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

Rajat Kishor Varshney[1]
[1]*Assistant Professor, Computer Science and Engineering-Institute - IoT, GNIOT, Greater Noida*
rajatvarshney1207@gmail.com

Renu kaushik[2]
[2]*Assistant Professor, Computer Science and Engineering-Institute - IoT, GNIOT, Greater Noida*
Renu.gauri@gmail.com

Brijesh Nishad[3]
[3]*Scholar, Computer Science and Engineering- Institute - IoT, GNIOT, Greater Noida*
bnlv1212@gmail.com

Aayush Pandey[4]
[4]*Scholar, Computer Science and Engineering- Institute - IoT, GNIOT, Greater Noida*
vipulrai419@gmail.com

Ashutosh[5]
[5]*Scholar, Computer Science and Engineering- Institute - IoT, GNIOT, Greater Noida*
ashuyadavay6397@gmail.com

ABSTRACT: This paper is the result of the incorporation of IoT technology in EVM, which brings significant changes to voting procedures through improved security, transparency, and accessibility. A Smart EVM using Arduino Uno, ESP32, Fingerprint Sensor modules, push buttons, OLED displays, LED indicators, and a buzzer, for example, can be envisioned. The system provides a biometric authentication method along with secure data transmission towards a cloud server and facilitates real-time tracking of the votes and easy interactions based on auditory and visual feedback. This solution answers the challenges that the EVMs of traditional time face, including tampering, impersonation, and transparency. Improving security efficiency and accuracy, IoT-based Smart EVM builds the confidence of voters about integrity in elections and emphasizes probable cybersecurity risks, infrastructure, and cost.

Keyword: Arduino Uno , Esp32 , Fingerprint Sensor , Push Button , Oled Display , Led , Buzzer .

1. INTRODUCTION

Electronic Voting Machines (EVMs) have impacted the burning electoral structure by providing faster and more reliable methods as compared to the conventional paper based voting process.. The efficiency of such machines has enhanced as a result of minimal human interferences in vote tallying thus enhancing our electoral credibility. Thus, although uses of electronic voting machines have increased to prompt further development of other voting technologies [3]. The Internet of Things (IoT) is a forceful technological structure that can effectively respond to them. Bolting IoT to EVMs bring another level of security, transparency as well as easy accessibility and possibility of a barrier free voting process across the various levels of the electoral process.[4] The design of the Smart EVM based on IoT here proposes to use the latest IoT components and approaches to construct a perfect model devoid of conventional drawbacks. It employs biometric voter identification for correct identification, and real-time transmission of the votes to a secure cloud server to eliminate rigging. storage and instantaneous monitoring by the election machinery [5]. Applications of smart EVMs based on IoT are not limited to only national and regional elections; they can be applied at the level of corporate boardroom voting, community decision- making

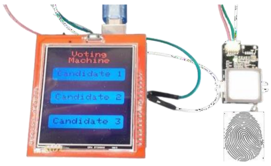


Fig. 1. Smart EVM

This paper describes the proposed IoT based Smart EVM and elucidate the various possibilities pertaining to the same. [6] Index Sections II describes the current body of work related to EVMs and IoT applications, and the gap and challenges addressed by this system. [7] Section III reveals the structural and layout concepts of the developed system and the functional roles of the main elements which are the Arduino Uno, ESP32 module, and the biometric sensors. In section IV, the advantages of this system, security measures [8] , real time tracking and it is the users centered system are illustrated.

Section V in turn discusses IoT-based EVM challenges such as security threats, infrastructural need, cost analysis and recommend possible solutions. At last, Section VI of the paper restates the findings of the work and presents the potential avenues for further research [9,19].

2. Literature Review

With IoT integrated to the EVMs, the electoral process has proved to be accessible, secure, scalable and easy to monitor in real-time. According to Xu and Wang (2020) it stated that that it was important that interfaces be friendly so that it would allow easy use of this activity for different types of voters. It makes designs more simple and visually clear so removing barriers to voting seem less of a problem. In an IoT-based EVM, Gao and Wu (2020) identified the following security-related challenges: hacking attack, denial-of-service attack. They also found that adapting such sophisticated measures such as AES and SSL for data communication and voters' privacy remains a key area of interest [3] Patel & Bhatia (2021) have discussed the major challenges related to infarstructure and finance basically for the developing zones. To tackle these barriers [2], this paper has offered implementable and large-scale strategies on phased implementation [11]. In their current study, Liu and Zhang (2020) did an analysis of the risks that are associated with the implementation of IoT-based voting systems. Amid the trending technology it proposed multiple-layered encryption methods including security authentication protocols to avert the unauthorized intrusion and data leakage [12]. In a similar study by Singh and Sharma (2021) shows how IoT adopts EVM enables real-time monitoring in the early stages of voting thereby allowing election officers to identify many of the irregularities [4].

