

A Blockchain-Powered E-Voting System with SHA-256 Encryption

Mr. Sarang Landge, Mr. Prajwal Madavi, Mr. Vaibhav Narayane, Mr. Pawan Kothalkar, Mr. Vedant Kulkarni, Prof. P.H. Dhole

“Department of Computer science and Engineering”

Sipna college of Engineering and Technology, Amravati, Maharashtra

Abstract

E-voting systems hold promise for revolutionizing the electoral process by offering efficiency, accessibility, and transparency. However, concerns about security and integrity have hindered their widespread adoption. In this research paper, we propose a blockchain-based e-voting system leveraging the SHA-256 algorithm to address these challenges. Our system utilizes blockchain technology to create a tamper-proof and immutable ledger of votes, ensuring transparency and accountability throughout the voting process. The SHA-256 algorithm is employed to secure data integrity, providing robust protection against unauthorized modifications. This paper presents the system architecture, implementation details, and security analysis, demonstrating its resistance to tampering and vulnerabilities. Furthermore, we evaluate the system's performance and usability, highlighting its potential to enhance the electoral process. By leveraging blockchain technology and the SHA-256 algorithm, our e-voting system offers a secure, transparent, and efficient platform for conducting elections, fostering trust and confidence among voters.

Keywords: Blockchain-based e-voting system, SHA-256 Algorithm

I Introduction

Due to their significance to our society, the election process should be transparent and reliable to ensure participants of its credibility [1]. In contemporary democracies, the integrity of electoral processes stands as a cornerstone, ensuring the legitimacy of elected representatives and the trust of citizens in their governance systems. However, traditional methods of voting have faced scrutiny due to issues such as electoral fraud, tampering, and logistical challenges. To address these concerns and enhance the transparency, security, and accessibility of voting mechanisms, emerging technologies like blockchain offer promising solutions.

Blockchain an overview

Blockchain is a decentralize data managing system, where the data are sequentially stored in an encrypted chain of blocks and distributed into a peer-to-peer (P2P) network. The idea of blockchain is generated from electronic Bitcoin system proposed by Satoshi Nakamoto. Bitcoin is considered the first application of the Blockchain concept to create a currency that could be exchanged over the Internet relying only on cryptography to secure the transactions. Blockchain is an ordered data structure that contains blocks of transactions. Each block in the chain is linked to the previous block in the chain. The first block in the chain

is referred to as the foundation of the stack. Each new block created gets layered on top of the previous block to form a stack called a Blockchain [4].

Each hash function is generated by SHA-256-bit hash. This algorithm is designed by the National Security Agency (NSA) in 2001 and was used as the protocol to secure all federal communications [8]. The SHA-256 will take any size plaintext as an input and encrypt it to a 256-byte binary value. The SHA-256 is always a 256-bit binary value, and it is a strictly one-way function. The figure 1 below shows the basic logic of the SHA-256 encryption.

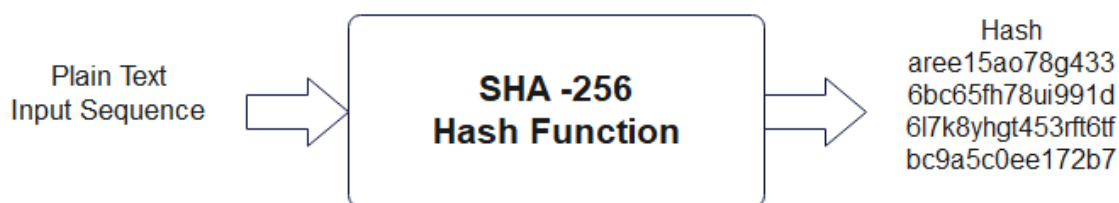


Figure 1;- Representation of SHA-256 Algorithm

Each header contains information that links a block to its previous block in the chain, which creates a chain linked to every vote casted. The primary identifier of each vote is the encrypted hash in the encrypted hash in the header. A digital fingerprint that was made combining two types of information; the information contained of new block created of voter's identity as well as the previous block in the chain.

