IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 4 July 2023, accepted 17 July 2023, date of publication 20 July 2023, date of current version 28 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3297492

RESEARCH ARTICLE

Blockchain-Based Secure Voting Mechanism Underlying 5G Network: A Smart Contract Approach

SACHI CHAUDHARY[1], SHAIL SHAH[1], RIYA KAKKAR[1], (Student Member, IEEE), RAJESH GUPTA[1], (Member, IEEE), ABDULATIF ALABDULATIF[2], (Member, IEEE), SUDEEP TANWAR[1], (Senior Member, IEEE), GULSHAN SHARMA[3], AND PITSHOU N. BOKORO[3], (Senior Member, IEEE)

[1]Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat 382481, India
[2]Department of Computer Science, College of Computer, Qassim University, Buraydah 52571, Saudi Arabia
[3]Department of Electrical Engineering Technology, University of Johannesburg, Johannesburg 2006, South Africa

Corresponding authors: Sudeep Tanwar (sudeep.tanwar@nirmauni.ac.in), Rajesh Gupta (rajesh.gupta@nirmauni.ac.in), and Gulshan Sharma (gulshans@uj.ac.za)

ABSTRACT **Purpose**: With the advancement and modernization of Information and Communication Technology, electronic voting (e-voting) has been adopted across the globe for conducting a secure and efficient voting procedure. However, e-voting can be easily exposed to various malicious attacks such as denial-of-service, malware, insider, compromised credentials, etc., that can risk the voter's privacy and affect the final voting results. Thus, we have considered the decentralized and immutable blockchain technology for completing the voting procedure securely. Nevertheless, many researchers have considered blockchain to mitigate the security and privacy issues of the voting procedure, but they ignored the aspect of cost-efficiency, latency, and response time while voting. **Method**: The idea of the proposed mechanism is to deploy and implement the smart contract in the Remix Integrated Development Environment (IDE) involving number of voters electing the candidate with various functionalities. Moreover, we considered the amalgamation of blockchain and IPFS to overcome the data storage cost issues of blockchain for voters and candidates communicating through 5G wireless network. The 5G network, with its low latency, high availability, and high reliability facilitates high data rate and reliable communication between voters and candidates to complete the voting procedure efficiently. **Results**: The deployed smart contract of the proposed voting mechanism highlight various functionalities required for electing the candidate by the voters. Moreover, the deployed smart contract is evaluated and analyzed considering various performance metrics such as gas consumption analysis for smart contract functions and number of voters, cost analysis for smart contract functions, bit error rate, and storage cost comparison with the traditional scheme. We have also verified the security of the proposed voting mechanism using Echidna security tool which shows the election of candidate without any threat. **Conclusion**: Finally, we have presented a blockchain-based voting mechanism in which IPFS and 5G is employed to avail the cost-efficient, reliable, and secure candidate election by the voters. Moreover, the voters and candidates can communicate with lower response time and high reliability using 5G network so that smart contract consisting of all the functionalities related to the candidate election can be executed efficiently in the Remix IDE.

INDEX TERMS Blockchain, smart contract, 5G, IPFS, e-voting, remix IDE, Echidna.

I. INTRODUCTION

Over the past decade, many countries have adopted voting methods in a modern democracy. As a result, the voting methods have significantly evolved, which can be utilized to elect the leader for a class committee to the election of a national leader. However, voting mechanisms have yet to be evolved to that extent in many countries. For example, the U.S. conducted the presidential election using paper voting. Paper voting is a type of voting system that uses paper

The associate editor coordinating the review of this manuscript and approving it for publication was Maurizio Casoni.

ballots in the form of election paper, where votes are counted manually, which is quite time-consuming and requires substantial human resources to complete the counting without delay. Thus, the concept of a paper voting system has several disadvantages of huge incurred cost, security, and storage issues for conducting elections at a large scale [1]. Moreover, older people can't vote manually at a polling station. Considering the aforementioned disadvantages, the voting methods have evolved greatly with the advancement of Information and Communication Technologies (ICT) [2], [3].

For instance, the first type of computerized voting system is a punch card system in which a voter uses a punch card device to indicate their votes on the punch card. Votes are counted by passing them through a punch card reader. Another type of voting system uses optical scanners in which voters indicate their preferences on a paper ballot by filling the bubbles corresponding to the particular candidate, which is being read by optical scanning devices [4]. However, the aforementioned voting systems do not ensure a secure, cost-efficient, and fast election for voters and candidates. Moreover, they can be prone to human errors or faults while manually handling the voting mechanism. Therefore, to mitigate the aforementioned challenges, many researchers have discussed electronic voting (e-voting) systems to avail a secure and cost-efficient election environment for voters and candidates. They have utilized various cryptographic techniques to ensure the security and integrity of the voting systems. For instance, Anie et al. [5] considered various cryptographic aspects such as digital signature, encryption, and threshold decryption to provide confidentiality, authenticity, and integrity in the voting mechanism. Then, Sheela and Franklin [6] designed an e-voting protocol that utilizes public-key cryptography to ensure security and integrity during the voting procedure. Their e-voting protocol has yet to consider real-time implementation and is also vulnerable to large-scale efficiency providence.

Furthermore, the authors of [7] considered an e-voting system that utilizes homomorphic encryption to ensure security and privacy in the voting mechanism. Homomorphic encryption allows computations to be performed on ciphertext without decrypting it first. Then, Suwarjono et al. [8] implemented cryptography techniques to ensure voter data secrecy during e-voting. Further, the security and privacy of voting data are ensured by utilizing Rivest-Shamir-Adleman (RSA) algorithm. Still, the applied cryptographic algorithm does not yield efficient results due to the high computation time required while performing the operations in an e-voting system. But, the aforementioned conventional cryptography mechanisms applied for a secure e-voting system can be vulnerable to various security attacks such as data manipulation, impersonation, data phishing attacks, etc., further disrupting the anonymity and integrity of the e-voting system. Further, it can pose several challenges, such as voter coercion, the anonymity of votes, voter's eligibility for voting, compromising voter's identity, mismatched fingerprints, and facial features leading to false acceptance and false rejections, which raises the need to introduce a secure and decentralized platform for preserve and secure e-voting [9]. Therefore, considering the aforementioned trust and privacy issues in the e-voting system, we have considered the amalgamation of blockchain technology with the Interplanetary File System (IPFS) protocol to provide a secure and efficient e-voting system for voters and candidates through 5G wireless network. The secure, decentralized, and immutable blockchain network with IPFS maintains security, cost-efficiency, and anonymity in the e-voting system, providing a transparent voting environment for voters and candidates [10].

Before getting insights into the e-voting system, we need to focus on the conventional voting mechanism to further understand the working of the e-voting and its advantages over traditional voting. Currently, many countries utilize conventional voting mechanisms, which are quite time-consuming and pose security challenges for voters and candidates involved in the election. Moreover, it is not feasible for elderly people to present physically at the polling booth for voting purposes. Figure 1 shows the procedure of the traditional voting mechanism, which initiates with the voters presenting their identity proof for authentication purposes so that it can be decided whether they are validated for voting. Then, the white electoral ballots are delivered to the voters personally, which they can use to vote for a particular candidate in an assigned secure space. However, data transactions involved in the traditional voting can easily be vulnerable to security attacks such as data manipulation, phishing, and spoofing and need to improve its accessibility for elder people with the adoption of innovative and advanced technologies that can be achieved with the help of e-voting system.

Towards this goal, we have highlighted the working of the e-voting system (as shown in Figure 2), which is bifurcated into various steps, which are mentioned as follows:

- *Request for vote*: In the e-voting system, users first log into the voting system using their credentials, then the system checks and confirms the social security number (SSN) and voting confirmation number candidates provided to them by the local authorities. The authenticity of the voter is required to check if they are authorized to cast a vote for a particular candidate. The e-voting system does not allow voters to generate their identities for registration purposes; otherwise, they can generate many fake identities to cast a vote illegally, increasing the probability of a Sybil attack against the e-voting system [12].
- *Casting a vote*: Voters have to either vote for one of the candidates or cast a protest vote. Vote casting is usually performed through a user-friendly interface after getting authenticated by the local authorities, which verify the SSN and voting confirmation number of voters.
- *Encrypting votes*: After the user casts his vote, the system generates an input that contains the voter identification number followed by the complete name

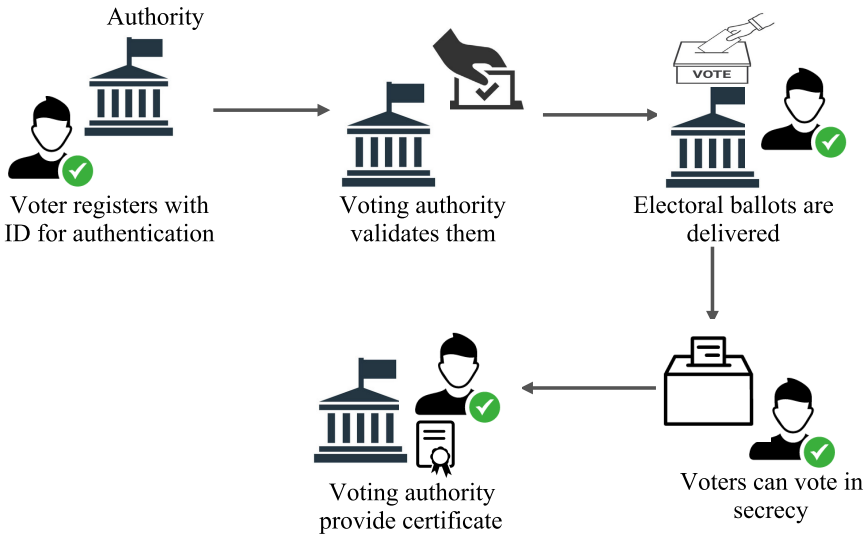


FIGURE 1. Traditional voting mechanism.

