Journal of Engineering and Technological Advances (JETA)
https://jeta.segi.edu.my/index.php/segi
2025 Vol. 10 No. 2

A COMPREHENSIVE REVIEW OF RECENT ADVANCES, PERSISTENT CHALLENGES AND FUTURE DIRECTIONS IN ELECTRONIC VOTING SYSTEMS (2020-2025)

Mohamed Feroz Bin Mohamed Moubark*, Ashley Ng Sok Choo

Faculty of Arts and Science, Universiti Malaya-Wales, Kuala Lumpur, Malaysia.

* Corresponding Author: feroz@umwales.edu.my TEL: (+6)-03-2617 3000

Received: 11 November 2025; Accepted: 16 November 2025; Published: 31 December 2025

doi: 10.35934/segi.v10i2.168

Highlights:

- Identifies security trade-offs in blockchain-based and post-quantum e-voting designs.

- Analyses accessibility limitations linked to system usability and digital infrastructure.

- Examines end-to-end verifiability mechanisms and governance requirements for trust.

Abstract: An electronic voting (e-voting) literature review focusing of articles published between 2020 and 2025 is conducted as a primary to understand the current changes and the problem of e-voting in a different view-point. The research design used to analyse the practicality of e-voting system employed three main themes, namely security enhancement; accessibility and inclusivity; and trust, verifiability and governance. This review also addresses current persisting challenges including the scaling constraints, quantum risks, unequal socio-technical adoption and split regulatory frameworks. Results have shown significant advances mostly to blockchain systems, post quantum cryptography, end to end verifiability and participatory design. Moreover, the analysed literature shows that, currently, the practical implementation of e-voting technologies has a number of limitations. The review recommends that safe and inclusive e-voting involves the overall strategies that are inclusive of technological leadership, human-computer interaction, policy and social science. The review concludes with the suggestion of hybrid cryptography models, international standards and additional longitudinal studies about the ultimate foundation of trust of digital voters.

Keywords: Electronic Voting; Blockchain Voting; End-to-End Verifiability; Digital Democracy; Quantum Cryptography

1. Introduction

Electronic voting (e-voting) has risen in the face of the old-fashioned voting system (physical ballot box) as a new fundamental development in the present-day democracy with a promise of improving greater efficiency, transparency and convenience. However, its acceptance continues to be a major challenge due to other perception particularly on security, inclusiveness and trust matters. Research by Hanisch *et al*. (2021) and Le *et al*. (2024) research team has indicated that systems that are prone to privacy risks, as well as cybersecurity attacks, tend to be vulnerable in biometric data operations, personal identity management and underlying cryptographic schemes. Regrettably, though, these shortcomings affect the confidence of the stakeholders in their willingness to implement e-voting system in large scale application.

Public's trust as the paramount for the e-voting system, empirical research demonstrates that the adoption of blockchain and smart-contract-based e-voting systems has been gradually deployed to promote verifiability and the technology's ability to audit (Kumar *et al*., 2020; Panja & Roy, 2021). Although these solutions prove the degree of enhanced transparency and resilience, there are still challenges in terms of scalability, utility and regulatory compliance. In one instance, post-quantum secure orchestration, e.g., Epoque, provides future-proof security assertions but undesirably, it leaves the general public with computational feasibility doubts and the adaptability to mass elections (Boyen *et al*., 2021). Equally, coercion is resistant and offers verifiable assurances through zero-knowledge procedures such as zkVoting, even though the mentioned processes have a tendency to be constrained by the complexity of the implementation (Park *et al*., 2022).

Ensuring two key factors (multi-factors) of inclusivity and accessibility are another pressing challenge to the e-voting system. Although the problem is supposed to be solved by making some groups of voters participate more by integrating blockchain-based solutions, other researchers demonstrate that some categories of voters can be restricted in their efforts to participate effectively by technical barriers, digital barriers and resource requirements (Hajian *et al*., 2024; Balakrishnan *et al*., 2021). Recent findings especially by Jumagaliyeva *et al*., (2024) indicate that even though artificial intelligence (AI) and inclusion of blockchain can boost network security and facilitate voting operations, but social-technical obstacle to equal participation remain. The problem of trust, verifiability and governance remains the order of the day on the academic discourse on electronic voting. Users also have the question of striking the right balance between transparency and their privacy, despite the end-to-end verifiable systems (Panja & Roy, 2021; Wang *et al*., 2024). The disconnect between pilot outcomes and theoretical frameworks is an indicator that it is high time that a more holistic operational strategy is embraced to equip technological innovations with sustainable governance procedures. This way, this study will introduce some key arguments of the trends that are emerging in electronic voting systems between the two years under discussion dedicated to inclusion efforts and advancements in security. This approach hoped will also elaborate on the long-term challenges and propose ways forward in the development that shall help close the gap between the emerging technologies and the trust that people have in digital democracy.