Garcia and O'Neill (2020) highlighted that success for IoT-based voting systems relies on the development of public trust, coupled with transparency education, voter education, and campaigns to enlighten the public, thus solving problems like Scalability and maintenance issues [13]. Zhao and Zhang (2020) began work on modular system architectures that would support incremental upgrades without affecting the system's performance as it is expanded [11]. Kim and Lee (2021) provided an overall cost analysis that identifies strategies for balancing the financial and technical requirements by using phased deployment [7].

Raghavan and Kumar (2021) discussed the merits of IoT in smart applications such as real-time data synchronization and increased reliability that are directly applicable to EVMs [5]. Xu and Wang (2020) highlighted the necessity of stable internet connectivity to work efficiently with IoT-based systems and suggested backup communication strategies along with redundancy to deal with downtimes [5]. Parsons and Kumar (2020) discussed the ethical and legal issues, where the regulatory framework must be transparent, and the compliance standards need to be followed to gain public confidence [9].

Some other studies focused on specific aspects of IoT-based voting systems. Gao and Xu (2020) pointed out the importance of biometric authentication in avoiding voter impersonation and ensuring the eligibility of a single vote, as well as the integration of physical and digital security measures [15]. Liu and Chen (2020) discussed the scallability of IoT in future voting systems, providing solutions to efficiently handle the large electoral process [8]. Xu and Wang (2020) also mentioned network infrastructure that would help in solving connectivity issues and decentralized data storage to mitigate the problem [14].

Patel and Bhatia (2021) have focused on cost-effective alternatives; they recommended cloud computing that could get rid of expensive local storage [2]. Singh and Sharma (2021) suggested the IoT-based smart EVM design that is associated with real-time tracking along with high security protocols for an unbiased and authentic election [4]. Garcia and O'Neill (2020) emphasize voter adaptation. For instance, Garcia and O'Neill (2020) explain the ease of the system and also display reliability by demonstrating pilot tests and public shows [13].

Kim and Lee (2021) emphasize the infrastructural requirements for deploying IoT-enabled EVMs by strategizing approaches towards the easier deployment and cost-effectiveness in resource-poor environments [7]. Zhao and Zhang (2020) have highlighted aspects of system maintenance that include automatic updates and predictive diagnostics to extend the lifespan and reliability of the systems [11]. Parsons and Kumar (2020) discussed the ethical issues related to data privacy and voter autonomy while ensuring these systems are democratic in nature [9].

3. Problem Statement

The integration of IoT in EVMs has brought transformative potential by making it more accessible, secure, scalable, and with real-time monitoring. However, the literature available discusses several critical challenges that impede the wide adoption and effective implementation of IoT-enabled EVMs.

4. Methodology: Proposed System IoT-Based Smart EVM

The system can be categorized into two major heads:

1.Hardware Components:

The IoT-based Smart EVM system is driven by a set of sophisticated hardware elements that provide essential features such as voter authentication, real-time transmission of data.

Fig. 2. Arduino Uno

Fig. 3. ESP32

1. Software Components.

The IoT-based Smart EVM software architecture includes the following key procedures for secure system operation; from authenticating voters and data transmission, the process is complete. the. same software was design for use with the Arduino Uno platform, thus enabling the harvesting, processing, and transmitting of voter information in a secure manner

