

# A novel smart contract based blockchain with sidechain for electronic voting

Rakshitha Channarayapatna Mullegowda<sup>1</sup>, Nirmala Hiremani<sup>1</sup>, Mahantesh Birje<sup>1</sup>,  
Nataraj Kanathur Ramaswamy<sup>2</sup>

<sup>1</sup>Department of Computer Science and Engineering, Visvesvaraya Technological University, Belagavi, India

<sup>2</sup>Department of Research and Development, Visvesvaraya Technological University, Belagavi, India

## Article Info

### Article history:

Received May 30, 2023

Revised Jul 7, 2023

Accepted Jul 17, 2023

### Keywords:

Blockchain

E-voting

Robust access control method

Sidechain

Tamper-proof

Vote coin

## ABSTRACT

Several countries have been researching digital voting methods in order to overcome the challenges of paper balloting and physical voting. The recent coronavirus disease 2019 (COVID-19) epidemic has compelled the remote implementation of existing systems and procedures. Online voting will ultimately become the norm just like unified payments interface (UPI) payments and online banking. With digital voting or electronic voting (e-voting) a small bug can cause massive vote rigging. E-voting must be honest, exact, safe, and simple. E-voting is vulnerable to malware, which can disrupt servers. Blockchain's end-to-end validation solves these problems. Three smart contracts-voter, candidate, and voting-are employed. The problem of fraudulent actions is addressed using vote coins. Vote coins indicate voter status. Sidechain technology complements blockchain. Sidechains improve blockchain functionality by performing operations outside of blockchains and delivering the results to the mainchain. Thus, storing the encrypted vote on the sidechain and using the decrypted result on the mainchain reduces cost. Building access control policies to grant only authorized users' access to the votes for counting is made simpler by this authorization paradigm. Results of the approach depict the proposed e-voting system improves system security against replay attacks and reduces the processing cost as well as processing time.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



## Corresponding Author:

Rakshitha Channarayapatna Mullegowda

Department of Computer Science and Engineering, Visvesvaraya Technological University

Belagavi-590018, India

Email: pr80341@gmail.com

## 1. INTRODUCTION

The fundamental need for a long-lasting democracy and effective government is trustworthy elections. Elections have always been characterized by challenges, mistakes, and institutional manipulations, which diminishes their legitimacy. Most conventional electronic voting systems are designed with centralized architectures, making them vulnerable to cyberattacks such as distributed denial of service attacks (DDoS) [1]. Paper ballots used in the past have a history of fraud and failure; they may be miscounted or misplaced in the mail. The traditional voting process includes expenses for personnel, the distribution of ballots, and security precautions. Every election, worldwide [2], often sees a huge cash injection. However, new digital technologies are required. Blockchain technology creates a decentralized ledger with a consistent perception of reality. A mutual, tamper-proof record and peer-to-peer networking technology called blockchain has been employed in digital currencies like Bitcoin and Ethereum. In this case, user anonymity is safeguarded by public or private key identities. Security and privacy are provided by a number of blockchain-based models

[3], [4]. The main obstacles to deploying blockchain technology are connected to speed and scalability, even if this technology offers confidentiality, privacy, accountability, and durability [5].

A private-chain is a sidechain that stores hashes in its own blocks on the public chain (Ethereum). We can build a sharding system on top of this side-chain since it offers a distributed randomness source. This is performed by launching the validator contract on the public Ethereum blockchain [6]. Research on blockchain technology has recently been increasingly focused on decentralization, which is a key component of blockchains and smart contracts (SCs), applications using blockchain technology as their primary technology. Contemporary academics are taking a closer look at the design of electronic voting (e-voting) systems due to their decentralization characteristics. As a result, they realized SCs and blockchains could be used to enhance the application's data quality and reduce expenses while keeping the software open and transparent at the same time [7]. By utilizing this feature for electronic voting, all voting-related data is processed as a transaction and kept in a block, preventing malicious network users from readily tampering with the data [8]. If the vote counting procedure was open, it would be possible to be independently verified, and fair, election-related issues may be avoided. As a result, the issues of the prevailing framework include voting process security, authentication, and data protection [9]. Although the current system gives voters anonymity, it is not thought to be transparent. When it comes to election outcomes, people are supposed to believe what the government says. Voter fraud, ballot stuffing, and booth capture are just a few of the various scams that occur throughout elections. This entire situation makes voting extremely difficult [10]. Effective rules need to be put in place, together with consideration for all the previously listed needs and the handling of them with persistence. Consequently, the following smart contracts are offered to address these issues.

- a. In this work, voter contract, candidate contract, and voting contract are presented.
- b. To store the public and private key, crypto server node is used.
- c. This work makes use of vote coins to prevent fraudulent activities. Voter status is represented by the vote coin.
- d. Besides, sidechain technique is used along with the blockchain. A sidechain is a network that performs some operations outside of its mainchain, and then returns the results to its mainchain for use. This type of network extends the capabilities of a mainchain. By storing the encrypted vote on the sidechain, and decrypting the result on the mainchain, we can lower the cost of the voting process.
- e. To avoid authorization of unauthorized users or voting officer, robust access control mechanism is presented. Only authorized users are granted access to the votes via this authorization model, making creating access control policies easier. This model also supports the role, task, and trust computing paradigm.

## 2. RELATED WORK

Hassan *et al.* [11] proposed an electronic voting system based on blockchains, which uses smart contracts to ensure a secure and practical election while protecting voter privacy. In order to improve the way political election decisions were made, the article demonstrated contextual research using a blockchain-based application to assess the potential of distributed ledger technology. Blockchain can also be used as an electronic voting system despite a number of legal and technological obstacles. As a result of this study, researchers developed an electronic voting method that increased voter participation, provided privacy protection, security, and transparency for users, while retaining liquid democracy for democratic elections. However, a blockchain-based system's capacity to scale had been impacted by electronic voting. Scalability problems were made worse by a blockchain network's expanding node count.

Chaisawat and Vorakulpipat [12] proposed data security for integrated e-voting using blockchain and message queue, in an effort to protect voter privacy, and present the process as open and efficient as possible by utilizing certain blockchain and message queue characteristics. The study extended the prior research and suggested an integrated model of electronic voting involving the use of a communications protocol. As a method of ensuring dependent data delivery, the message queue was deemed to be a viable solution since it could be used for transaction buffering, error handling, as well as for blockchain's event message listener. The outcome demonstrated the system's ability to function successfully in a production setting, and the implementation of a message queue handling technique to address blockchain problems in unexpected ways.

Tso *et al.* [13] proposed a decentralized electronic voting and bidding system based on a blockchain and smart contract to provide everyone who used the application with an opportunity to participate in the opening phase, which met all security requirements for electronic applications. Additionally, the authors employed cryptographic methods including homomorphic and oblivious transfer encryptions to strengthen privacy protection. They used an integration of blockchain technology and privacy-protecting encryption to

enable everyone to take part in the beginning phases. In addition to increasing anonymity of participants, data transmission privacy, and data reliability and verifiability, the technique enabled voting and bidder participation in the preliminary round. When compared to other electronic voting and bidding systems, the suggested approach had been safer and more effective. Nevertheless, the structure was distinct for various secret sharing techniques. Therefore, the research required us to evaluate several covert sharing mechanisms in order to identify the best option.

