Analysing the Potential Vulnerabilities in Online Voting Protocols: Homomorphic Encryption Approach

Yao Charles Azameti[1*], Wiiliam Asiedu[2], George Asante[3]

[1,2,3]Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development, Kumasi, Ghana.

ARTICLE INFO

Article history:
Received 14 March 2025
Revised 21 April 2025
Accepted 23 April 2025
Published 1 September 2025

Keywords:
Blockchain Voting
Homomorphic Encryption
Electronic Voting Security

DOI:
10.24191/jcrinn.v10i2.515

ABSTRACT

Online voting offers a hopeful alternative to traditional voting approaches by improving accessibility, efficiency, and transparency in elections. However, despite their potential, these systems are prone to a variety of security vulnerabilities. This research aims to analyze the crucial vulnerabilities that can compromise the integrity, confidentiality, and availability of online voting systems. Key threats examined include cyber-attacks such as denial of service (DoS), man-in-the-middle (MITM) attacks, and malware injection, as well as issues related to voter authentication, anonymity, and coercion resistance. Additionally, the research evaluates the effectiveness of cryptographic techniques like homomorphic encryption, zero-knowledge proofs, and blockchain in mitigating these risks. The study provides a comprehensive review of existing protocols, identifies gaps in their security architectures, and proposes enhanced mechanisms to address the vulnerabilities. The ultimate goal is to contribute to the development of more robust and secure online voting systems that ensure voter trust and uphold democratic principles.

1. INTRODUCTION

Casting votes online has emerged as a viable alternative to traditional voting systems, offering enhanced convenience, efficiency, and transparency. As societies move towards digitalization, government and organizations alike are increasingly exploring the potential of online voting systems to conduct elections. These systems promise to reduce logistical barriers, improve voter turnout, and provide immediate results, all while minimizing the costs associated with physical polling stations and paper ballots. Despite these advantages, the widespread adoption of online voting has been slow, primarily due to concerns about the security and reliability of these systems. The significance of online voting lies in its ability to maintain integrity, transparency, and security within the electoral process. By integrating modern digital technologies, online voting protocols aim to ensure the accuracy of electoral data, minimize the risk of tampering or fraud, and enhance public trust in election outcomes.

This section will delve into research works in the field of online voting protocols, examining the evolution of design paradigms, encryption techniques, and implementation strategies. A key challenge of online voting protocols is their reliance on a central point of control for vote casting and validation. Unlike decentralized systems, where multiple nodes independently verify transactions, most online voting systems are centralized, with votes processed through a single authoritative entity. This centralization usually creates vulnerabilities, as it becomes a single point of failure that could be targeted by cyberattacks or internal manipulation. Additionally, the trust placed in a single authority can reduce transparency and make it harder for participants to independently verify the integrity of the election process. This reliance on centralized systems raises concerns about the resilience of online voting to malicious attacks and

[1*] Corresponding author. *E-mail address*: ytornyeviadi@gmail.com

undermines the potential for trust among participants. Moreover, cryptographic techniques play a pivotal role in ensuring the security and privacy of votes in online voting protocols. Advanced cryptographic methods such as zero-knowledge proofs, homomorphic encryption, and multi-party computation allow voters to cast their ballots anonymously while ensuring the verifiable aggregation of votes. By integrating these cryptographic tools into the voting process, online voting protocols aim to strike a balance between privacy and transparency, thereby safeguarding the integrity of elections.

2. LITERATURE SURVEY

The following review of literature provides a comprehensive overview of the evolution of online voting systems, from their conceptual foundations to practical implementation. By examining the strengths, limitations, and challenges of existing systems, insights will be gleaned into best practices and areas for improvement in the development of an efficient and secure voting systems. This review will inform the subsequent chapters, building upon prior research to propose a novel voting protocol that addresses the complexities and exigencies of modern democratic processes.

2.1 Online voting system

Online Voting, also referred to as E-Voting is a method of casting votes using electronic devices connected to the internet, typically allowing voters to participate in elections remotely. The system facilitates greater accessibility by enabling voting from any location with an internet connection, reducing the need for physical polling stations. Online voting protocols often integrates various security features, such as encryption, digital signatures, and biometric verification, to ensure the integrity, confidentiality, and authenticity of the voting process. E-Voting promised to increase voter turnout and efficiency, online voting also faces significant challenges, including security risks, digital divide issues, and concerns about voter privacy and coercion. The shift from traditional paper-based voting methods to internet-based voting (I-voting) has gained significant attention in recent years due to its potential to improve electoral processes.

Smith and Clark's research delves into the transition from traditional voting methods to internet-based voting (I-voting), underscoring benefits like cost reduction, improved vote accuracy, and greater accessibility, while also addressing significant challenges such as the digital divide, which limits access to online voting for certain demographics, and security risks including potential cyberattacks, voter fraud, and data breaches; they advocate for the development of standardized electronic voting (e-voting) systems to mitigate these risks but note that barriers such as inadequate security protocols, the complexity of voter authentication, and lack of public trust pose significant obstacles to widespread adoption of I-voting. Despite these challenges, they argue that I-voting could enhance voter participation and democratization, provided that these issues are carefully addressed (Smith & Clark, 2005). Thakur et al. (2014) explored the evolution of voting systems, highlighting the transition from traditional methods to mobile voting (m-voting) using Near Field Communication (NFC) and biometric verification. Their study addresses challenges like low voter turnout, particularly among youth, and proposes a mobile voting model that leverages common-off-the-shelf (COTS) mobile phones. Their proposed model enhances voter mobility, transparency, and ease of use while mitigating security risks. This approach aims to increase electoral engagement and accessibility across diverse demographics, making voting more efficient and inclusive (Thakur et al., 2014). In another research conducted by Al-Shammari et al, discusses the advantages of electronic voting systems (E-voting), highlighting their potential to outperform traditional voting methods through enhanced accessibility, reduction of voter errors, and cost-effectiveness. It emphasizes how features such as audio interfaces for visually impaired voters and simplified ballot management contribute to a more efficient voting process. Additionally, it points out the significant savings in costs associated with the use of DRE voting machines compared to paper ballots (Al-Shammari et al., 2012).

