Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

*Digital Object Identifier 10.1109/ACCESS.2017.DOI*

# 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), SUDEEP TANWAR[1], (SENIOR MEMBER, IEEE), GULSHAN SHARMA[2], PITSHOU N. BOKORO[3]**

[1]Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India (e-mails: 19bce230@nirmauni.ac.in, 19bce232@nirmauni.ac.in, 21ftphde56@nirmauni.ac.in, rajesh.gupta@nirmauni.ac.in, sudeep.tanwar@nirmauni.ac.in)
[2]Department of Electrical Engineering Technology, University of Johannesburg, Auckland Park 2006, South Africa. (email: gulshans@uj.ac.za, pitshoub@uj.ac.za)

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

**ABSTRACT** With the advancement of technology, electronic voting (e-voting) has been adopted widely for conducting a real-time election procedure efficiently and securely. But, an e-voting system can be exposed to various vulnerabilities such as denial of service, malware, compromised credentials, insider attacks, etc., which can risk the voter's privacy in the voting system. Thus, to mitigate the security and confidentiality issues of e-voting, we propose a blockchain and smart contract-based secure and transparent voting mechanism in this paper over fifth-generation (5G) wireless networks. The employed interplanetary file System (IPFS) with blockchain technology facilitates cost-efficient and reliable voting for the voters and candidates in the election procedure. Furthermore, we have deployed a smart contract of the proposed voting mechanism to show all the functionalities involved in the election procedure. Additionally, we utilized the Echidna tool for the security and vulnerability assessment of the proposed voting mechanism smart contract. Finally, the proposed mechanism has been simulated and analyzed by deploying the smart contract in Remix Integrated Development Environment (IDE) considering metrics such as gas consumption analysis based on smart contract functions and the number of votes and cost analysis (i.e., transaction and execution cost) based on the smart contract functions.

**INDEX TERMS** Blockchain Technology, Smart Contracts, 5G, IPFS, E-voting, Security

## I. INTRODUCTION

OVER the years, many countries have adopted voting methods in 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 are not evolved to that much 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 ballots in the form of election paper, where votes are counted manually, which is quite time-consuming and requires a huge human resource 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, it is impossible for older people to 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 [6] designed an e-voting protocol that utilizes public-key cryptography to ensure security and integrity during the voting procedure. But, their e-voting protocol has not considered the 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 is ensured by utilizing Rivest-Shamir-Adleman (RSA) algorithm, but 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].

### A. TRADITIONAL VOTING MECHANISM

Currently, many countries are still utilizing 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.

### B. WORKING OF E-VOTING SYSTEM

In this section, we have highlighted the working of the e-voting system (as shown in Figure 2), which is bifurcated into various steps, which is 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 of 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 own 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 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 need to 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].

### C. MOTIVATION

Many researchers have implemented e-voting systems utilizing cryptography techniques that a malicious attacker can