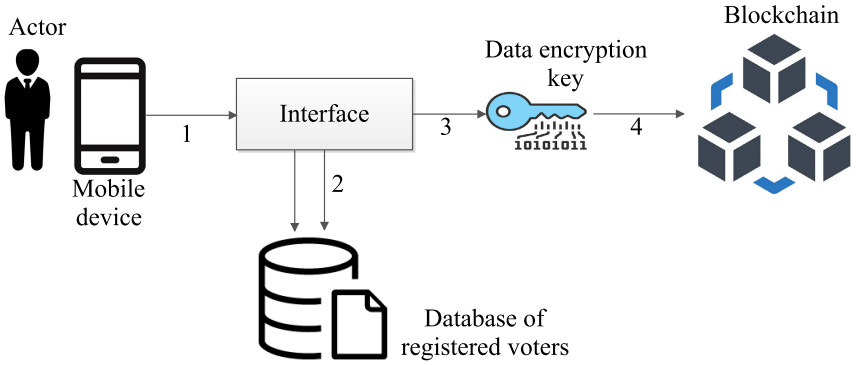


FIGURE 2. E-Voting system.

of the voter as well as the hash of the previous vote. In this way, each input will be unique to ensure the uniqueness of the encrypted output. Furthermore, the information related to each vote can be encrypted using a secure hash algorithm (SHA) one-way hash function that can't be reversed, ensuring the voter information's confidentiality.

- *Addition of vote to the Blockchain*: The encrypted votes must be stored in a secure and decentralized blockchain network so voters can vote for a particular candidate, ensuring a transparent and private election environment. For that, Figure 3 shows how voting information for the candidates can be recorded in the blockchain network in which each block gets linked to the previously casted vote for n number of candidates. Further, the smart contract can be executed for secure data storage in the blockchain. The execution of a smart contract proves to be efficient and secure to perform and add the data transactions to the blockchain after fulfilling the pre-determined conditions of the smart contract. Moreover, any centralized or third-party system can't interrupt the execution of data transactions, eliminating the security issues associated with data storage [13].

Furthermore, many researchers have implemented e-voting systems utilizing cryptography techniques that a malicious attacker can easily forge or manipulate. Moreover, the attackers can modify the data associated with candidates and voters involved in the election, which can affect the election's final result. For instance, Anjima and Hari [14] discussed a secure cloud e-voting system using Homomorphic Elliptical Curve Cryptography. Nevertheless, data stored at a cloud server can be vulnerable to various security attacks, impacting the voting procedure's transparency and confidentiality. Considering the outlook of the literature, we have proposed a blockchain-based secure voting mechanism using IPFS over the 5G network by implementing the smart contract to provide a secure voting environment for the involved voters and candidates. Moreover, the 5G wireless network equipped in the mobile device of the voters through which they can elect the candidate and voting data can be transferred with high availability and reliability to the blockchain based on the implemented smart contract [15].

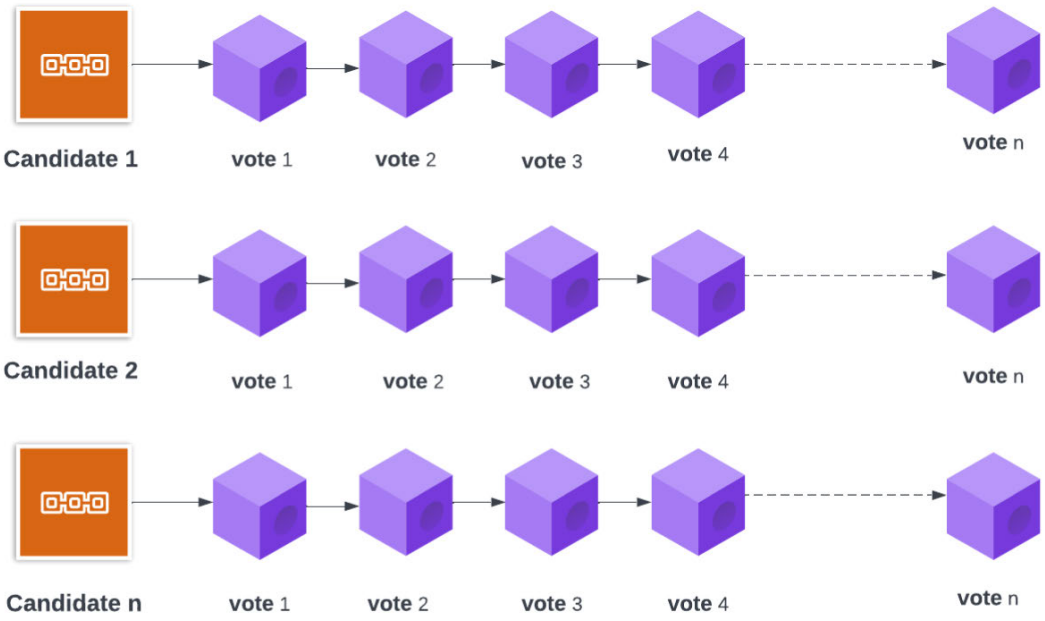


FIGURE 3. Blockchain structure for candidates [11].

The research contributions of the paper are as follows:

- We have proposed a secure blockchain and IPFS-enabled e-voting mechanism for participants in the election.
- We have employed an IPFS-based cost-efficient protocol with the proposed voting mechanism to avail a secure and reliable voting environment for the voters and candidates in the election.
- We have utilized the 5G wireless network to improve the communication between voters and candidates in terms of high efficiency and availability so that voting transactions can be performed efficiently through blockchain.
- Further, we have deployed a smart contract for the proposed voting mechanism considering all the functionalities required for a secure and reliable election to elect the winning candidate. Moreover, we have performed a security analysis of the voting mechanism using the Echidna tool to secure the election procedure without any bugs or threats.
- The simulation of the proposed voting mechanism is evaluated and analyzed on an Ethereum test network considering parameters such as gas consumption analysis based on smart contract functions and the number of votes, and cost analysis for smart contract functions. Moreover, we have compared the proposed mechanism with traditional scheme in terms of storage cost and bit error rate.

The organization of the rest of the paper is as follows. Section II presents the literature survey. Section III discusses the System Model and Problem Formulation. Section IV presents the proposed voting mechanism. Next, section V shows the performance evaluation of the proposed voting mechanism. Then, Section VI presents the security analysis of the smart contract of the proposed mechanism. Section VII opportunities and challenges of the proposed mechanism. Finally, Section VII concludes the paper with future work.

II. LITERATURE SURVEY

To develop a democratically responsible and secure voting mechanism, many researchers have implemented blockchain technology to overcome the issues of traditional voting systems. Table 1 shows the comparative analysis of state-of-art voting approaches with the proposed voting mechanism. Some research works are: Kaveri et al. [9] proposed a blockchain-integrated distributed e-voting framework to support rational and open plans. They have considered e-voting along with the facility to enable the citizens to update their votes within a fixed duration. Then, Lalitha et al. [24] presented a decentralized online voting mechanism, which uses Ethereum and helps validate votes using Aadhar Cards. Also, the fingerprints and faces are verified using a database. Further, encrypting the votes prevents the vote from tampering and enables a voter only to vote once. The results are also provided quickly, reducing counting errors and labor costs.

Similarly, Alvi et al. [21] adopted an Ethereum 2.0 blockchain platform focused on ensuring safe, secure, and completely transparent voting by preserving the privacy of the voters' data against malicious attacks. However, they did not focus on scalability, delay rate, and reliability issues due to the execution of huge transactions over the blockchain. Then, Kohad et al. [22] improved the performance of the

TABLE 1. Comparative analysis of different state-of-the-art explainable AI frameworks.

