# A DECENTRALIZED VOTING SYSTEM USING BLOCKCHAIN

**[1]ABITH SAM CHERIAN, [2]BRINDA A, [3]SYEDA AMTUL FIZZA, [4]VARUN R**
**[5]DR. CHANDRAMOULI H**

[1,2,3,4]Student, [5]Assistant Professor
Department of Computer Science
East Point College of Engineering and Technology
Bengaluru.

***Abstract*- The elevated utilization of information technology seems to revolutionize both the provision of governmental services and the vivacity of democracy. E-voting or Electronic voting symbolizes modern democracy. E-voting will be at its best when complied with the existing legal and regulatory framework. "Vote", the word means to determine or to elect or select from a list or who will run the country or the organization or a group. To find leaders selected by people is the prime aim of voting (Scenario: Citizens electing their country leaders). Most countries, India is no exception, have trouble voting. Some of the issues at stake are incorrect voting during elections, inexperienced personnel, inaccessible or insecure polling stations, and inadequate voting equipment. The new indigenous flagship internet-based voting system solves this exact problem. It should be noted that users, in this case, citizens, have a large time frame during the voting period with the system running. The objective of this paper is to come up with a new solution, does come with a small learning curve, citizens will have to be trained on how to exercise their right to vote online**

***Index terms:*** **Trust, voter participation, Accessibility, Privacy, Digital identity, Elections.**

## *1.I*NTRODUCTION:

E-voting is widely used in society life. But it is not obvious how to ensure the outcome is respected when the decision is financially or politically related. The correctness, security and privacy are always the most important characters. Secure e-voting is a kind of secure multi-party computation. In the voting process, a set of people make their choices and the choices of them could be kept secretly. Most of the e-voting schemes need a trusted public bulletin board to provide a consistent view to all voters. However, it is not clearly for election administrator to show the public bulletin board can be completely trusted. Some people realize blockchain can be used as the bulletin board because the content is publicly trusted.

Blockchain served as a decentralized database provides new tools for creating trustless and decentralized system. In the blockchain system, there is no trusted centralized coordinator. Instead, each node that is involved in the blockchain system holds the data block locally. Blockchain is maintained by a decentralized and open-membership peer to peer network. At first, this technology is designed for money transfer. With the development of it, researchers are trying to reuse Blockchain in other research areas such as coordinating the Internet of Things, carbon dating and health-care. This sparked the invention of Ethereum , which is well known as a milestone in the development of blockchain. It owns a Turing complete programming language and users can realize the function by the smart contract in the Ethereum network.

A decentralized voting system using blockchain technology is a voting system in which the process of casting and counting votes is accomplished using distributed ledgers and cryptography. In this system, votes are recorded and tallied on a blockchain network, which is a decentralized and distributed digital ledger. This allows for increased transparency and security in the voting process, as well as reducing the potential for fraud or manipulation. The use of blockchain also ensures that each vote is recorded only once and cannot be altered or deleted, providing a tamper-proof record of the election results.