AboSamra *et al.* [14] developed a cryptographic electronic voting system to reduce the complexity of the system and ensure a comparable level of security and vote anonymity with Mixnet-based e-voting systems, eliminating the need for anonymous channels. A combination of cryptographic methods was used to make the SAC e-voting system safe, offering higher levels of security, privacy, and anonymity. Implementation and simulation phases of the scheme were used to verify the practicality, scalability, efficiency, and lightness of the SAC e-voting method. These stages are used to determine protocol run time, message size, the number of voters waiting in a queue for a vote, the average waiting time per voter, network latency, central processing unit (CPU) and link utilization, and link throughput. This study was not concerned with formal verification of e-voting procedures. Taş and Tanrıöver [15] had presented a double-layer encryption model to avoid any possible manipulations of the election the final result. The suggested system's voting and counting stages were validated using simulation results, which demonstrated that they functioned appropriately. In this research, voting ballots were transferred among system nodes after being encrypted using homomorphic encryption. The only transactions that were guaranteed to be documented as subsequently mined into blocks were legitimate voter ballots. The authors came to the conclusion that the system ensured voter anonymity, does not require a central authority, and maintains the recorded votes in a distributed structure. However, the system could be enhanced to increase the time dimension's security.

While e-voting provides convenience, it does raise questions about the security of the network and privacy of communications. Communication and networking experts are concerned with e-voting security. In order to enhance e-voting security, Yi [16] proposed the use of blockchains in peer-to-peer (P2P) networks for e-voting. Voting records were synchronized using distributed ledger technology (DLT) to prevent vote manipulation. An elliptic curve cryptography based (ECC) user credential model was used to offer authentication and non-repudiation. Last but not least, they developed a withdrawal model that enabled voters to change their votes prior to a predetermined deadline. A blockchain-based system for e-voting on a P2P network combined with the aforementioned designs provided the conditions for e-voting. Using Linux platforms, a blockchain-based multiple candidates voting system was developed to prove and validate the idea. Based on the results of the installation, it was demonstrated that the system was workable and secure. While blockchain technology is safe, it was vulnerable to quantum attacks because it used ECC public key encryption.

Hu *et al.* [17] have presented a novel blockchain-based voting scheme for internet of everything (IoE) systems that emphasizes traits such as equity, eligibility, decentralization, compatibility, anonymity, resistance to coercion, and verifiability. The authors integrated the blind signature methodology and cryptography commitment. Additionally, they automate the internet of energy's voting system using smart contracts. The voting method could prove simple to integrate into the IoE system using smart contracts. They included a comparison study using cutting-edge blockchain-based electronic voting, as well. The findings of the research demonstrated that IoEPAV, a practical anonymous voting scheme for IoE, was very effective, decentralized, verified, and anonymous. In order to increase efficiency, the approach contained the restriction that parallel processing could not be used during the voting process.

Shahzad and Crowcroft [18] had presented electronic voting using adjusted blockchain technology and this study offered a system that protected the data's security by employing efficient hashing algorithms. A blockchain-based approach was employed in this study to evaluate the effectiveness of hashing algorithms, the formation and sealing of blocks, the accumulation of data, and the declaration of results. In the study, the authors made a statement that it understood the blockchain's security and data management concerned and offered a better representation of the electronic voting process. But it requires a lot of work to improve the availability of internet connection to avoid the latency in communication. The proposed smart contract and robust access control are made to safeguard the electoral data in an immutable and economical fashion. This is done by reviewing the existing literature in an effort to guarantee the highest level of security in electronic voting and to address blockchain's performance issues.

### 3. PROPOSED METHOD

To enhance the security against fraudulent activities, smart contract based blockchain with sidechain is introduced in this work. Namely, in this approach, the commission that conducts elections is in charge of initiating and concluding the election through communication using smart contracts. Smart contracts describe

the roles played in election agreements as well as the many elements and transactions that take place throughout the establishment and execution of the agreement. Currently, three smart contracts are active on the blockchain that is being proposed with sidechain-based e-voting. Voting contracts, candidate contracts, and voter contracts are among the smart contracts. Through these three contracts, voting, voter registration, and voter authentication are all carried out between the voter and the blockchain.

- a. Voter contract: To ensure the anonymity of voters, the voter contract stores the hash value of their information during the registration process. This hash value is used to verify the identity of voters during the voting process.
- b. Candidate contract: The candidate contract contains information about the candidates in the chain.
- c. Voting contract: A vote coin is used to cast votes after the voter authentication process is completed, a candidate is selected from the list provided by the candidate contract, and the election is conducted.
- d. Vote coin: A vote coin represents the voter's status as a voter. The voter does not cast his ballot if the vote coin's balance is 1. If the vote coin's balance is 0, the voter has already cast their ballot.
- e. Blockchain with sidechain: The cast vote is encrypted by using a public key generated by the election commission and stored in a crypto server. An encrypted ballot is received by the voting contract, which is then placed as a block in the chain. A sidechain network is presented in order to enhance the security of the storage on the blockchain network. The purpose of sidechains is to augment the capabilities of blockchains by performing some activities outside of them and returning the results to the mainchain. Therefore, the encrypted vote can be stored on the sidechain and the result decrypted on the mainchain, thereby reducing the cost.
- f. Data access control: According to this approach, there will be  $n$  voting blocks for every  $n$  votes. Once the election has ended, the election commission begins the counting process. To avoid authorization of unauthorized users or voting officer, robust access control mechanism is presented. It is easier to implement access control policies with this authorization model so that only authorized users can access the votes for counting. As well as supporting the role, task, and trust computing paradigms, this model also supports the role-based model. During the counting process, every accessed vote is decrypted using the private key from the crypto server.

The entire decrypted vote is transferred to the voting contract. Once the voter has sent their vote coin to the public key of the preferred candidate, it is counted without disclosing the identity of the voter. Candidate contracts handle the procedure of counting votes by providing information on the candidate's account and publishing the results.

#### 4. METHOD

This section explains study in order, including how it was designed and how it was done (through algorithms, pseudocode, or other means). The architecture of the suggested system, which is made up of many modules, shows how research was planned. Each module has been shown in different steps with the help of the appropriate algorithms. In this part, it also discussed an effective access control method with the appropriate equations.

##### 4.1. Architecture of the proposed e-voting system

A schematic illustration of the overall architecture of the proposed e-voting system is presented in Figure 1. The proposed e-voting system has 4 stages that are registration stage, voting setup stage, voting stage and result stage. These stages are explained as follows.