2. Literature Review

Electronic voting (e-voting) systems for instance as described by Panja *et al*. (2021) and Hajian *et al*. (2024) have been viewed as the key to the modernization of the democratic electoral systems coupled with the influence of a more efficient, faster performance and inclusive voting system. However, the e-voting technologies are not implemented internationally and adequately because they are complicated with a variety of issues. Such barriers are essential due to the fact that it is primarily concerned with improvement of security, accessibility and inclusiveness and trust, verifiability and governance which are three core dimensions that are vital to the integrity and reliability of any e-voting system. Concretely, these dimensions provide a multidimensional outlook of technical, social and regulatory on the influence to which the e-voting systems are subjected which eventually determine the effectiveness and adoptability of the e-voting system.

The use of e-voting systems by many electoral officials and voters is still being questioned for a fact, despite the sophisticated technologies that are used, due mainly to their credibility and accuracy. This scepticism was based on the history of security vulnerabilities and system weaknesses found in previous deployments. Moreover, cyberattacks, digital exclusion and lack of transparency were all contributing factors that hampered the maximum exploitation of the potential of e-voting. In that regard, researchers and practitioners are channelling more efforts towards creating methods and approaches of constructing safer, more inclusive and trustful e-voting platforms by making pointed amends to these key areas. (Balakrishnan *et al*., 2021; Wang *et al*., 2024).

2.1 Security Enhancement

The main central and ultimate concern is the problem of security of the electronic voting systems, as the flaws in the design and implementation can compromise the integrity of the election and the trust of the voter population. Vinayachandra *et al*. (2025) suggested AES (Advanced Encryption System) and RSA (Rivest, Shamir, Adleman) in combination with blockchain technology to enhance reliability and accuracy of data protection in e-voting. It has been indicated that blockchain and smart contracts should be integrated to enhance transparency and tamper-proof system in voting systems (Panja & Roy, 2021; Wang *et al*., 2024). System architectures based on blockchain, especially those that utilize permissioned ledgers have proved to offer immutable audit trails, along with the minimization of the probability of data manipulation in both transmission and storage (Balakrishnan *et al*., 2021). Moreover, Shekhar and Yadav (2025) established Elliptic Curve Digital Signature Algorithm (ECSDA) with integration of time-based authentication. It is in a way that, if someone tries to intercept and resend a vote after a given period, the system with ECSDA will reject it as expired. This would minimize the tampering of votes by 1.92% and by time is 5.23 ms. In addition, any alteration of the vote would nullify the signature in case the signatures are mathematically bound on the identity of the voter and the specific content of the vote. It implies that according to the authors, the attackers are unable to modify the votes without being caught and the blockchain e-voting systems are made to be more secure.

The fact that, where the security of e-voting systems is meant to ensure voter privacy, verifiability and resistance to coercion is an in-process which has involved the adoption of more sophisticated and advanced cryptographic techniques. The scheme of e-voting, introduced by Kho *et al*. (2025), is demonstrably safe and offers the confidentiality, anonymity and the coercion resistance. Simultaneously, it also possesses sensible computational performance. Good cryptographic design can improve the technical integrity of e-voting as demonstrated in their work. However, it has to be supported by transparent implementation to maintain the level of trust. Additionally, a reinforced user-centred design before extensive application by the population.

There is another motivating development of cryptography lately, in addition to blockchain, to support a more secure e-voting environment, especially against new quantum-based threats, has gained interest in conceptualizing future e-voting. Boyen *et al*. (2021) designed a post-quantum security end-to-end verifiable system, which is resistant to the rise of the adversary with an advanced computational power. In addition to this, Zero-Knowledge Proof (ZKP) mechanisms have been discussed to support privacy among voters and also make such a process verifiable (Le *et al*., 2024). Meanwhile, the ability to integrate biometrics has been viewed as one of the authentication methods, however, discussion still surrounds its ethical consequences and potential security and privacy abuse (Hanisch *et al*., 2021). Although biometric solutions can enhance identity check, the privacy, the misuse of the data, as well as lack of access to those unwilling or unable to give away their biometric information are still an issue of concern. Collectively, these results emphasize that, although technological workarounds (temporary solution) are evolving at a fast rate, it is still a critical challenge to find a balance point between security and the rights of voters.

