Survey On Secure E-Voting Platform

Mr.Sanskar Vilas Patil
Rajendra Mane Polytechnic, Ambav(Devrukh)
Department of Computer Science
sanskarpatil1826@gmail.com

Miss. Komal Mahadev Parit
Irth Solution
Software Developer
komalparit295@gmail.com

Mr.Sourabh Suresh Patil
Government Collegeof Engineering,Ratnagiri
Artificial Intelligence & Data Science
sourabhpatil9597@gmail.com

Mr. Prashant Bajirao Patil
Mphasis Limited Department of
Delv Senior Software Engineer
prashant.patil033@gmail.com

ABSTRACT:

E-voting systems are increasingly being explored with the aim of taking over from traditional paper-based voting and may offer several advantages, including efficiency, accessibility, and cost-cutting. These systems include DRE machines, internet-based voting, to even blockchain-enabled voting solutions. However, this shift toward e-voting is attended by a raft of significant hurdles on security, secrecy in voting, dependability of the systems, and scalability.

This survey paper covers the current status of e-voting systems and related work and literature regarding the design, implementation, and evaluation. These topics will range from security vulnerabilities regarding DRE and Internet voting to privacy and anonymity concerns with respect to maintaining confidentiality of voters, accessibility and usability of e-voting platforms for the diverse voter population, and the increasingly emerging blockchain technology that provides secure and transparent processes toward voting. The survey underlines important gaps in present research and points to a number of future directions that might help in building up integrity, transparency, and trustworthiness in e-voting systems. In overcoming the challenges lying ahead, e-voting has the potential to significantly improve democratic processes and enhance voter participation.

INDEX TERMS : ***Online Voting , Secure Voting Platform, Voter Authentication, OTP Verification, SMS Gateway, Encryption, Web Application Development, Voting Results , Election Management System***

I.INTRODUCTION

Electronic voting (e-voting) systems have emerged as a significant advancement in electoral processes, leveraging technology to improve efficiency, accessibility, and accuracy in elections. Traditional voting methods, such as paper ballots, are often prone to human error, fraud, and logistical challenges. E-voting systems aim to address these issues by digitizing the process, offering solutions that range from Direct Recording Electronic (DRE) voting machines used at polling stations to internet-based voting systems that allow citizens to vote remotely.

The adoption of e-voting systems has the potential to enhance voter participation by making the process more accessible, particularly for individuals with disabilities, those living abroad, or people in remote locations. Moreover, e-voting can reduce the time required for counting votes and provide faster, more accurate results.

However, the implementation of e-voting systems comes with significant challenges, particularly concerning security, privacy, and public trust. Ensuring that e-voting systems are secure from cyberattacks, protecting voter anonymity, and verifying the integrity of election results are critical concerns. Additionally, usability issues, including accessibility for people with disabilities and technological literacy, must be addressed to ensure that all eligible voters can participate effectively.

This paper explores the development, implementation, and challenges of e-voting systems, with a focus on security, usability, and accessibility. It provides a survey of existing systems, associated research, and potential future developments, highlighting both the benefits and risks involved in modernizing the electoral process.

II. ASSOCIATED WORK

The integration and refinement of successive technologies have marked the development of e-voting systems, all intended to transform the manner in which elections are conducted. From the early use of DRE devices to the latest thoughts on the utilization of blockchain solutions, the development of e-voting technologies reflects an ever-growing determination to overcome those evident limitations of traditional paper-based voting. This section covers the historical and state-of-the-art efforts in e-voting research, focusing on the main technological innovations in security measures, as well as pending challenges faced by these systems.

1. Direct Recording Electronic Systems:

DRE systems were among the first to be widely deployed with regard to e-voting technologies. In these systems, voters are able to directly cast their votes into an electronic system, without their vote being recorded on a paper-based ballot and then counted manually [1]. Early DRE systems aimed at minimizing human error and quickening the tallying process to give an efficient solution from other older methods. It did not take long, though, for concerns about security and transparency. Then, studies started to reveal that DRE machines were vulnerable to at least several kinds of malignant attacks, including the installation of malicious software capable of falsifying vote counts undetectably [2]. In this regard, numerous research studies have been done to enhance the security protocols of DRE systems, including the addition of voter-verified paper audit trails that create a physical record of every vote cast [3].