###### 4.1.1. Registration stage

This stage encompasses two distinct registration units, namely voter registration and candidate registration. The registration stage serves as the initial step in the implementation of the proposed electronic voting system. Individuals who meet the eligibility criteria, specifically being over the age of 18, have the opportunity to register their personal information and obtain their certificate from the Certification Authority Agent in advance of the scheduled election date.

- a. Voter registration: The term "voter" refers to all individuals who are registered to vote in their local election district and have the right to vote. As part of its duties, the election commission provides and maintains a current list of registered voters. The result is that every eligible voter must visit their local voter registration office in order to be verified as a legitimate voter. During the identity verification stage, it is necessary to keep track of who has voted as an initial step in the process as shown in algorithm 1. Furthermore, it serves as a control measure in order to prevent unregistered persons from voting in the election.

- b. Candidate registration: The registration process for candidates is similar to that for voters because a candidate is also a voter. A candidate must complete the voter registration process by providing their party symbol, seat number, and area in order to complete the candidate registration process as mentioned in algorithm 2. Candidate contract completes registration by adding a candidate’s information to the BlockChain.

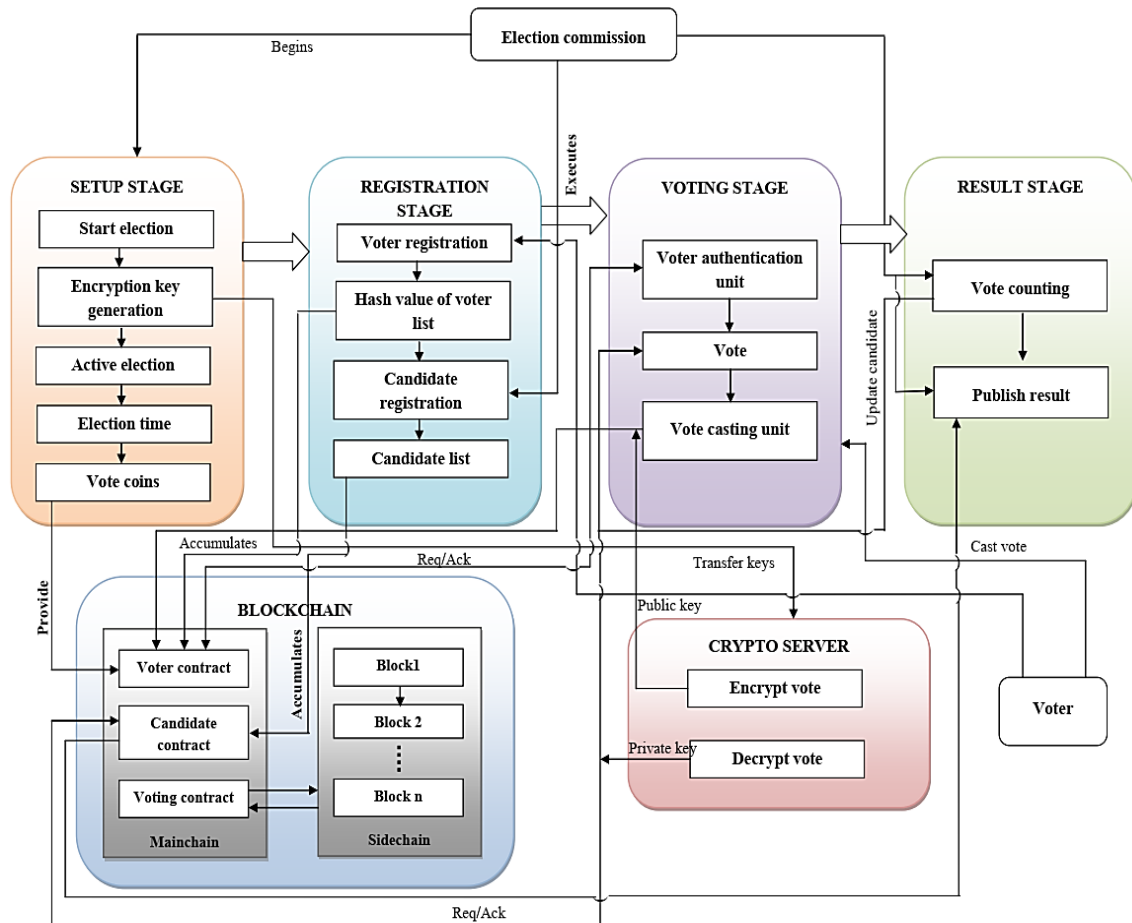


Figure 1. The overall architecture of the proposed e-voting system

**Algorithm 1. Voter registration**

Input: Credentials (Vtrid), mobile number (Vtrnum), voter name (Vtrnam), security key (sk)

Output: Hash value (hv), voter public key (Vtrpub), voter private key (Vtrpvt)

1. Check the validation of  $Vtr_{id}$
2. If the validation is not true, the ID is considered as invalid.
3. If the validation is true, credentials of the voters are given as input.
4. Based on the input credentials hash value is generated as  $hv = \text{Hash}(\text{credentials})$ .
5. Then, a onetime password (OTP) will be sent to the mobile of voters.
6. If both sent and entered OTP match,  $Vtr_{pub}$  and  $Vtr_{pvt}$  will be generated using key generation algorithm.
7.  $Vtr_{pvt}$  will be sent to the mobile number of the voter.
8. After receiving the acknowledgement from the voter,  $hv$  and  $Vtr_{pub}$  will be included to the blockchain.
9. After the completion of above process, the voter receives message like registration completed successfully.

**Algorithm 2. Candidate registration**

Input: Vtrid, Vtrnum, Vtrnam, sk, Place of nominated candidate (cp), seat number (sn), party symbol (sym)

Output: Candidate information (Cinf)

1. Verify that the candidate is a registered voter.
2. The voter registration function will be executed if the candidate is not a registered voter.
3. Then, cp, sn and sym are given as input during candidate registration.
4. The candidate’s information is added to the BlockChain by a candidate contract.
5. At final, the candidate receives message like registration completed successfully.

#### 4.1.2. Voting setup stage

Traditional or electronic, every voting system requires a setup in which the system is configured to manage the current election. At this point, the number and location of polling stations are determined, and ballots are created and tailored to the number and type of candidates. The configuration of voting is the second phase of this system. This phase consists of the start election and the active election.

- a. Start election: The election commission starts the election. The election commission connects to blockchain by employing a vital set of public and private keys as illustrated in algorithm 3. The registration contract is then sent to a transaction containing  $n$  vote coins, along with the election's start and end times. Once you have generated the keypair, which consists of a public key and a private key, you can send it to the crypto server, where it will be used for the encryption and decryption of votes.