2.2 Accessibility and Inclusivity

Approachability and non-discrimination are also very important in establishing the validity of the e-voting systems. Despite the intentions of the e-voting platforms to strengthen the voice of citizen voters, there are still obstacles in terms of convenience and flexibility to some groups of people. Literature provides evidence that people such as with disabilities, older adults and others (for instance with low digital literacy) become systematically excluded in the case of an architecture that lacks universality in structure and design (Hajian Berenjestanaki *et al*., 2024). These issues point out that the purely technical advancement solution itself is not enough to address these problems.

It has also been hailed as a form of voting that facilitates absentee voting especially amongst the expatriates and voters in geographically remote areas (Balakrishnan *et al*., 2021). Nevertheless, as it was observed by Panja and Roy (2021), infrastructural obstacles in underdeveloped areas continue to limit the adoption, especially in the regions with low access to the internet. Moreover, on the one hand, mobile-based have been proposed to widen accessibility, yet the constant security and usability questions are not dealt with (Wang *et al*., 2024).

Furthermore, it is a persistent issue to make e-voting accessible and inclusive to people with disabilities, as well as those with less digital literacy. Article written by Rabitsch *et al*. (2023) have proposed the prevalence of physical, cognitive and technological barriers to impartial electoral participation. The writers concluded, to guarantee equitable voting access to people with disabilities could only be overcome through 1) inclusive policies 2) training of staff and 3) assistive technologies. The writers also emphasize that in the democratic process, participation of all is equally important and as such trust among marginalised voters can be significantly increased with the sincerity and commitment of governance together with openness of procedures to accessibility.

The recent work of Shekhar and Yadav (2025) also gives emphasis on inclusivity in terms of equal voting rights. As an example. they suggest a further extension in the form of complaint systems and support of disabled voters, whereas another work by Vinayachandra and Prasad (2025) emphasize the prospects of Advanced Encryption Standard (AES) in connection with the Rivest–Shamir–Adleman (RSA)-based blockchain frameworks, which would make it possible for distance voting (to reduce the nonattendance) and expand the area of accessibility. E-voting involve system and as a meant to achieve inclusivity, we have to deal with digital literacy gaps. Le *et al*. (2024) state that despite the potential improvements in security with the use of or adapting advanced cryptographic protocols, poorly intuitive interface design especially by means of choices, possible to frighten non-technical users away. This irony between the technological and intuitiveness, makes the subject of human-centered design especially important when it comes to e-voting systems.

2.3 Trust, Verifiability and Governance

One can argue that trust, verifiability and governance issues are the ones that have the most significant implications to the integrity of any given electoral system. Within the framework of the implementation of the e-voting system, it is inherently linked to the concept of verifiability and governance mechanisms. One of the verifiable protocols called End-to-end verifiable (E2E-V) schemes described by Boyen *et al*. (2021) is imagined to provide the voters with a feeling that their votes have been properly registered and counted. Le *et al*. (2024) support this suggestion by constructing the schemes on zero-knowledge/mix-net networks to not just offer transparency through the anonymity mechanism but also auditability. Also, both Vinayachandra and Prasad (2025) and Shekhar and Yadav (2025) in their articles stress that blockchain systems being based on the principle of smart contracts ensure transparent governance and audit trails. The final one is that the votes are immutable and this reduces being controlled by discretion and maximizes voter confidence.

Technical assurances alone are however not enough to bring about the trust; well-structured governance structures are however necessary. According to Hajian Berenjestanaki *et al*. (2024), the governance structures should take into consideration oversight, accountability and legal compliance to have legitimacy. Similarly, Waniya *et al*. (2023) stressed that regulatory and legal requirements must be considered on the issue of sensitive information when dealing with biometrics, which means that privacy should be dealt with ethically. The most crucial factors of trust are the social and psychological ones. According to Wang *et al.* (2024), voters remain hesitant about its implementation, in many cases, due to the past experience of the failure of electronic voting trials. Voters argued that it lacks transparency. This explains why there was the need to combine the three (Trust, Verifiability and Governance); whereby technology is made verifiable and that participatory model of governance which promotes transparency, through which accountability as well as trust are achieved, at each electoral process level.