## 2. SYSTEM ARCHITECTURE

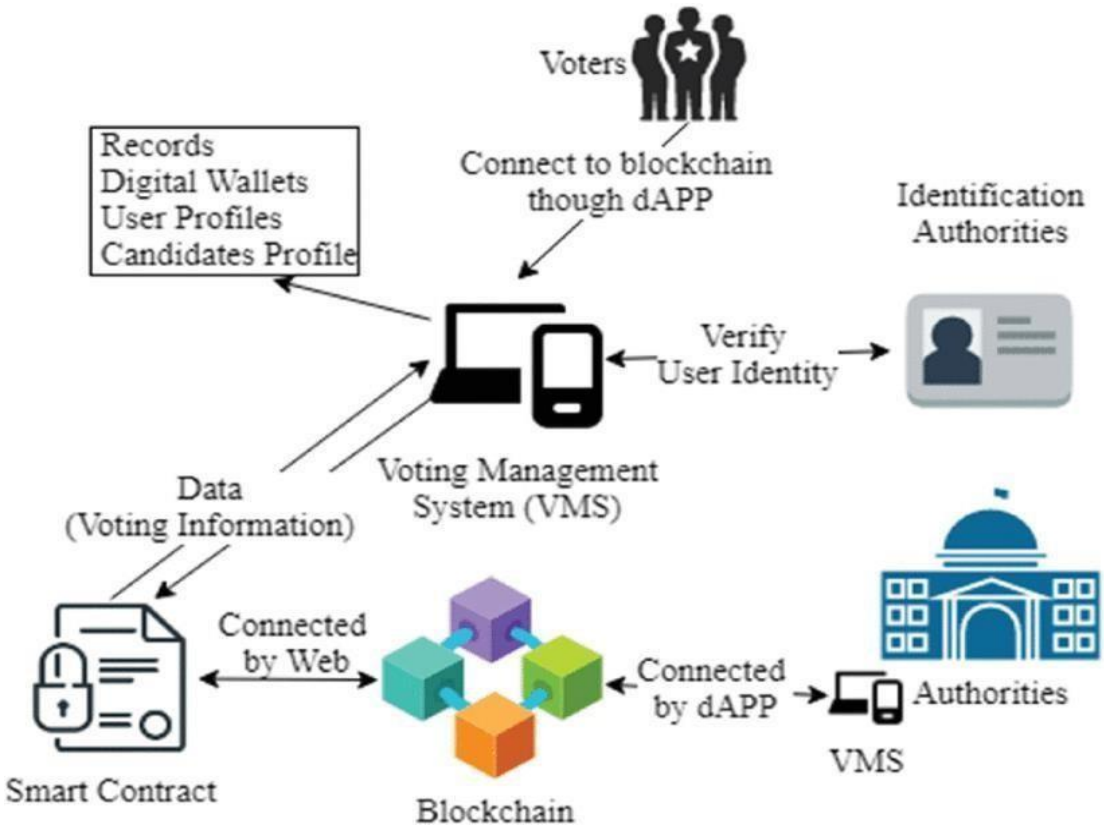



Figure1.1: VOTING SYSTEM ARCHITECTURE.

When analyzing a decentralized voting system using blockchain technology, it's important to consider the following factors:

Security: It is important to evaluate the level of security provided by the system and how it protects against potential threats such as hacking, fraud, or manipulation of the results. This includes the use of cryptographic techniques and secure voter authentication methods
Transparency: The system should allow for transparency in the voting process and the ability for all participants to view and verify the authenticity and integrity of the votes.
Accessibility: The system should be accessible to all eligible voters, regardless of location or physical ability, and should remove barriers caused by geographical locations.
Audibility: The system should provide an auditable record of the voting process and the results, which can be used to verify the outcome and detect any potential errors or fraud.

Scalability: The system should be able to handle a large number of voters and votes, and should be able to accommodate future growth as needed.

Decentralization: The system should not rely on a central point of failure and use distributed ledger technology to achieve decentralization.

Interoperability: The system should be able to interact with other systems and platforms seamlessly and can be used with other decentralized systems for more complex use cases.

Compliance: The system should comply with legal and regulatory requirements, such as data privacy and accessibility laws, to make sure it can be used in real-world elections.
It's worth noting that a decentralized voting system using Blockchain is still a new technology, and it's still facing some challenges, such as ensuring voter privacy while providing transparency. In addition, the interoperability and regulatory compliance issues can make it difficult to implement in real-world elections.

## 3. IMPLEMENTATION

The process of voting is run by maintaining our system that is backed up by the blockchain. The hashes of transaction for every voter has stored on the chain and all the results of the election are also stored on the blockchain and from there the result of the election can be viewed on the resulting dashboard of the users. The system first verifies whether the voter is the country nationality holder and It also checks whether the voter has already voted or not if he still has a vote coin, the system allows him to cast vote. After verifying the voting details i.e. voter identifier, vote, and timestamp was stored in the chain which saves vote details.
The whole process is elaborated in