Another paper presented by Ahmad et al. provide a comprehensive overview of the evolution of electronic voting systems, categorizing them into four main types: punch card, optical scanning, direct recording electronic (DRE), and remote internet voting, while highlighting the benefits such as improved transparency, faster processing, enhanced security, and greater accessibility for remote and disabled voters. However, they identify several vulnerabilities and challenges, including susceptibility to cyberattacks,

tampering with digital infrastructure, privacy concerns with remote internet voting, and potential software malfunctions in DRE systems. The authors stress that while e-voting systems offer significant advantages, public trust can only be maintained through addressing these security risks, ensuring the integrity of election data, and implementing stronger verification mechanisms to prevent manipulation or fraud (Ahmad et al., 2021). A Survey conducted by Mursi et al. (2013), provided a comprehensive review of the evolution and state of electronic voting systems. The paper outlines the challenges associated with transitioning from traditional paper-based voting methods to electronic systems, focusing on the conflicting requirements of privacy, security, transparency, and fairness. The survey categorizes various e-voting schemes, discusses their cryptographic underpinnings, and examines the advantages and disadvantages of different approaches.

Key security concerns include voter authentication, vote integrity, privacy, and resistance to coercion. The paper further details the vulnerabilities of both traditional and modern voting systems, including punch cards, optical scanners, DRE (Direct Recording Electronic) systems, and online voting. The authors discuss the role of cryptographic mechanisms like homomorphic encryption, zero-knowledge proofs, and visual cryptography in enhancing the security of electronic voting. The survey concluded with a comparative analysis of different e-voting schemes, highlighting gaps in current technologies, especially in terms of scalability and trustworthiness and advocates for improvements in cryptographic protocols and suggests that biometric tokens and robust end-to-end verifiability are promising avenues for future secure e-voting systems (Mursi et al., 2013). In the quest to modernize India's voting process, Ganesh Prabhu et al, presents a new method also known as Smart Online Voting System to allow citizens to vote remotely via an online platform that uses facial recognition and OTP (One-Time Password) authentication.

This system eliminates the need for physical presence at polling stations, enabling users to vote from anywhere using a computer or mobile phone. It also offers an offline option where voters can use RFID tags instead of traditional voter IDs. The voting process involves two-step authentication, first through facial recognition and then by verifying an OTP sent to the registered mobile number. Results are updated in real-time in a central database, ensuring quick access and minimizing vote tampering. Despite its innovations, the system has several issues as it relies heavily on stable internet and technology, which may not be available to all. The system as well faces security risks like cyber-attacks, phishing, and denial-of-service (DoS) attacks. Again, storing biometric data in a central database raises privacy concerns that, the central database could be the point of failure or attack, and also the potential for voter coercion or fraud, especially in remote voting situations, is a significant challenge.

Thus, while the system enhances convenience and efficiency, addressing these security and privacy concerns became critical to its success (Ganesh Prabhu et al., 2021). To address the persistent challenges associated with online voting systems, such as security vulnerabilities, voter privacy concerns, accessibility issues, and lack of transparency, another paper proposes a more advanced solution that integrates enhanced security protocols and innovative technologies aimed at improving the security, accessibility, and convenience of elections by allowing citizens to vote online from any location. This system is designed to ensure high security using a combination of cryptographic techniques, face recognition, and password protection, which together form a robust authentication process. Users log in with a unique voter ID generated by the Electoral Commission of India, and their votes are cast through a web interface after verifying their identity with both a password and a facial image stored in the database. The system aims to increase voter turnout by making the process more accessible, especially for citizens in remote locations or those with mobility issues. The online voting system promises to speed up the counting process, reduce human errors, and eliminate vote tampering or rigging, offering a more transparent and reliable method of conducting elections.

The integration of face recognition technology further strengthens the security of the system by ensuring that only verified users can vote, yet it faces several crucifixions since the system remains vulnerable to cyberattacks such as hacking or denial-of-service (DoS) attacks that poses privacy concerns due to the storage of sensitive data like facial images in a central database, also the system has been criticized of being difficult for non-tech-savvy users or those without reliable internet access to use. Additionally, voters must place their trust in the technology, as the process lacks transparency, which led to concerns about the accuracy and security of their vote compared to traditional methods (Kaliyamurthie et al., 2013).

2.2 The need for blockchain

In online voting systems, centralization has long been a point of vulnerability. Centralized authorities whether election officials, government bodies, or electronic voting machines hold significant control over the voting process, from voter registration to vote tallying and result verification. This centralization creates opportunities for manipulation, fraud, and even cyber-attacks, as seen in numerous instances of compromised electronic voting machines and tampered elections.

The reliance on a central authority and database also introduces trust issues, as citizens must trust that officials and their systems are secure, impartial, and functioning properly. At the heart of it all is blockchain technology, which promised to offers a decentralized alternative, which addresses these critical concerns. By distributing the control of the voting ledger across multiple nodes, blockchain removes the reliance on any single authority. Each transaction, or vote, is encrypted, time-stamped, and verified by a network of nodes, ensuring that no single party can alter the results without detection. This decentralized structure not only provides transparency and security but also ensures the integrity of the voting process. Blockchain's tamper-resistant ledger, public verifiability, and resilience to attacks make it an ideal solution for transforming how elections are conducted, offering a modern, scalable solution to the vulnerabilities of centralized voting systems.