Recent studies emphasize and add to the fact that the citizen trust into e-voting is not merely based on technologically guaranteed issues. Clear communication and management should be put in that the system is credible. Abdala and Leets (2025) found out that institutional trust in government and technological trust are significant in its role to influence the willingness of citizens to participate in e-election. In their study, they have indicated that adoption of the e-voting systems mechanisms greatly relies on verifiability that must be intertwined with responsible governance procedures and responsible methods of communication so as to increase the voter turnout.

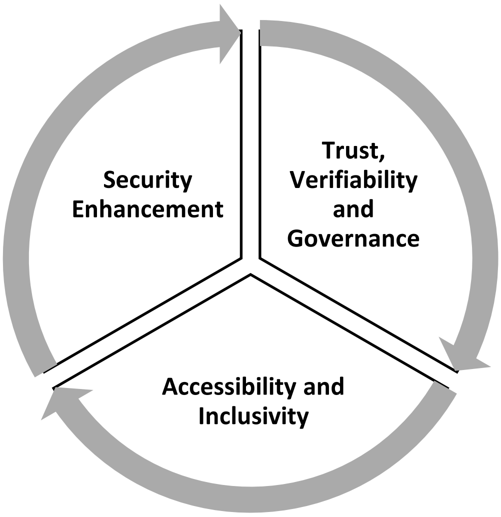
Security Enhancement
Trust, Verifiability and Governance
Accessibility and Inclusivity

Figure 1. E-Voting Foundations

3. Theoretical Model

The framework unites the theories and models that are central to the contemporary study of electronic voting (e-voting) that is being covered in three dimensions, as illustrated in **Figure *1***; a better safety, accessibility and inclusivity, and a sense of trust, verifiability and governance. It will also seek to clarify the ways in which these theories support each other as well as identify the gaps that may be used as inspiration to future studies.

3.1. Variable 1: Security Enhancement

Technically, the heart of secure enhancement in e-voting is End-to-End Verifiability (E2E-V). It demands that from this perspective balloted vote fall cast-as-intended, recorded-as-cast and tallied-as-recorded so that it ensures ballot secrecy. Panja (2021) has mentioned that the E2E-V system bases on verification to individual voters as well as the general audience through strong bulletin-board auditing. Recently, these security assurances have been further enhanced with the incorporation of Post-Quantum (PQ) cryptography. PQ is the form of lattice-based constructions with inbuilt Zero-Knowledge (ZK) proofs to ensure privacy and verifiability despite the existence of malicious devices (Boyen *et al*., 2021). PQ voting emphasizes an adversarial paradigm where if the client devices compromised; the design aim is to constrain the effect of such compromise in ways according to the author that do not sacrifice verifiability.

3.2. Variable 2: Accessibility and Inclusivity

Voter accessibility and availability has to be considered in legitimate e-voting so that the diverse electorates should have access to a secure system. In a recent review of technology, the system properties of the categories accessibility and usability are conceived as co-equal to security and verifiability, listing availability, universal access, simplicity and understandability as design requirements (Hajian *et al*., 2024). The usage of smart contracts would automate the rules of an election and facilitate remote voting. According to Balakrishnan *et al*. (2023) smart contracts would be able to detect multiple vote and fake votes. Along with this, online voting integrate with Blockchain technology provides a way of accessibility platforms operational during the needs (Balakrishnan *et al*., 2023). Taken together, these theories emphasising human and technology (socio-technical approach) that inter-twines security with human-centered design and flexibility in operations.

3.3. Variable 3: Trust, Verifiability and Governance

Trust (as the fundamental or backbone for the e-voting) is the result of a combination of visible verifiability and trustworthy governance, (verifiability + governance = Trust). The subject of trustworthiness in references to eligibility, fairness, accountability, transparency and auditability that reveal how systems have earned and maintained the focus of the voter's trust (Hajian *et al*., 2024). Research on governance was also central to 'identity management'; a comparison of federated and Self-Sovereign Identity (SSI) solutions. SSI offered a threat-based perspective of confidentiality, integrity, availability and privacy in reference to voter onboarding and verification (Le *et al*., 2023). The use of smart contracts in governing also guarantees automated-rule-application and the ability to audit decentralized systems that limit discretionary rulemaking, ensuring verifiability (Kumar et al., 2020). These two theories will help in answering this question because of combination of formal verifiability, institutional (governance) and technical accountability.

3.4 Gaps and Implications

Although much has been done, there are still major loopholes in the areas of security, access and governance. The conflicting nature of high privacy and the universal verifiability on heterogeneous or diverse spaces, remains a matter of concern (Panja & Roy, 2021; Hanisch *et al*., 2021). The bindings between usability and cryptographic protocols should also be more effective so that voters are not disregarded (Hajian et al., 2024; Balakrishnan et al., 2023). The regulations must allow accountability and interoperability without centralization of trust (Le *et al*., 2023; Kumar *et al*., 2020). The in-depth study of the future requires integration of formal security proofs, human-subject experimentation and operation audits to overcome the gap between the theory and the practice.