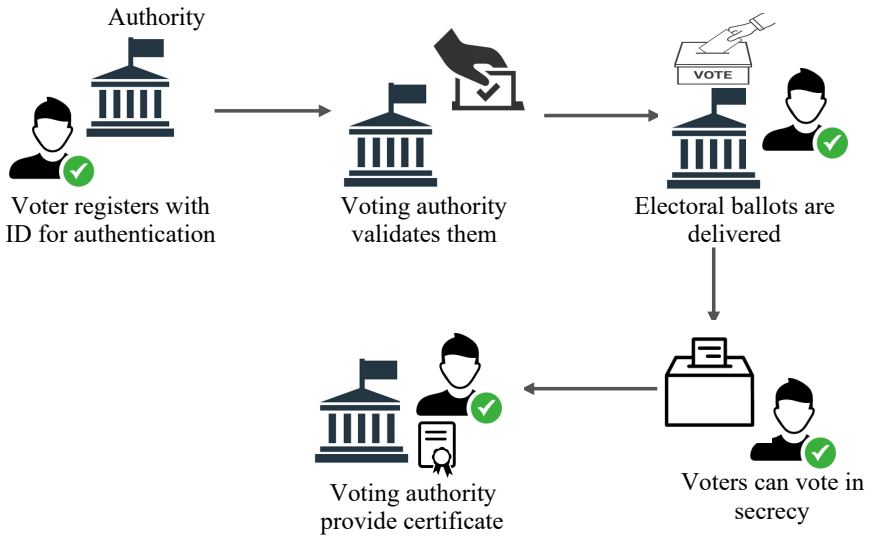



FIGURE 1: Traditional voting mechanism

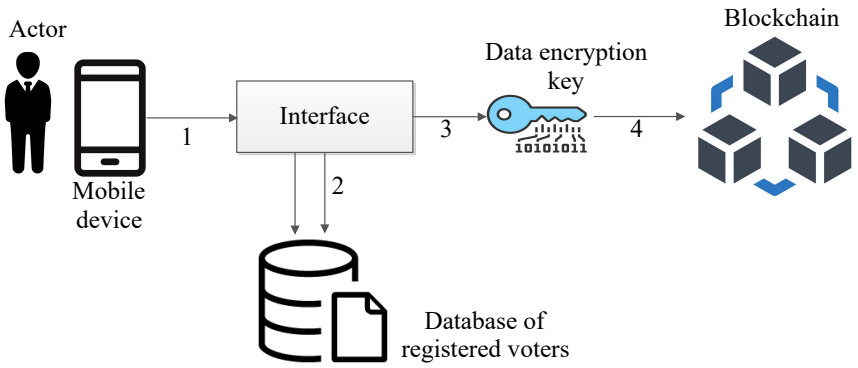



FIGURE 2: E-Voting system.

easily forge or manipulate. Moreover, the data associated with candidates and voters involved in the election can be modified by the attackers, which can affect the election's final result. For instance, Anjima et al. [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 by implementing the smart contract to provide a secure voting environment for the involved voters and candidates.

### D. RESEARCH CONTRIBUTIONS

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.
- 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 in Remix Integrated Environment (IDE) on an Ethereum test network considering parameters such as gas consumption analysis based on

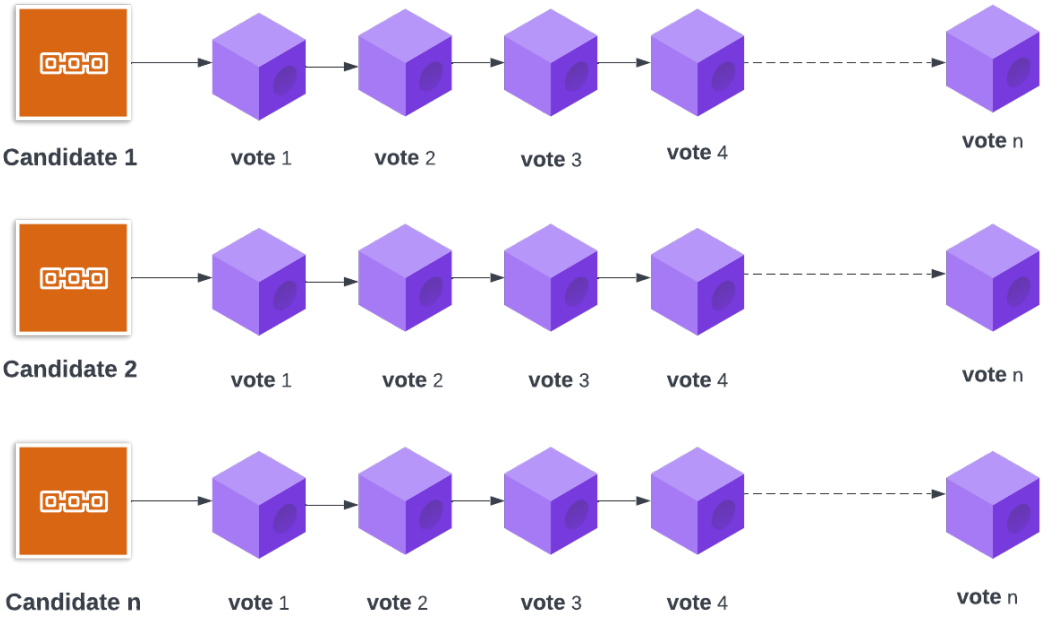



FIGURE 3: Blockchain structure for candidates [11].

smart contract functions and the number of votes and cost analysis for smart contract functions.

### E. ORGANIZATION

The organization of the rest of the paper is as follows. Section 2 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 opportunities and challenges of the proposed mechanism. Finally, Section VII concludes the paper with future work.