Osgood (2016), explores the need for blockchain in voting systems, highlighting the current vulnerabilities in electronic and paper-based voting, such as susceptibility to fraud, hacking, and lack of scalability, and argues that blockchain offers a secure, tamper-proof, and transparent alternative by distributing voting data across a decentralized ledger. In this paper, Osgood point out few weaknesses in the proposed blockchain voting protocols which include the challenge of securing voter authentication, risks of voter intimidation in remote voting, the potential for network attacks, and the reliance on internet infrastructure, which may limit the system's feasibility in certain regions (Osgood, 2016).

Again, a blockchain-based e-voting system that aims to improve the security, transparency, and privacy of elections by utilizing a private, permissioned blockchain infrastructure has been proposed by (Hjalmarsson et al., 2018). This system benefits from key blockchain strengths such as immutability, verifiability, and decentralized consensus, ensuring that votes are tamper-proof and publicly auditable, yet anonymous, as each vote is appended to a distributed ledger only after consensus is reached by multiple nodes. It also introduces smart contracts to automate election processes, including voter registration, vote tallying, and verification, reducing human error and central authority involvement, which lowers the potential for fraud and manipulation.

However, the system is not without critics. While the blockchain provides transparency, it does not inherently ensure voter authentication, requiring additional government identity verification services, which introduces points of vulnerability. Again, the system is challenged in resisting voter coercion, particularly in remote or unsupervised voting environments, limiting its suitability for large-scale, unsupervised elections. Also, the reliance on blockchain technology brings concerns about scalability, as high transaction throughput may be required for national elections, and existing blockchain implementations may struggle with performance under high voter turnout. Additionally, the proposed system faces the potential risk of a 51% attack, where a malicious entity could gain control of the majority of network nodes to manipulate results. This vulnerability is a known issue in public blockchains. However, the paper addresses this concern by employing a permissioned blockchain, which restricts node participation to trusted institutions, thereby reducing the likelihood of such an attack.

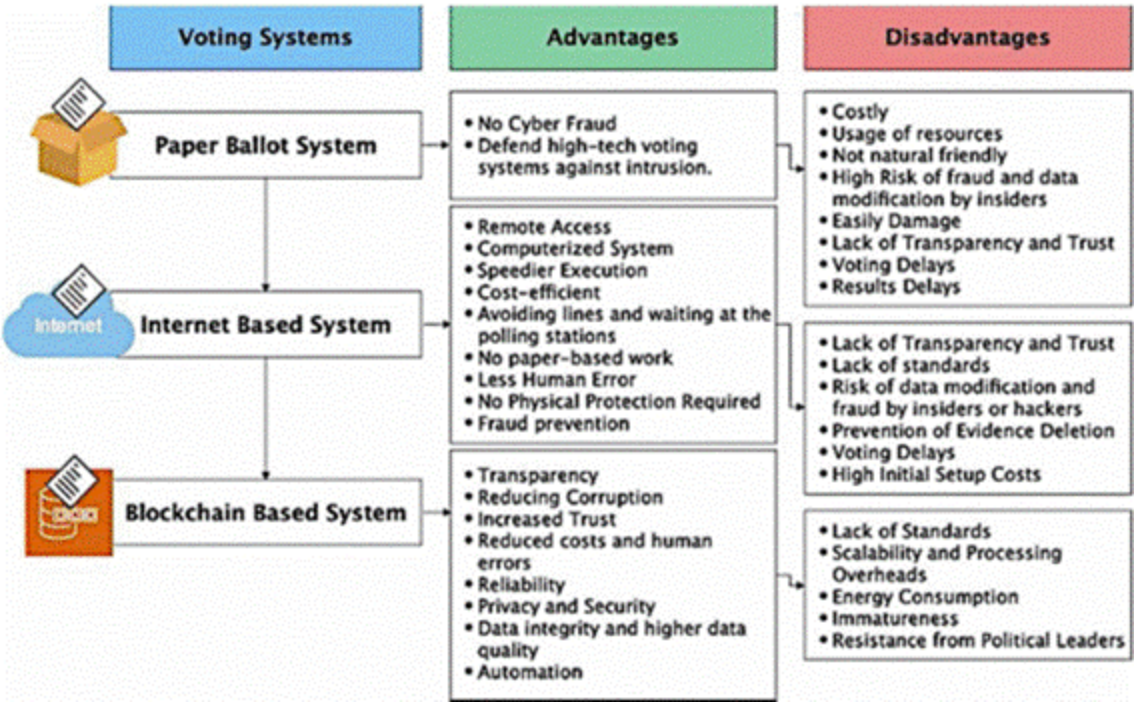

Fig. 1. Blockchain: The blockchain structure

Source: Jafar et al. (2022)

Fig. 1 compares three voting systems: Paper Ballot, Internet-Based (Online), and as well Blockchain-Based, concluding on the fact that while paper ballots are secure from cyber fraud but costly and inefficient, internet-based voting systems offer remote access and efficiency but face transparency and security issues, and blockchain-based voting systems provide enhanced transparency, security, and automation but encounter challenges with scalability, energy consumption, and high setup costs. The research further proposes a cost-efficient and scalable e-voting system based on Ethereum blockchain to address the shortcomings of conventional voting methods, such as lack of transparency, security, and scalability. The paper argued that blockchain can ensure immutable, tamper-proof of election data while reducing costs and improving efficiency, making it suitable for large-scale elections by employing off-chain solutions and sharding techniques to handle high volumes of transactions. However, the protocol faces several issues, including reliance on trusted authorities to manage the off-chain components, potential security risks from quantum attacks, and related issues with scalability as the blockchain grows, which may turn to increase latency and storage requirements (Jafar et al., 2022).