4. Findings and Discussion

This section contains main findings of the literature in categories of security, accessibility and trust. Besides, it explains how the findings are relevant to the research questions addressing the continued gaps and implications.

4.1 Finding 1: Security Enhancement

Modern studies (summarised as in **Figure 2.** Supporting flowchart based on the articles reviewed) show that the shift to supplementary blockchain mechanisms, to strict and formally defined, end-to-end verifiable (E2E-V) protocols that maintain ballot integrity and secrecy of the voter is taking place (Panja & Roy, 2021). The frameworks proposed by Boyen *et al*. (2021), which combine lattice-based cryptography with zero-knowledge proofs, can be adapted for post-quantum environments and enhance verifiability even against strong adversarial models. Subsequent studies further address the coercion resistance, strengthen system integrity through permissioned blockchains and emphasize the importance of principled privacy assessments in biometric authentication (Park *et al*., 2024; Wang *et al*., 2024; Hanisch *et al*., 2021). Shekhar and Yadav (2025) present the empirical results that their model based on ECDSA comprehended lower rate of vote changes. The data presented by Shekhar and Yadav (2025) shows that 1.92% than the average 3.48% (based on 30,000 voters) of the previous blockchain systems, thus improving integrity.

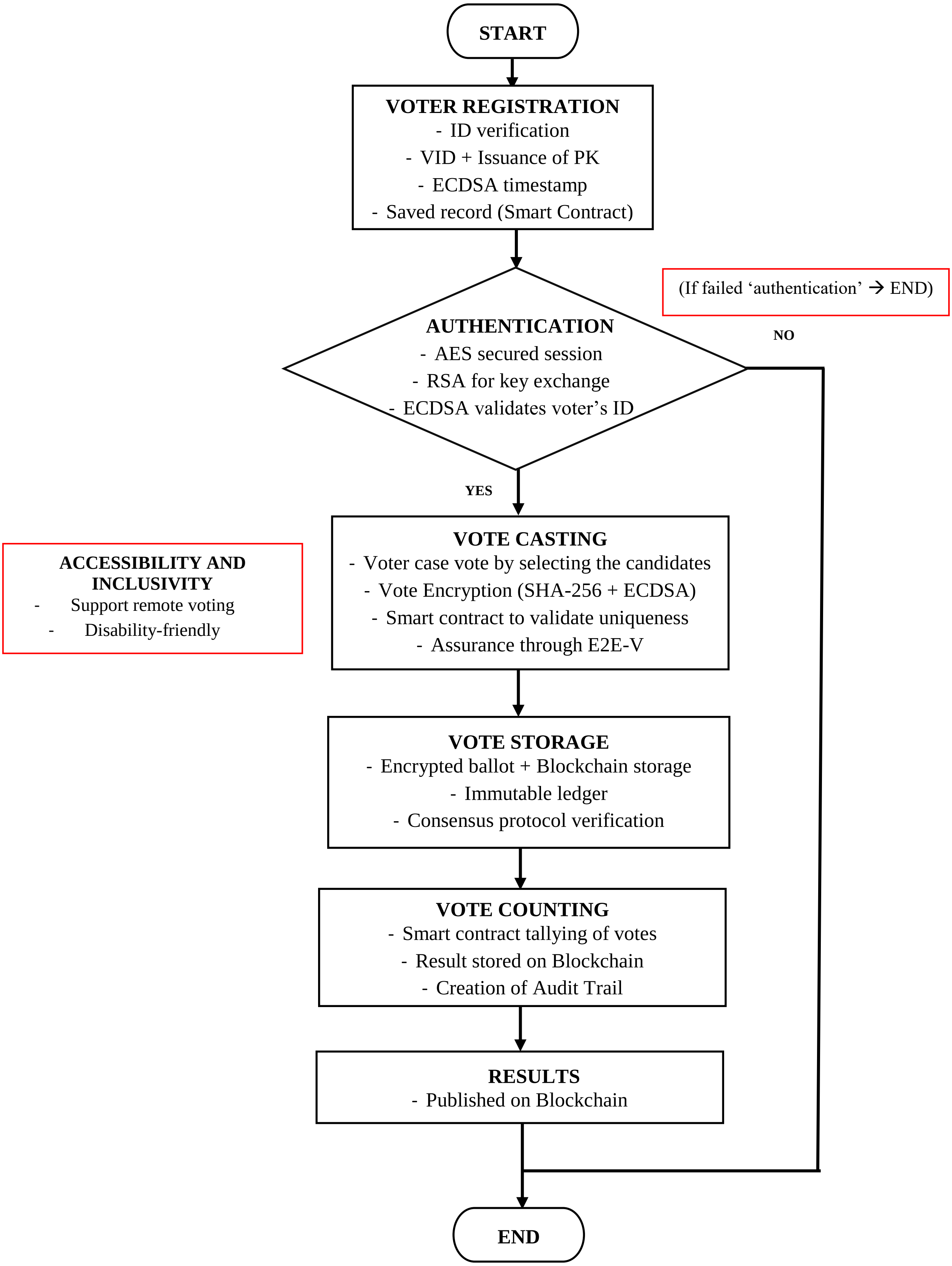
START
VOTER REGISTRATION
- ID verification
- VID + Issuance of PK
- ECDSA timestamp
- Saved record (Smart Contract)
(If failed 'authentication' → END)
NO
AUTHENTICATION
- AES secured session
- RSA for key exchange
- ECDSA validates voter's ID
YES
ACCESSIBILITY AND INCLUSIVITY
- Support remote voting
- Disability-friendly
VOTE CASTING
- Voter case vote by selecting the candidates
- Vote Encryption (SHA-256 + ECDSA)
- Smart contract to validate uniqueness
- Assurance through E2E-V
VOTE STORAGE
- Encrypted ballot + Blockchain storage
- Immutable ledger
- Consensus protocol verification
VOTE COUNTING
- Smart contract tallying of votes
- Result stored on Blockchain
- Creation of Audit Trail
RESULTS
- Published on Blockchain
END