##### Algorithm 3. Start election

Input: Vote coin (vc), election starting time (Tstart), election ending time (Tend)

1. Join election commission to blockchain using public and private keys.
  2. To register a contract with vc, Tstart and Tend, send a transaction.
  3. Transfer public and private keys to crypto server.
- b. Active election: As part of the voter contract, a transaction containing one vote coin, as well as the start and end times of the election is transmitted to the public key of each voter as illustrated in algorithm 4. All transactions are recorded in the blockchain. Due to this system, it is not possible to conceal the transactions involved in sending vote coins to voters or their voting status.

##### Algorithm 4. Active election

Input: vc, Tstart, Tend, Vtrpub

Output: vc

1. Voter contract creates  $vc=1$
2. Send transaction to Vtrpub with  $vc=1$ , Tstart and Tend
3. Each and every transaction is uploaded to BlockChain.

#### 4.1.3. Voting stage

The voting process consists of two distinct components, namely voter authentication and vote casting. The voting procedures refer to the established protocol for the act of casting votes during the proceedings of the Steering Committee. There is a requirement for voters, supervisory authorities, and candidates to possess certified, transparent, and verifiable information pertaining to all stages of the voting process.

- a. Voter authentication: Voter contracts manage the authentication process. Signing into their wallets with the private key is the final step in the authentication process as illustrated in algorithm 5. Once the voter has provided their authentication credentials, they must submit them. According to this scenario, the voter contract receives the credentials and creates a hash value from them, which is then compared to other hash values on the blockchain. Both hash values must be equivalent in order for the voter to cast a ballot.

##### Algorithm 5. Voter authentication

Input: Vtrid, Vtrnum, Vtrnam, sk,

Output: hv

1. Input the credentials of voter.
  2. Generate hv based on credentials.
  3. If hv matches with the hv in the list of voter registration, authentication will be succeeding. Else it will be failed.
- b. Vote casting: It is possible to vote using this system by submitting a transaction, which includes a transaction index, a timestamp, a choice by the candidate, and a transaction hash. Following the completion of the authentication procedure, the voter can cast a ballot.

Following the authentication procedure, the voter is presented with a ballot that lists candidates and displays a party symbol. There will be a list of candidates available for voters to choose from and they will be able to vote using a vote coin. Following this, the voter will receive his or her voter identification card. By using the public key of the election commissioner, the cast vote is stored on the sidechain of the blockchain as illustrated in algorithm 6.

##### Algorithm 6. Vote casting

Input: Vtrpvt

Output: vote ID (IDvote)

1. Once the authentication process is complete, the voter receives a ballot containing a list of candidates and the symbol of the party.
2. The voter can select from a list of candidates and cast his or her vote using a video camera.
3. Voter will then receive their IDvote.

4. The casted ballot (B) is secured on the side chain of the blockchain through voter contract using the public key of election commissioner, i.e.,  $B_{Enc} = Enc(B, Electioncommission_{pub})$

Main and side chain: Because of the classic blockchain single-chain paradigm's tendency to bundle and store transactions into blocks on the chain, the primary blockchain chain's performance, including transaction throughput and confirmation times, has been adversely affected by the increase in transactions. Further, due to the open and transparent nature of the blockchain, the main chain cannot maintain private data on a large scale, whereas the side chain can be considered a separate chain or system [19], [20]. According to Figure 1, this study takes into account one main chain and one side chain. Public access is provided to the information stored in the main chain blocks. As part of this study, the main chain blocks are used to store information concerning the votes cast for each candidate.

#### 4.1.4. Result stage

This step comprises voting and the publication of results units. The official process of selecting a person for public office or approving or rejecting a political idea through voting is known as an election. The voting process was completed by entering the ballot.

- a. Vote counting: During the counting process, the election commission enters the private key into the system. Before transferring the voting coin to the candidates' public keys, the voting contract will decrypt each encrypted ballot. After the coin is given, the vote is counted based on the candidate's contract, which is shown in algorithm 7. According to the number of coins in a candidate's wallet, his vote total is ultimately determined by the number of votes he receives.

#### Algorithm 7. Vote counting

Input:  $B, Election\ commission_{pub}, U, R, T$

Output: Candidate account (Cac)

1. Send request for accessing casted vote
2. If the user or voting officer from election commission is valid, the request will be sent for trust calculation
3. If the trust is less than threshold value, access denied.
4. Else robust control access scheme analyses the following assignments such as role, task and permission assignments.
5. Based on the trust, access is granted
6. After accessing the  $B_{Enc}$ , it will be decrypted using  $Election\ commission_{pvt}$ , i.e.,

$$B = Dec(B_{Enc}, Election\ commission_{pvt})$$

7. The voting contract delivers a vc transaction to each selected candidate's public key.
8. As a result of reviewing

- b. Access control: To access the encrypted cast vote from the side chain, robust access control mechanism is used. It is possible for some access control models to grant hazardous rights as they are unaware of how permissions are transferred from one user to another [21]. Our system provides a robust access control mechanism where a user's tasks, roles, and trust values are used to determine permissions.

According to the proposed access control system, tasks are assigned to users based on their roles, and permissions are assigned to tasks in order to perform the tasks assigned. Therefore, the proposed approach uses intermediary tasks and computes trust value rather than granting rights to roles.

The following list of components used in the suggested model is described:

- Users (U): Users are considered subjects of access control if they actively interact with the access control system,  $u_i \in U \forall i \in \{1, 2, \dots, m\}$ , here m is the total number of users or voting officers in the suggested system.
- Roles (R): Roles are job functions that a subject (user) assumes in an organization, and which outline the duties and powers assigned to the user.  $r_i \in R \forall i \in \{1, 2, \dots, n\}$ , here n is the total number of roles in the suggested system. For instance,  $R = \{Election\ commission, counting\ authority\ result\ announce\}$ .
- Tasks (T): An individual task represents a fundamental unit of work or action carried out by a role in the proposed system.  $t_i \in T \forall i \in \{1, 2, \dots, p\}$ , here p denotes the total number of tasks. For instance,  $T = \{Vote\ coin\ counting\ vote\ counting\ result\ announcing\}$ .
- Trust (Tr): Subjects are permitted access to data based on their trust value.  $Tr(u_i) \in \mathfrak{R}, \forall u_i \in U$ , here  $\mathfrak{R}$  denotes the real number. The trust is calculated as (1),

$$Tr = (\varphi_1 \times z_{exp}) + (\varphi_2 \times z_{int}) + (\varphi_3 \times z_g) - (\varphi_4 \times z_{mac}) + (\varphi_5 \times z_d) \quad (1)$$