## II. LITERATURE SURVEY

In order 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. [19] 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.

Further, the authors of [20] 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 with the usage of a consensus mechanism. Additionally, a chain security framework is also applied to make votes secure using encryption which also reduces the probability of a 51% attack. 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. [21] 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. [17] 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. [22] 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 blind voters, fingerprint scanning is used along with Iris scanning. Further, Vairam et al. [23] considered an e-voting system containing all the legitimate voting functions. Here, blockchain is used

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

| Author | Year | Purpose | Pros | Cons |
|---|---|---|---|---|
| Alvi *et al.* [15] | 2020 | Blockchain enabled e-voting framework using smart contracts and side-chain | Cost-effective, better performance | Lacks real-time implementation |
| Takahashi *et al.* [16] | 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.* [17] | 2021 | Ethereum blockchain-based decentralized voting platform | Provides inter-state residency, distributed ledger provides access to everyone, secured and unaltered in nature, accuracy in counting, no fraud possible, the solved problem of trust among users | Some tampering possible, little less transparency provided. |
| Sober *et al.* [18] | 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 |
| 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.* [19] | 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 still persist, not cost-effective |
| Farooq *et al.* [20] | 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.* [21] | 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 |
| The proposed mechanism | 2023 | Blockchain-based secure voting mechanism | Secure, reliable, and cost-efficient | - |

to offer security and transparency for fair elections. Then, Ramalingam et al. [24] 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. [15] 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 not considered other aspects such as cost-efficiency, efficiency, and availability in their voting system. Motivated by the above-mentioned challenges, we have proposed a blockchain and IPFS-based voting mechanism 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 several 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 for 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 and 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 $\Upsilon$ 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 $\epsilon$ and $\varepsilon$ 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, $\epsilon'$ and $\varepsilon'$ 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 need to be stored securely through the blockchain network [25]. 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 $\theta_{\alpha_a}$ and $\vartheta_{\gamma_g}$ 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 in the election. 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 voting system which comprises of the v a number of voters$\{\alpha_1, \alpha_2, \ldots\ldots, \alpha_v\} \in \alpha_a$ who are going to vote in the election and the c number of candidates $\{\gamma_1, \gamma_2, \ldots\ldots, \gamma_m\} \in \gamma_g$ who are contesting in the election. The candidate list is given by the election commission and there are c a 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:

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

However, voters and candidates involved in the election need to register themselves with the election commission, which is discussed in the next layer of the proposed voting mechanism, which 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.

### 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. Then, 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 $\zeta$, 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, but they should store their voting data in IPFS for a cost-efficient 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 $\zeta$

