WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Remote E-Voting System: Challenges and Opportunities

Dr. Kamalraj R[1], Ashish Kumar[2]

[1]Professor, Department of CS & IT, JAIN (Deemed To Be University) Bangalore, INDIA r.kamalraj@jainuniversity.ac.in
[2]Student, Department of CS & IT, JAIN (Deemed To Be University) Bangalore, INDIA ashishsinghssm0@gmail.com
DOI: https://doi.org/10.55248/gengpi.5.0324.0608

Abstract—

Electronic voting, sometimes known as "e-voting," has evolved as a cutting-edge method to simplify the political process while providing voters with convenience and accessibility. Remote e-voting devices may become more secure, effective, and user-friendly if artificial intelligence (AI) is implemented. In this study, the function of AI in distant e-voting systems is examined, along with the difficulties in implementing it and possible solutions.

This paper explores the security issues of distant electronic voting in open elections. We look at the viability of conducting national federal elections online in particular. In terms of the security of the hosts and the Internet itself, this article focuses on the shortcomings of the infrastructure that is currently in place. We come to the conclusion that our infrastructure is not suitable for distant Internet voting at the moment.

Keywords— Remote e-voting, AI, Natural language processing, challenges, solutions.

Introduction:

In many countries, technology is heavily used during elections, which is sometimes required. Creating voter records, drawing electoral boundaries, supervising and training employees, printing ballots, putting voter education programs into action, recording votes cast, tabulating votes, and collecting and announcing election results are a few examples. Technology may improve political accountability, simplify election administration, and save overall expenses if it is implemented appropriately.

Remote voting may take place in person somewhere other than an assigned polling station or at another time, or votes may be cast by an appointed proxy.

In India, many political parties have requested the EC to make sure that NRIs (Non-Resident Indians), or migratory workers, who are unable to afford to fly home to fulfil their right to vote, can cast ballots for their region from the place they are employed in.

Electronic voting has the ability to completely change how countries organize elections by providing benefits including lower costs, more accessibility, and quicker result processing. While incorporating AI into voting systems has the potential to increase their functionality, doing so also presents a number of difficulties that must be resolved if the election process is to be trusted and remain legitimate.

The rapid development of AI technologies has opened the door for creative uses in a variety of fields, including the political process. With the ability to ensure accuracy, security, and transparency, remote e-voting devices with AI capabilities have the potential to completely change the way elections are conducted. E-participation has been defined as the use of ICT supported platforms to facilitate the participation in the democracy and governance [1].

This study used an organized mapping process to review the literature and clarify these problems. This essay contributes the following: Identifying well-known ideas for artificial intelligence (AI) remote electronic voting and their methods of verification, highlighting ideas that made use of well-known cryptographic techniques, and emphasizing ideas that focused on cost and time. Additionally, it lists performance metrics, the main benefits and drawbacks of various platforms, and the most popular machine learning techniques. It also highlights various potential research directions for creating a technologically based remote polling system.

Initially, e-voting was proposed to be a solution to the challenges of paper-based voting to ensure accurate and bias-free elections [2]. The studies show that the utilization of electronic voting may entail the following challenges: data integrity, reliability, transparency, the secrecy of the ballot, consequences of breakdown, uneducated voters, specialized IT skills, storage of equipment, security, consequences of fraud and cost [3].

Literature review:

Systems for electronic voting (or "e-voting") have drawn interest as a way to improve and modernize the political process. In recent literature, several aspects of artificial intelligence's potential and difficulties have been discussed in relation to the integration of distant e-voting machines.

Remote electronic voting machines (RVMs) are a proposed voting system for domestic migrants in India, who often face difficulties in exercising their voting rights due to internal migration. The Election Commission of India (ECI) has developed a prototype of RVMs and invited political parties to witness its demonstration on January 16, 2023[4]. The main objectives of RVMs are to increase voter participation and turnout by enabling migrant voters to vote from their place of work or residence without travelling to their home district or state [5]. To make the voting process more believable, accessible, and palatable to all parties involved.