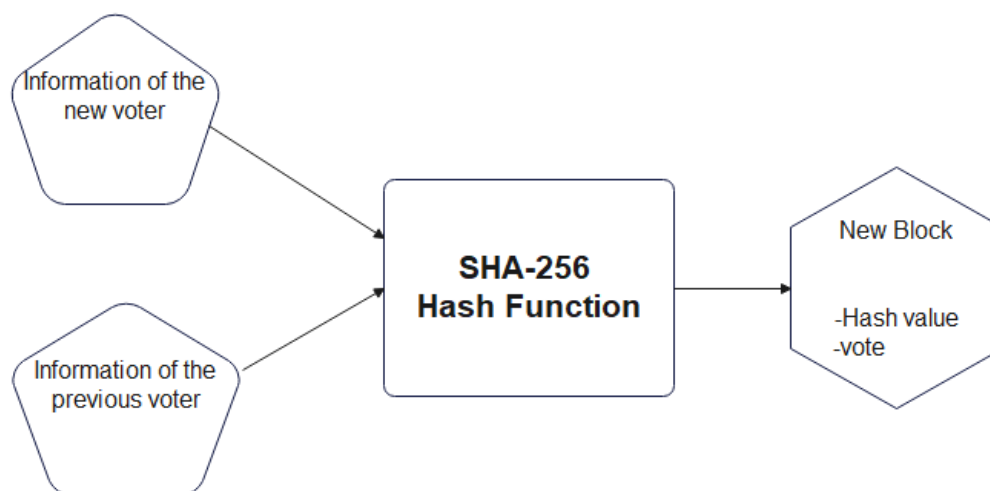


Figure 2 Creation of new block containing a hash value and a vote.

As soon as a block is created, it is sent over to the Blockchain. The system will keep an eye on incoming blocks and continuously updating the chain with respect to the nodes which are generating new votes and modify the chain when new blocks arrived.

II Literature Review

Authors	Title	Methodology	Key Takeaways
Kashif Mehboob Khan	Secure Blockchain voting system based on blockchain technology	Strong Architecture of e-voting systems, Voting process	Architecture of proposed e-voting system
Asraful Alam	Towards Blockchain-Based E-voting system	Distributed ledger where data is distributed in network	Voting model using blocks in merkle tree
D.D. Kumar	Secure Electronic Voting System using Blockchain Technology	App for e-voting system using SHA-256 Algorithm for creating hash	Understanding SHA-256 Algorithm and creating Block using it
Ayed Ahmed Ben	A conceptual Secure Blockchain-Based Electronic Voting system	Blockchain technology for proposing new various designs of e-voting system	Security and Authentication is designing the e-voting system and structure of Blocks
Chinnapong Angsuchotmetee	BlockVOTE: An Architecture of Blockchain-based Electronic Voting System	e-voting system Architecture with Decentralized Approach and consensus handling mechanism of Blockchain	Roles and Responsibilities of voter and admin, block vote concept in ballot and trustable e-voting system

S. Aruna	Highly Secured Blockchain Based Electronic voting system Using SHA3 and Merkle root	Avoiding Redundancies and immutable votes in permanent records.	Creating hash value with SHA3 in blocks and building integrity In vote's database.
----------	---	---	--

III Proposed system

In our design we created a web platform for e-voting system which uses a blockchain technology behind it, To secure a vote in a block that cannot be change throughout the process of voting, It ensures complete authenticity and security, and provide accurate and fair results to create transparency among the voters. Here the blockchain creates a block of vote with voter's details into a hash function which connects the previous hash function also builds link between the previous votes.