Here,  $\varphi_1, \varphi_2, \varphi_3, \varphi_4$  and  $\varphi_5$  denote the weighting coefficients within [0, 1].  $Z_{exp}$  denotes a user takes into account the overall duration of time (OD) that user has been logged into the system,  $Z_{int}$  denotes the user's level of trust in the system based on their previous interactions with it,  $Z_{max}$  indicates the trust value of the user based on the media access control (MAC) address of the device the user tries to use to interface with the

system,  $Z_g$  denotes the number of access grants and  $Z_d$  denotes the number of access denies. These factors are defined as follows,

$$\begin{cases} Z_{exp} = \phi_1 \times Tr_{in}, & \text{if } OD = 1 \\ Z_{exp} + \psi_+ & \text{if } OD > 1 \\ Z_{exp} - \psi_+ & \text{if } timeelapse \end{cases} \quad (2)$$

$$\begin{cases} Z_{int} = \phi_2 \times Tr_{in}, & \text{if } q = 1 \\ Z_{int} + \psi_+ & \text{if } q > 1 \end{cases} \quad (3)$$

$$\begin{cases} Z_{mac} = \phi_3 \times 0 & \text{if no modification to MAC addresses} \\ Z_{mac} - \psi_+ & \text{if any MAC address changes} \end{cases} \quad (4)$$

$$\begin{cases} Z_g, Z_d = \phi_4, \phi_4 \times 0 & \text{if } l = 1 \\ Z_g + \psi_+ & \text{if } l > 1 \\ Z_g - \psi_+ & \text{if } l > 1 \end{cases} \quad (5)$$

Here,  $q$  denotes the number of interactions,  $l$  denotes the number of access grants and denies,  $Tr_{in}$  denotes the initial trust value (threshold trust) which is considered as 0.5,  $^+\psi_+$  denotes gradually rising user trust levels and  $^-\psi_+$  denotes gradually lowering of the level of user trust.

- Permissions (V): Permission is the right of access to perform any task.  $v_i \in V \forall i \in \{1, 2, \dots, r\}$ , here  $r$  denotes the whole number of permissions. For instance,  $V = \{Read, write, read \text{ and } write\}$ .
- Assignments: In the suggested scheme, various assignments listed below are utilized;
- User-role assignment (AUR): Users are assigned roles based on their duties, power, and qualifications within an organization, and roles are created for distinct tasks within the organization. Users and roles in AUR can be assigned to one another in a many-to-many connection; that is, a user may be given one or more roles, and vice versa. It is represented as  $A_{UR} \subseteq U \times R$ .
- Role-task assignment (ART): It is the purpose of this assignment to generate tasks for various job functions inside an organization, and roles will be assigned tasks in accordance with their job functions. A role can be assigned to several tasks and vice versa in ART. Roles and tasks have a many-to-many relationship. It is represented as  $A_{RT} \subseteq R \times T$ .
- Permission-task assignment (APT): In this part, tasks are given permissions to carry out the tasks that have been given to them. APT is a many-to-many plot of commissions with permission to perform tasks. It is represented as  $A_{PT} \subseteq P \times T$ .

Figure 2 shows the strong access control technique for side chain voting. The system verifies user credentials after receiving an access request, as illustrated in the figure. If the user's credentials are verified, the access request goes to the trust evaluation module; otherwise, the user is blocked. i) estimates trust value. If the whole trust value is lower than the threshold trust value, access to the system and related data is refused; if it is higher, access is given. After logging in, tasks, roles, and users are assigned permissions. Delegated roles allow users to do a range of jobs, and each position has its own rights based on its tasks. Thus, roles only have permissions while executing tasks. Finally, the user receives the data. Main chain voting contract decrypts data using private key.

**Publish result:** After casting a ballot, every vote becomes a block, adding to the chain. After the vote is entered, it will immediately be counted since there is no chance of tampering or manipulation. The result is subsequently displayed in the result panel, as shown in algorithm 8.

#### Algorithm 8. Publish result

Input: Cac  
 Output: Winnig candidate (Cwin)  
 Check Cac to find winner  
 Result list is generated as  
 $list = result(sym, sn, C_{ac}, C_{win})$   
 At final, Cwin is published.



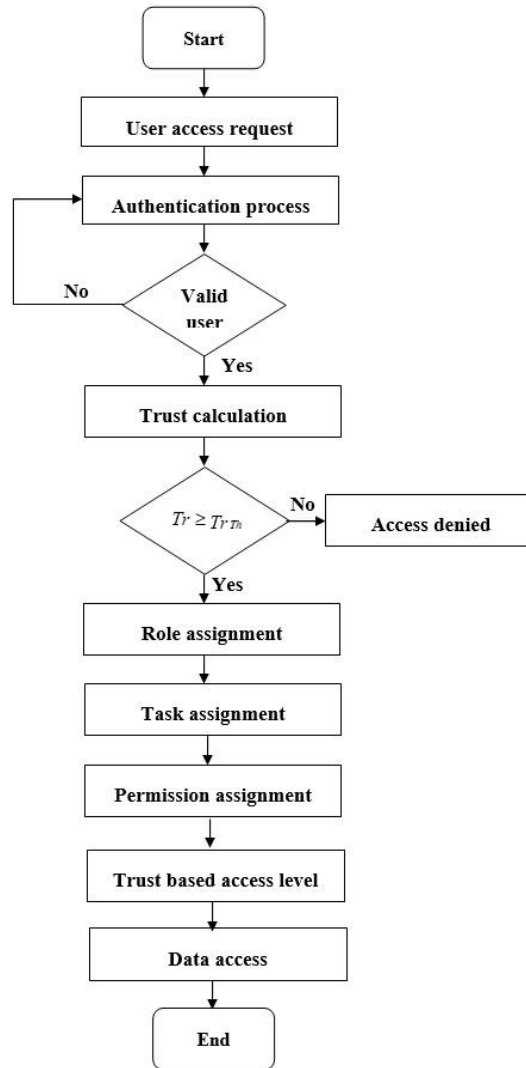


Figure 2. The flowchart of the robust access control scheme

## 5. RESULTS AND DISCUSSION

In this section, we present a simulation of a blockchain-based electronic voting system and discuss its performance. The interaction of stakeholders and election officers is examined through a series of simulations. A performance evaluation of the immutable electronic voting system is performed by simulating the retrieval and processing of events. Evaluation of the voting system is achieved by analyzing the number of modification requests, percentage of read shares, handling the security risks associated with replay attacks, and smart contract operations by concurrently computing the system. The voting system integrates and connects entity configurations and connections to achieve this objective.

Through the application of Ethereum's proof of stake consensus algorithm, we test whether the framework is feasible by specifying nodes connecting to individual components. The simulation is conducted using a computer with an Intel i7 processor and 16 GB of RAM and an Ubuntu 16.04.1 LTS operating system and simulation environment is summarized in Table 1.

A simulation is run on the Ethereum Ropsten network, which is a peer-to-peer blockchain network in which over 10,000 nodes interact with one another in real time. By increasing the number of nodes to analyze transaction confirmation times, it is not possible to increase the transaction cost. In the experiment, the hash rate was 210690.12 G/s, the difficulty was 3491.86 TH, and the block time was 13.2 s. Further, we developed a set of operations with solidity that was modeled as smart contract functions in the Ethereum network using a Remix IDE. Besides, the performance of the proposed e-voting system is compared with that of e-voting (blockchain with side chain) with discretionary access control (DAC) [22] and e-voting (blockchain with side chain) with no access control. In Table 2, the entire state of the simulations is summarized based on the blockchain network simulations.