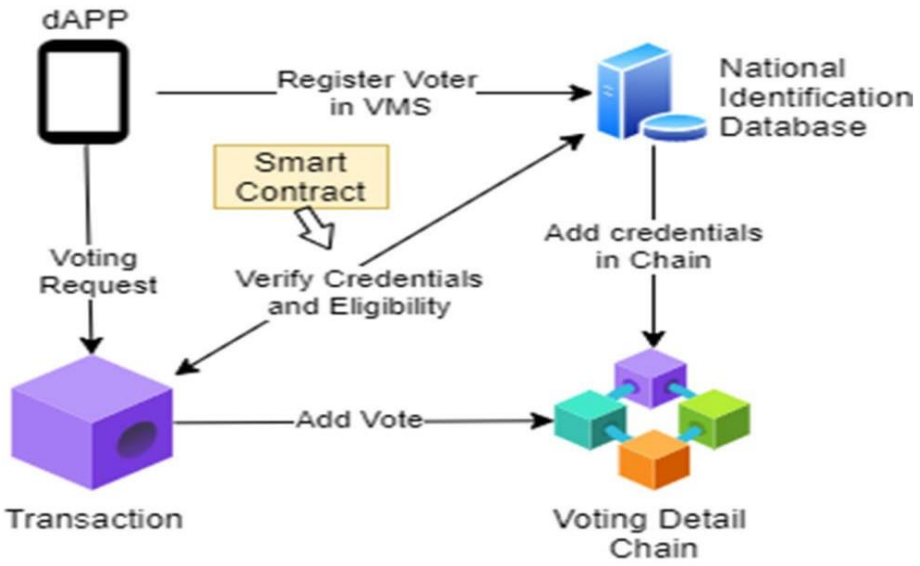



FIGURE 1.2 SMART CONTRAST USED IN THE PROPOSED VMS.

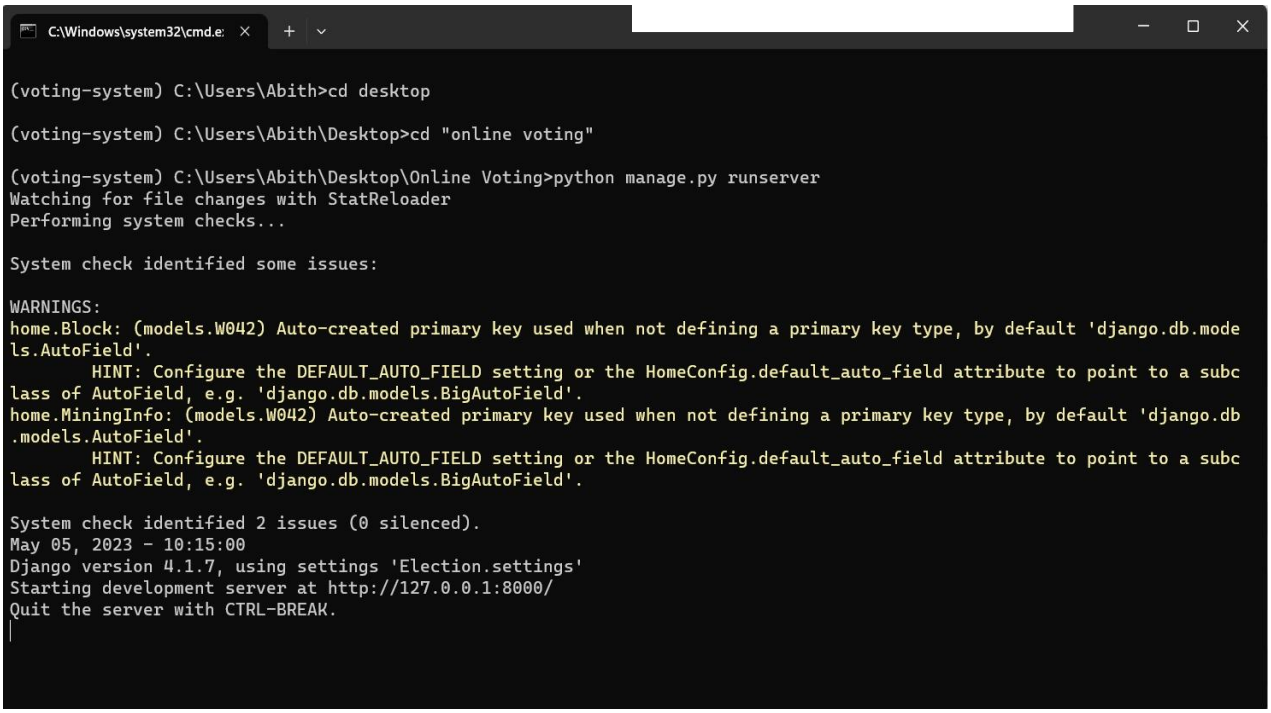
Voting Management System consists of different components discussed in this section. It has a user interface for secure interaction of voters with the system, which also includes front-end security. A dAPP interface has been implemented front end of the VMS. The dAPP is a decentralized application based on blockchain technology. It runs on a P2P blockchain network. The user identification is critical because the user enters his/her credentials on that interface, so it should be tamper-free and simple. The system provides full fair access to every voter and provides traceability after casting the vote. The voter login the system by his/her credentials. System uses the ID details of the user and verify them with the Database to register the user in the system.