2. Internet Voting:

Another form of voting that came along was internet voting. It came with the goal of increasing accessibility by enabling voters to cast their votes from any location using the internet. This was particularly appealing to absentee voters, the military stationed abroad, and the disabled [4]. Convenience and the probability of increasing voter turnout notwithstanding, internet voting has equally been faced by a number of serious security challenges. Among other serious security threats to the integrity of internet voting, DDoS attacks, phishing, and man-in-the-middle attacks have been identified [5]. This led the researchers to explore applications of advanced cryptographic techniques such as end-to-end encryption and secure multi-party computation in safeguarding voter information and maintaining confidentiality and integrity of votes [6]. Many times, the adoption of such security features provides a trade-off between system complexity and user accessibility.

3. Blockchain-Based E-Voting Systems:

Among the revolutionary solutions proposed to address the challenges related to e-voting, blockchain technology has been outstanding, offering a completely decentralized and transparent record of votes that is resistant to tampering [7]. Blockchain-based e-voting systems leverage blockchain's intrinsic security features, including cryptographic hashing and consensus mechanisms, to achieve end-to-end verifiability and broader confidence by voters in the process [8]. These systems give voters an independent method to verify that their votes have been cast and tabulated correctly without disclosing their privacy. In fact, pilot projects, along with several academic studies, have already proven the feasibility of blockchain-based voting. However, scalability remains a big challenge, especially in nation-scale elections with millions of voters [9]. A couple more issues regarding the computational and energy costs of blockchain transactions prevent its wide-scale usage for election purposes [10].

4. Biometric Authentication in E-Voting:

Other developments have integrated biometric technologies such as fingerprint recognition, face recognition, and iris scanning in attempts to further enhance voter authentication and reduce fraud in e-voting [11]. Biometric authentication can be used in constructing a robust identification of the voters for the purpose of ascertaining that only eligible persons vote in an election. Biometric authentication, however, engages sensitive information about the personality of the individuals concerned and raises the issue of misuse of such information should it fall into the wrong hands or be compromised in any breach [12]. Researchers have voiced the need for stringent data protection measures and laws that govern the usage of biometric information in voting systems [13].

5. End-to-End Verifiable Voting Systems:

Among the most significant attributes in state-of-the-art e-voting systems is end-to-end verifiability; this enables the voter to verify whether his or her vote has been correctly cast, recorded, and counted, without revealing the individual choice:. There are systems, such as Prêt à Voter, Scantegrity, and Helios, each using different cryptographic protocols for that purpose, be it homomorphic encryption or mix-nets [15]. This kind of system could even provide a voter with a receipt-some sort of verification code-that would enable him or her to verify that his or her vote is indeed included in the final list, thus increasing transparency and confidence in the process. These systems are generally quite sound from the theoretical viewpoint, but in practice, most of them face problems related to voter understanding and usability because the verification processes can be somewhat complex and barely understandable by the average voter [16].

6. Legal and Regulatory Issues:

The deployment of e-voting systems also needs to consider some legal and regulatory issues. The legitimacy of e-voting depends upon the compliance of e-voting with the set of standards developed by national and international electoral organizations. Legal frameworks need to take care of the issues like data protection, system certification, and post-election auditing as ways of making sure that the process maintains its integrity [17]. Other researchers have discussed that comprehensive directives and best practices must be developed so as to guide the implementation of an e-voting system by ensuring security, transparency, and accessibility meet the set standard criteria for use [18].

7. Comparative Studies and Pilot Programs:

Different pilot projects and comparative studies about different e-voting technologies were carried out in various countries and jurisdictions. For instance, Estonia has been at the forefront of internet voting, having first conducted it during national elections in 2005 [19]. Comparative analyses of the Estonian system have yielded rich insights into both the practical challenges and benefits of Internet voting, like the importance of voter education and trust in the technology [20]. Other countries, such as Brazil and India, have

embarked on the use of DRE systems; these have achieved variable success, pointing to the diverse approaches toward e-voting and the need for context-specific solutions [21].
In general, related work on e-voting is dynamic and in evolution; nowadays, modernization of the elective processes has been very intensive, taking into consideration the solution of very significant issues of security, privacy, and accessibility. Although there have been considerable developments, full-scale implementation of large-scale systems still depends on studies and development that will increase reliability, transparency, and the trust of citizens.