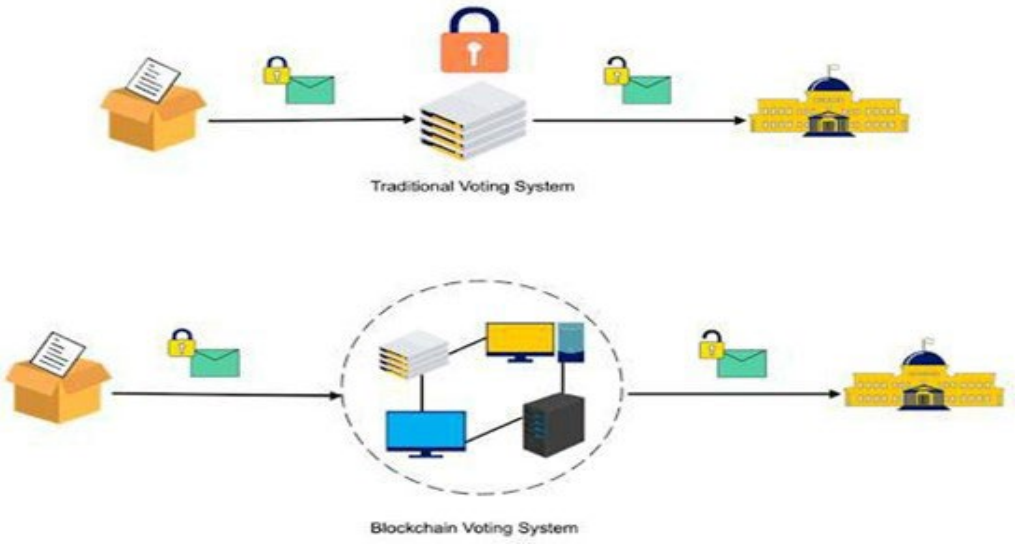

Fig. 2. Traditional (e-voting) vs. blockchain voting system

Source: Jafar et al. (2021)

The aim of using such a data structure is to achieve provable immutability of the blockchain. If any piece of data is altered, the block's hash containing this piece needs to be recalculated or be updated, and the hashes of all subsequent blocks also need to be recalculated (Nofer et al., 2017). This means only the hash of the latest block has to be used to guarantee that all the data remains unaltered. In blockchain solutions, data stored in blocks are formed from all the validated transactions during their creation, in this regards no one can insert, delete or alter the transactions within a block that has already undergone validation without it being noticed (Stephen & Alex, 2018). The initial zero-block, called the "genesis block," usually contains some network settings, for example, the initial set of validators (those who issue the blocks). In further reviews, blockchain technology addressed flaws in the current electoral process by making the polling process transparent and easily available, preventing fraudulent voting, bolstering data security, and verifying poll results. The centralized nature of blockchain prevent tampering or manipulation at the server level, blockchain systems inherently protect against such risks by recording votes on a distributed, immutable ledger. Even though Helios emphasizes individual and universal verifiability, its reliance on a single server contrast with the decentralized and trustless nature of blockchain, which eliminates the need for users to the voting processes (Xiao et al., 2020).

The primary distinction between the two voting systems is seen in Fig. 2. In the traditional online voting systems, votes are cast through a central authority, which makes it easy for someone to alter or change a record; nobody is aware of how to verify that record. In contrast, in decentralized voting systems, data is stored across multiple nodes, making it impossible for someone to manipulate every node and alter the data. As a result, votes cannot be destroyed and can be effectively verified by tallying with other nodes . Elections are won at the polling stations, according to electoral regulations, hence Agbesi and Asante (2019), concluded that if the system permits figures to be manipulated, it could tarnish the reputation of the election process. The problem of manipulating polling station results has led to mistrust in the electoral body and unrest in a number of African countries. However, this research believes that the blockchain revolution presents an opportunity to include auditability, integrity, trust, and transparency into the transmission and storing of results from many locations. These specifications can be met since blockchain technology allows for the creatin of decentralized systems, and multiple stakeholders will own the database rather than just one system administrator in the case of traditional e-voting (Kshetri & Voas, 2018). A detailed literature reviewed of Helios Online voting protocol proposed by Adida (2008), revealed that Helios voting protocol, while offering robust security and transparency through cryptographic techniques such as homomorphic encryption, the ElGamal cryptosystem, and zero-knowledge proofs, relies on a

centralized server for tallying votes, which paved way for potential vulnerabilities related to trust and single points of failure. Instead of implementing blockchain to distribute votes across multiple nodes in a decentralized network, ensuring immutability and transparency through an open ledger, Helios remains dependent on a central authority for vote counting and validation.

2.3 Homomorphic encryption

Based on the history of cryptology, homomorphism was first put out as a possible remedy for the computation without decrypting problem in blockchain voting systems by Rivest et al. (1978) back in 1978. Many attempts were made by analysts worldwide to develop a homomorphic scheme with few operations after Rivest et al. A homomorphic encryption method offers a way to calculate encrypted data directly while maintaining privacy. Homomorphic encryption was used to conduct calculations on ciphertext, producing an encrypted output in the process (Probor et al., 2023). In order to perform computations on data, the majority of encryption systems permit third parties to decrypt the data. Anytime a third party is involved in data computation, security issues arise. It is greatly desired to have an encryption scheme that permits calculation on encrypted data without decryption (Al Badawi et al., 2021). These kinds of encryptions systems are known as homomorphic encryptions. When calculations are performed on encrypted data, homomorphic encryption ensures that the results are the same to those obtained from calculations performed on unencrypted data (Tebaa et al., 2012). A previous definition of homomorphic encryption was an encryption technique in which an algebraic operation on the plaintext is equal to another algebraic operation on the ciphertext (Ogburn et al., 2013). Wu and Haven carried out two experiments in Using variance and mean of massive sets of encrypted data through linear regressions. The number of Homomorphic Encryption for massive Scale Statistical Analysis, wherein they computed the data points in these tests rose to one million and four million elements, respectively (Wu, 2012).