Author	Year	Purpose	Pros	Cons
Alvi *et al.* [16]	2020	Blockchain enabled e-voting framework using smart contracts and side-chain	Cost-effective, better performance	Lacks real-time implementation
Takahashi *et al.* [17]	2021	Blockchain-enabled voting for high-security NFT	It provides non-interchangeable assets, highly secure	Not cost-effective, hard to implement in real life.
Puneet *et al.* [18]	2021	Ethereum blockchain-based decentralized voting platform	Provides inter-state residency, distributed ledger provides access to everyone, secured and unaltered, accuracy in counting, no fraud possible, the solved problem of trust among users	Some tampering possible, little less transparency provided.
Sober *et al.* [19]	2021	Interoperable oracle based on blockchain voting framework	Highly inter-operable, remarkable cost efficiency achieved due to single signature verification	Expensive to implement the smart contract in a real-life scenario, not as secure as compared to other systems
Suwarjono *et al.* [8]	2021	Cryptography based secure electronic voting system	Provides confidentiality and data-integrity	Quite slow and complex procedure.
Rathee *et al.* [20]	2021	E-voting system deployment with IoT enabled smart cities	Secure against message alteration, DDoS, and DoS attacks	Data storage cost and latency issues are not considered
Alvi *et al.* [21]	2022	Blockchain-based mechanism for secure digital voting system	High security and transparency	Need to focus on scalability, delay rate, and reliability
Kohad *et al.* [22]	2022	Blockchain-based e-voting with multiobjective genetic algorithm	Improved scalability	Security and privacy concerns
Pawlak *et al.* [23]	2018	Blockchain-based intelligent and multi-agent-based e-voting system	Verifiable and less complex	Security, efficiency, and data storage cost challenges
Kaveri *et al.* [9]	2022	Reliable e-voting system with the use of blockchain	Easy to verify votes, open system, rational in decision making, smarter and reliable than traditional systems.	Threat to system as update and changing of votes feature enabled, not secure
Lalitha *et al.* [24]	2022	Blockchain-based decentralized online voting mechanism	Voting from any place, authentication through Aadhar card, tamper-proof, provides election outcomes quickly, reduces manual cost and provides higher accuracy in counting.	Some chances of vote tampering persist, not cost-effective
Naidu *et al.* [25]	2022	Blockchain and homomorphic encryption for protected voting	Secure against data manipulation and tampering	No discussion on response time and latency
Farooq *et al.* [26]	2022	Transparent voting system using blockchain technology	Reduces injustice during voting, reliable, transparent, secure voting transactions	Not perfect to be implemented on a large scale
Zhu *et al.* [27]	2022	Multi-district elections based on blockchain-enabled e-voting system	Authentication provided to all citizens for their votes, proper counting of votes through division in different layers, highly secured, satisfy multi-district election needs	Availability issues, cost issues
Kumar *et al.* [28]	2023	Blockchain and smart contract-based e-voting system	Transparent and authenticated	Ignored the scalability, latency, and cost-related challenges
The proposed mechanism	2023	Blockchain-based secure voting mechanism	Secure, reliable, and cost-efficient	-

blockchain network for voting in terms of scalability by utilizing the multiobjective genetic algorithm with the sharding, but it can cause vulnerability to the data against various security attacks such as cyber, collusion, and phishing. Later, the authors of [23] proposed an intelligent and multi-agent system utilizing blockchain for an effective e-voting system. The proposed system needs to improve its security against various attacks, such as data manipulation, impersonation, and phishing. Further, to ensure the security and privacy in the voting system, Naidu et al. [25] considered the amalgamation of blockchain and homomorphic encryption to ensure the verifiable and immutable data transactions during the voting procedure without any tampering of data. The aforementioned authors did not consider improving the latency and response time of data communication in the voting system. In this regard, the authors in [20] implemented the blockchain-based e-voting system for IoT-enabled smart cities. They have utilized the 802.11 network to enable communication between participants of the voting system in which latency, scalability, response time, and reliability aspects are not considered to that extent.

Further, considering the scalability of the system, the authors of [26] proposed an efficient mechanism to make the voting process transparent through blockchain. They have provided a digital platform to conduct voting through blockchain, which further improves the scalability of the system using a consensus mechanism. A chain security framework is also applied to make votes secure using encryption, reducing the probability of a 51% attack. Nevertheless, despite the improved security in the voting system, the aforementioned researchers did not consider the various aspects of the voting system, such as vote repetition, dead votes, improper registration, problems in reflecting voting results, etc. Thus, considering the aforementioned challenges in the voting system, Zhu et al. [27] proposed a multi-district voting system based on blockchain technology. All the voters are authenticated for registration based on the formed two-layer system. The bottom layer keeps a record of votes in a particular district, and the upper layer records the total votes of people in the election. Then, Puneet et al. [18] presented distributed voting framework based on Ethereum, which provides high integrity and inter-state residing voters to vote efficiently. It also provides high trust and transparency in the voting system with the help of cryptographically secured votes cast by the voters. Next, Subha et al. [29] discussed a blockchain-based voting system with high security. Iris recognition is used to identify unique patterns through infrared and produces an encrypted bit pattern to match the voting process to confirm a person's identity. For partially sighted voters, fingerprint scanning is used along with Iris scanning. Further, Vairam et al. [30] considered an e-voting system containing all the legitimate voting functions. Here, blockchain is used to offer security and transparency for fair elections. Then, Ramalingam et al. [31] proposed an e-voting system using proxy multi-signature based on blockchain. It aims to resolve the problems in other blockchain-enabled e-voting systems, like high maintenance costs and storage space requirements. Alvi et al. [16] provides the side-chain concept instead of an expensive ethereum based blockchain to produce an e-voting framework. They aim to provide a cost-effective solution using a side-chain mechanism that performs operations using the same currency and further returns the results to the main chain for computations. The researchers have tried to provide security in the e-voting system with the help of a decentralized blockchain network. But, they have yet to consider other aspects such as cost-efficiency, efficiency, response time, bit error rate, and availability in their voting system. Motivated by the above-mentioned challenges, we have proposed a blockchain and IPFS-based voting mechanism using 5G network which provide a secure, efficient, and cost-efficient voting environment for voters and candidates.

III. SYSTEM MODEL AND PROBLEM FORMULATION

This section discusses the system model and problem formulation of the proposed voting mechanism, which is mentioned as follows:

A. SYSTEM MODEL

The proposed voting mechanism is designed for participants, i.e., voters and candidates, with the help of blockchain. The proposed voting mechanism involves communication between stakeholders, i.e., voters, candidates, and the election commission, to execute the election efficiently over a 5G network. The election commission acts as an administrator body and provides the data of the voter's list. Voters and candidates can request registration from the election commission to get themselves authenticated for the election. Then, the election commission checks and confirms the validity of the participants involved in the voting. The data of new voters are also added to the election commission so that voters can vote for an individual candidate only.

Moreover, the total votes for each candidate are displayed throughout the voting procedure to enable a transparent environment for the participants. After voters and candidates get validated by the election commission, a smart contract executes to confirm if data associated with voters and candidates can be added to the blockchain network through an intermediary IPFS protocol. Thus, data transactions between voters and candidates can be performed securely with the help of a blockchain network. Now, the total votes for a particular candidate being managed by the election commission can be considered to announce the winning candidate based on the maximum votes cast by the voters for the particular candidate.

B. PROBLEM FORMULATION

In the proposed voting mechanism, we have considered v number of voters $\{\alpha_1, \alpha_2, \ldots\ldots, \alpha_v\} \in \alpha_a$ willing to vote in the election and c number of candidates $\{\gamma_1, \gamma_2, \ldots\ldots, \gamma_m\} \in \gamma_g$ participate in the election for winning it with the maximum number of votes. Now, the election commission Υ can communicate with voters and candidates to authenticate their identity before participating in the election. Thus, we can define the communication between voters, candidates, and the election commission in the voting mechanism, which is mentioned as follows:

$$\sum_{a=1}^{v} \alpha_a \xrightarrow{\epsilon} \Upsilon \; and \; \Upsilon \xrightarrow{\epsilon'} \sum_{a=1}^{v} \alpha_a \tag{1}$$

$$\sum_{g=1}^{m} \gamma_g \xrightarrow{\varepsilon} \Upsilon \; and \; \Upsilon \xrightarrow{\varepsilon'} \sum_{g=1}^{m} \gamma_g \tag{2}$$

where ϵ and ε signify the registration request of v the number of voters and c number of candidates to the election commission to participate in the voting mechanism. Then, ϵ' and ε' represent the validation by the election commission to check their authenticity before they get involved in the voting mechanism.