Table 1. Simulation environment summary

Parameter	Specifications
Ethereum network	Ropsten
Consensus	Proof of stake
IDE	Remix
Smart contract language	Solidity
Ethereum network	Ropsten

### 5.1. Analysis of the access control

Immutability is one of the defining characteristics of blockchain [23], and it is an important consideration when deciding to use blockchain technology for electronic voting or other mission-critical applications [24]. Observations have shown that some of the data must be readable for data stakeholders in the voting system; hence the election authority will be sharing such data. Figure 3 shows the degree of immutability of such readable data for the increasing number of nodes in the network. As illustrated in the figure, degree of immutability of the proposed e-voting system is increased to 4.8% and 9.3% than that of e-voting with DAC and e-voting w/o access control respectively. By making incorrect changes to the view of the data, a malicious user may attempt to corrupt the view and attempt to commit those corrupted changes as updated authenticated views. An efficient access control mitigates such possibility from an election authority accepting or rejecting a change.

Table 2. State of simulation network

State	Rate
Average transaction per second	12 TPS
Average block size	40.2 KB
1 ETH	1818.85USD
Average transaction cost	0.04 ETH
Median transaction cost	1.23 ETH
Average block creation time	0.192s
Blockchain size	300 GB
Reward fee for each block	2.4 ETH
Fee in reward	23.7%
Block count	10,300,110
Hash rate	210690.12 GH/s
Gas rate	\$0.03 per transfer

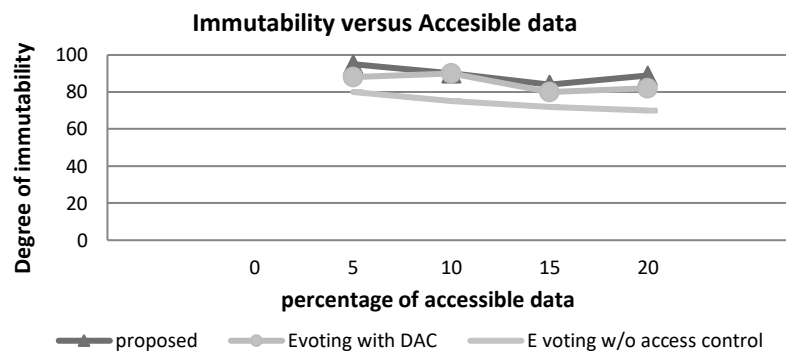


Figure 3. Access control of data

### 5.2. Analysis of the system security to replay attacks

In order to perform replay attacks on the voting system, old change request messages with digital signatures attached may be used. It is possible to maintain track of the current change in a data view by using timestamp synchronization on computation nodes [25]. A message with a timestamp that is less than the latest timestamp for the data will be ignored. Figure 4 shows the system security against replay attacks for the various number of nodes in the network. It can be analyzed from the figure that with the modest variations, the system is efficient to handle all reply to attacks for increasing number of nodes. Compared to e-voting with DAC and e-voting w/o access control, system security of the proposed e-voting system is increased to 1.2% and 20.2% respectively.

**5.3. Analysis of average transaction processing time and average transaction cost**

A smart contract is one of the most well-known characteristics of blockchain technology. The deterministic nature of this technology makes it possible to guarantee a high level data integrity without any involvement from humans [26]–[28]. Figures 5 and 6 represent the average transaction processing cost and time for different smart contract operations. Voting contracts need to be carefully written with all the security concerns and the data must be put in blockchain. For block creation fee, mining rewards everything adds up here, hence it is processing cost is higher than voter and candidate contract. Namely, the processing cost of the proposed e-voting system is reduced to 3% and 6% than that of e-voting with DAC and e-voting w/o access control respectively. In the proposed e-voting system, voting contract takes much more time due to blockchain and security when compared to voter contract and candidate contract. However, compared to e-voting with DAC and e-voting w/o access control, processing time of the proposed e-voting system is reduced to 39% and 54% respectively.

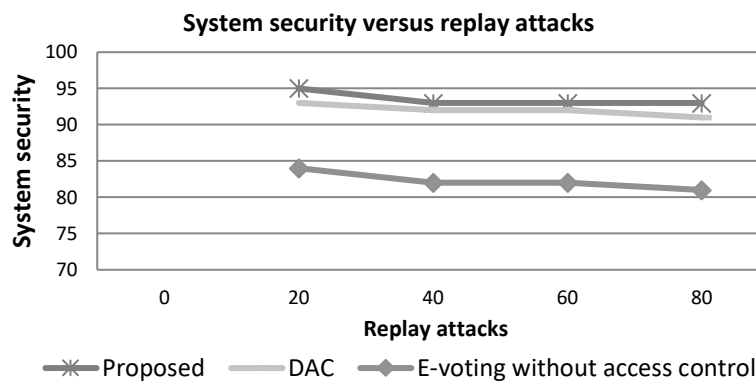


Figure 4. System security for replay attacks

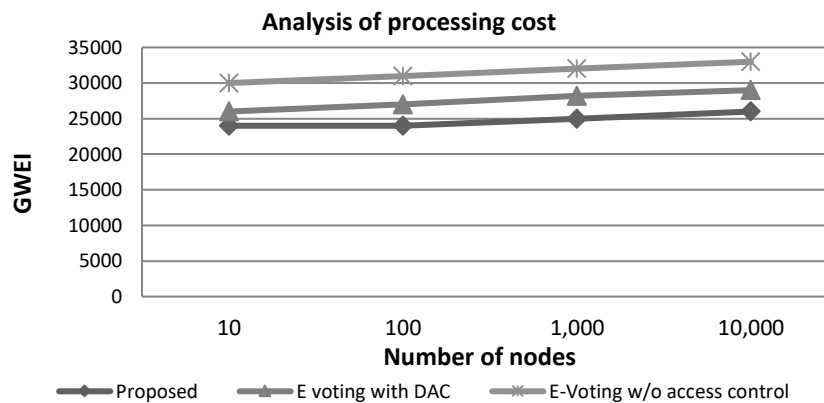


Figure 5. Average processing cost of smart contract operations

**5.4. Scalability**

The currently available Blockchain platforms struggle with a number of scalability challenges, making it difficult to accept a wide variety of applications without sacrificing efficiency. So in this paper scalability has been taken into consideration while writing smart contracts [29], [30]. Figures 7 and 8 illustrate the scalability of the proposed blockchain-based architecture for the electronic voting system in terms of throughput and response time for the network’s increased voter participation. Figure 7 shows how an increase in the number of voters might result in a 5% increase in response time. As shown in the table, there are 12 transactions per second on average. However, a rapid increase in the voting rate may result in a decrease in the average transaction rate per second. As a result, the throughput rate has decreased by up to 8% shown in Figure 8. The proposed blockchain-based framework for immutable electronic voting is scalable and effective for dynamic voting situations because there is little impact on the system’s response time and throughput.