The user gets a unique OTP to log in to the system. The OTP has generated each time the voter login into VMS. The purpose of using the dAPP system is to ensure the reliability of VMS; as decentralization makes processing efficient at all nodes. If one node of the system during the voting system gets vulnerable, all the other nodes are not harmed. The node which gets vulnerable is reinstate by other nodes.

Smart contracts are providing a secure connection between the user and the network while executing a transaction in the chain. These are the rules that are implemented on the entire blockchain and cannot be neglected under any condition. All the nodes have to follow the smart contracts to save the vote in the system successfully.

The first smart contract is for user verification between IA and the VMS; it uses the Can-Cast-Vote function which checks the requirements of the system to make sure the specified voter can vote. After verification, it enters the voter details record for further use. The voter is being connected with a voting smart contract that specifies which candidates

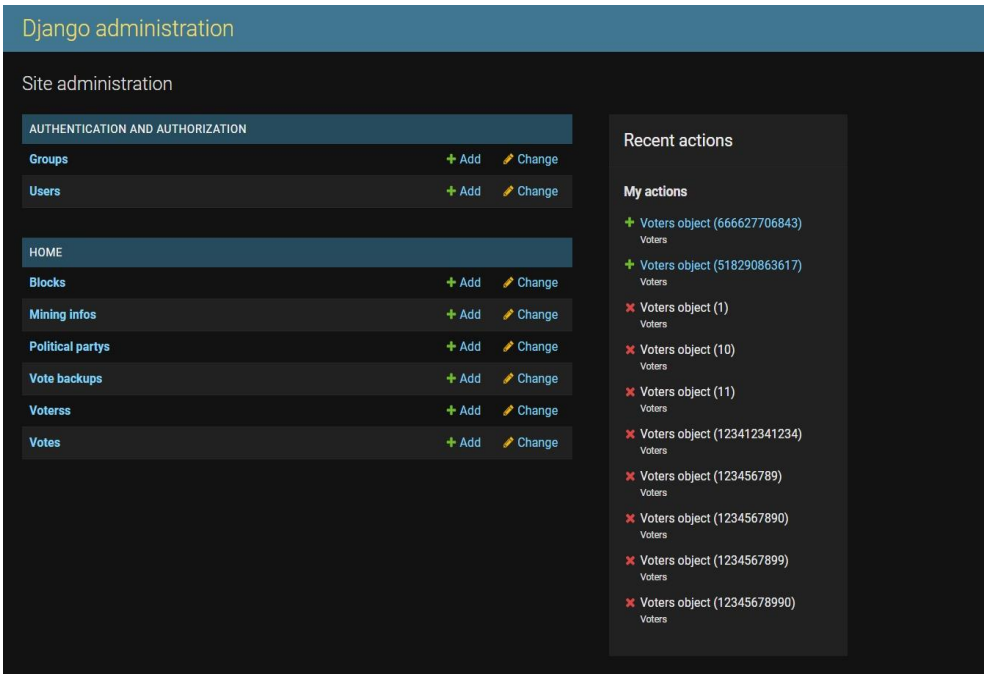
### 3.1. FETCHING THE IP ADRESS




Cryptographic hash keeps the data hidden from any intruder in the system; it has multiple benefits that include the privacy of the user's identity. Cryptographic hash uses encryption to keep the transaction secure when it is transmitted on the network to be added

to a node, only the authorized owner of the transaction can decrypt the transaction and view the content using his private key. The tracking of the user's vote is made possible by providing the voter with the address of his transaction; as soon as the vote is cast the voter is notified through SMS and email. Voters can track their vote in blockchain through the hash value of the transaction that is provided on the registered phone number. The voting data includes all the information saved while casting the vote. The data remains secured, unharmed, and hidden. The only person with the tracking information is the voter, who can view and verify his voting information. The transaction is saved in a block and locked using the public key of the voter. While tracking the vote, the node is identified by the voter's public key. The voter uses his private key to view the transaction made by his wallet. Voters can only view the vote; they can never change or delete the vote once it is cast. Any user information being transferred in a transaction is encrypted by cryptography. The process of casting vote in VMS is further elaborated in Fig. 10. It shows that while casting vote the voter adds a digital signature to the transaction. This digital signature keeps the transaction secure.