2.4 Homomorphic encryptions in elections

Recently, Homomorphic encryption has been used in the development of online voting platforms and this is driven by the requirement to create cutting-edge security measures in order to enable the widespread adoption of online voting around the globe (Alvarez & Hall, 2003). In the year 2010, homomorphic encryption-based voting was introduced by George and Sebastian, the plan succeeds in achieving receipt-freeness, secrecy, and coercibility. Both yes/no and multi-candidate voting can be conducted using this approach (George & Sebastian, 2010). Huszti presented a voting mechanism based on homomorphic encryption and the Crammer mechanism. Andrea Huszti's voting mechanism integrates homomorphic encryption with the Cramer mechanism, creating a secure electronic voting system that allows encrypted votes to be tallied without ever needing decryption, which intended to maintain voter confidentiality and data integrity. The system achieves essential properties such as eligibility (ensuring only authorized voters can vote), privacy (votes cannot be traced back to individuals), verifiability (voters can confirm their vote was counted correctly without revealing it), receipt-freeness (preventing voters from proving how they voted to avoid coercion), and coercibility resistance (ensuring voters cannot be forced to vote a certain way). Votes are encrypted at the point of casting, and homomorphic encryption allows vote aggregation directly on encrypted data, preserving the privacy of individual votes. The use of anonymous channels further ensures that voters' identities remain hidden throughout the process.

However, despite its robust cryptographic underpinnings, the system is vulnerable to significant security risks. First, side-channel attacks techniques that exploit physical characteristics of the system, such as timing information, power consumption, or electromagnetic leaks could potentially extract sensitive information during vote encryption or tallying. Also, the security of the system hinges on the assumption that authorities managing the decryption keys are trustworthy; any collusion among these authorities or compromise of key management protocols could result in vote manipulation or exposure of voter identities. Additionally, key leakage, whether through insider threats, poor key management, or advanced cryptographic attacks, could undermine the encryption process's security, allowing adversaries to decrypt votes. In all, the reliance on anonymous channels poses a challenge; if these channels are compromised or improperly implemented, it could lead to the de-anonymization of voters, breaking the privacy and receipt-freeness guarantees of the system (Huszti, 2011). A novel voting technique based on the blind signature RSA and the additive homomorphic characteristic of the Paillier cryptosystem was proposed by (Hussien

& Aboelnaga, 2013), effectively achieves eligibility, confidentiality, privacy, uniqueness, and correctness. However, the technique remains vulnerable to potential attacks on key management, possible collusion between authorities compromising voter anonymity, and susceptibility to cryptographic weaknesses in the Paillier cryptosystem, such as chosen ciphertext attacks, which could undermine the security guarantees if not properly mitigated.

Similarly, Yi and Okamoto (2013) proposed a voting technique that ensures voter privacy even under physical coercion or malware attacks on the voter's device, by only revealing the election outcome (win or lose) without disclosing the specific count of yes or no votes; however, several attacks including the potential for side-channel attacks, where adversaries could infer voting patterns through indirect data leaks, and susceptibility to software and hardware manipulation that could compromise the integrity of the results or allow tampering without detection .

A voting system based on homomorphic encryption was presented at a conference session that was captured by Zhao (2014) in order to guarantee anonymity, privacy, and dependability by using homomorphic encryption with the RSA cryptosystem to securely encrypt voting data; however, the system is vulnerable to certain attacks, such as chosen-ciphertext attacks (CCA), key exposure risks, and the inefficiency of RSA in handling large datasets, which could affect scalability and performance, and it also relies on the trustworthiness of key distribution and management. A partly homomorphic cloud-based mobile voting system was described in another conference proceedings published by Will et al. (2015). To demonstrate the system's usefulness, the paper put it into practice. Qualification, non-reuse, non-traceability, verifiability, accuracy of tally, non-coercibility, auditability, accessibility, equity, soundness, and integrity are all attained by the system. However, the system remains susceptible to threats like potential insider attacks, cloud infrastructure breaches, denial-of-service attacks, weaknesses in cryptographic protocols, and privacy risks during data transmission, which could compromise voter anonymity, the integrity of the voting process, and overall system trustworthiness. According to Yang et al. (2018), each ballot is encrypted using the exponential ElGamal cryptosystem before to submission in order to safeguard the confidentiality of the votes. Additionally, the system makes sure that proofs are created and kept for every vote element during the voting process. Before counting, these proofs can be used to confirm each ballot's eligibility and validity without having to decode or read the ballot's content. However, their protocol is never without risks which include susceptibility to chosen-ciphertext attacks, potential inefficiency with large datasets due to RSA's computational overhead, and the reliance on RSA's key length, which could be weakened by advances in quantum computing.

Ravindran and Kalpana (2013) also argued that more capacity is needed for both encryption and re-encryption. In order to pack the encrypted data, data packing is utilized. They proposed a secure voting platform where votes are encrypted, re-encrypted, packed (zipped), and transmitted over insecure channels to ensure privacy, fairness, robustness, and verifiability. Upon receiving the encrypted votes, the system validates each vote, and if valid, proceeds with decryption and unpacking to tally the result and determine the winner. The voter's credentials are verified by the platform’s verifier authority, ensuring eligibility compliance while maintaining individual and universal verifiability. Despite these security features, the process could be vulnerable during the packing and unpacking processes, as improper implementation could allow data leakage or manipulation. Furthermore, transmitting encrypted votes over insecure channels may expose the encrypted votes to man-in-the-middle attacks or replay attacks. And if the verifier authority is compromised, it could lead to unauthorized access or tampering with voter credentials or votes, undermining the system’s security guarantees. Balasubramanian and Jayanthi (2016) introduced a secure voting system that employs the Paillier cryptosystem, known for its additive homomorphic encryption, allowing the tallying of encrypted votes without revealing individual vote content. Voters are assured that their vote is recorded in the Voting Table, enabling them to verify whether their vote was counted while maintaining the confidentiality of each vote. The system restricts participation to eligible voters, ensuring compliance with election requirements.