E-voting system solution will include four main requirements that can be illustrated as shown below:

- **Authentication:** Only eligible voters can vote for a specific subject, Registration for voting is only manually registered on administration level and registered in big number with general data, Login and password for accessing vote is provided by authorize authority.
- **Anonymity:** E-voting system should not contain any link between voter's identities and ballots. The voter has to remain anonymous during and after the election.
- **Accuracy:** Duplicate values of votes and every vote should be counted in e-voting system for more accurate and reliable results.
- **Verifiability:** The system should verify to make sure that all votes are counted correctly, and authenticates user that his/her vote is counted correctly with a pop up message, This four factors supports our solution mobility, flexibility and efficiency.

Representation of the E-voting System

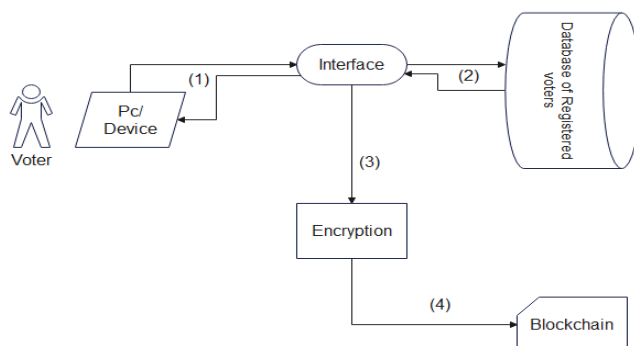


Figure 3: Representation of e-voting system

(1) Requesting to vote:- The voter will have to log in to the web platform of e-voting system using the essential credentials email and password provided by administrators of e-voting system. The system will check the information entered and if it matches with the database then login of Voter will be successful and pop up message will be displayed on the interface.

(2) Casting a vote: After login on the interface of e-voting system the voter will show the voting subject assigned to it, and by opening it the minimum time to cast a vote on platform will be 10 minutes, after time out voter will have to login and cast vote for not considering the duplicate values of votes.

(3) Encrypting votes: After the voter casting vote the system will generate an input that contains the voter identification details and name as well as the hash of the previous vote. This way each input will be unique and ensures that the encrypted data will be unique. This input information will be encrypted using SHA-256 algorithm, which is a one-way hash function that has no known reverse to it.

(4) Adding the vote to the Blockchain: After a block is created, the information is recorded in the corresponding Blockchain of voter's information and vote. Each block gets linked to the previously cast vote.

This is the overall representation and workflow of our e-voting system, there are main two modules; voter and admin their roles are important for working of e-voting system. Below figures shows the representation of roles of voter and administrative.