Now, the voting data (registration) associated with the voters and candidates must be stored securely through the blockchain network [32]. For that, we have considered an intermediary IPFS protocol that stores the voting data in a cost-efficient way after the execution of the smart contract for

validating the data. Once the smart contract authenticates the voting data, it can be stored in the IPFS protocol. Moreover, IPFS permits voting data to get added to the blockchain network by returning them the hash keys θ_{α_a} and ϑ_{γ_g} for voter and candidate. Now, the voting data transactions can be added and accessed through the blockchain network by ensuring a secure voting mechanism using public key cryptography corresponding to the public and private key of the voter $(\psi^{\alpha_a}, \omega^{\alpha_a})$, which is defined as follows:

$$\Psi(\alpha_a, \gamma_g) = (\theta_{\alpha_a}, \vartheta_{\gamma_g}) \tag{3}$$

$$\lambda^{\psi^{\alpha_a}}(\kappa^{\omega^{\alpha_a}})(\Psi(\alpha_a, \gamma_g)) = \Psi(\alpha_a, \gamma_g) \tag{4}$$

Next, the voting data contains the total number of votes by the voters that can be used to elect the winning candidate. Thus, the maximum number of votes decides the winning candidate, and that winner's information can be transferred to the election commission for the further procedure to appoint that particular candidate.

IV. THE PROPOSED VOTING MECHANISM

In this section, Figure 4 shows the proposed voting mechanism in detail as a 3-layered architecture which is bifurcated into three layers, i.e., the Stakeholders layer, election commission layer, and winner layer, which is mentioned as follows:

A. STAKEHOLDERS LAYER

The stakeholder's layer is the first layer of the proposed voting mechanism which comprises of v number of voters$\{\alpha_1, \alpha_2, \ldots\ldots, \alpha_v\} \in \alpha_a$ associated with the u number of mobile devices $\{\mu_1, \mu_2, \ldots\ldots, \mu_u\} \in \mu_U$ who can vote in the election to elect the c number of candidates $\{\gamma_1, \gamma_2, \ldots\ldots, \gamma_m\} \in \gamma_g$ who are contesting for winning the election. Next, the election commission gives the candidate list, and there are c number of candidates participating in the election. Thus, voters can elect candidates after being verified by the election commission. The above-mentioned associations are represented as follows:

$$\alpha_a \xrightarrow{elect} \sum_{g=1}^{m} \gamma_g \tag{5}$$

Moreover, the voting data acquired from the voters with the help of 5G-enabled mobile devices for electing the candidate should be foremost registered with the election commission that needs to be further validated by the smart contract which is discussed in the next layer of the proposed voting mechanism. However, before discussing about the election commission, we need to highlight the ultra-intelligent features of 5G such as high efficiency, high data rate, low response time, which helps to process the voting data reliably and efficiently for selecting the candidate in the election. Next, the election commission also monitors and keeps track of the data associated with the voters and candidates. Also, if any new voter is arriving for the vote, then their data can be managed by the election commission. So that voters can also vote for an individual candidate maintaining integrity in the election environment. Further, validation of voting data by the election commission and execution of the smart contract for performing the voting data transactions through blockchain is discussed in the election commission layer.

B. ELECTION COMMISSION LAYER

Now, the communication between voters and candidates is explained in the previous layer (stakeholders layer), corresponding to the data associated with the voters and candidates processed through the 5G-enabled wireless technology considered with the mobile devices through which voters can vote to elect the candidate. So that, efficient processing of voting data due to the usage of a 5G communication network can be considered for verification and anonymity by implementing the smart contract (after authenticating with the election commission) for further voting transactions through blockchain. Voting data associated with voters and candidates can easily be exploited by malicious attackers, making it vulnerable to various security attacks such as data manipulation, impersonation, cyber-attacks, etc. Thus, the security and privacy of the voting need to be strengthened to protect the confidential data of voters and candidates in the voting mechanism, which can be achieved with the election commission and blockchain network. So the data of voters and candidates can be verified by the election commission in the election commission layer. If the election commission validates the identity of voters and candidates, then their data can be tracked or monitored by the election commission. For that, voters of age greater than 18 can only be registered and their details are further added to the election commission data through the blockchain network. The candidates are also registered and their details are matched with the election commission data before displaying them to the general public for voting. Further, the voters validated by the election commission can only vote for the desired candidate once. Moreover, the votes are displayed in the voting procedure. However, the identity of the voters is protected using encoded identities displayed on the dashboard. The election commission manages various aspects of voting data ζ, such as displaying the total number of votes for respective candidates, election name, number of candidates, and their associated data for the public.

$$\sum_{a=1}^{v} \alpha_a = total\ votes \tag{6}$$

$$\sum_{g=1}^{m} \gamma_g = total\ candidates \tag{7}$$

$$\Upsilon = \{\zeta(\sum_{a=1}^{v} \alpha_a), \zeta(\sum_{g=1}^{m} \gamma_g)\} \tag{8}$$

Next, the data of voters and candidates can be added and accessed through the blockchain network that works as a distributed, immutable, and decentralized public ledger

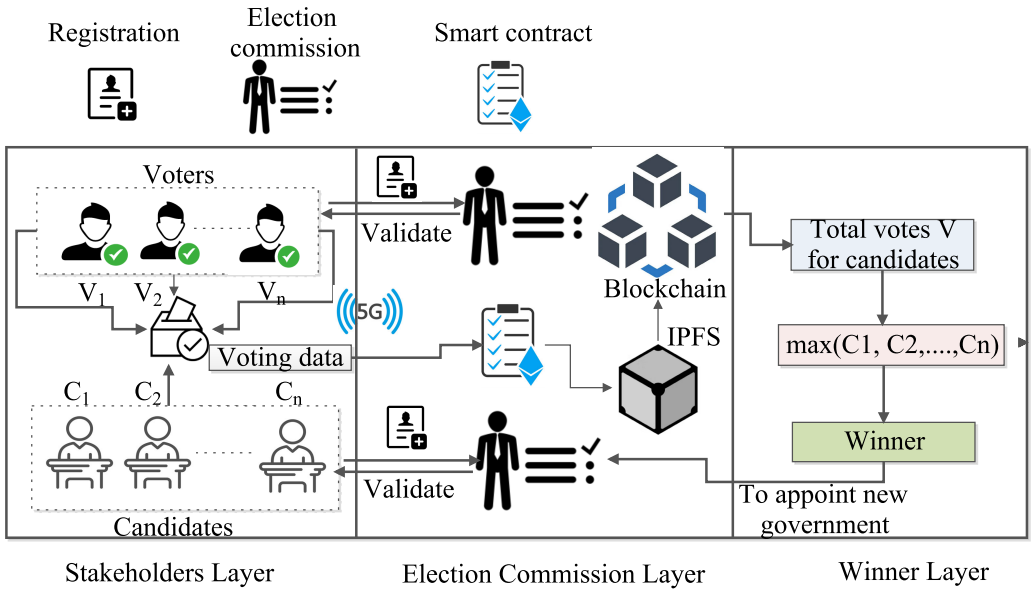


FIGURE 4. The proposed voting mechanism.

technology that facilitates secure and protected access of voting data transactions (verified by the election commission). Moreover, the blockchain utilized the proof-of-work (PoW) consensus protocol to validate and authenticate the data transactions of voters and candidates involved to complete the voting procedure. In PoW, all the participants of the voting mechanism should agree on the same decision while verifying and validating the data transactions that is generated by the miners. Miners validate the data block by solving the cryptographic puzzle and they also get rewarded for the same. However, voting data access and storage should be performed through IPFS for a cost-efficient and reliable voting mechanism. For that, voting data authenticated by the election commission can register themselves by executing the smart contract, which is written based on pre-determined conditions. Once verified by the smart contract, voting data ζ can be stored in the IPFS that can be further accessed through the blockchain network in a secure and decentralized manner.

$$\sum_{a=1}^{v} \alpha_a \xrightarrow{register} \text{smart contract} \tag{9}$$

$$\sum_{g=1}^{m} \gamma_g \xrightarrow{register} \text{smart contract} \tag{10}$$

$$\zeta(\sum_{a=1}^{v} \alpha_a), \zeta(\sum_{g=1}^{m} \gamma_g) \xrightarrow{\varepsilon} \text{IPFS} \tag{11}$$

where ε signifies the voting data storage in IPFS after the execution of the smart contract.

C. WINNER LAYER

The data acquired from the election commission layer which is validated by the election commission is forwarded to the winner layer to complete the voting procedure in the election based on the total number of votes. Thus, the total votes from the election commission layer which can be accessed through the secure blockchain network are considered as an output for the winner layer to determine the winning candidate based on the maximum number of votes (N). The final results can be viewed when all the voters have voted. Also, the intermediate results can be viewed and displayed based on the permission granted by the election commission.