This associated work in the domain of e-voting contributed a lot toward secure and efficient voting systems. However, the application of such systems at a larger scale proved to be difficult in regard to security, usability, and accessibility. Drawing from such practical experiences of previous systems, this paper proposes an e-voting solution that is accessible, secure, and efficient to answer these challenges.

III. LITERATURE SURVEY

The literature in e-voting systems is so varied, touching on the gradual development of voting technologies, security and privacy issues, system usability, the use of blockchain among other emerging technologies, and biometrics. The paper presents a critical review of existing research in highlighted areas of key developments, challenges, and future directions within the filed of e-voting.

A) Security Issues in the E-Voting Systems

E-voting systems have a variety of advantages, including increased accessibility, faster counting of votes, and convenience for all parties involved. However, they also raise severe security risks that need to be overcome to ensure the integrity, secrecy, and trustworthiness of electoral processes. The most critical security concerns associated with e-voting systems include vulnerability to cyberattacks, ensuring voter privacy and anonymity, integrity of the system, and end-to-end verifiability. Each of these challenges is discussed in more detail below.

1. Vulnerability to Cyberattacks

E-voting systems are highly vulnerable to cyberattacks, especially internet-based voting and DRE systems. These commonly include:
- Malware and Virus Infections: Attackers may inject dirty malware into the voting machines to manipulate the vote tallying or impact voting in subtle, undetectable ways. Several studies have shown that most of the DRE systems are unable to safeguard against these types of malware; they are therefore susceptible to vote hacking [1].
- DDoS Attacks: The online voting systems are vulnerable to DDoS attacks, wherein large chunks of traffic congestion jam the server, rendering the system unavailable for voters. This can affect the whole process of elections and bring into question its credibility [2].

- Phishing and Social Engineering: The attacker can engage in phishing, whereby the voters are induced into divulging credentials or are misled to spurious portals for voting. This would hamper the authentication of voters and result in sham votes [3].

- Man-in-the-Middle Attacks: In internet voting, this is an attack in which malicious users intercept data en route between the voter and the voting server and tamper with it. It can let them modify or steal votes without voters' knowledge [4].

2. Ensuring Voter Privacy and Anonymity

Voter privacy and anonymity are essential to protecting voter choices and averting coercion. Based on this, numerous challenges arise in e-voting systems:

Reconstruction Attacks: These are where the attackers take advantage of system weaknesses in attempting to rebuild the choices of the voters from the very data of voting-a thing that leads to the violation of anonymity for the voters [5].

Voter Activity Tracking: Most e-voting systems, especially those involving internet-based platforms, inadvertently track the activity of the voters by IP or cookies among other uniquely identifying information. Such tracking may have dire implications on voter privacy [6].

- Transparency vs. Privacy of Blockchain: Blockchain-based voting systems guarantee transparency but, at the same time, cannot assure anonymity for the voters because of the immutable and traceable nature of blockchain transactions [7]. Any balance of transparency and privacy in this regard could be enabled only with sophisticated cryptographic techniques like zero-knowledge proof, which again introduces complexity in the system [8].

3. System Integrity and Tamper-Resistance

Integrity ensures that the e-voting system captures the choices of each elector properly, and their choice is recorded and counted accurately. The integrity of the system is a hard challenge to maintain because:

Software and Hardware Manipulation: E-voting systems are susceptible to tampering with software and even hardware, such as the alteration of the components of a voting machine. A major challenge is that both software and hardware should be kept secure from manipulation.

Insider threats involve individuals who have access to the electronic voting system and can be administrators or developers. If they become malevolent, or if their accounts are compromised, they can apply serious threats. Insider threats are particularly difficult to mitigate because they involve people with privileged access.

Secure Audit Trails: An e-voting system should allow for secure audit trails that would facilitate the verification of election results [11]. Ensuring these audit trails are tamper-resistant and indicate the actual outcome of the election poses a challenge when trying to provide a balance between transparency with the protection of voter privacy.

4. End-to-End Verifiability

Other features indispensable in ensuring votes are cast, captured, and tabulated as intended without revealing the privacy of voters include end-to-end verifiability. Challenges to achieving end-to-end verifiability include:

The presence of verifiability would be assured through cryptographic protocols like homomorphic encryption, mix-nets, and secure multiparty computation [12]. However, these are still complex to present to the ordinary voter, hence less practical to deploy in practice.