Despite these features, vulnerabilities exist, particularly with the integrity of the Voting Table, as it serves as the central point of vote verification and could be susceptible to tampering, fraud, or unauthorized access, potentially undermining the accuracy of the vote count. Additionally, the homomorphic encryption used, while secure, can introduce risks such as partial data leakage, where attackers could exploit patterns in the encrypted data or perform side-channel attacks to infer sensitive information about the votes.

Moreover, if any component in the cryptographic process is flawed or compromised, such as improper key management or weak encryption parameters, the confidentiality and correctness of the entire voting system could be jeopardized.

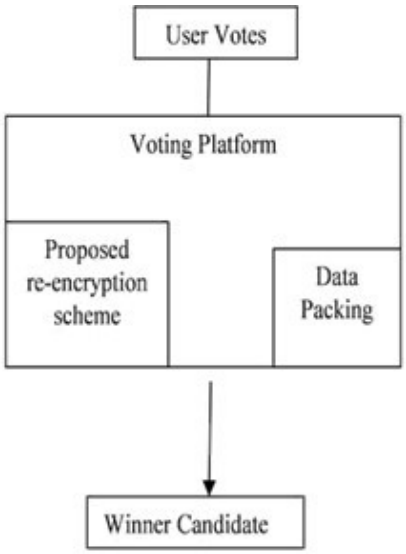

Fig. 3. Flow chart of the proposed system

Source: Balasubramanian and Jayanthi (2016)

2.5 Integration of homomorphic encryption and blockchain in voting protocol

In 1978, Blakley (1979) independently introduced methods for dividing a secret into multiple shares that can be distributed among mutually distrustful agents. This paper outlines a homomorphic property achieved by these and other secret sharing schemes, enabling the combination of multiple secrets through direct computations on the shares. This property minimizes the need for trust among agents and expands the applicability of secret sharing to various new challenges. One application presented here offers a simpler and more efficient approach to verifiable secret sharing compared to earlier methods. Another application described provides a fault-tolerant solution for conducting verifiable secret-ballot elections (Benaloh, 1987).

Jabbar and Alsaad (2017) introduced their first voting techniques based on homomorphic encryption, which allows mathematical operations to be performed directly on encrypted votes (ciphertext) without decrypting them, enabling privacy-preserving tallying in which the votes remain confidential throughout the process; however, with this protocol the possibility of side-channel attacks during the cryptographic operations were later observed, where an attacker could infer information about the encrypted data, as well as challenges related to key management, such as improper handling or exposure of encryption keys that could compromise the system's security. Additionally, if the homomorphic encryption scheme is not properly implemented or the cryptographic parameters are weak, it may result in inefficiencies, performance bottlenecks, or weakened resistance to cryptographic attacks, which could be exploited to manipulate or disrupt the election process.

Qu et al. (2022) proposed a blockchain-based electronic voting system utilizing homomorphic signcryption, which eliminates the need for a traditional trusted third party by using smart contracts to publicly manage the voting process on the blockchain, with ballots encrypted and signed through homomorphic encryption and signcryption algorithms. These algorithms allow the system to efficiently

aggregate votes and produce a homomorphic tally, improving voting efficiency and reducing the computational burden on voters, making the system scalable and practical for large-scale elections. However, there are potential risks associated with smart contract bugs or exploits, which could lead to unauthorized access, tampering, or even denial-of-service attacks on the voting process. Additionally, although blockchain offers transparency, if the encryption keys or signcryption processes are compromised, the confidentiality of votes could be at risk, leading to potential vote manipulation or privacy breaches. And also, relying on blockchain's consensus mechanisms alone might expose the system to vulnerabilities such as 51% attacks, which could disrupt the integrity of the voting process or prevent accurate tallying of results, hence the need to combine the two strong techniques to protect the integrity of each vote cast (Sayeed & Marco-Gisbert, 2019) .

Fan et al. (2020) proposed a voting system where voters use digital signature algorithms to sign their ballots before submission, ensuring that each voter can verify their own vote, and the system can authenticate the origin of the vote; however, as the number of voters and candidates increases, the computational burden and complexity of the ballot tallying and verification process also grow significantly, potentially leading to performance bottlenecks. The risk of signature forgery if the digital signature scheme is not robust enough may occur, the possibility of denial-of-service attacks targeting the computational resources needed for verification, and the increased exposure to replay or man-in-the-middle attacks during the transmission of signed ballots, especially if secure channels are not properly enforced. If the signature verification process is not efficiently scaled, the system may become vulnerable to delays or inaccuracies in tallying, compromising the timeliness and reliability of the election outcome.

3. RESULT

Upon numerous reviews of the existing works in online voting protocols, the findings reveal that existing online voting protocols face significant vulnerabilities, which include centralization risks that create single points of failure, a lack of transparency that undermines voter trust, susceptibility to security breaches such as side-channel and chosen-ciphertext attacks, and scalability challenges that hinder their performance in large-scale elections. Security weaknesses such as susceptibility to Denial of Service (DoS) attacks, malware injections, and Man-in-the-Middle (MITM) attacks were identified, particularly in centralized systems where a breach could lead to widespread manipulation. Privacy concerns were evident, as many protocols failed to guarantee voter anonymity and confidentiality, exposing voters to coercion and vote-selling. Additionally, many systems lacked verifiability and transparency, making it difficult for voters to confirm that their votes were accurately counted, which erodes trust in the system. Scalability was another issue, with existing systems struggling to handle large-scale elections efficiently, leading to delays and security risks.