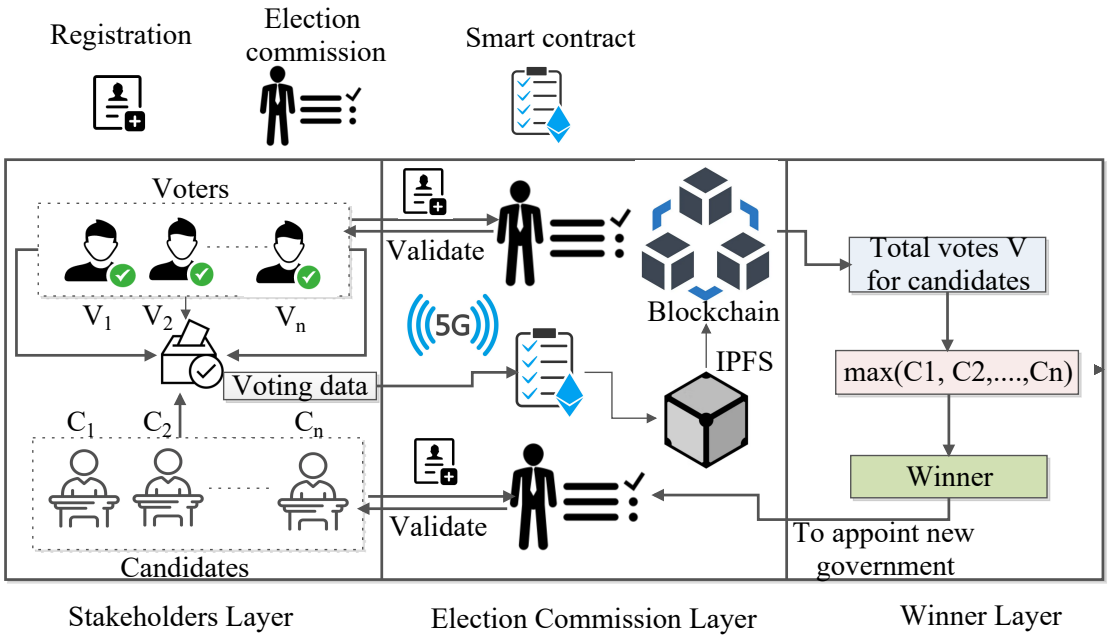



FIGURE 4: Proposed System

can be stored in the IPFS that can be further accessed through the blockchain network in a secure and decentralized manner using a 5G network.

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

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

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

where $\varepsilon$ 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 is forwarded to the winner layer to complete the voting procedure in the election. This is the final layer of the voting mechanism system in which the final results for selecting the candidate are displayed. Thus, the total votes from the election commission layer 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 at the end when all the voters have voted. Also, the intermediate results can be viewed and displayed based on the permission granted by the election commission.

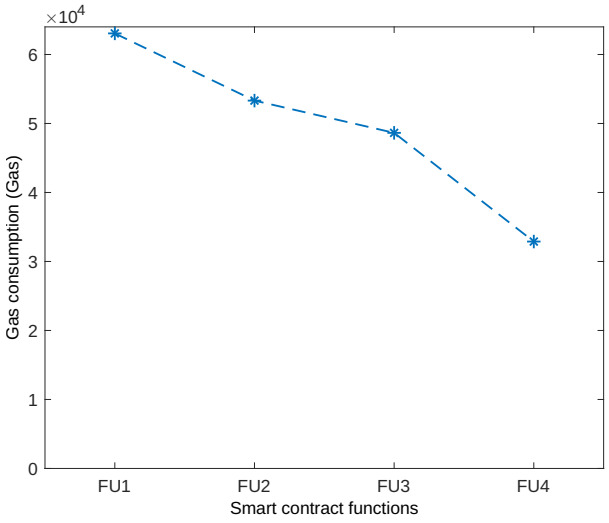
$$\max \sum_{a=1}^{v} \{N(\alpha_1^{\gamma_1}), N(\alpha_2^{\gamma_2}), \ldots\ldots, N(\alpha_v^{\gamma_g})\} = \text{winner} \tag{12}$$

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

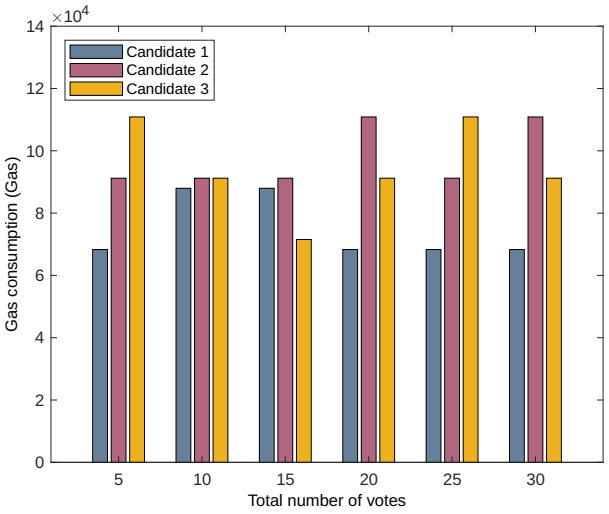
The final results display the winning candidate along with the total votes of all the candidates who were contesting the election. These results are further used by the election commission and the candidate getting the maximum votes becomes part of the elected government by winning the election. This system can also be used for finding 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 commence the process of appointing the new government for a country based on the results shown in the final layer.

## V. PERFORMANCE EVALUATION

In this section, we have discussed the implementation of a smart contract that has been 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. Moreover, we have performed the analysis and evaluation of the proposed voting mechanism in Python programming language considering various performance aspects such as gas consumption analysis and cost analysis based on the smart contract functions and a number of votes.




(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.