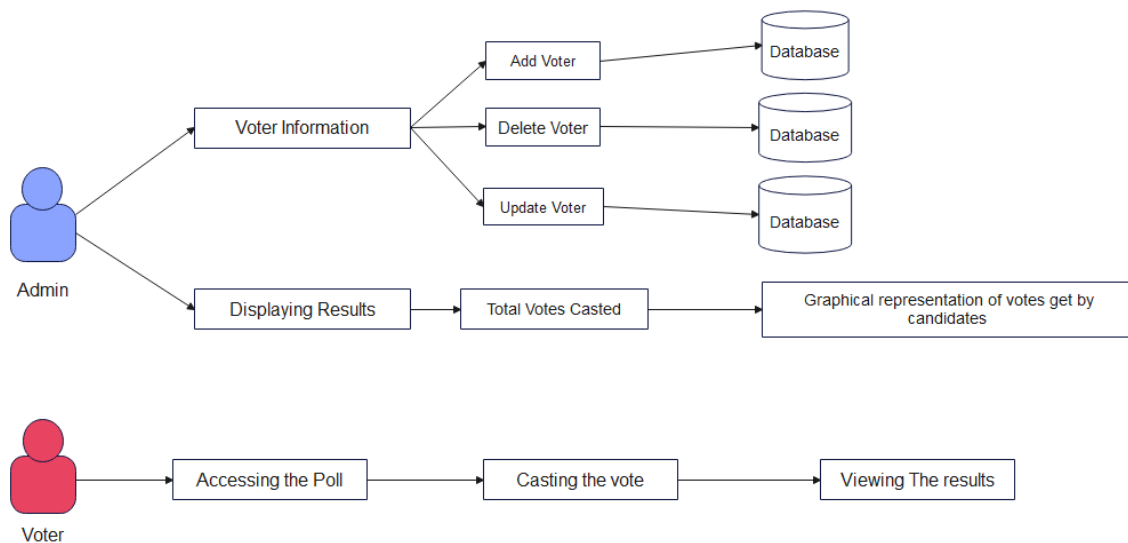


Figure 4 Representation of roles voter and admin.

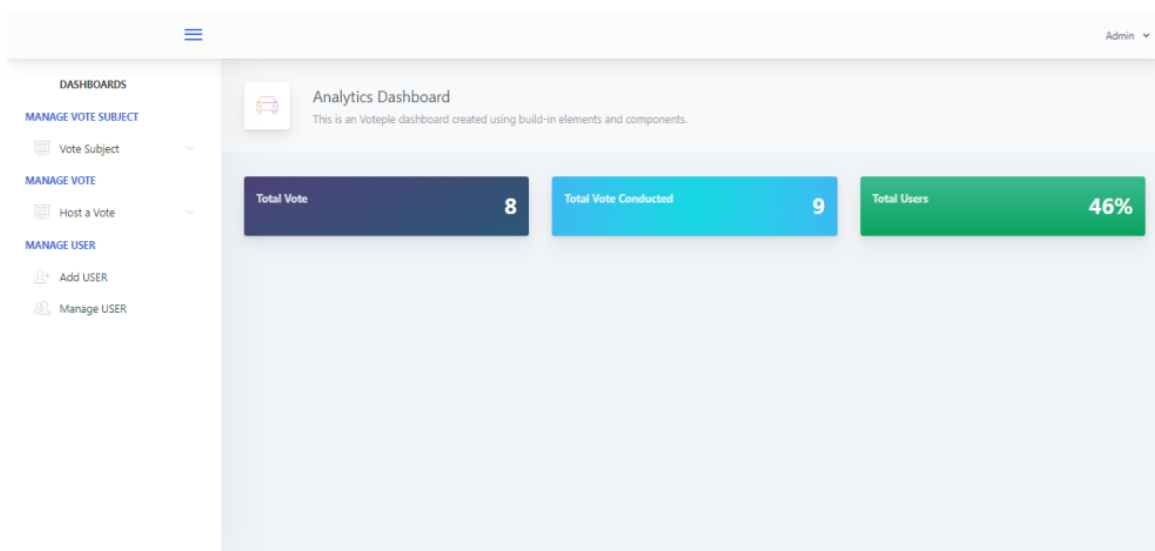
Roles and Responsibilities:

Voter: - In our system voter has very less roles and activities for casting a vote on e-voting for creating a user-friendly interface and not creating it more complex, voter can access the only poll which is assigned to the voter from administration. After opening the poll casting their vote on the options created by admin in a specific time frame, Voter should be authenticated by a message that his/her vote is considered as a counted. Then the fast and accurate result should be displayed on the screen.

Admin: - Admin controls all details of voter and their activities, Admin assigns the poll to the valid voters with a specific date and time, the poll will be available on that specific date and time. Adding voter, deleting voter and Updating voter's information to the main database can be done manually through admin's login and data can be changed on the server also. Admin get the record of total number of votes and percentage of voting according to the registered voters. And display election results in graphical representation on the admin dashboard. Admin can know the duplicate votes and incorrect entries of voter's information to execute transparency of voting.