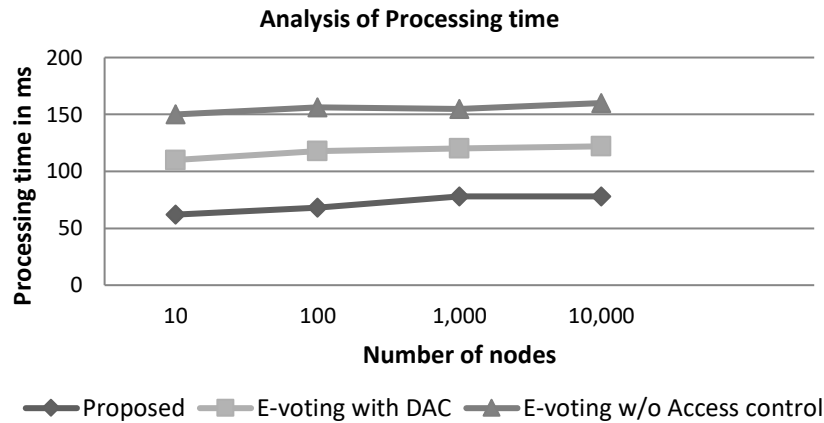


Figure 6. Average transaction processing time

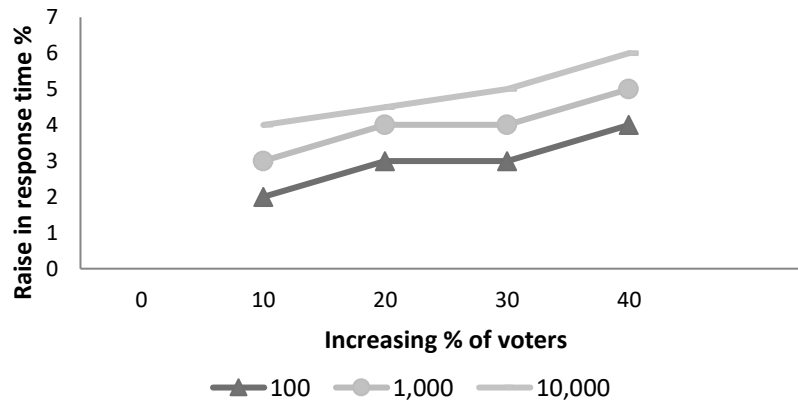


Figure 7. Raise in response time

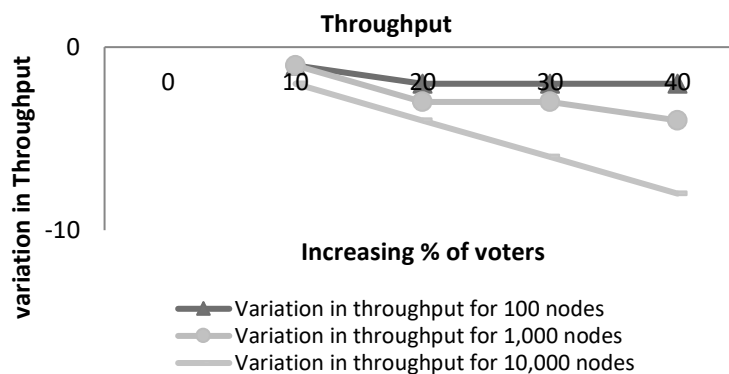


Figure 8. Throughput

## 6. CONCLUSION

To enhance the security against the fraudulent activities in E-voting system, a novel smart contract based blockchain with sidechain and robust access control are presented in this approach. The proposed blockchain with sidechain includes three smart contracts that are voter, candidate and voting contracts. The casted vote on each candidate is encrypted and stored as block in sidechain. Besides, using vote coin, fraudulent voting is prevented. To access the encrypted vote from the blockchain, robust access control mechanism is used. This mechanism performs based on role, task, and trust computing paradigm. Once the

access is granted, the election officer will access the decrypted vote from the mainchain of the blockchain. From the simulations we observed that with novel smart contracts and robust access control the proposed blockchain mechanism ensures efficient security for the voted data in terms of immutability in comparison with the existing work. Simulation results depicted that proposed scheme reduces processing time and cost of smart contracts. The performance of blockchain transaction rate is better than the existing work due to the inclusion of sidechain technique. The proposed e-voting system obtains the scalability of 5%. Besides, system security is improved to 94% against replay attacks.

## ACKNOWLEDGEMENTS

We would like to convey our heartfelt gratitude to All India Council for Technical Education (AICTE) for providing a Doctoral Fellowship to support our research.