3.2.ADMIN PAGE

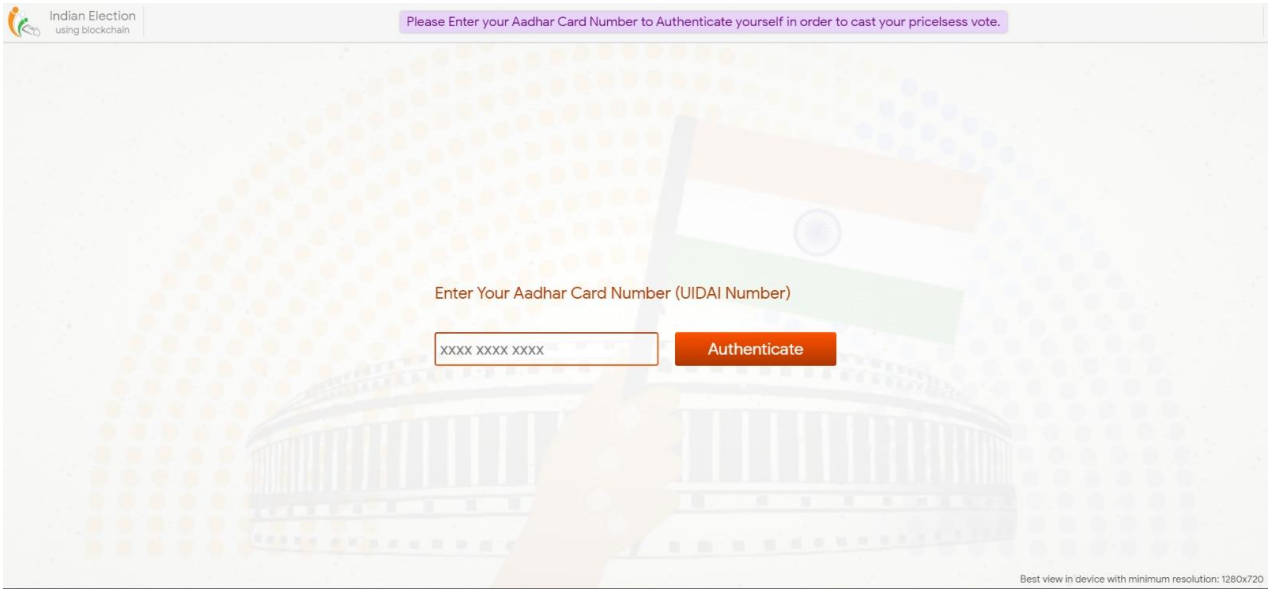


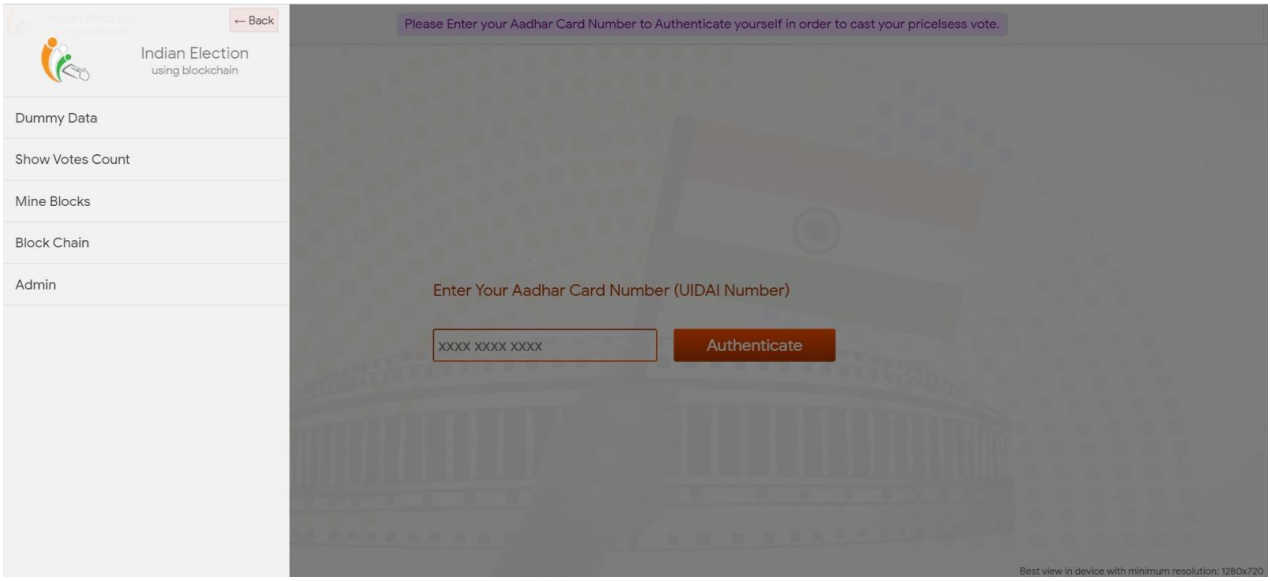

The uniqueness of users can be established by using their computerized National ID. When voters enter their details, those are then verified with the assistance of identifying authorities. This makes sure that a person's identity is not being used by another voter. By taking credentials, the authorities verify, if the person is eligible to cast a vote in the election or not and whether any transaction hash has already been assigned to his/her National ID. If voter is eligible, the s s awarded to every voter wallet. Verifying the user by this method also enables the s s imposed by the law and cast the vote. When the voter casts the vote, a transacti e voter. Furthermore, the wallet balance of