Usability vs. Security Trade-offs: Verifiable voting systems have to make a trade-off between security and usability [13]. Overly complex and difficult-to-use systems discourage participation from the voters, while simpler systems sacrifice vital security features.
Voter Understanding and Trust: For end-to-end verifiability to be meaningful, voters have to understand how they can verify that their votes were recorded and counted correctly [14]. This demands voter education and clear communication that can become difficult in electorates of a larger size and diversity.

5. Secure Voter Authentication

Voter authentication is crucial to ensure that only those who are eligible to vote do get to vote and that no single voter gets to vote more than once. Security challenges in voter authentication include:

This may include weak authentication methods: Several e-voting systems have extremely weak authentication methods, including password/ PINs [15] that could be compromised by phishing, guessing, or brute-force attack.
Biometric Authentication Risks: Although biometric methods provide stronger authentication, such as fingerprint and facial identification [16], the risks in this class concern the storage and protection of sensitive data regarding the biometric characteristics. The breaking of biometric data may have serious privacy implications and is irreversible compared to passwords.

• Usability of Strong Authentication: Stronger authentication methods, such as multi-factor authentication may improve the security but also present usability challenges, especially to less technology-savvy voters or those with various kinds of disabilities [17].

6. Scalability and Performance

Scalability and performance are the critical determinants of successful implementations of e-voting systems, particularly in large-scale elections. The challenges include:

Large Voter Populations: E-voting systems should be able to handle hundreds, thousands, or even millions of voters simultaneously without degradation in performance. Poor scalability results in slow response time or system crashes, thus allowing the possible abortion of the voting process by discouraging participation.

- Blockchain Scalability: In spite of the security that blockchain-based voting systems can prove to offer, they usually pose scalability issues for reasons such as the high computational and storage needs necessary to manage a decentralized ledger [19]. This often makes it slow in terms of transaction processing rates, making it impossible in practice in national elections on large scales.

7. Regulatory and Compliance Challenges

E-voting systems should be compliant with certain legal and regulatory standards put forward to safeguard the rights of all voters and make fair elections possible. Challenges include:

Conforming to Various Legal Frameworks: There are several legal requirements that exist within the many countries and regions, in respect of elections. Thus, it may be difficult to design a single form of an e-voting solution which can suit all countries [20]. Indeed, it is complex to ensure conformation to these diverse legal frameworks in light of the observance of local laws and regulations.

Certification and Standardization: E-voting systems have to be thoroughly tested and certified regarding their security and usability [21]. However, due to the absence of uniform testing procedures, such testing is likely to result in non-uniform assessment results, yielding systems that have unequal security levels.
Successful deployment of an e-voting system calls for the overcoming of these challenges in security. It is only through sustained research and development in cryptography, system design, and voter education that these hurdles can be overcome and e-voting emerges as a secure and trustworthy alternative to traditional methods of voting.

B) Accessibility and Usability in E-Voting Systems

Accessibility and usability are the prime determinants of overall effectiveness, inclusivity, and user experience in the process of voting. Ensuring that persons with disabilities, or those with limited technical skills and language barriers, may be put in an easier position to use an e-voting system is at the very heart of democratic participation. This section presents the main challenges and considerations for accessible and user-friendly e-voting systems design, together with possible solutions and best practices.

1.Accessibility Challenges

One of the critical issues of e-voting, accessibility, refers to all voters being able to participate independently in the voting process in private. Major challenges in accessibility include:

Voter Disabilities: Voters with physical disabilities, such as limited mobility, vision impairments, or hearing loss may find difficult to use the interface of conventional e-voting. Traditional methods of voting require hand-based fine motor abilities or clear vision for which these voters cannot participate in the process.

E-voting systems are daunting for those people who are unfamiliar with the digital world. Examples include elderly voters and those that have limited contact with technological devices [2]. Lack of technological literacy may result in voter errors, frustration, and/or a refusal to take part in the voting process.

Language barriers, attributed to the multicultural nature of societies, may severely obstruct the potential for accessibility in e-voting. If the interface of e-voting is availed in one language only, then non-native speakers cannot comprehend the instructions and thus may not be able to complete their votes accurately.