Furthermore, most systems failed to implement sufficient coercion resistance mechanisms, leaving voters vulnerable in unsupervised settings. Weak voter authentication also opened the door for identity theft and impersonation. Blockchain technology, while addressing some of these issues by decentralizing voting processes and improving transparency, still faced scalability challenges and risks such as a 51% attack. Although blockchain increases transparency, it does not inherently solve voter anonymity, authentication, or coercion resistance issues. Similarly, homomorphic encryption, which allows encrypted data to be processed without decryption, has shown promise in securing vote tallying, but its high computational complexity presents challenges in large-scale elections. In all, in as much as online voting systems have improved accessibility and efficiency, they still suffer from significant vulnerabilities, especially in the areas of security, privacy, scalability, and voter authentication.

Technologies like blockchain and homomorphic encryption offer potential solutions, but they require further development to overcome challenges related to performance and scalability. The findings emphasize the need for a new approach that integrates enhanced security measures, such as robust voter authentication, decentralized consensus mechanisms, and scalable cryptographic protocols. There is the need to proposed

a hybrid blockchain-based voting protocol with homomorphic encryption aims to address these issues and create a more secure, transparent, and trustworthy system for large-scale elections.

4. CONCLUSION

The analysis conducted throughout this study highlights the persistent vulnerabilities and technical limitations of existing online voting systems, particularly regarding security, scalability, privacy, and user trust. Despite notable advancements in cryptographic techniques and system design, issues such as centralized control, susceptibility to cyber threats, and lack of verifiability continue to impede the full realization of secure and trustworthy online elections. While blockchain and homomorphic encryption each offer promising solutions, they also come with their respective challenges blockchain with its scalability and privacy limitations, and homomorphic encryption with its computational intensity. To address these gaps, future research should focus on the development and refinement of hybrid voting protocols that integrate the strengths of both technologies blockchain for its decentralized and tamper-resistant infrastructure, and homomorphic encryption for privacy-preserving vote tallying. Such hybrid solutions should aim to minimize computational overhead while ensuring real-time scalability, making them viable for national and large-scale elections. Emphasis should also be placed on addressing known cryptographic risks such as side-channel attacks, key leakage, and collusion among verification authorities. Moreover, beyond the technical domain, there is a pressing need for interdisciplinary studies that examine the social, legal, and operational challenges surrounding the deployment of secure online voting systems. These include issues related to voter accessibility, digital literacy, inclusivity, and public perception. Systems must be designed with a user-centric approach to foster trust, ensuring transparency and verifiability without compromising usability or voter anonymity. In conclusion, the transition to secure, scalable, and transparent online voting systems is both a technical and societal endeavor. A multidimensional approach that combines cutting-edge cryptography, robust system architecture, and thoughtful policy design is essential. By advancing in these directions, future voting systems can uphold democratic integrity and adapt to the evolving landscape of digital governance.

5. ACKNOWLEDGEMENTS/FUNDING

The authors would like to thank AAMUSTED community, FASME, and all lecturers of the IT Department for their support during the research. The authors did not receive any specific funding for this work.

6. CONFLICT OF INTEREST STATEMENT

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

7. AUTHORS' CONTRIBUTIONS

The authors were responsible for all aspects of the research including conceptualization, methodology, data collection, analysis, and writing of the manuscript.

8. REFERENCES

Adida, B. (2008). Helios: Web-based open-audit voting. In *USENIX Security Symposium* (Vol. 17, pp. 335–348).

Agbesi, S., & Asante, G. (2019). Electronic voting recording system based on blockchain technology. In *2019 12th CMI Conference on Cybersecurity and Privacy (CMI) (pp.* 1–8). IEEE. https://doi.org/10.1109/CMI48017.2019.8962142

Ahmad, A. H., Tabassum, F. N., Ayaz, S. A., Bahir, N., & Meelam, M. (2021). Electronic voting system: Nature, origin and its global application. *International Journal of Innovation, Creativity and Change*, *15*(2), 1334–1337.

Al Badawi, A., Polyakov, Y., Aung, K. M. M., Veeravalli, B., & Rohloff, K. (2021). Implementation and performance evaluation of RNS variants of the BFV homomorphic encryption scheme. *IEEE Transactions on Emerging Topics in Computing*, *9*(2), 941–956. https://doi.org/10.1109/TETC.2019.2902799

Al-Shammari, A. F. N., Villafiorita, A., & Weldemariam, K. (2012). Understanding the development trends of electronic voting systems. In *2012 Seventh International Conference on Availability, Reliability and Security* (pp. 186–195). IEEE. https://doi.org/10.1109/ARES.2012.76

Alvarez, R. M., & Hall, T. E. (2003). *Point, click, and vote: The future of Internet voting*. Rowman & Littlefield.

Balasubramanian, K., & Jayanthi, M. (2016). A homomorphic crypto system for electronic election schemes. *Circuits and Systems*, *07*(10), 3193–3203. https://doi.org/10.4236/cs.2016.710272

Benaloh, J. C. (1987). Secret sharing homomorphisms: keeping shares of a secret (Extended Abstract). In A. M. Odlyzko (Ed.), *Advances in Cryptology --- CRYPTO' 86* (pp. 251–260). Springer Berlin Heidelberg.

Blakley, G. R. (1979). Safeguarding cryptographic keys. *Managing Requirements Knowledge, International Workshop On* (pp. 313-313). IEEE Computer Society. https://doi.org/10.1109/MARK.1979.8817296

Fan, X., Wu, T., Zheng, Q., Chen, Y., Alam, M., & Xiao, X. (2020). HSE-Voting: A secure high-efficiency electronic voting scheme based on homomorphic signcryption. *Future Generation Computer Systems*, *111*, 754–762. https://doi.org/10.1016/j.future.2019.10.016

Ganesh Prabhu, S., Nizarahammed., A., Prabu., S., Raghul., S., Thirrunavukkarasu, R. R., & Jayarajan, P. (2021). Smart online voting system. In *2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)* (pp. 632–634). IEEE. https://doi.org/10.1109/ICACCS51430.2021.9441818

George, V., & Sebastian, M. (2010). An adaptive indexed binary search tree for efficient homomorphic coercion resistant voting scheme. *International Journal of Managing Information Technology*, *2*(1), 1–9.