A group of independent experts from Germany's Platform for AI of the Federal Ministry of Education and Research (BMBF) and the National Academy of Science and Engineering (acatech) thoroughly examined the potential and risks that AI posed to the elections in Germany in September 2021. Drawing from their work, this Spotlight introduces the most important and currently significant AI-driven opportunities to influence elections and individual opinion forming [6].

The results of a web search reveal a few other nations that have utilized or tested with remote voting systems, such as: Austria, Estonia, Switzerland and Norway. However, numerous nations have also abandoned or postponed their initiatives for remote voting, including: Ireland, The Netherlands, Germany and United Kingdom.

1. Role of AI in Remote E-Voting Machines:

Artificial Intelligence (AI) has revolutionized the way political campaigns are conducted. AI is being used to predict voter behavior, develop prediction models, and identify voters most likely to support a specific candidate.

The general speech of the voter can be learned via AI. It can assist voters in being informed about various political topics and assisting them in making decisions about candidates through the use of micro-targeting campaigns. Artificial Intelligence (AI) has the capability to acquire knowledge from voter behavior and data, including voting trends, preferences, feedback, and errors. This can assist in detecting and fixing abnormalities, mistakes, or attacks in addition to improving the remote electronic voting system's usability, performance, and dependability.

1.1 Voter Authentication:

By analysing biometric information such as voice patterns, facial recognition, and fingerprint data, AI can be used to improve voter authentication procedures. This guarantees that the e-voting system is only accessible to legitimate voters.

Voter lists, candidates, and election duration are all part of the election preparation service. Verifying an individual's eligibility to vote is the basis of voter registration. It is the duty of voters to register before to the election [7].

1.2 Fraud Detection:

Artificial intelligence (AI) systems are able to recognize patterns and abnormalities that are symptomatic of dishonest behaviour, including manipulating the results or voting twice. Unusual voting patterns can be recognized by machine learning algorithms, which can then generate alerts for more thorough study.

1.3 Natural Language Processing (NLP) for Accessibility:

In order to increase inclusivity and enable a wider spectrum of voters to participate, AI-powered NLP technology can help voters with impairments by translating based on text polling choices into speech or visual language.

1.4 Predictive Analytics:

Artificial intelligence (AI) can produce insights into probable voter participation and preferences by analysing past voting data and societal patterns; this knowledge can aid in distributing resources and campaign strategy.

Challenges:

Various legal, technological, and ethical procedures as well as agreements can be used to mitigate any concerns associated with the usage of AI systems in relation to elections. This specifically entails guarding against false or manipulative information as well as the curation or automated filtering of media material that is crucial for forming political opinion. The labelling specifications for material produced by AI as well as misinformation in general, as well as the implementation of effective platform standards, are among the key regulations. Other regulations include the transparency of selection processes and the right to justification in the context of electoral content moderation.

In order to ensure the efficiency of the process, the voter needs to have access to and authentication from the system using an identifying number, certain personal data, or an encrypted key. The system ought to demand that voters generate secret numbers throughout the registration procedure in order to cast their ballots. With the use of these codes, those with voting rights ought to have no trouble casting their ballots.

The last worry we have is that an attacker can rig an electronic election by simply creating enough doubt about the outcome; they don't even need to compromise the system. In the past few years, social media disinformation efforts have become a menace to society, as evidenced by their capacity to cast doubt on the voting process during the 2020 US presidential election. It made sense for more people to choose to vote by mail in reaction to the pandemic. A Harvard Kennedy School study found that around 65% of Trump voters believed that Trump was the actual winner of the 2020 election [8].

2.1 Security and Privacy:

Elections always require a high level of security in order to protect voter privacy and the integrity of final results. Implementing AI in remote e-voting systems raises concerns about the security and privacy of voter data. Malicious actors could attempt to manipulate AI algorithms or exploit vulnerabilities in the system.

2.2 Bias and Fairness:

Certain demographic groups may be excluded by artificial intelligence models used for identifying fraud or authentication due to biases that they may display. Furthermore, voting might occur in an unregulated setting. Obtaining an individual's free and uninhibited vote might be challenging. A significant difficulty is ensuring equity and fairness in based on artificial intelligence electronic voting systems.