Remote access to absentee voters: Voters who are overseas, in remote locations, or otherwise unable to access the polling stations can cast a vote using internet-based e-voting [4]. Ensuring secure, reliable, and user-friendly access to such systems is one of the major challenges.

2. Usability Challenges

Usability: It means how easily and efficiently voters can interact with the e-voting system. Poor usability will discourage voters from casting their votes effectively or weaken the trust of the voters in the system. Some important challenges regarding usability:

Complexity in User Interfaces: Where the user interfaces of the e-voting systems are either complicated or unintuitive, this may serve to confuse the voters [5]. The confused voter risks making such mistakes as miscasting a vote or not completing the voting process. Poorly designed interfaces are bound to affect those voters who have some form of disability, or even mere unfamiliarity with technologies.

Cognitive Load: The more complicated the directions in which the system puts their users, or the more screens the system confronts its users with, the more there is to remember [6]. This also goes for increased burdens for those who are cognitively disabled, of limited reading capacity, and so on. All these could lead to voters' making an error or incompletely marking a ballot.

Lack of Feedback: Feedback is required at many stages in the voting process to convince the voters that their particular actions (e.g., casting of vote) have been executed successfully [7]. Systems that provide no appropriate feedback will leave the voters doubting whether their votes have been recorded.

3. Designing Accessible and Usable E-Voting Systems

These challenges can only be overcome by making access and usability of paramount importance in the development or design process of an e-voting system. Here are some strategies that might go a long way toward fulfilling that:

Integrating Assistive Technologies: Screen readers, Braille displays, voice recognition, switch devices, and the like-are examples of assistive technologies to be incorporated into the system in order to make voters with a disability use such a system independently [8]. For example, screen readers can convert text to speech for visually impaired voters, while switch devices can allow those with limited mobility to navigate the system.

Easy-to-Use and Simplified Interfaces: The design of user interfaces should be made simple, clear, and intuitive; they should require as few steps as possible to finish the process. In this regard, large buttons, high contrasts in colors, and fonts can enhance readability and facilitate ease of use [9]. Also, there is a place for visual and audio cues that will help voters navigate the process.

Multilingual Support: Availability of e-voting interface in multiple languages would support voters speaking different languages. Instructions and information can be made available to voters in their preferred language, and this approach minimizes confusion and hence errors.

Accessible Verification: Systems that include verification steps on the part of the voter should provide confirmation of the cast vote in an accessible manner [11]. This may include audio confirmations, visual checks, or other accessible verification methods that do not compromise voter privacy.

User-Centered Design and Testing: The involvement of various types of voters in the design and testing stages helps a lot in the identification of and finding a solution to the problem of accessibility and usability concerning the e-voting system. The user-centered design practices, such as usability tests conducted with people with disabilities, can provide critical insight into just how such a system could be made more inclusive.

Clearly, Providing Instructions and Help: There should be clear instructions displayed that explain each step to the voter [13]. Providing help options, both on-screen and through help hotlines that are accessible, will provide additional support for voters who may need additional assistance during a vote.

4. Real-World Implementations and Case Studies

A few countries and organizations have been able to realize some accessible and user-friendly e-voting systems which offer some lessons and best practices:

Estonian Internet Voting System: Estonia has been at the forefront of providing internet voting with a system that is accessible to different sets of voters even from abroad [14]. Some of the major features that distinguish it from other elections are an intuitive interface, multilingually, and high security; hence, it has been a model in terms of accessible e-voting.

U.S. Accessible Voting Systems: According to HAVA, all the voting systems in the United States should provide accessibility for voters with disabilities [15]. Due to this reason, numbers of accessible voting solutions are being implanted, including ballot-marking devices that accommodate a wide range of disabilities while maintaining

privacy and independence for all voters.
Accessible Features in Brazil's DRE Systems: Brazil has implemented features to make the DRE voting machines more accessible, [16]. such as audio instructions and Braille keypads for visually impaired voters. This allows all voters to participate independently in the process.