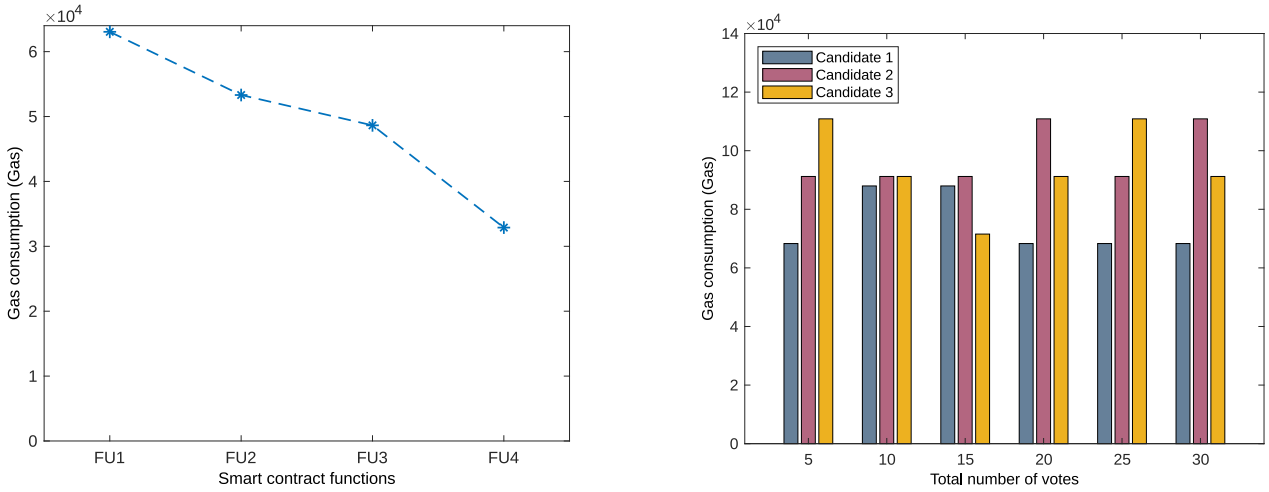
$$\max \sum_{a=1}^{v} \{N(\alpha_1^{\gamma_1}), N(\alpha_2^{\gamma_2}), \ldots\ldots, N(\alpha_v^{\gamma_g})\} = \text{winner} \tag{12}$$

$$winner \xrightarrow{displayto} \text{citizens} \tag{13}$$

The final results display the winning candidate and the total votes of all the candidates contesting the election is displayed through the blockchain network to maintain the security and integrity of the data. The election commission uses these results, and the candidate getting the maximum votes becomes part of the elected government by winning the election. This system can also be used to find the winning party based on the maximum number of votes received by a party in the election. Moreover, the results can be further used by the governor and the election commission to appoint a country's new government based on the results shown in the final layer.

V. PERFORMANCE EVALUATION

In this section, we have discussed the implementation of a smart contract deployed and implemented in Remix Integrated Environment (IDE) to show the working of the voting mechanism in detail and how the voters elect the winning candidate in the election. For that, we have different functionalities of smart contracts deployed for the proposed voting mechanism. Additionally, the 5G toolbox in Matlab



(a) Gas consumption for smart contract functions.

(b) Gas consumption for the total number of votes.

FIGURE 5. Comparative analysis of gas consumption for smart contract functions and the total number of votes of the proposed mechanism.

is considered to incorporate the 5G wireless network by set up of network parameters to improve the data rate and availability of voting associated with the voters and candidates that is further validated by the smart contract to complete the voting procedure through public blockchain network. Moreover, we have analyzed and evaluated the proposed voting mechanism in Python programming language, considering various performance aspects such as gas consumption analysis (based on the smart contract functions and the number of votes), cost analysis for smart contract functions, storage cost, and bit error rate.

A. GAS CONSUMPTION ANALYSIS

The performance evaluation of the proposed voting mechanism is analyzed considering the gas consumption determined based on the different smart contract functions,i.e., FU1 for adding candidates, FU2 for authorizing the voter and candidate, FU3 to determining the total number of votes, FU4 is to end the election, and the total number of votes for electing the winning candidate. Figure 5a highlights the gas consumption incurred for different smart contract functions involved in electing the candidate based on the number of votes voted by the voters. In this context, implementation of the smart contract of the proposed voting mechanism involves various functionalities such as FU1, which incurs the highest gas consumption to add the candidates for the election procedure and FU4 exhibits the lowest gas consumption to end the election procedure.

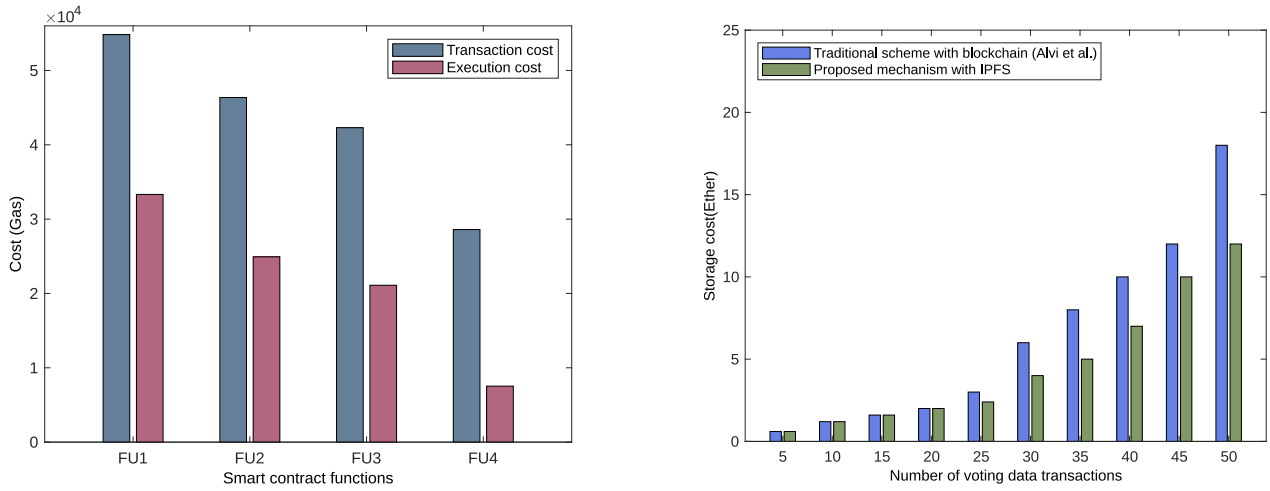
Figure 5b shows the gas consumption analysis based on the surge in the number of votes in the election. We have considered three candidates (candidate 1, candidate 2, candidate 3) in the election and voters can vote for these candidates to decide the winning candidate. We have performed the simulation by deploying the smart contract in an Ethereum test network to analyze the gas consumption of the proposed voting mechanism with the increment in voters electing for Candidate 1, candidate 2, and Candidate 3. For example, gas consumption for candidate 1 first increases with fewer votes (votes $\leq$ 15), then decreases and becomes constant with the increase in votes.

B. COST ANALYSIS

Figure 6a illustrated the cost analysis performed for the proposed voting mechanism based on the smart contract functions (FU1, FU2, FU3, and FU4). We have shown the comparison between transaction and the execution cost incurred for the smart contract functions in which transaction cost seems to be at a higher level than the execution cost for all the functionalities. However, adding candidates (FU1) requires higher transaction costs and the election can be ended (FU4) with the minimum transaction cost. Similarly, the FU1 function tends to acquire a higher execution cost, and FU4 tends to acquire a minimum execution cost. Furthermore, Figure 6b compares the storage cost of the proposed mechanism (IPFS) with the traditional scheme that utilizes blockchain to secure the digital voting system. However, traditional scheme acquire high data storage cost for performing the voting data transactions due to the usage of blockchain [21]. On the other hand, proposed mechanism incorporated IPFS which yields the improved data storage cost than the blockchain for accessing and storing the voting data transactions cost-efficiently associated with the voters and candidates participating in the voting mechanism. Moreover, The increase in number of voting data transactions results into low data storage cost in the proposed mechanism with IPFS, but initially less number of transactions involved for voting mechanism with IPFS and blockchain reflect approximately same level of storage cost.

C. BIT ERROR RATE

Figure 7 visualizes the comparison of bit error rate between wirless network technology, i.e., 4G and LTE-A, and



(a) Cost for smart contract functions.

(b) Storage cost comparison.

FIGURE 6. Comparative analysis of the cost for smart contract functions and storage cost comparison of the proposed mechanism with the conventional approach.