### 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 6 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

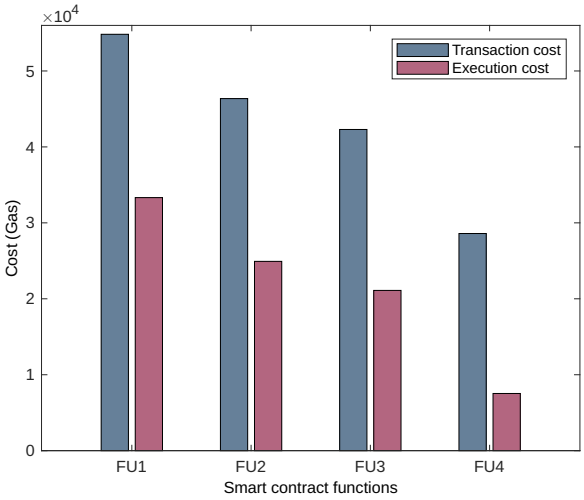



FIGURE 6: Cost for smart contract functions.

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, the addition of candidates (FU1) acquires 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.

### C. 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.

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

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

FIGURE 7: Election function

### D. ELECTION()

Figure 7 and Figure 8 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.

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

FIGURE 8: Election function

### E. ADDCANDIDATE()

Figure 9 highlight the function which allows storing the candidate information, such as the name of the candidate or the person who wants to represent himself in the election process. 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.

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

FIGURE 9: addCandidate function.

### F. GETNUMCANDIDATE()

Figure 10 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 of 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.

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

FIGURE 10: getNumCandidate function.

### G. AUTHORIZE()

Figure 11 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.

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

FIGURE 11: Authorize function.

### H. VOTE()

Figure 12 highlights the vote function that first checks various conditions before the execution of the smart contract. It first checks the foremost condition whether the voter who is present to vote has already voted because if he already has voted, 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.

```
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 12: Vote function.

### I. END()

Figure 13 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 end() ownerOnly public {
    selfdestruct(owner);
}
```

FIGURE 13: End function.

## VI. SMART CONTRACT SECURITY ANALYSIS

Figure 14 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.


FIGURE 14: Security analysis of the proposed mechanism over Echidna tool.

## VII. OPPORTUNITIES AND CHALLENGES

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

### A. OPPORTUNITIES

The blockchain and IPFS-based voting mechanism has various opportunities, which is 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 [26]
- 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 by 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 [27]. 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, but this cannot be achieved because various people are needed to write and approve the contracts that can forge the security of the voting mechanism [28].

## VIII. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a blockchain-based secure and trustworthy voting mechanism using IPFS and 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 the number of voters communicating with the number of candidates and the election commission to elect the winning candidate securely. 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 based on the smart contract functions and the total number of votes and cost analysis (transaction and execution cost) for smart contract functions in the secure voting procedure.

In the future, we can also implement smart contracts to allow users to update their votes in a certain time duration with a high amount of security and authentication. Also, the smart contract implementation can be practically shown in a wider real-time scenario.

## REFERENCES


[1] S. Al-Maaitah, M. Qatawneh, and A. Quzmar, "E-voting system based on blockchain technology: A survey," in 2021 International Conference on Information Technology (ICIT), pp. 200–205, 2021.

[2] M. Faisal, M. Hossain, and M. Bhuiyen, "Design and implementation of electronic voting system (evs)," IOSR Journal of Electrical and Electronics Engineering, vol. 9, pp. 56–63, 01 2014.

[3] B. Smyth, "Ballot secrecy: Security definition, sufficient conditions, and analysis of helios," J. Comput. Secur., vol. 29, p. 551–611, jan 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," Security & Privacy, IEEE, vol. 6, pp. 40 – 46, 06 2008.

[5] H. Anie, M. Alia, and A. Hnaif, "E-voting protocol based on public-key cryptography," International Journal of Network Security & Its Applications, vol. 3, pp. 87–98, 07 2011.

[6] A. S. Sheela and R. G. Franklin, "E-voting system using homomorphic encryption technique," in Journal of Physics: Conference Series, vol. 1770, p. 012011, IOP Publishing, 2021.

[7] P. Rahul, TarteBabita, W. Sapana, Z. Bhakti, and P. Rajesh, "A secure e-voting system using face recognition and dactylogram," 2016.