5. Future Directions in Accessibility and Usability

The ongoing development of e-voting systems will provide for continued advancement of systems in terms of accessibility and usability. Research and development in this area should be directed toward the following areas of concern:

Innovative Assistive Technologies: Investigations into new assistive technologies, such as haptic feedback devices and augmented reality interfaces, may further improve the accessibility of e-voting systems.
Improved User Testing and Feedback: Involving various groups of voters in usability testing on a continuous basis and integrating their feedback into the design of systems will be helpful in keeping e-voting systems accessible and user-friendly.
Standardization and Best Practice: Standard guidelines and best practices can be developed for accessible e-voting, making it easier for various countries and organizations to design systems that are accessible to all types of voters [19]. International collaboration and sharing will be of immense value in encouraging accessibility and usability in e-voting of the future.

In this manner, electoral bodies ensure, through design for accessibility and usability, the full participation by and independent engagement of all eligible voters in the democratic process. This not only increases the inclusiveness of voters but also enhances the overall integrity and legitimacy of elections conducted using electronic voting technologies.

IV. FUTURE WORK

In the field of e-voting systems, future research should be directed to enhancement in security, accessibility, and scalability due to various challenges arising in the usage of digital voting. For instance, there will be the need for developing more secure cryptographic protocols, such as post-quantum cryptography, against emerging threats like quantum computing. Similarly, further explorations of blockchain can enhance the transparency and trust of e-voting systems, although research needs to take into consideration the issues of scalability and privacy concerns related to blockchain.
Improvement of accessibility and usability does remain a critical research direction, with a particular focus on interface design that caters to access needs for all voters, not excluding those with disabilities or limited digital literacy. This integrates advanced assistive technologies like voice recognition and gesture control, making e-voting more inclusive.

It is also very relevant to conduct research on the use of artificial intelligence and machine learning and improve voter authentication and fraud detection so that only eligible voters can have a say in elections, and the system is resilient against sophisticated attacks.

There is a need for comprehensive studies on voter behavior, trust, and the social impact of e-voting technologies. These will be fundamental in formulating systems that would meet not just the technical requirements but also make gains in confidence among the electorates

E-voting systems are increasingly being explored with the aim of taking over from traditional paper-based voting and may offer several advantages, including efficiency, accessibility, and cost-cutting. These systems include DRE machines, internet-based voting, to even blockchain-enabled voting solutions. However, this shift toward e-voting is attended by a raft of significant hurdles on security, secrecy in voting, dependability of the systems, and scalability. This survey paper covers the current status of e-voting systems and related work and literature regarding the design, implementation, and evaluation. These topics will range from security vulnerabilities regarding DRE and Internet voting to privacy and anonymity concerns with respect to maintaining confidentiality of voters, accessibility and usability of e-voting platforms for the diverse voter population, and the increasingly emerging blockchain technology that provides secure and transparent processes toward voting. The survey underlines important gaps in present research and points to a number of future directions that might help in building up integrity, transparency, and trustworthiness in e-voting systems. In overcoming the challenges lying ahead, e-voting has the potential to significantly improve democratic processes and enhance voter participation.

V. CONCLUSION

In this overview of the general status of e-voting systems, we have presented an overview from multiple angles: the technological developments, security challenges, users' acceptance, and the general feasibility for introducing electronic voting within different contexts. Our results clearly show that while e-voting systems do have some crucial potential advantages-increasing voter access, lowering the costs, and processing results in less time-they also make a raising of important critical challenges, particularly regarding security, privacy, and public trust.

The analysis has shown that security remains an elusive dream because vulnerabilities in the software, hardware, and network infrastructure undermine the integrity of the process. Also, privacy issues such as those related to voter coercion and those ascribed to ensuring ballot secrecy add complexity to the broad base adoption of the E-voting systems. It also underlined a significant breach in public trust, with the key drivers of this being characterized by scares over hacking, fraud, and possible misuse of data.
However, in spite of these problems, the potentiality of e-voting systems cannot be discarded. In those few jurisdictions where it has been conducted successfully, it has

emerged that with proper security provisions, transparency in their processes, and education of the voters, the e-voting system can work to increase democratic participation and make the conduct of elections easier.

In this regard, it is advisable that, in the future, research efforts be targeted at evolving more secure and user-friendly systems to address these identifications of the survey-in the areas of cryptographic techniques, better methods of voter authentication, testing, and auditing. Further efforts should also be made to enhance public trust through transparency and education of the general public on security issues, involving them in development and evaluation processes.

However, the successful implementation of the e-voting system also depends on whether these technical and social challenges are surmounted. The way forward will call for continued research, innovation, and collaboration among technologists, policymakers, and the general public in a move to build secure, reliable, and trusted systems for e-voting.