Figure 2. Supporting flowchart based on the articles reviewed

4.2 Finding 2: Accessibility and Inclusivity

Recent research (**Figure 2.** Supporting flowchart based on the articles reviewed) repositions the accessibility and usability as major design properties and moves the availability, inclusivity and simplicity into a par with the security and verifiability (Hajian Berenjestanaki *et al*., 2024). Smart contracts are considered to automate the rules of elections and make them accessible remotely, yet undoubtedly, issues of device security and usability are still present (Balakrishnan *et al*., 2023). Anomaly detection solutions based on AI and blockchain logging are suggested as the way to maintain availability under pressure, however, implementations in the real world still face challenges related to the infrastructure and literacy (Jumagaliyeva *et al*., 2024; Panja & Roy, 2021; Wang *et al*., 2024).

4.3 Finding 3: Trust, Verifiability and Governance

Electronic voting is trusted due to the ingredients or components of verifiability and credible governance, which is enabled by other properties including: eligibility, fairness, accountability and transparency (Hajian Berenjestanaki *et al*., 2024). The fundamental aspect of Identity management is in place, where both federated identities and Self-Sovereign Identity (SSI) have trade-offs when considering their use in voter enrolment in terms of the confidentiality, integrity and privacy of the process (Le *et al*., 2023). Further, it is suggested that decentralized smart contracts can automate governance and auditing processes and minimize discretionary control in the process, protecting the verifiability (Kumar et al., 2020). Additionally, End-to-end verifiable (E2E-V) mechanisms also focus on the crucial resolution between discrepancy and confidentiality and between transparent tallying to uphold ballot confidentiality (Panja and Roy, 2021). Shekhar and Yadav (2025) also note that embedding rules directly into smart contracts could strengthened the governance issue, while Vinayachandra and Prasad (2025) stress that audit logs of immutable blockchain are vital for long-term trust.

4.4 Implications

It is becoming more consistent as consequences with verifiable-by-design architectures, which combine privacy and governance provisions into the design. Notably, the issue of compromise between post-quantum security and efficiency still exists. Addition is, the accessibility frameworks will have to be transferred into design guidelines. Identity and audit governance must be embedded without compacting trust.

5. Recommendations

On the basis of the synopsized or summarised results, evidence-based guidance, with the important caution that rigorous testing and considered piloting are required. Any broader or official implementation of novel e-voting systems, until and unless rigorous testing has been done would appear negligent at best.