[8] S. Suwarjono, L. Sumaryanti, and L. Lamalewa, "Cryptography implementation for electronic voting security," E3S Web of Conferences, vol. 328, p. 03005, 01 2021.

[9] V. Vijeya Kaveri, V. Meenakshi, A. S, A. P, and K. B, "Blockchain based reliable electronic voting technology," in 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC), pp. 1713–1717, 2022.

[10] A. Kumari, R. Gupta, and S. Tanwar, "Amalgamation of blockchain and iot for smart cities underlying 6g communication: A comprehensive review," Computer Communications, vol. 172, pp. 102–118, 2021.

[11] R. Gupta, S. Tanwar, and N. Kumar, "Blockchain and 5g integrated softwarized uav network management: Architecture, solutions, and challenges," Physical Communication, vol. 47, p. 101355, 2021.

[12] J. R. Douceur, "The sybil attack," in Peer-to-Peer Systems (P. Druschel, F. Kaashoek, and A. Rowstron, eds.), (Berlin, Heidelberg), pp. 251–260, Springer Berlin Heidelberg, 2002.

[13] T. Chen, Z. Li, H. Zhou, J. Chen, X. Luo, X. Li, and X. Zhang, "Towards saving money in using smart contracts," pp. 81–84, 05 2018.

[14] V. S. Anjima and N. N. Hari, "Secure cloud e-voting system using fully homomorphic elliptical curve cryptography," in 2019 International Conference on Intelligent Computing and Control Systems (ICCS), pp. 858–864, 2019.

[15] 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 2020 11th International Conference on Electrical and Computer Engineering (ICECE), pp. 467–470, 2020.

[16] H. Takahashi and U. Lakhani, "Voting blockchain for high security nft," in 2021 IEEE 10th Global Conference on Consumer Electronics (GCCE), pp. 358–361, 2021.

[17] Puneet, A. Chaudhary, N. Chauhan, and A. Kumar, "Decentralized voting platform based on ethereum blockchain," in 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), pp. 1–4, 2021.

[18] M. Sober, G. Scaffino, C. Spanring, and S. Schulte, "A voting-based blockchain interoperability oracle," in 2021 IEEE International Conference on Blockchain (Blockchain), pp. 160–169, 2021.

[19] V. Lalitha, S. Samundeswari, R. Roobinee, and L. S. Swetha, "Decentralized online voting system using blockchain," in 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), pp. 1387–1391, 2022.

[20] 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.

[21] 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 2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD), pp. 950–955, 2022.

[22] S. P, P. P, and S. L. R, "Voting system based on blockchain and using iris recognition," in 2021 4th International Conference on Computing and Communications Technologies (ICCCT), pp. 164–168, 2021.

[23] T. Vairam, S. Sarathambekai, and R. Balaji, "Blockchain based voting system in local network," in 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), vol. 1, pp. 363–366, 2021.

[24] M. Ramalingam, D. Saranya, and R. ShankarRam, "An efficient and effective blockchain-based data aggregation for voting system," in 2021 International Conference on System, Computation, Automation and Networking (ICSCAN), pp. 1–4, 2021.

[25] 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.

[26] A. Jangada, N. Dadlani, S. Raina, V. Sooraj, and A. Buchade, "De-centralized voting system using blockchain," in 2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), pp. 1–5, 2022.

[27] 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 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA), pp. 253–258, 2022.

[28] F. D. Giraldo, B. Milton C., and C. E. Gamboa, "Electronic voting using blockchain and smart contracts: Proof of concept," IEEE Latin America Transactions, vol. 18, no. 10, pp. 1743–1751, 2020.

## AUTHORS BIOGRAPHY

**SACHI CHAUDHARY** is currently a final year B.Tech student at Nirma University, Ahmedabad, India. Her research interest includes, Machine Learning, Blockchain, and security.

**SHAIL SHAH** is currently a final year B.Tech student at Nirma University, Ahmedabad, India. His research interest includes, Machine Learning, Blockchain, and Cryptocurrency.