## REFERENCES

- [1] O. Daramola and D. Thebus, "Architecture-centric evaluation of blockchain-based smart contract e-voting for national elections," *Informatics*, vol. 7, no. 2, May 2020, doi: 10.3390/informatics7020016.
- [2] C. K. Adiputra, R. Hjort, and H. Sato, "A proposal of blockchain-based electronic voting system," in *Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, 2018, pp. 22–27, doi: 10.1109/WorldS4.2018.8611593.
- [3] V. Suma, "Security and privacy mechanism using blockchain," *Journal of Ubiquitous Computing and Communication Technologies*, vol. 1, no. 1, pp. 45–54, Sep. 2019, doi: 10.36548/jucct.2019.1.005.
- [4] S. Shakya, "Efficient security and privacy mechanism for block chain application," *Journal of Information Technology and Digital World*, vol. 1, no. 2, pp. 58–67, Dec. 2019, doi: 10.36548/jitdw.2019.2.001.
- [5] S. T. Alvi, M. N. Uddin, and L. Islam, "Digital voting: a blockchain-based e-voting system using biohash and smart contract," in *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, Aug. 2020, pp. 228–233, doi: 10.1109/ICSSIT48917.2020.9214250.
- [6] Y. Abuidris, R. Kumar, T. Yang, and J. Onginjo, "Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding," *ETRI Journal*, vol. 43, no. 2, pp. 357–370, Apr. 2021, doi: 10.4218/etrij.2019-0362.
- [7] N. Kshetri and J. Voas, "Blockchain-enabled e-voting," *IEEE Software*, vol. 35, no. 4, pp. 95–99, Jul. 2018, doi: 10.1109/MS.2018.2801546.
- [8] C.-H. Roh and I.-Y. Lee, "A study on electronic voting system using private blockchain," *Journal of Information Processing Systems*, vol. 16, no. 2, pp. 421–434, 2020.
- [9] A. Navya, R. Roopini, A. S. SaiNiranjana, and B. J. Prabhu, "Electronic voting machine based on blockchain technology and aadhar verification," *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 4, no. 2, 2018.
- [10] S. Shukla, A. N. Thasmiya, D. O. Shashank, and H. R. Mamatha, "Online voting application using ethereum blockchain," in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Sep. 2018, pp. 873–880, doi: 10.1109/ICACCI.2018.8554652.
- [11] C. A. ul Hassan *et al.*, "A liquid democracy enabled blockchain-based electronic voting system," *Scientific Programming*, pp. 1–10, Jan. 2022, doi: 10.1155/2022/1383007.
- [12] S. Chaisawat and C. Vorakulpipat, "Towards achieving personal privacy protection and data security on integrated e-voting model of blockchain and message queue," *Security and Communication Networks*, pp. 1–14, Sep. 2021, doi: 10.1155/2021/8338616.
- [13] R. Tso, Z.-Y. Liu, and J.-H. Hsiao, "Distributed e-voting and e-bidding systems based on smart contract," *Electronics*, vol. 8, no. 4, Apr. 2019, doi: 10.3390/electronics8040422.
- [14] K. M. AboSamra, A. A. AbdelHafez, G. M. R. Assassa, and M. F. M. Mursi, "A practical, secure, and auditable e-voting system," *Journal of Information Security and Applications*, vol. 36, pp. 69–89, Oct. 2017, doi: 10.1016/j.jisa.2017.08.002.
- [15] R. Taş and Ö. Ö. Tanrıöver, "A manipulation prevention model for blockchain-based e-voting systems," *Security and Communication Networks*, pp. 1–16, Apr. 2021, doi: 10.1155/2021/6673691.
- [16] H. Yi, "Securing e-voting based on blockchain in P2P network," *EURASIP Journal on Wireless Communications and Networking*, no. 1, Dec. 2019, doi: 10.1186/s13638-019-1473-6.
- [17] H. Hu *et al.*, "A practical anonymous voting scheme based on blockchain for internet of energy," *Security and Communication Networks*, pp. 1–15, Aug. 2022, doi: 10.1155/2022/4436824.
- [18] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," *IEEE Access*, vol. 7, pp. 24477–24488, 2019, doi: 10.1109/ACCESS.2019.2895670.
- [19] L. Yang *et al.*, "An access control model based on blockchain master-sidechain collaboration," *Cluster Computing*, Jan. 2023, doi: 10.1007/s10586-022-03964-x.
- [20] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, and K.-K. R. Choo, "Sidechain technologies in blockchain networks: An examination and state-of-the-art review," *Journal of Network and Computer Applications*, vol. 149, Jan. 2020, doi: 10.1016/j.jnca.2019.102471.
- [21] M. S. Rahaman, S. N. Tisha, E. Song, and T. Cerny, "Access control design practice and solutions in cloud-native architecture: a systematic mapping study," *Sensors*, vol. 23, no. 7, Mar. 2023, doi: 10.3390/s23073413.
- [22] Ninghui Li, "How to make discretionary access control secure against trojan horses," in *2008 IEEE International Symposium on Parallel and Distributed Processing*, Apr. 2008, pp. 1–3, doi: 10.1109/IPDPS.2008.4536104.
- [23] M. N. Birje, G. R. H. R. C. M., and M. T. Tapale, "Blockchain technology review: consensus mechanisms and applications," *International Journal of Engineering Trends and Technology*, vol. 71, no. 5, pp. 27–39, 2023, doi: 10.14445/22315381/IJETT-V71I5P204.
- [24] E. B. Sifah, Q. Xia, K. O.-B. O. Agyekum, H. Xia, A. Smahi, and J. Gao, "A blockchain approach to ensuring provenance to outsourced cloud data in a sharing ecosystem," *IEEE Systems Journal*, vol. 16, no. 1, pp. 1673–1684, Mar. 2022, doi: 10.1109/JSYST.2021.3068224.
- [25] M. N. Birje, R. H. Goudar, C. M. Rakshitha, and M. T. Tapale, "A review on layered architecture and application domains of blockchain technology," in *2022 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, Jul. 2022, pp. 1–5, doi: 10.1109/ICECET55527.2022.9872729.




- [26] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 2901–2925, Sep. 2021, doi: 10.1007/s12083-021-01127-0.
- [27] H. Taherdoost, "Smart contracts in blockchain technology: a critical review," *Information*, vol. 14, no. 2, Feb. 2023, doi: 10.3390/info14020117.
- [28] M. Patel, B. Gohil, S. Chaudhary, and S. Garg, "Smart offload chain: a proposed architecture for blockchain assisted fog offloading in smart city," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 4, pp. 4137–4145, Aug. 2022, doi: 10.11591/ijece.v12i4.pp4137-4145.
- [29] A. I. Sanka and R. C. C. Cheung, "A systematic review of blockchain scalability: Issues, solutions, analysis and future research," *Journal of Network and Computer Applications*, vol. 195, Dec. 2021, doi: 10.1016/j.jnca.2021.103232.
- [30] A. Hafid, A. S. Hafid, and M. Samih, "Scaling blockchains: a comprehensive survey," *IEEE Access*, vol. 8, pp. 125244–125262, 2020, doi: 10.1109/ACCESS.2020.3007251.

## BIOGRAPHIES OF AUTHORS







**Rakshitha Channarayapatna Mullegowda**    received B.E and M. Tech in the field of Computer Science and Engineering. Her research areas include network security, automata and computability, and blockchain technology. She has published a few papers in the International journal and Conferences. She is currently pursuing her Ph.D. in the Department of Computer Science and Engineering under AICTE Doctoral Fellowship scheme at Visvesvaraya Technological University, Karnataka, India. She can be contacted at email: rakshitha.m@vtu.ac.in.







**Nirmala Hiremani**    received B.E and M.Tech in the area of computer science and engineering. She obtained her Ph.D. at Visvesvaraya Technological University in the domain of wireless sensor networks. Her research interests are WSN, internet of things, machine learning and artificial intelligence, she has published several research papers in international journals and conferences. She is currently working as assistant professor, Department of Computer Science and Engineering, Visvesvaraya Technological University, Karnataka, India. She can be contacted at email: nirmalavtup@gmail.com.



**Mahantesh Birje**     received B.E., M. Tech. and Ph.D. in the field of computer science and engineering. His current research areas include cloud computing, internet of things, data mining, and security. He has published 32 research papers in International referred journals, 2 Book Chapters, and 28 papers in international conferences. He has chaired sessions of some international conferences. He is a reviewer of some international journals of IEEE, Elsevier, and Springer. Currently he is a professor in the Department of Computer Science and Engineering, VTU, Belagavi. He can be contacted at email: mnbirje1@gmail.com.



**Nataraj Kanathur Ramaswamy**     is currently, Director, Research and Development at Visvesvaraya Technological University, Belagavi. He has around 27 years of teaching experience with industry interactions. He has served the VTU at various levels as BOE Member, Paper Setter, and DCS for VTU digital valuation, journal reviewer for IEEE and Springer. He has received funds from different funding agencies. He is currently guiding five research scholars in Visvesvaraya Technological University Belgaum. He is a recognized research guide, Ph.D. thesis evaluator of various universities across the country. He can be contacted at email: rnddirector@vtu.ac.in.