Hjalmarsson, F. P., Hreioarsson, G. K., Hamdaqa, M., & Hjalmtysson, G. (2018). Blockchain-based e-voting system. In *IEEE International Conference on Cloud Computing, CLOUD* (pp. 983–986). IEEE. https://doi.org/10.1109/CLOUD.2018.00151

Hussien, H., & Aboelnaga, H. (2013). Design of a secured e-voting system. In *2013 International Conference on Computer Applications Technology (ICCAT)* (pp. 1–5). IEEE. https://doi.org/10.1109/ICCAT.2013.6521985

Huszti, A. (2011). A homomorphic encryption-based secure electronic voting scheme. *Publ. Math. Debrecen*, *79*(3–4), 479–496. https://doi.org/10.5486/PMD.2011.5142

Jabbar, I., & Alsaad, S. N. (2017). Design and Implementation of secure remote e-voting system using homomorphic encryption. *Int. J. Netw. Secur.*, *19*(5), 694–703.

Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for electronic voting system—Review and open research challenges. *Sensors*, *21*(17), 5874. https://doi.org/10.3390/s21175874

Jafar, U., Aziz, M. J. A., Shukur, Z., & Hussain, H. A. (2022). A cost-efficient and scalable framework for e-voting system based on Ethereum blockchain. In *2022 International Conference on Cyber Resilience (ICCR)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICCR56254.2022.9996026

Kaliyamurthie, K. P., Udayakumar, R., Parameswari, D., & Mugunthan, S. N. (2013). Highly secured online voting system over network. *Indian Journal of Science and Technology*, *6*(6), 1–6. https://doi.org/10.17485/ijst/2013/v6isp6.15

Kshetri, N., & Voas, J. (2018). Blockchain-Enabled E-Voting. *IEEE Software*, *35*(4), 95–99. https://doi.org/10.1109/MS.2018.2801546

Mursi, M. F. M., Assassa, G. M. R., Abdelhafez, A., & Samra, K. M. A. (2013). On the development of electronic voting: a survey. *International Journal of Computer Applications*, *61*(16). https://doi.org/10.5120/10009-4872

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183–187. https://doi.org/10.1007/s12599-017-0467-3

Ogburn, M., Turner, C., & Dahal, P. (2013). Homomorphic Encryption. *Procedia Computer Science*, *20*, 502–509. https://doi.org/10.1016/j.procs.2013.09.310

Osgood, R. (2016). The future of democracy: Blockchain voting. *COMP116: Information Security*, 1–21.

Probor, M. N., Ahmed, M., Kabir, S. B., Fuad, M. M., & Bushra, T. (2023). *Blockchain based e-voting system with homomorphic encryption and threshold signature*. Brac University.

Qu, W., Wu, L., Wang, W., Liu, Z., & Wang, H. (2022). An electronic voting protocol based on blockchain and homomorphic signcryption. *Concurrency and Computation: Practice and Experience*, *34*(16). https://doi.org/10.1002/cpe.5817

Ravindran, S., & Kalpana, P. (2013). *Data Storage Security Using Partially Homomorphic Encryption in a Cloud*. https://api.semanticscholar.org/CorpusID:62933905

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126. https://doi.org/10.1145/359340.359342

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences*, *9*(9), 1788. https://doi.org/10.3390/app9091788

Smith, A. D., & Clark, J. S. (2005). Revolutionising the voting process through online strategies. *Online Information Review*, *29*(5), 513–530. https://doi.org/10.1108/14684520510628909

Stephen, R., & Alex, A. (2018). A review on blockchain security. *IOP Conference Series: Materials Science and Engineering*, *396*(1), 12030.

Tebaa, M., El Hajji, S., & El Ghazi, A. (2012). Homomorphic encryption method applied to Cloud Computing. In *2012 National Days of Network Security and Systems* (pp. 86–89). IEEE. https://doi.org/10.1109/JNS2.2012.6249248

Thakur, S., Olugbara, O. O., Millham, R., Wesso, H. W., & Sharif, M. (2014). Transforming voting paradigm - The shift from inline through online to mobile voting. In *2014 IEEE 6th International Conference on Adaptive Science & Technology (ICAST) (pp.* 1-7). https://doi.org/10.1109/ICASTECH.2014.7068115

Will, M. A., Nicholson, B., Tiehuis, M., & Ko, R. K. L. (2015). Secure voting in the cloud using homomorphic encryption and mobile agents. In *2015 International Conference on Cloud Computing Research and Innovation (ICCCRI)* (pp. 173–184). IEEE. https://doi.org/10.1109/ICCCRI.2015.30

Wu, D. J. (2012). *Using homomorphic encryption for large scale statistical analysis*. FHE-SI-Report, Univ. Stanford, Tech. Rep. TR-dwu4.

Xiao, S., Wang, X. A., Wang, W., & Wang, H. (2020). Survey on blockchain-based electronic voting. In H. and M. H. Barolli Leonard and Nishino (Ed.), *Advances in Intelligent Networking and Collaborative Systems* (pp. 559–567). Springer International Publishing. https://doi.org/10.1007/978-3-030-29035-1_54

Yang, X., Yi, X., Nepal, S., Kelarev, A., & Han, F. (2018). A secure verifiable ranked choice online voting system based on homomorphic encryption. *IEEE Access*, *6*, 20506–20519. https://doi.org/10.1109/ACCESS.2018.2817518

Yi, X., & Okamoto, E. (2013). Practical Internet voting system. *Journal of Network and Computer Applications*, *36*(1), 378–387. https://doi.org/10.1016/j.jnca.2012.05.005

Zhao, Z. (2014). An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. *Journal of Medical Systems*, *38*, 1–7. https://doi.org/10.1007/s10916-014-0013-5