Trust in the government was a contributor to the success of the introduction of e-voting in Estonia, and their president even advises countries to “build trust before introducing e-voting”[9].

2.3 Technical Reliability:

Dependence on AI increases the chance of technological mistakes or malfunctions, which might scuttle the election. Voters must have a solid internet connection in order to participate. Only a small number of countries have widespread internet access, are able to access it, and utilize e-government services. It is crucial to create resilient artificial intelligence that can cope with a range of demands and circumstances.

2.4 Verification and Transparency:

Given the complexity of artificial intelligence, accurate justifications for its choices might be challenging. To keep the public's trust, outcomes provided by AI must be transparent and verifiable.

Additionally, a biometric voter verification technology that incorporates facial recognition software may result in false positives or negatives in voters verification, aiding in fraud or depriving persons of their right to vote.

3. Trust Issues:

Legitimacy and a successful democracy depend greatly on the confidence that voters and other election stakeholders have in the outcomes and the electoral process. Stakeholders, including voters, should be able to trust that the election results accurately reflect the will of the electorate [10].

3.1 Believe in the Government Organization in Charge of Elections:

Consequently, all parties involved in the election process, including voters and political parties, must be able to have faith in the impartiality and independence of the organization in charge of conducting the elections. Voter participation in an election may be influenced by one's intention to accept or use voting technology, according to one study [11]. Election stakeholders will view the implementation of any election technology—or any election reform, for that matter—with scepticism, resistance, or non-participation if there is any mistrust among the electorate. This includes remote e-voting technologies.

3.2 Believe in Remote E-voting Technologies:

Any voting technology's acceptance can be influenced by users' perceptions of its advantages and disadvantages. Voters' perceptions of the security and privacy protections offered by remote electronic voting may therefore be negatively impacted by prior knowledge of and experience with electronic systems that have been beset by security and privacy difficulties[12]. It is imperative to illustrate the measures taken to safeguard the privacy and security of the internet voting system in order to enhance voters' confidence in these technologies. One way to achieve this is by implementing government education programs and making sure the system is subject to testing by both experts and voters.

4. Solutions and Future Directions:

4.1 Robust AI Models:

Developing AI models that are resistant to attacks and capable of adapting to new threats is essential. Ongoing research into adversarial machine learning can contribute to this goal. Track anomalies and unwanted access in AI algorithms on a constant basis. Utilize auditing tools powered by AI to quickly detect and address security problems.

4.2 Ethical AI Design:

Integrating ethical considerations into AI design, development, and deployment can help mitigate biases and ensure fairness in e-voting systems. In order to reduce prejudice, make sure that the training data used to create artificial intelligence algorithms is diverse and inclusive of all voters.

To address any new prejudices or difficulties with justice, conduct routine audits and evaluations of artificial intelligence systems' bias.

4.3 Multi-layered Security:

Implementing multi-layered security protocols, including encryption, blockchain, and continuous monitoring, can enhance the overall security of e-voting systems.

Investigate methods like homomorphic encryption and federated learning to keep voter data private while AI algorithms work on it.

4.4Voter Education:

Educating voters about the benefits and functioning of AI in e-voting can increase public acceptance and understanding of the technology. To educate people about the advantages, functionality, and security features of AI-enhanced electronic voting, launch extensive voter education campaigns.

DISCUSSION

The goal of this study was to examine how electronic voting technology might spread within the South African setting by utilizing three dimensions from Rogers DoI model. From the viewpoints of the IEC and the voters, the study also investigates potential influences on the adoption process. The research indicates that the three elements would have a significant impact on the IEC and voters' intentions to use electronic voting. A number of elements came to light as a result of the research: environment, resources and infrastructure, technology's usefulness, ease of use, and trustworthiness. These criteria are predicated on the patterns that surfaced from the information obtained from the interview and the questionnaire.