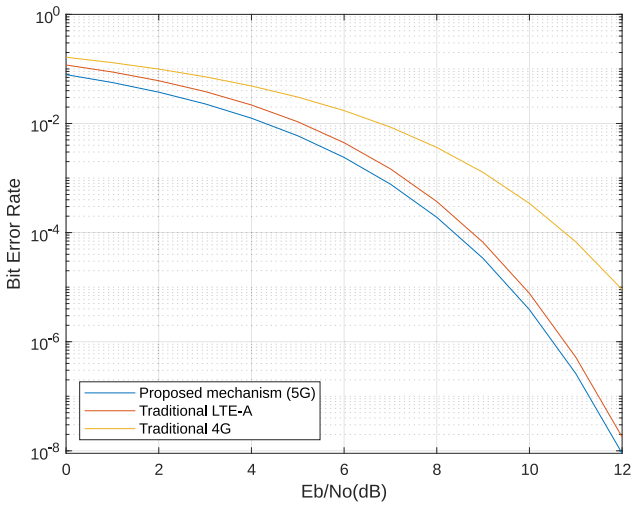


FIGURE 7. Bit error rate.

```
struct Candidate {
    string name;
    uint voteCount;
}

struct Voter {
    bool authorized;
    bool voted;
    uint vote;
}
```

FIGURE 8. Smart contract structure.

```
function Election(string memory _name) public {
    owner = msg.sender;
    electionName = _name;
}
```

FIGURE 9. Election function.

proposed mechanism using 5G network based on the number of bits transmitted in the voting procedure defined by E_b/N_o. The voting data transactions between voters and candidates is executed with 5G network which results into low bit error rate and high data rates than the traditional 4G and LTE-A network. As 5G wireless network facilitates low latency and high reliability with a wide frequency spectrum of frequency range (FR1 lies between *425 MHZ* and *7.25 GHZ* that processes the voting data transactions reliably..

D. IMPLEMENTED SMART CONTRACT

The smart contract of the proposed voting mechanism is written and deployed in Remix IDE, an Ethereum-based platform for developers to test their applications. The smart contract consists of the candidate and voter associated with the candidate's name, the count of votes, authorization performed for voters and candidates, and the vote given for the candidate, respectively. All the functions are related to these two data structures as these two stakeholders are the most important in the voting process.

1) Election()

Figure 8 and Figure 9 show the smart contract structure and election function, which allows storing the sender's name or the voter voting in the election. This function also involves the election name, which is very important so that users can know about the election for which they are voting through the blockchain network, whether it is the same election where they want to vote.

2) addCandidate()

Figure 10 highlight the function which allows storing the candidate information, such as the candidate's name or the person who wants to represent himself in the election process.

```
function addCandidate(string memory _name) ownerOnly public {
    candidates.push(Candidate(_name,0));
}
```

FIGURE 10. addCandidate function.

```
function getNumCandidate() public view returns(uint) {
    return candidates.length;
}
```

FIGURE 11. getNumCandidate function.

```
function authorize(address _person) ownerOnly public {
    voters[_person].authorized = true;
}
```

FIGURE 12. Authorize function.

This function creates a new data value for candidates and stores it for users or voters to allow them to vote for those new candidates.

3) getNumCandidate()

Figure 11 highlights the function which allows reporting for all the candidates that have presented themselves for voting candidacy. Using this function, the voter can get information on the number of candidates participating in the election. It is an essential function as it gives the voter insights about the present candidate in the election.

4) authorize()

Figure 12 shows the function which can set the predefined value of authorization from false to true, as it is a way to authorize the voters for them to vote. It is performed by using unique addresses for each voter. The voters can only vote when authorized to vote and are allowed to vote only once. It is quite analogous to how people below 18, or people who do not belong to a particular territory, are not authorized to vote, further confirming the security and transparency in the voting mechanism.

5) vote()

Figure 13 highlights the vote function that first checks various conditions before the execution of the smart contract. It first checks whether the voter who is present to vote has already voted because if he already has, he shouldn't be allowed to vote again. The second condition is whether the voter is authorized to vote. The function authorize() gives authorization to the voter, whereas the function vote() checks whether the authorization has been given to the voter. Another feature of this function is that it marks the voter as voted to prevent him from voting again by increasing the number of votes to the given candidate and the total votes by 1.

6) end()

Figure 14 shows the end function, which represents the end of the voting mechanism and is lightweight as it handles the destruction of the candidates or the election.

```
function vote(uint _voteIndex) public {
    require(!voters[msg.sender].voted);
    require(voters[msg.sender].authorized);
    voters[msg.sender].vote = _voteIndex;
    voters[msg.sender].voted = true;
    candidates[_voteIndex].voteCount += 1;
    totalVotes += 1;
}
```

FIGURE 13. Vote function.

```
function end() ownerOnly public {
    selfdestruct(owner);
}
```

FIGURE 14. End function.

```
Echidna 2.0.1
Tests found: 1
Seed: 3536215289766174291
Unique instructions: 197
Unique codehashes: 1
Corpus size: 1
Tests
echidna_vote: PASSED!
```

FIGURE 15. Security analysis of the proposed mechanism over Echidna tool.

VI. SMART CONTRACT SECURITY ANALYSIS

Figure 15 shows the security analysis performed for the proposed voting mechanism over Echidna fuzzy security analysis tool to detect security vulnerabilities or issues in the proposed mechanism. Echidna fuzzy tool is utilized for property or fuzzy-based testing of the Ethereum smart contracts of the proposed mechanism. The figure depicts that the smart contract of the proposed mechanism is confirmed and checked with the Echidna security tool to show that it does not contain any vulnerability or threat by detecting any illegitimate access control or transaction performed. Thus, stakeholders can participate in the voting mechanism performing transactions without any threat or vulnerability.

VII. OPPORTUNITIES AND CHALLENGES

This section highlights the various opportunities and challenges associated with the e-voting system, which are mentioned as follows:

A. OPPORTUNITIES

The blockchain and IPFS-based voting mechanism has various opportunities, which are discussed as follows:

- One of the most critical problems that today's top cyber-attack specialists must deal with is DDOS attacks. Due to its distributed structure, blockchain networks continue functioning normally even if some nodes go down due to a DDoS attack. Every time the nodes are reconnected, everything is synchronized to maintain

consistency, integrity, and transparency, making protocol and data loss impossible. Blockchain technology's overall architecture is intended to eliminate single points of failure with the help of concurrent and independent functions of blockchain nodes.

- Blockchain is a distributed ledger that can be accessed by all members and is considered an immutable ledger for recording transactions. This unchangeable transaction can only be recorded once and can be independently verified. As a result, neither the system participants nor the recorded transactions can be changed nor removed, improving the integrity and trust in the system.
- E-voting on the blockchain offers both openness and anonymity. The vote results that are recorded in the blockchain can be approved by the participants or impartial outside observers, ensuring the integrity of the election.
- Long-term cost savings can be achieved by blockchain technology with the help of IPFS. Setting up and running a secure data storage system in a distributed architecture is associated with high costs and security risks. Blockchain with IPFS is touted as being more affordable and safer than traditional database applications due to the feature of IPFS to store the data in the form of the hash using a cryptographic hash function [33]
- It offers immediate outcomes in which votes can be evaluated in various voting locations before being tallied in central units in some electronic voting procedures. Even if these procedures take a long time, it could take longer to declare the election results. Election results can be safely announced in minutes rather than hours using e-voting with blockchain.

B. CHALLENGES

Over the past few years, blockchain-based e-voting has received numerous complaints. According to several academics, the blockchain system concerns with e-voting can lead to new risks, such as preventing malware from infecting voters' phones and laptops. As an illustration, MIT (Massachusetts Institute of Technology) specialists have discovered a vulnerability in a mobile voting application used during the 2018 West Virginia midterm elections. Hackers can change the number of votes due to the vulnerability discussed for mobile voting applications. Moreover, it can be vulnerable to the security flaws in smart contracts or the well-known theoretically possible threat of a 51% assault against such systems [34]. Thus, We presume voters can vote using a secure blockchain and IPFS-based framework. Even though the proposed voting mechanism is secure, hackers can use malicious software that has already been installed on the voter's device to cast or alter a vote. The following are the main issues with an e-voting system that uses smart contracts:

- In the event of a user error, changing the votes is quite challenging as the user are only allowed to vote once.
- While creating a smart contract for the entire population of a country, loopholes are available. It is challenging to ensure that the voting procedure and its aspects are followed precisely as decided for conducting a secure election.
- Third-party interference is another challenge in the blockchain-based e-voting system. For that, smart contracts are designed to eliminate third-party authorities. However, this cannot be achieved because various people are needed to write and approve the contracts that can forge the security of the voting mechanism [35].

