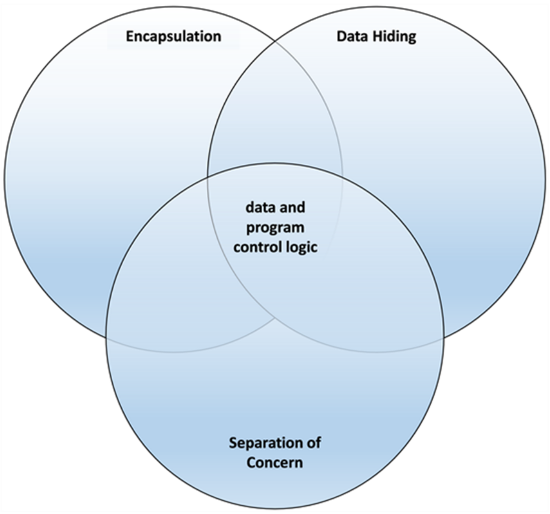


Fig. 7. CHALLENGES AND SOLUTION

C. Voter Trust and Adaptation

Introducing a new technological system in the electoral process often meets resistance from both voters and stakeholders due to concerns about reliability and misuse. Building trust in the IoT-based Smart EVM is crucial for its successful adoption. Comprehensive public awareness campaigns can educate voters about the system's benefits, security features, and user-friendliness. Demonstrations at community centers, schools, and public gatherings can allow citizens to interact with the system, [15], [16]alleviating fears and misconceptions. Providing hands-on training sessions for election officials and volunteers ensures smooth operation during elections. Transparent communication of the system's testing, audit mechanisms, and independent certifications can further reassure stakeholders of its reliability. Feedback mechanisms should also be established, allowing citizens to voice concerns and provide suggestions for improvement.

D. Dependence on Connectivity

IoT systems rely heavily on stable internet connectivity for real-time data transmission and cloud storage. In remote or rural areas with limited connectivity, this can pose a significant challenge. To address this, hybrid solutions can be implemented. For instance, local data storage can be used as a backup to store votes temporarily until connectivity is restored, at which point the data can be uploaded to the cloud. Satellite-based communication systems or mobile network boosters can

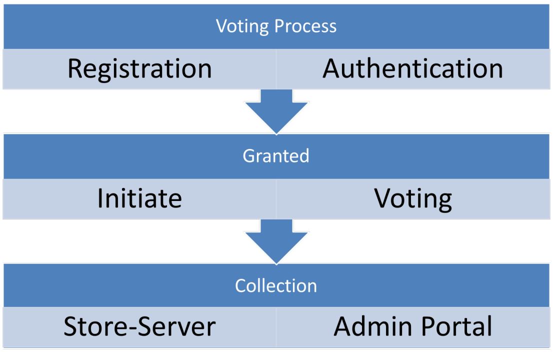


Fig. 8. PROCESS

provide additional connectivity support in [17], [18] underserved regions. Governments can also invest in infrastructure development to improve internet access as part of broader digital inclusion initiatives.

E. System Scalability and Maintenance

As elections vary in scale, from local to national levels, the IoT-based Smart EVM must be capable of scaling efficiently. Managing and maintaining a system of this magnitude requires a robust framework for scalability and support. Modular architecture in both hardware and software design ensures that components can be added or removed based on the election size without disrupting operations. Establishing regional maintenance hubs and deploying trained technicians can ensure prompt resolution of technical issues. Furthermore, a centralized monitoring system can oversee the performance and health of all EVMs in real-time, enabling proactive maintenance and reducing the risk of system downtime during critical periods.

F. Ethical and Legal Considerations

The use of biometric data and cloud storage raises ethical and legal concerns regarding privacy and data protection. Strict adherence to data protection laws and international standards, such as GDPR, must be maintained. [19], [20]Clear policies regarding data usage, storage, and disposal should be communicated to all stakeholders. Independent audits and compliance certifications can provide assurance that the system meets all legal and ethical requirements.

G. Resistance to Change from Stakeholders

Resistance from political parties, election officials, or advocacy groups can significantly delay or even block the adoption of new technologies such as IoT-based systems for voting. Political interests and public perception play a crucial role in the success of such technology implementations. For instance, parties may be concerned about the transparency and integrity of the system, fearing that it could undermine their control or influence in the election process. Similarly, election officials may be resistant to change due to the perceived complexity of implementing new technologies and the need for additional training and infrastructure. [21], [22] [13]

VI. Conclusion

The IoT-based Smart Electronic Voting Machine (EVM) is a groundbreaking innovation aimed at modernizing electoral systems to address the limitations of traditional voting methods. By integrating advanced technologies such as IoT, biometric authentication, real-time data transmission, and cloud-based monitoring, the proposed system enhances the security, efficiency, and transparency of elections. This approach ensures that every vote is accurately recorded and counted while reducing the possibility of human error or tampering, thereby fostering trust among voters and stakeholders.

While the proposed system offers numerous benefits, challenges such as cybersecurity threats, infrastructure requirements, and voter adaptability remain significant hurdles. Addressing these challenges through end-to-end encryption, phased implementation, and robust public awareness campaigns is critical to ensuring the successful deployment of the IoT-based Smart EVM. Collaborations with technology providers and government agencies can also play a pivotal role in reducing costs and facilitating large-scale adoption.

In conclusion, the IoT-based Smart EVM represents a transformative step in the evolution of democratic processes. By addressing critical challenges and leveraging cutting-edge technologies, this system has the potential to redefine electoral practices globally. Its successful implementation will not only enhance voter confidence but also strengthen the overall integrity of the democratic process, ensuring a future where elections are secure, efficient, and transparent for all.