VI. ACKNOWLEDGEMENT

I would like to express my sincere appreciation to all those who contributed to the successful completion of this research paper, *"Enhancing Electoral Integrity: Survey of a Secure E-Voting Platform."* My deepest thanks go to my advisor, [Mr. Prashant Patil], whose expertise, guidance, and encouragement have been invaluable throughout the research process. I also extend my gratitude to my colleagues and peers for their insightful discussions and support. Additionally, I am thankful for the resources and assistance provided by [Miss. Komal Parit.]. Finally, I am deeply grateful to my family for their constant support and encouragement.

VII. REFERENCES

1. Adida, B. (2008). Helios: Web-based open-audit voting. In *Proceedings of the 17th USENIX Security Symposium*.

2. Halderman, J. A., & Teague, V. (2015). The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election. In *Proceedings of the 5th International Conference on E-Voting and Identity*.

3. Rivest, R. L., & Wack, J. P. (2006). On the notion of “software independence” in voting systems. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 366(1881), 3759-3776.

4. Kulyk, O., Volkamer, M., Kobsa, A., & Hughes, S. (2015). Providing voters with responsible explanations for their choices to enhance their trust in voting systems. In *Proceedings of the 14th International Conference on Trust, Security and Privacy in Computing and Communications*.

5. Benaloh, J., Rivest, R. L., Ryan, P. Y., Stark, P. B., Teague, V., & Vora, P. (2014). End-to-End Verifiability. In *Handbook of Financial Cryptography and Security*.

6. Goodman, N., Volkamer, M., & Ryan, P. Y. (2014). Usability and accessibility of the Prêt à Voter e-voting system. In *Proceedings of the 6th International Conference on Electronic Voting: Verifying the Vote*.

7. Estonian National Electoral Committee. (2020). *E-Voting in Estonia: Overview*. Estonian Ministry of Interior.

8. Dini, G., & Martinelli, F. (2006). A secure and usable e-voting system based on blind signatures and k-anonymity. In *Computer Security Applications Conference*.

9. Gjøsteen, K. (2011). Analysis of an internet voting protocol. In *International Workshop on Security Protocols*.

10. Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, P., & Halderman, J. A. (2014). Security Analysis of the Estonian Internet Voting System. In *Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS)*.

11. Volkamer, M., & Renaud, K. (2013). Enhancing e-voting privacy and verifiability through trusted computing. In *Journal of Information Security and Applications*, 18(3), 202-216.

12. Krimmer, R., Duenas-Cid, D., & Krivonosova, I. (2021). Cryptographic voting protocols: A systems security perspective. *Journal of Information Security and Applications*, 57, 102652.

13. Xia, Y., & Clark, J. A. (2018). Securing e-voting against emerging threats: A review. *Journal of Cybersecurity*, 4(1), tyy003.

14. Riera, A., & Brown, P. (2003). Bringing confidence to electronic voting. In *Electronic Government: Concepts, Methodologies, Tools, and Applications*.

15. Bederson, B. B., & Lee, B. (2007). Electronic voting systems as a mechanism for open, fair, and accessible elections. In *Communications of the ACM*, 50(3), 58-63.

16. Goggin, G., & Hollier, S. (2017). Digital accessibility: The practice and politics of disability inclusion. In *New Media & Society*, 19(5), 783-794.

17. Gritzalis, D. (2002). Principles and requirements for a secure e-voting system. *Computers & Security*, 21(6), 539-556.

18. Rodrigues, B., Sousa, P., & Ferreira, H. S. (2019). Usability evaluation of e-voting systems: A systematic literature review. In *Journal of Universal Computer Science*, 25(5), 546-570.

19. Park, D. S., Lee, H. J., & Im, Y. (2017). Blockchain-based secure e-voting system. In *Proceedings of the IEEE Symposium on Dependable Computing (PRDC)*.

20. Solvak, M., & Vassil, K. (2018). Could the Estonian internet voting be trusted? Overview and analysis of existing studies. In *International Journal of Electronic Governance*, 10(2), 130-147.

21. Simons, B., & Jones, D. W. (2012). Internet voting in the U.S. In *Communications of the ACM*, 55(10), 68-77.

22. Schryen, G., & Rich, E. (2010). Security in large-scale internet elections: A retrospective analysis of elections in Estonia, the Netherlands, and Switzerland. In *IEEE Transactions on Computers*, 59(5), 748-761.