VIII. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a blockchain and IPFS-enabled secure, efficient, and trustworthy voting mechanism using a 5G wireless network. The employed IPFS protocol is incorporated with the blockchain network to ensure a cost-efficient voting mechanism for voters and candidates. The proposed voting mechanism involves communicating between voters, candidates, and the election commission to securely and efficiently elect the winning candidate over the 5G network. The 5G, with its ultra-intelligent features, offers a high data rate, low response time, and high reliability communication between participants for voting. Furthermore, we have deployed a smart contract of the voting mechanism in Remix IDE, which comprises various functionalities to elect the candidate by the voters in a secure and transparent voting environment. We have also contemplated and performed the security analysis of the proposed voting mechanism using the Echidna security tool to show that the functionalities do not contain any vulnerability or threat. Moreover, the performance analysis of the proposed voting mechanism is evaluated with various performance metrics such as gas consumption analysis, cost analysis for smart contract functions and the total number of votes, storage cost, and bit error rate to highlight the reliable and efficient proposed voting procedure than the traditional schemes.

In the future, we will implement smart contracts to allow users to update their votes in a certain time duration with a high amount of security and authentication. The smart contract implementation can be practically shown in a dynamic and real-time scenario. Moreover, we will explore and design the consensus protocol for validating the voting data transactions in the voting procedure, which can further revamp and improve the security and privacy of voting.

REFERENCES

[1] S. Al-Maaitah, M. Qatawneh, and A. Quzmar, "E-voting system based on blockchain technology: A survey," in *Proc. Int. Conf. Inf. Technol. (ICIT)*, Jul. 2021, pp. 200–205.

[2] M. Faisal, M. D. Hossain, and M. R. B. Bhuiyen, "Design and implementation of electronic voting system (EVS)," *IOSR J. Electr. Electron. Eng.*, vol. 9, no. 5, pp. 56–63, 2014.

[3] B. Smyth, "Ballot secrecy: Security definition, sufficient conditions, and analysis of Helios," *J. Comput. Secur.*, vol. 29, no. 6, pp. 551–611, Oct. 2021.

[4] D. Chaum, A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. Sherman, and P. Vora, "Scantegrity: End-to-end voter-verifiable optical- scan voting," *IEEE Secur. Privacy Mag.*, vol. 6, no. 3, pp. 40–46, May 2008.

[5] H. K. Al Anie, M. A. Alia, and A. A. Hnaif, "E-voting protocol based on public-key cryptography," *Int. J. Netw. Secur. Its Appl.*, vol. 3, no. 4, pp. 87–98, Jul. 2011.
[6] A. C. S. Sheela and R. G. Franklin, "E-voting system using homomorphic encryption technique," *J. Phys., Conf. Ser.*, vol. 1770, no. 1, Mar. 2021, Art. no. 012011.
[7] H. R. Patil, B. TarteBabita, S. S. Wadekar, S. B. Zurunge, and R. Phursule, "A secure e-voting system using face recognition and dactylogram," *Int. Eng. Res. J. (IERJ)*, vol. 2, no. 2, pp. 758–762, 2016.
[8] S. Suwarjono, L. Sumaryanti, and L. Lamalewa, "Cryptography implementation for electronic voting security," in *Proc. E3S Web Conf.*, vol. 328, 2021, p. 03005.
[9] V. V. Kaveri, V. Meenakshi, S. Ananth, P. Akshayavarshini, and B. KavyaShree, "Blockchain based reliable electronic voting technology," in *Proc. 3rd Int. Conf. Electron. Sustain. Commun. Syst. (ICESC)*, Aug. 2022, pp. 1713–1717.
[10] A. Kumari, R. Gupta, and S. Tanwar, "Amalgamation of blockchain and IoT for smart cities underlying 6G communication: A comprehensive review," *Comput. Commun.*, vol. 172, pp. 102–118, Apr. 2021.
[11] R. Gupta, S. Tanwar, and N. Kumar, "Blockchain and 5G integrated softwarized UAV network management: Architecture, solutions, and challenges," *Phys. Commun.*, vol. 47, Aug. 2021, Art. no. 101355.
[12] J. R. Douceur, "The Sybil attack," in *Peer-to-Peer Systems*, P. Druschel, F. Kaashoek, and A. Rowstron, Eds. Berlin, Germany: Springer, 2002, pp. 251–260.
[13] T. Chen, Z. Li, H. Zhou, J. Chen, X. Luo, X. Li, and X. Zhang, "Towards saving money in using smart contracts," in *Proc. IEEE/ACM 40th Int. Conf. Softw. Eng., New Ideas Emerg. Technol. Results*, Jun. 2018, pp. 81–84.
[14] V. S. Anjima and N. N. Hari, "Secure cloud e-voting system using fully homomorphic elliptical curve cryptography," in *Proc. Int. Conf. Intell. Comput. Control Syst. (ICCS)*, May 2019, pp. 858–864.
[15] R. Kakkar, R. Gupta, S. Agrawal, S. Tanwar, and R. Sharma, "Blockchain-based secure and trusted data sharing scheme for autonomous vehicle underlying 5G," *J. Inf. Secur. Appl.*, vol. 67, Jun. 2022, Art. no. 103179.
[16] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "A blockchain based cost effective digital voting system using sidechain and smart contracts," in *Proc. 11th Int. Conf. Electr. Comput. Eng. (ICECE)*, Dec. 2020, pp. 467–470.
[17] H. Takahashi and U. Lakhani, "Voting blockchain for high security NFT," in *Proc. IEEE 10th Global Conf. Consum. Electron. (GCCE)*, Oct. 2021, pp. 358–361.
[18] D. Khoury, E. F. Kfoury, A. Kassem, and H. Harb, "Decentralized voting platform based on Ethereum blockchain," in *Proc. IEEE Int. Multidisciplinary Conf. Eng. Technol. (IMCET)*, Nov. 2018, pp. 1–4.
[19] M. Sober, G. Scaffino, C. Spanring, and S. Schulte, "A voting-based blockchain interoperability Oracle," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Dec. 2021, pp. 160–169.
[20] G. Rathee, R. Iqbal, O. Waqar, and A. K. Bashir, "On the design and implementation of a blockchain enabled e-voting application within IoT-oriented smart cities," *IEEE Access*, vol. 9, pp. 34165–34176, 2021.
[21] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6855–6871, Oct. 2022.
[22] H. Kohad, S. Kumar, and A. Ambhaikar, "Scalability of blockchain based e-voting system using multiobjective genetic algorithm with sharding," in *Proc. IEEE Delhi Sect. Conf. (DELCON)*, Feb. 2022, pp. 1–4.
[23] M. Pawlak, A. Poniszewska-Marańda, and N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system," *Proc. Comput. Sci.*, vol. 141, pp. 239–246, Jan. 2018.
[24] V. Lalitha, S. Samundeswari, R. Roobinee, and L. S. Swetha, "Decentralized online voting system using blockchain," in *Proc. Int. Conf. Appl. Artif. Intell. Comput. (ICAAIC)*, May 2022, pp. 1387–1391.
[25] P. R. Naidu, D. R. Bolla, G. Prateek, S. S. Harshini, S. A. Hegde, and V. V. S. Harsha, "E-voting system using blockchain and homomorphic encryption," in *Proc. IEEE 2nd Mysore Sub Sect. Int. Conf. (MysuruCon)*, Oct. 2022, pp. 1–5.
[26] M. S. Farooq, U. Iftikhar, and A. Khelifi, "A framework to make voting system transparent using blockchain technology," *IEEE Access*, vol. 10, pp. 59959–59969, 2022.
[27] H. Zhu, L. Feng, J. Luo, Y. Sun, B. Yu, and S. Yao, "BCvoteMDE: A blockchain-based e-voting scheme for multi-district elections," in *Proc. IEEE 25th Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, May 2022, pp. 950–955.
[28] R. Kumar, L. Badwal, S. Avasthi, and A. Prakash, "A secure decentralized e-voting with blockchain & smart contracts," in *Proc. 13th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence)*, Jan. 2023, pp. 419–424.
[29] P. Subha, P. Padmasree, and R. L. Sowndharya, "Voting system based on blockchain and using Iris recognition," in *Proc. 4th Int. Conf. Comput. Commun. Technol. (ICCCT)*, Dec. 2021, pp. 164–168.
[30] T. Vairam, S. Sarathambekai, and R. Balaji, "Blockchain based voting system in local network," in *Proc. 7th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Mar. 2021, pp. 363–366.
[31] M. Ramalingam, D. Saranya, and R. ShankarRam, "An efficient and effective blockchain-based data aggregation for voting system," in *Proc. Int. Conf. Syst., Comput., Autom. Netw. (ICSCAN)*, Jul. 2021, pp. 1–4.
[32] K. Kapadiya, U. Patel, R. Gupta, M. D. Alshehri, S. Tanwar, G. Sharma, and P. N. Bokoro, "Blockchain and AI-empowered healthcare insurance fraud detection: An analysis, architecture, and future prospects," *IEEE Access*, vol. 10, pp. 79606–79627, 2022.
[33] A. Jangada, N. Dadlani, S. Raina, V. Sooraj, and A. R. Buchade, "Decentralized voting system using blockchain," in *Proc. IEEE Int. Conf. Blockchain Distrib. Syst. Secur. (ICBDS)*, Sep. 2022, pp. 1–5.
[34] M. J. H. Faruk, M. Islam, F. Alam, H. Shahriar, and A. Rahman, "Bie vote: A biometric identification enabled blockchain-based secure and transparent voting framework," in *Proc. 4th Int. Conf. Blockchain Comput. Appl. (BCCA)*, Sep. 2022, pp. 253–258.
[35] F. D. Giraldo, M. C. Barbosa, and C. E. Gamboa, "Electronic voting using blockchain and smart contracts: Proof of concept," *IEEE Latin Amer. Trans.*, vol. 18, no. 10, pp. 1743–1751, Oct. 2020.