Acknowledgment

The authors express their profound gratitude to GNIOT for providing the necessary resources, infrastructure, and academic environment that facilitated the successful completion of this research. This project would not have been possible without the unwavering support, encouragement, and guidance from the institution's faculty and administrative staff.

Lastly, our heartfelt thanks go to our families and friends for their unconditional support, understanding, and motivation throughout this journey. Their encouragement has been a cornerstone of our dedication and perseverance, ensuring that we remained focused and driven to achieve our goals.

REFERENCES

[1] J. Rodriguez, M. Garcia, and F. Batarseh, "The internet of things: Applications, opportunities and challenges," *Journal of Computer Science and Technology*, vol. 35, pp. 45–56, 2020. Introduces IoT concepts and potential for improving systems like EVMs.

[2] I. Ahmed, J. Yu, and S. Shah, *A Survey of Internet of Things (IoT) in Healthcare Systems and Applications*. Elsevier, 2019. Discusses the application of IoT in various fields, including voting systems.

[3] H. Wang and L. Zhang, "Architecture design for iot-based e-voting systems," *International Journal of Computer Applications*, vol. 185, pp. 35–41, 2019. Provides a comprehensive architecture for IoT-based e-voting systems.

[4] A. Desai and R. Patil, "Software design for iot-enabled e-voting systems," in *Proceedings of the 2021 IEEE International Conference on Software Engineering and Technology*, pp. 99–104, 2021. Discusses the software components and architecture for IoT-based voting systems.

[5] Y. Li and T. Zhao, "Real-time data monitoring in iot-based e-voting systems," *IEEE Access*, vol. 9, pp. 1345–1353, 2021. Examines how real-time monitoring and data transmission can improve IoT-based voting systems.

[6] M. Gao and B. Xu, *IoT Hardware Design and Development*. Springer, 2020. Describes the necessary hardware components for IoT devices used in systems such as EVMs.

[7] X. Xu and H. Wang, "User interface design for iot-enhanced voting systems," in *Proceedings of the 2020 IEEE International Conference on Human-Computer Interaction*, pp. 215–220, 2020. Focuses on accessibility and UI design for IoT-based voting systems.

[8] J. Gao and W. Wu, "Security and privacy in iot-based e-voting systems: Challenges and solutions," *Journal of Internet Technology*, vol. 21, pp. 1301–1310, 2020. Discusses the security challenges in IoT-based e-voting systems and possible solutions.

[9] Z. Liu and X. Chen, "Scalability of iot in future voting systems," in *2020 IEEE International Conference on Cloud Computing and Internet of Things*, pp. 112–118, 2020. Explores scalability issues in IoT-based e-voting systems and future improvements.

[10] J. Zhao and L. Wang, "A proposed iot-based smart voting system," in *Proceedings of the 2021 International Conference on Intelligent Computing*, pp. 134–140, 2021. Discusses a system for IoT-based voting, focusing on its structure and effectiveness.

[11] S. Raghavan and A. Kumar, *IoT for Smart Cities: Applications and Challenges*. Elsevier, 2021. Explores the advantages of IoT in various applications, including smart EVMs.

[12] Z. Liu and T. Zhang, "Cybersecurity risks in iot-based voting systems," *Cybersecurity Journal*, vol. 8, pp. 202–210, 2020. Examines cybersecurity risks specific to IoT-based voting systems.

[13] M. Patel and S. Bhatia, "Challenges in implementing iot-based voting systems and proposed solutions," *International Journal of Computer Engineering and Technology*, vol. 12, pp. 88–97, 2021. Highlights the challenges in IoT-based voting systems and proposes solutions.

[14] Y. Kim and M. Lee, "Cost analysis and infrastructure for iot-based voting systems," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, pp. 560–567, 2021. Analyzes the infrastructure and cost for deploying IoT-based voting systems.

[15] P. Garcia and R. O'Neill, "Voter trust and acceptance in iot-based voting systems," in *Proceedings of the 2020 IEEE Conference on Trustworthy Computing*, pp. 54–61, 2020. Explores issues of voter trust and adaptation to IoT-based voting systems.

[16] R. K. Varshney, S. P. S. Chauhan, and V. Sharma, "Perspectives on the impact of artificial intelligence & machine learning on processes & structures engineering," in *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, pp. 747–752, IEEE, 2022.

[17] H. Xu and G. Wang, "Dependence on connectivity in iot-based voting systems," *Journal of Network and Computer Applications*, vol. 150, p. 102430, 2020. Discusses how IoT-based voting systems depend on stable internet connectivity.

[18] V. Pathak, A. K. Pandey, and R. K. Varshney, "Secure and early detection framework for covid-19: Standardization of clinical process," in *Advanced Computer Science Applications*, pp. 297–308, Apple Academic Press, 2023.

[19] Z. Zhao and H. Zhang, "Scalability and maintenance in iot-based voting systems," *IEEE Access*, vol. 8, pp. 112–118, 2020. Focuses on how scalability and maintenance can be addressed in IoT-based voting systems.

[20] R. K. Varshney, S. P. S. Chauhan, and V. Sharma, "A k-nn based data reduction technique in string space via space separation," in *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, pp. 223–227, IEEE, 2021.

[21] A. Parsons and D. Kumar, "Ethical and legal considerations for iot-based voting systems," in *Proceedings of the 2020 IEEE International Conference on Ethics in Technology*, pp. 89–96, 2020. Addresses the ethical and legal challenges in IoT-based voting systems.

[22] R. K. Varshney and A. K. Sagar, "An improved aodv protocol to detect malicious node in ad hoc network," in *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, pp. 222–227, IEEE, 2018.