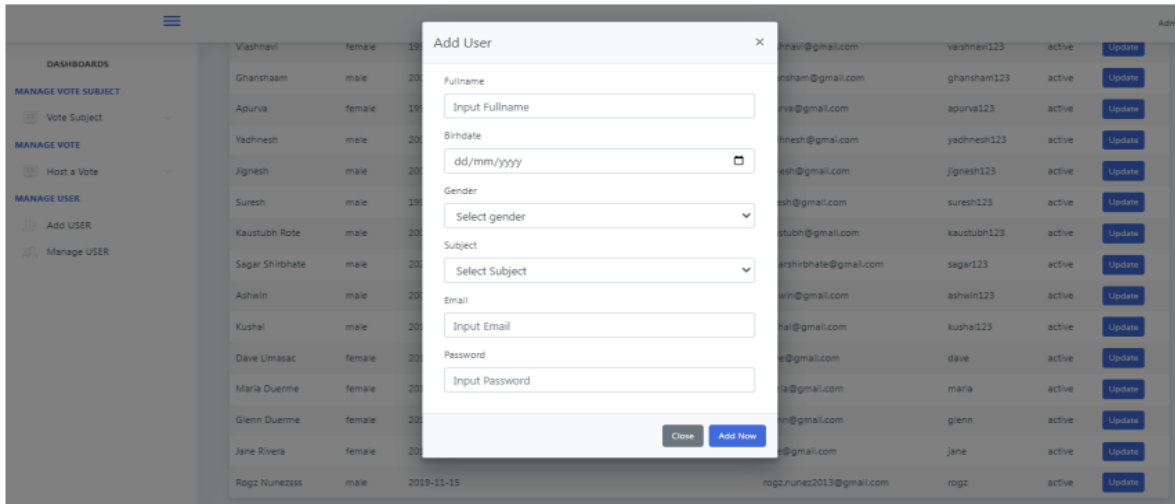
IV Results

(1)Admin dashboard:- After Admin login on admin dashboard it shows the total votes, total votes are conducted through polls and the voting percentage compared with all the registered voters. Three main operations admin can perform are Manage vote, Create voting subject,



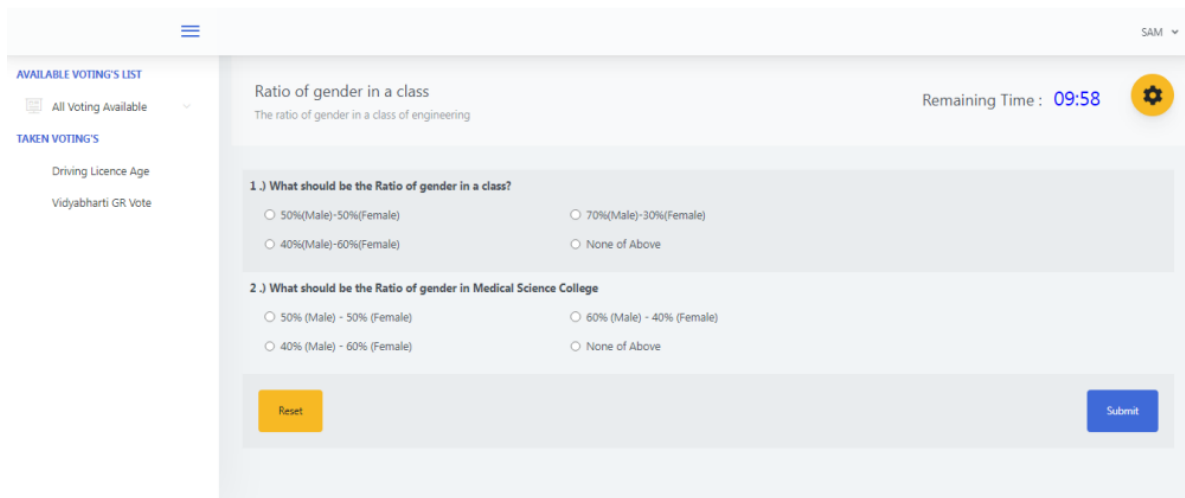
Manage voter's details, In manage vote, the poll is assigned to the eligible voters. In manage user, the new voters are added manually by adding all details and credentials. Vote subject is adding the main voting subject with its options, date, and time for voting.