A group of specialists from IIT Madras and other IITs will assist the ECI in conducting a pilot program of the remote voting technology in the following two to three months. The ECI plans to roll out the remote voting system in stages, starting with one state's capital city and eventually spreading to various states and regions. The ECI hopes to make the remote voting facility available for all eligible voters in the country by 2027[13].

The results indicate that the acceptance of electronic voting may be influenced by factors such as technological trust. The participants believed that concerns about privacy and security might make it difficult for them to trust electronic voting technologies and, as a result, adopt them. These participants believed that if electronic voting were not sufficiently safe, their right to vote may be in jeopardy and their participation information could be changed or misused by hackers. This belief was based on their knowledge of or experience with previous computerized systems that have been impacted by privacy and security concerns.

CONCLUSION

Election efficiency and accessibility can be greatly increased by incorporating AI into electronic voting systems. To ensure the legitimacy and security of the democratic process, it is imperative to solve the related issues. It is conceivable to create AI-driven E-Voting systems that respect the concepts of justice, transparency, and inclusivity through vigorous study and collaboration.

The idea of a remote e-voting facility is impressive, and it is likely to enhance democracy. However, there are some obstacles to overcome, and these obstacles are being addressed to make sure that the system has the right checks and balances in place to make voting remotely free, fair, and secure in every way.

The primary goal of this study is to examine and analyse recent studies on remote voting systems, which largely uses artificial intelligence (AI) technologies. However, creating and deploying an electronic voting system is not a straightforward task. Authentication, security, reliability of data, transparency, and credibility are only a few of the issues that voting technology must address. A study on artificial intelligence technology for remote electronic voting is compiled in this report through a methodical mapping investigation.

Ultimately, voting ought to be accessible and embraced by the whole public since it is a fundamental right rather than a privilege for every individual. The Remote E-Voting System can be implemented, even if it is a difficult task. Does electronic voting have a future in India? Time will tell, but it's crucial to recognize that there's more to remote electronic voting than just a technological difficulty.

REFERENCES

[1] Islam, M. S. (2008) Towards a sustainable e-Participation implementation model. European Journal of ePractice, Vol.5, No.10 .

[2] Daramola, O.; Thebus, D. Architecture-Centric Evaluation of Blockchain-Based Smart Contract E-Voting forNational Elections. Informatics 2020,7, 16.

[3] Esteve, J.B.; Goldsmith, B.; Turner, J. International Experience with E-Voting./IFESIVreport.pdf (accessed on 15 July 2020).

[4] How do remote electronic voting machines work? - The Hindu, January 04, 2023.

[5] Election Commission To Demonstrate Remote Electronic Voting Machines - Everything You Should Know (thequint.com), 30 Dec 2022.

[6] AI and Elections – Observations, Analyses and Prospects | Heinrich-Böll-Stiftung | Tel Aviv - Israel (boell.org),27 January 2022 by Jessica Heesen.

[7] https://www.researchgate.net/publication/343565582_A_Systematic_Review_of_Challenges_and_Opportunities_of_Blockchain_for_EVoting

[8] G. Pennycook and D. G. Rand, “Research note: Examining false beliefs about voter fraud in the wake of the 2020 presidential election.,” Harvard Kennedy School (HKS) Misinformation Review., 2021.

[9] P. Teffer, “Build trust before you introduce e-voting, says estonian president).” https://euobserver. com/digital/138394, June 2017. Accessed: March 10th, 2021.

[10] S. Kimbi, Y. Nkansah-Gyekye, and K. Michael, "Towards A Secure Remote Electronic Voting in Tanzania Organizational Challenges," Advances in Computer Science: an International Journal, vol. 3, no. 5, pp. 122-131, September 2014.

[11] Z. Irani, P.E.D Love, and A. Montazemi, "eGovernment: past, present and future," European Journal of Information Systems, vol. 16, no. 2, pp. 103-105, 2007.

[12] M. Achieng and E. Ruhode, "The Adoption and Challenges of Electronic Voting Technologies Within the South African Context," International Journal of Managing Information Technology, vol. 5, no. 4, pp. 1- 12, November 2013.

[13] Remote Voting Facility in India - Explained, Pointwise -ForumIAS Blog, March 24th, 2021.