5.1 Security Enhancement - Accessibility and Inclusivity - Trust, Verifiability and Governance

The concept behind this research study is that a secure electronic voting process has to be driven fundamentally, in a manner that considers the complexities or interconnection of security upgrading, accessibility and inclusiveness along with trust in terms of verifiability and governance. Security-wise, end-to-end verifiable protocols, post-quantum cryptography and tamper-evidence ledgers are essential measures in coercion proof, client security and tally changes (Panja & Roy, 2021; Boyen *et al*., 2021; Wang *et al*., 2024). Similarly, unless accessibility and inclusivity are prioritized, even the most sophisticated systems are likely to fail to serve voters with low digital literacy, disabilities or other connectivity issues. Accordingly, the accessibility requirements have to be integrated into the procurement, testing and design stages to ensure that they are accessible to all voters and enable fair participation (Hajian *et al*., 2024; Balakrishnan *et al*., 2023).

Moreover, to maintain widespread confidence, there must be verifiably transparent and credibly governed by auditable processes, risk-based identity system certification and regulatory regimes that strike the right balance between equity, accountability and auditability (Le *et al*., 2023; Kumar *et al*., 2020). At this juncture, it is advised that upon collaborative efforts to guarantee the security, inclusiveness and democratic legitimacy of e-voting system, unity between regulating bodies, election authorities, technology developers and civil society established. The objective is to define and implement minimum technical and accessibility, co-design of inclusive privacy, regulatory sandboxes and audit artifact releases (Hanisch *et al*., 2021; Hajian *et al*., 2024).

Developing the e-voting concept is a process that ought to balance between innovation and the utmost significance of electoral fairness and people’s confidence. Take note that without any further extensive research and confirmation, it is risky of going ahead of all the preparation by rushing into their implementation.

6. Conclusion

The development of electronic voting systems is shaped by the combined influence of security, accessibility and governance considerations. End-to-end verifiable designs and advanced cryptographic mechanisms contribute to protecting ballot integrity and voter privacy. Nevertheless, the practical implementation faces challenges related to coercion resistance, device security and system complexity. At the same time, limitations in accessibility, such as digital literacy gaps, physical constraints and network availability, restrict effective participation, particularly if they are not adequately addressed during the system design and deployment. Governance aspects, including transparent auditing, accountable identity management and clearly defined oversight mechanisms, further influence the perception of electronic voting systems and public trust. Overall, these findings indicate that the effectiveness and legitimacy of electronic voting systems depend on both the technical security performance and also on the balanced integration of usability, inclusivity and governance within a coherent socio-technical framework.

Acknowledgement

The authors would like to express sincere gratitude to everyone who contributed, both directly and indirectly especially to all the original writers of the articles reviewed, to the completion of this study. We would like to thank the Universiti Malaya-Wales for providing the supports for this study.

Credit Author Statement

Conceptualization, M.F.; data curation, M.F.; writing-original draft preparation, M.F.; writing-reviewing and editing, A.N.

Conflict of Interest Statement

The authors declare that there is no conflict of interest regarding the publication of this study.

Artificial Intelligence (AI) Transparency Statement

Artificial intelligence tools (ChatGPT, Gemini) were used only to enhance grammar, clarity and manuscript readability. They were not used to generate, analyse or interpret data nor to create scientific hypotheses, conclusions or literature reviews. All content remains the intellectual product of the original authors. Any AI-assisted text was carefully checked, revised and validated to ensure compliance with research integrity and publisher guidelines.

References

Abdala, M. B., & Leets, P. (2025). Trust in government or in technology? What really drives the use of internet voting. Government Information Quarterly. *Advance online publication*. https://doi.org/10.1177/10659129251321424

Ahmed, A. A., & Ali, N. H. M. (2025). Secure e-voting system utilizing fingerprint authentication, AES-GCM encryption and hybrid blind watermarking. Journal of Applied Engineering and Technological Science, 6(2), 997–1018.

Abo-Akleek, F., Mowafi, M., Taqieddin, E. S., & Shatnawi, A. S. (2025). Leveraging blockchain for robust and transparent e-voting systems. *Cyber Security and Applications, 3*, 100086. https://doi.org/10.1016/j.csa.2025.100086

Balakrishnan, N., Karthikeyan, P. C., Aruna, S., Dharshini, G. S. D., & Akshaya, D. (2021). Smart contracts and blockchain based e-voting. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12(11)*, 4511–4517.

Boyen, X., Haines, T., & Müller, J. (2021). Epoque: Practical end-to-end verifiable post-quantum-secure e-voting. *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23)*, 2215–2229.

Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, C. (2024). Blockchain-based e-voting systems: A technology review. Electronics, *13(1)*, 17. https://doi.org/10.3390/electronics13010017.