(2) Adding voters manually: - Adding new voters on e-voting system, by adding essential information like name, Date of birth for determining eligibility by age



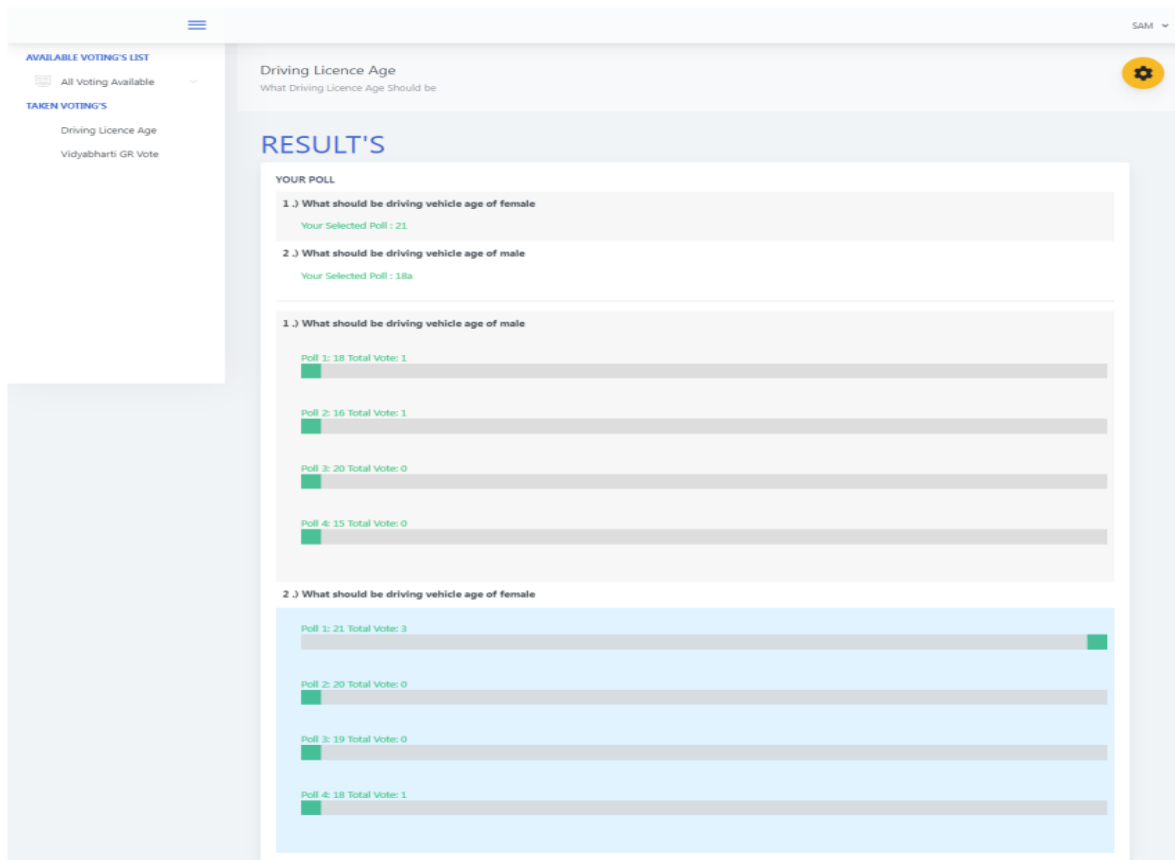
Email and password is provided for login purpose of voter for casting vote. Voting Subject is assigned to user according to the eligibility criteria.

(3) Casting vote by user: - After login on user's portal and accessing the poll which is assigned, the options are displayed with voting subject and description of poll.



After opening the poll maximum 10 minutes or time assigned to user is started dropping and user must vote in that remaining time, Submit, and reset buttons are provided for submitting the choice and resetting the selected choice respectively. The Vote submitted message is shown on the voter's login panel.