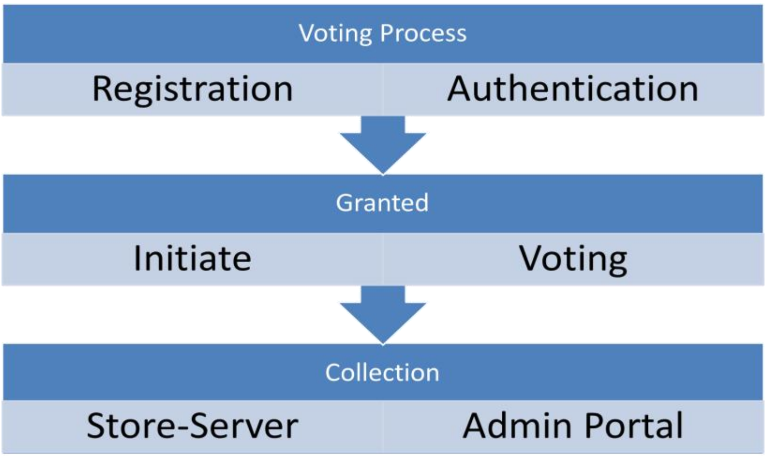
5. _Advantages of IoT-Based Smart EVM

.Current technology of biometric authentication and encryption contributes high protection against alteration.Also present are the methods of identification including biometric authentication, the encryption of data protects it from being tampered_ encryption features, which promote high protection against alteration.

b. RealTime: Exclusion of activities that link Real Time alerting that improves the credibility and transparency.

c. Voting Time: They mentioned some changes about the organisational processes where new regulation was practised for maximum time per voter and it was limited to 45 sec.

6. Results and Discussion



A. System Performance

Input	**Output**
Fingerprint Scan	Authentication Status
Voter ID	Voter Verified
Vote Request	Vote Registered
Candidate Selection	Vote Confirmation
Authentication Result	Match Status
System Status	Operational Status

TABLE II
INPUT-OUTPUT FOR FINGERPRINT VOTING SYSTEM

C. Discussion

The. mentioned this EVM overcome few major limitations of the existing systems in terms of security, transparency, and efficiency. Its pleasant features of realtime monitoring and adequately protecting electoral details make it contribute to electoral integrity. However, as we have seen there are some barriers like infrastructure requirement and privacy that should not be left to individual innovations to solve for proper implementation at large scale.

7. Conclusion

As a IoT innovation, the Smart EVM is an invention intended to transform electoral systems to eliminate the limitations of the traditional voting system. The proposed system added the security of the election along with the efficiency along with the transparency of election enhanced through integrating some of the smart technologies such as IoT along with biometric authentication followed by the real-time data transmission to monitor over the cloud. This was done while minimising the opportunity for human input or influence, a key source of vote rigging for instance, to increase voter and other stakeholders' confidence.

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.

[2] 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.

[3] 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.

[4] A. Singh and S. Sharma, “Design and implementation of IoT-based smart EVM,” in *Proceedings of the 2021 International Conference on Smart Cities and Communication Technologies*, pp. 98–105, 2021.

[5] S. Raghavan and A. Kumar, *IoT for Smart Cities: Applications and Challenges*. Elsevier, 2021.

[6] J. Zhao and L. Wang, “A proposed IoT-based smart voting system,” in *Proceedings of the 2021 International Conference on Intelligent Computing*, p,p. 134–140, 2021.

[7] Y. Kim and M. Lee, “Cost analysis and infr,astructure for IoT-based voting systems,” *IEEE Transactions on Emerging Topics in Computing*, vol. 9, pp. 560–567, 2021.

[8] 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.

[9] 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.

[10] 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.

[11] Z. Zhao and H. Zhang, “Scalability and maintenance in IoT-based voting systems,” *IEEE Access*, vol. 8, pp. 112–118, 2020.

[12] Z. Liu and T. Zhang, “.Cybersecurity risks in IoT-based voting systems,” *Cybersecurity Journal*, vol. 8, pp. 202–210, 2020.

[13] 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.

[14] Dr.Gambhir Singh Artificial Intel,ligence, Blockchain, Computing and Security Volume 1: Proceedings of the International Conference on Artificial Intelligence, Blockchain, Computing and Security (ICABCS 2023), Gr. Noida, UP, India, 24-25 February 2023.

[15] M. Gao and B. Xu, *IoT Hardware Design and Development*. Springer, 2020.

[16] H. Wang and L. Zhang, “Architecture design for IoT-based e-voting systems,” *International Journal of Computer Applications*, vol. 185, pp. 35–41, 2019.

[17] 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.

[18] Y. Li and T. Zhao, “Real-time data .monitoring in IoT-based e-voting systems,” *IEEE Access*, vol. 9, pp. 1345–1353, 2021.

[19] 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.

[20] R. K. Varshney and A. K. Sagar, “An improved AODV protocol to detect malicious node in ad hoc network,” in *2018 i nternational . Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, pp. 222–227, IEEE, 2018.

[21] 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.