SACHI CHAUDHARY is currently pursuing the B.Tech. degree with Nirma University, Ahmedabad, India. Her current research interests include machine learning, blockchain, and security.

SHAIL SHAH is currently pursuing the B.Tech. degree with Nirma University, Ahmedabad, India. His current research interests include machine learning, blockchain, and cryptocurrency.

RIYA KAKKAR (Student Member, IEEE) received the bachelor's and M.Tech. degrees from Banasthali Vidyapith, Jaipur, India, in 2018 and 2021, respectively. She is currently a full-time Ph.D. Research Scholar with the Computer Science and Engineering Department, Nirma University, Ahmedabad, Gujarat, India. She has authored or coauthored some publications, including papers in SCI indexed journals and IEEE ComSoc sponsored international conferences. Some of her research findings are published in top-cited journals and conferences, such as IEEE Systems Journal, IEEE Internet of Things Journal, *Journal of Information Security and Applications*, *International Journal of Energy Research* (Wiley), IEEE CITS, IEEE ICC, and IEEE INFOCOM. Her current research interests include electric vehicles, blockchain technology, 5G communication networks, and machine learning. She is also an active member of the ST Research Laboratory (www.sudeeptanwar.in).

RAJESH GUPTA (Member, IEEE) received the B.Eng. degree from the University of Jammu, India, the master's degree in technology from Shri Mata Vaishno Devi University, Jammu, India, in 2013, and the Ph.D. degree in computer science and engineering from Nirma University, Ahmedabad, Gujarat, India, under the supervision of Dr. Sudeep Tanwar. He is currently an Assistant Professor with Nirma University. He has authored/coauthored some publications, including papers in SCI indexed journals and IEEE ComSoc sponsored international conferences. Some of his research findings are published in top-cited journals and conferences, such as IEEE Transactions on Industrial Informatics, IEEE Transactions on Network and Service Management, IEEE Transactions on Network Science and Engineering, IEEE Transactions on Green Communications and Networking, IEEE Transactions on Computational Social Systems, *IEEE Network Magazine*, IEEE Internet of Things Journal, *IEEE Internet of Things Magazine*, *Computer Communications*, *Computer and Electrical Engineering*, *International Journal of Communication Systems* (Wiley), *Transactions on Emerging Telecommunications Technologies* (Wiley), *Physical Communication* (Elsevier), IEEE ICC, IEEE INFOCOM, IEEE GLOBECOM, and IEEE CITS. His H-index is 30 and I10-index is 59. His current research interests include device-to-device communication, network security, blockchain technology, 5G communication networks, and machine learning. He is an active member of the ST Research Laboratory. He was a recipient of the Doctoral Scholarship from the MeitY, Government of India, under the Visvesvaraya Ph.D. Scheme. He was a recipient of the Student Travel Grant from WICE-IEEE to attend IEEE ICC 2021 held in Canada and International Travel Grant from SERB, Government of India, to attend IEEE ICC 2023. He has been awarded best research paper awards from IEEE SCIoT 2022, IEEE ECAI 2021, IEEE ICCCA 2021, and IEEE IWCMC 2021. He is selected as a Young Researcher to attend the prestegious Heidelberg Lauerate Forum (HLF 2023) will be held in Germany. His name has been included in the list of Top 2% Scientists Worldwide published by Stanford University, USA, in 2021 and 2022. He was felicitated by Nirma University for their research achievements bagged, from 2019 to 2020 and from 2021 to 2022.

ABDULATIF ALABDULATIF (Member, IEEE) received the M.Sc. and Ph.D. degrees in computer science from RMIT University, Australia. He is currently an Assistant Professor with the College of Computer, Qassim University, Saudi Arabia. His current research interests include applied cryptography, cloud computing, and data mining.

SUDEEP TANWAR (Senior Member, IEEE) received the B.Tech. degree from Kurukshetra University, India, in 2002, the M.Tech. degree (Hons.) from Guru Gobind Singh Indraprastha University, Delhi, India, in 2009, and the Ph.D. degree in wireless sensor networks, in 2016. He is currently a Professor with the Computer Science and Engineering Department, Institute of Technology, Nirma University, India. He is also a Visiting Professor with Jan Wyzykowski University, Polkowice, Poland, and the University of Pitesti, Pitesti, Romania. He has authored two books and edited 13 books, and more than 250 technical articles, including top journals and top conferences, such as IEEE Transactions on Network Science and Engineering, IEEE Transactions on Vehicular Technology, IEEE Transactions on Industrial Informatics, IEEE Wireless Communications, IEEE Networks, ICC, GLOBECOM, and INFOCOM. He initiated the research field of blockchain technology adoption in various verticals, in 2017. His H-index is 67. He actively serves his research communities in various roles. His current research interests include blockchain technology, wireless sensor networks, fog computing, smart grids, and the IoT. He is a Final Voting Member of the IEEE ComSoc Tactile Internet Committee, in 2020. He is a member of CSI, IAENG, ISTE, and CSTA. He is also a member of the Technical Committee on Tactile Internet, IEEE Communication Society. He is also leading the ST Research Laboratory, where group members are working on the latest cutting-edge technologies. He has been awarded the best research paper awards from IEEE IWCMC-2021, IEEE GLOBECOM 2018, IEEE ICC 2019, and Springer ICRIC-2019. He has served many international conferences as a member for the Organizing Committee, such as the Publication Chair for FTNCT-2020, ICCIC 2020, and WiMob2019, a member of the Advisory Board for ICACCT-2021 and ICACI 2020, the Workshop Co-Chair for CIS 2021, and the General Chair for IC4S 2019 and 2020 and ICCSDF 2020. He is also serving on the editorial boards for *Computer Communications*, *International Journal of Communication Systems*, and *Security and Privacy*.

GULSHAN SHARMA received the B.Tech., M.Tech., and Ph.D. degrees. He was a Postdoctoral Research Fellow with the Faculty of EBIT, University of Pretoria, South Africa, from 2015 to 2016.

He is currently working as a Senior Lecturer with the Faculty of Engineering and the Built Environment of the University of Johannesburg, South Africa. He is a Y Rated Researcher from National Research Foundation (NRF) of South Africa. He is working as an Academic Editor of International Transactions on Electrical Energy System Journal and Journal of Electrical and Computer Engineering, Hindawi. He has published more than 100 research papers in international journals and conferences and has been continuously engaged in guiding research activities at graduate/post-graduate and Ph.D. levels. His area of interest includes power system operation and control, renewable power generation, FACTS and application of AI techniques to power systems.

PITSHOU N. BOKORO (Senior Member, IEEE) received the bachelor's degree in electrical engineering from the Durban University of Technology, a master's degree in electrical engineering from the University of Johannesburg, South Africa, and the Ph.D. degree from the University of the Witwatersrand, Johannesburg. He is an Associate Professor with the Faculty of Engineering and the Built Environment of the University of Johannesburg. He holds Senior Membership with the South African Institute of Electrical Engineers (SMSAIEE) as well as with the Institute of Electrical and Electronics Engineers (SMIEEE). He has published over 100 research papers (which include over 50 journal articles and 70 conference papers) in indexed journals and peer reviewed conference proceedings. He authored a couple of book chapters in reputed books published by IGI-Global and IET. He serves as a specialist editor in Energy and Power Systems for the SAIEE Africa Research Journal (ARJ). He has supervised to completion over 18 master's students (which include master's and doctoral students). His major research interests include renewable energy systems, power systems, power system reliability, distributed generation, surge arresters, insulation and dielectrics, power quality, condition monitoring, microgrid, the internet of things, and applied artificial intelligence.