(4) Results: - Results of all the active voting polls are reflected on the admin's dashboard



Vote count is shown on specific options and graphical representation of vote's shown below options.

V Conclusion

In conclusion, the implementation of an electronic voting system utilizing Blockchain technology presents a promising avenue for enhancing the integrity, transparency, and accessibility of electoral process. By leveraging the immutability and decentralization features of Blockchain, offers secure and tamper-resistant voting mechanisms, ensuring the accuracy and legitimacy of election results.

Furthermore, the adoption of electronic voting system can potentially address longstanding issues such as voter fraud, manipulation, and distrust in traditional voting systems. Through cryptographic techniques and distributed consensus mechanisms, Blockchain-based electronic voting system enhances voter trust by providing transparent and auditable records of every transaction within the voting process.

However, it's important to acknowledge that the successful implementation of electronic voting system requires careful consideration of various technical, regulatory, and social factors. Challenges such as scalability, privacy concerns, regulatory compliance, and user acceptance need to be addressed to realize the full potential of Blockchain-based electronic voting system.

VI References

- [1] Kashif Mehboob Khan, Juniad Arshad, Muhammad Mubashir Khan, et al., "Secure Digital voting system based on Blockchain Technology," International Journal of Electronic Government Research, vol. 14(1), pp. 53-62, Jan 2018.
- [2] Asraful Alam, S.M. Zia Ur Rashid, Md.Abdus Salam, Ariful Islam, et al., "Towards Blockchain-Based E-voting System", International Conference on Innovations in Science, Engineering and Technology(ICISET), pp.102, Oct 2018.
- [3] D.Dwijesh Kumar, D.V. Chadini, and Dinesh Reddy, et al., "Secure Electronic Voting using Blockchain Technology", International Journal of Smart Home, vol.14(2), pp. 31-38, 2020.
- [4] Ayed Ahmed Ben, et al., "A conceptual secure Blockchain-based electronic voting system," International Journal of Network Security & Its Applications, vol 9(3), May 2017
- [5] Chinnapong Angsuchotmetee, Pisal Setthawong, Sapjaren Udomviriyalanon, et al., "BlockVOTE: An Architecture of a Blockchain-based Electronic Voting System" University of Birmingham, 10 May 2020.
- [6] S.Aruna, M.Maheshwari, and A.Saranya, et al., "Highly Secured Blockchain Based Electronic Voting System Using SHA3 and Merkle Root", IOP Conference Series: Materials Science and Engineering, 2020
- [7] Albin Benny, Aparna Ashok Kumar, Abdul Basit, Betina Cherian, and Amol Kharat, et al., University of Mumbai, Pillai College of Engineering, Students, 11 July 2020.
- [8] J. Douceur, et al., "The Sybil Attack", International Workshop on peer to peer systems, 7 March 2002.
- [9] Aleksander Essex, et al., "Internet voting in Canada: a cyber security perspective", The centre for e-democracy, Western University Canada, 2016
- [10] M. K. Alomari, et al., "E-voting adoption in a developing country," Transforming Government: People, Process and Policy, vol. 10, no. 4, 2016
- [11] S. Nakamoto, et al., "Bitcoin: A peer-to-peer electronic cash system, bitcoin.org, 2009.
- [12] C. Meter and A. Schneider and M. Mauve, et al., "Tor is not enough: Coercion in Remote Electronic Voting Systems". arXiv preprint, Feb 2017
- [13] Vaibhav Anasune, Pradeep Choudhari, Madhura Kelapure and Pranali Shirke Prasad Halgaonkar, "Online Voting: Voting System Using B-chain", International Research Journal of Engineering and Technology(IRJET), vol 06, June 2019.
- [14] G Bhavan, i , "Survey on Blockchain Based E-Voting Recording System Design", International Journal of Innovative Research in Science, engineering and Technology, vol 7, Issue 11, Nov 2018.