**RIYA KAKKAR** is a Full-Time Ph.D. Research Scholar in the Computer science and Engineering Department at Nirma University, Ahmedabad, Gujarat, India. She received her Bachelor as well as Master of Technology from the Banasthali Vidyapith, Jaipur, India in 2018 and 2021, respectively. She has authored or co-authored some publications (including papers in SCI Indexed Journal and IEEE ComSoc sponsored International Conference). Some of her research findings are published in top-cited journals and conferences such as IEEE Systems Journal, IEEE IoT Journal, JISA Journal, Wiley IJER, IEEE CITS, IEEE ICC, IEEE INFOCOM, and many more. Her research interest includes, Electric Vehicles, Blockchain Technology, 5G Communication Network, and Machine Learning. She is also an active member of ST Research Laboratory (www.sudeeptanwar.in).

**RAJESH GUPTA** is working as an Assistant Professor at Nirma University, Ahmedabad, Gujarat, India. He received his Ph.D. in Computer Science and Engineering from Nirma University under the supervision of Dr. Sudeep Tanwar. He received his Bachelor of Engineering in 2008 from the University of Jammu, India and Master's in Technology in 2013 from Shri Mata Vaishno Devi University, Jammu, India. He has authored/co-authored 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 IoT 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, IEEE CITS, and many more. His research interest includes Device-to-Device Communication, Network Security, Blockchain Technology, 5G Communication Network, and Machine Learning. His h-index is 29 and i10-index is 47. He is also a recipient of Doctoral Scholarship from the MeitY, Govt. of India under the Visvesvaraya Ph.D. Scheme. He is a recipient of Student Travel Grant from WICE-IEEE to attend IEEE ICC 2021 held in Canada. He has been awarded best research paper awards from IEEE SCIoT 2022, IEEE ECAI 2021, IEEE ICCCA 2021, and IEEE IWCMC 2021. His name has been included in the list of Top 2% scientists worldwide published by Stanford university, USA, consecutively in 2021 and 2022. He was felicitated by Nirma University for their research achievements bagged in 2019-20 and 2021-22. He is also an active member of ST Research Lab.

**SUDEEP TANWAR** (Senior Member, IEEE) is currently working as 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 in Pitesti, Romania. He received B.Tech in 2002 from Kurukshetra University, India, M.Tech (Honor's) in 2009 from Guru Gobind Singh Indraprastha University, Delhi, India and Ph.D. in 2016 with specialization in Wireless Sensor Network. He has authored two books and edited 13 books, 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 63. He actively serves his research communities in various roles. His research interests include blockchain technology, wireless sensor networks, fog computing, smart grid, and the IoT. He is a Final Voting Member of the IEEE ComSoc Tactile Internet Committee, in 2020. He is a Senior Member of IEEE, Member of CSI, IAENG, ISTE, and CSTA, and a member of the Technical Committee on Tactile Internet of IEEE Communication Society. 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 of 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, a Workshop Co-Chair for CIS 2021, and a General Chair for IC4S 2019, 2020, and ICCSDF 2020. He is also serving the editorial boards of Computer Communications, International Journal of Communication System, and Security and Privacy. He is also leading the ST Research Laboratory, where group members are working on the latest cutting-edge technologies.

**GULSHAN SHARMA** is presently working as Senior Lecturer in Department of Electrical Power Engineering, Durban University of Technology, South Africa. He is acting as DRC Chair and FRC Representative of Department of Electrical Power Engineering, Durban University of Technology. He has received Y Rated Researcher award from National Research Foundation (NRF) of South Africa. He is acting as Associate Editor of International Transactions on Electrical Energy Systems, Wiley and Regional Editor of Recent Advances in Electrical & Electronics Engineering, Bentham Science. He has more than 13 years of teaching and research experience. He has the qualifications of B. Tech, M. Tech and Ph.D. from institutes of national importance. He was a Post-Doctoral research fellow at Faculty of EBIT, University of Pretoria, South Africa from 2015 to 2016. He has published several research papers in international journals and conferences of high repute 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, smart grid, hybrid electric vehicles and application of AI techniques to power systems.

**PITSHOU N. BOKORO** (Member, IEEE) received the M.Phil. degree in Electrical Engineering from the University of Johannesburg, Johannesburg, South Africa in 2011, and the Ph.D degree in Electrical Engineering from the University of the Witwatersrand, in 2016. He is currently an Associate Professor with the University of Johannesburg, Johannesburg, South Africa. His research interests include modelling and reliability prediction of insulating materials and dielectrics, power quality, and renewable energies. He is a senior member of the South African Institute of Electrical Engineers.