Hanisch, S., Todt, J., Patino, J., Evans, N., & Strufe, T. (2021). A false sense of privacy: Towards a reliable evaluation methodology for the anonymization of biometric data. *Proceedings of the 2021 ACM on Asia Conference on Computer and Communications Security (ASIA CCS '21)*, 1502–1516. https://doi.org/10.56553/popets-2024-0008

Jayakumari, B., Sheeba, S. L., Eapen, M., Anbarasi, J., Ravi, V., Suganya, A., & Jawahar, M. (2024). E-voting system using cloud-based hybrid blockchain technology. *Journal of Safety Science and Resilience, 5*, 102–109. https://doi.org/10.1016/j.jnlssr.2024.01.002

Jumagaliyeva, A., Muratova, G., Tulegulov, A., Rystygulova, V., Serimbetov, B., Yersultanova, Z., & Shegetayeva, A. (2024). The impact of blockchain and artificial intelligence technologies in network security for e-voting. *International Journal of Electrical and Computer Engineering (IJECE), 14(6),* 6723–6733. DOI: 10.11591/ijece.v14i6.pp6723-6733

Kho, Y.-X., Heng, S.-H., Tan, S.-Y., & Chin, J.-J. (2025). A provably secure coercion-resistant e-voting scheme with confidentiality, anonymity, unforgeability and CAI verifiability. *PLOS ONE, 20*(6), e0324182. https://doi.org/10.1371/journal.pone.0324182

Kumar, R., Badwal, L., Prakash, A., & Avasthi, S. (2020). A secure decentralized e-voting with blockchain & smart contracts. *International Journal of Advanced Science and Technology, 29(5),* 11869–11875. http://sersc.org/journals/index.php/IJAST. DOI: 10.1109/Confluence56041.2023.10048871.

Le, A., Epiphaniou, G., & Maple, C. (2024). A comparative cyber risk analysis between federated and self-sovereign identity management systems. *Data & Policy, 6*, e43. doi:10.1017/dap.2023.41

Panja, S., & Roy, B. (2021). A secure end-to-end verifiable e-voting system using blockchain and cloud server. *Journal of Information Security and Applications, 59*, 102815. https://doi.org/10.1016/j.jisa.2021.102815

Park, S., Choi, J., Kim, J., & Oh, H. (2022). zkVoting: Zero-knowledge proof based coercion-resistant and E2E verifiable e-voting system. https://eprint.iacr.org/2024/1003.pdf

Rabitsch, A., Moledo, A., & Lidauer, M. (2023). Inclusive elections? The case of persons with disabilities in the European Union. *South African Journal of International Affairs, 30*(3), 535–553. https://doi.org/10.1080/10220461.2023.2275669

Razali, M. H., Jamal, A. A., Abdullah, F. S., Zakaria, M. D., Wan Nik, W. N. S., & Hassan, H. (2025). E-voting on Ethereum blockchain. *Journal of Advanced Research in Applied Sciences and Engineering Technology, 50*(2), 186–194. https://doi.org/10.37934/araset.50.2.186194

Shekhar, C., & Yadav, R. K. (2025). An innovative and secured electronic voting system based on Elliptic Curved Signing Approach (ECDSA) and digital signatures. *International Journal of Information Technology, 17,* 2679–2684. https://doi.org/10.1007/s41870-025-02405-3

Tanwar, S., Gupta, N., Kumar, P., & Hu, Y.-C. (2024). Implementation of blockchain-based e-voting system. *Multimedia Tools and Applications*, *83*, 1449–1480. https://doi.org/10.1007/s11042-023-15401-1

Vinayachandra, & Krishna Prasad, K. (2025). Blockchain based cryptographic algorithm for data protection in electronic voting system. *EAI Endorsed Transactions on Internet of Things*, *11(1),* 1–12. doi: 10.4108/eetiot.7680

Wang, B., Guo, F., Liu, Y., Li, B., & Yuan, Y. (2024). An efficient and versatile e-voting scheme on blockchain. *Cybersecurity*, *7*, *62*. https://doi.org/10.1186/s42400-024-00226-8

Waniya, J. S., Palmer, M., Kathrine, G. J. W., Xavier, S. B., & Aarthi, S. (2023). Decentralized blockchain based online voting system with biometric authentication. *Proceedings of the 2023 8th International Conference on Communication and Electronics Systems (ICCES) (pp. 632–638)*. IEEE. https://doi.org/10.1109/ICCES57224.2023.10192776