23. Volkamer, M., & Schmidt, J. (2014). Verifiability of electronic voting in practice: An analysis of Helios voting system and its usability. *Journal of Information Security and Applications*, 19(1), 123-135.

24. Stark, P. B., & Wagner, D. (2012). Evidence-based elections. *IEEE Security & Privacy*, 10(5), 33-41.

25. Delaune, S., & Kremer, S. (2007). Formal analysis of e-voting protocols. In *International Workshop on Formal Aspects of Security and Trust*.

26. Ryan, P. Y. A., & Schneider, S. A. (2006). Prêt à Voter with re-encryption mixes. In European Symposium on Research in Computer Security.

27. Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. IEEE Software, 35(4), 95-99.

28. Bernhard, M., Halderman, J. A., & Rescorla, E. (2017). Public evidence from secret ballots. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security.

29. Kshetri, N. (2016). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89.

30. Zhou, L., Wang, Q., Zeng, W., & Liu, X. (2020). E-voting scheme based on blockchain and ring signature. IEEE Access, 8, 24468-24481.

31. Kiayias, A., & Yung, M. (2004). The vector-ballot e-voting approach. In Public Key Cryptography Conference.

32. Kakarla, M. C., & Reddy, S. (2016). Study of blockchain-based decentralized e-voting. In International Journal of Computer Applications, 146(15), 11-16.

33. Liu, J., Zhang, Y., & Wan, Z. (2019). E-voting based on zero-knowledge proof with blockchain. IEEE Access, 7, 123258-123266.

34. Olumuyiwa, T. J., & Samuel, A. O. (2017). Survey of various e-voting methods. International Journal of Computer Applications, 162(10), 6-11.

35. Braun, N., & Neff, M. (2020). Blockchain-based e-voting: System design and usability concerns. Journal of Digital Voting Systems, 11(2), 97-106.

36. Graff, M., & Martinez, P. (2015). Security threats in online voting systems. Journal of Computer Security, 23(3), 291-312.

37. Iovino, V., & Visconti, I. (2017). A secure and efficient e-voting scheme based on homomorphic encryption. IEEE Transactions on Dependable and Secure Computing, 14(2), 171-184.

38. Schilling, J., & Weibel, M. (2017). Verifiable e-voting systems and privacy concerns. In Proceedings of the 12th International Workshop on Trust, Security, and Privacy.

39. Fernandes, A. M., & Santos, C. (2019). Multi-channel e-voting: Security and trust in electronic elections. International Journal of Information Security, 18(2), 245-262.

40. Zissis, D., & Lekkas, D. (2011). Securing e-Government and e-voting with an open cloud computing architecture. Government Information Quarterly, 28(2), 239-251.

41. Bonneau, J., & Gaw, S. (2007). The impact of security perceptions on voting system design: A public policy approach. Journal of Political Science, 53(4), 737-746.

42. Wang, S., & Lin, H. (2019). E-voting with secure homomorphic encryption in the cloud. Computers & Security, 78, 101-113.

43. Adida, B., & Laurie, B. (2006). Verifying vote privacy with secure multi-party computation. In Proceedings of the ACM Workshop on Privacy in the Electronic Society.

44. Preneel, B., & Mitrokotsa, A. (2015). Secure and verifiable electronic voting over a network of insecure nodes. Journal of Network and Computer Applications, 48, 52-63.

Author's:

Mr. Prashant Bajirao Patil. currently Delv Senior Software Engineer in Mphasis Limited. He guide me technical things and help to implement algorithm.

Miss. Komal Mahadev Parit. currently Software Engineer in Irth Solution. She guide me technical things and help to implement algorithm.

Mr. Sanskar Vilas Patil is currently pursuing a Polytechnic Diploma in Computer Science & Engineering at Rajendra Mane Polytechnic, Ambav (Devrukh). He is publishing this paper under the esteemed guidance of Mr. Prashant Patil and Miss. Komal Parit.

Mr. Sourabh Suresh Patil is currently pursuing a B.Tech in Artificial Intelligence & Data Science at Government College of Engineering, Ratnagiri. He has helps in conducting a comprehensive survey on e-voting system.