voters is also updated to zero voting coin, which eliminates the possibility of doubling a vote from the same user. When a voter casts a vote, the blockchain updates and saves the vote of the voter, which means that the user is not be able to cast a vote again unless a new VC is issued.

## 4. METHODOLOGY

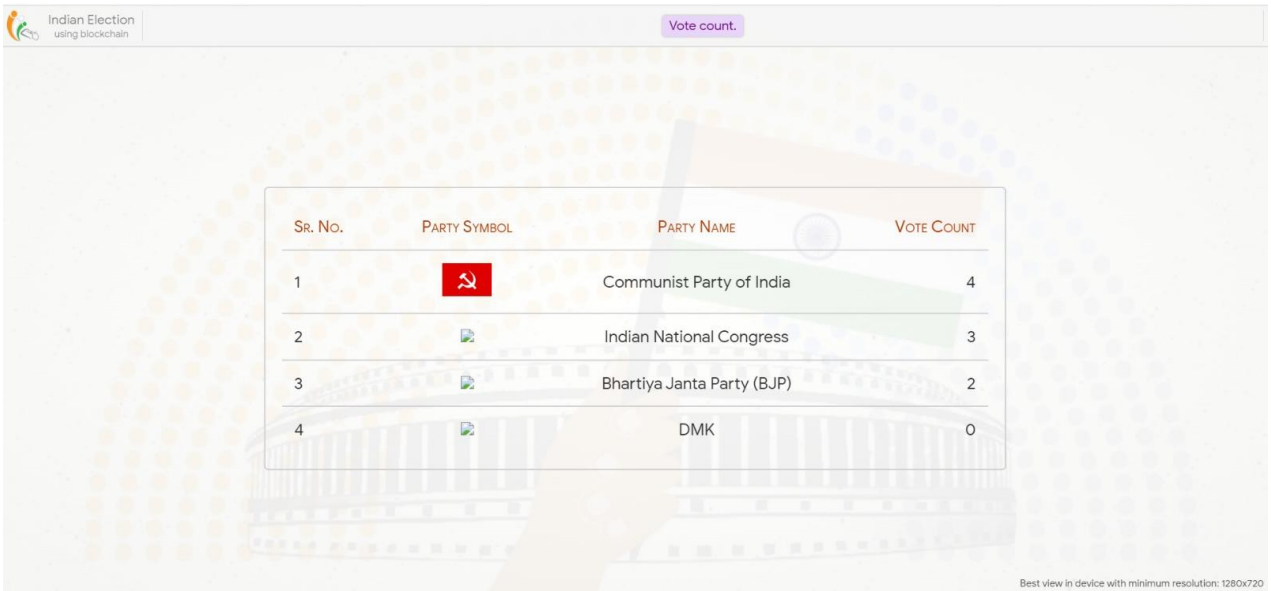
A high-level architecture of the proposed system has been presented. It shows how the main stakeholders; Voters, VMS, AA, and IA work together to perform certain voting tasks. All voters are connected to VMS directly through dAPP; it is either a mobile application or a web portal. The identification authority verifies voters registering in the system. Any voter who is verified and eligible to vote is allowed in the application to take part in voting.

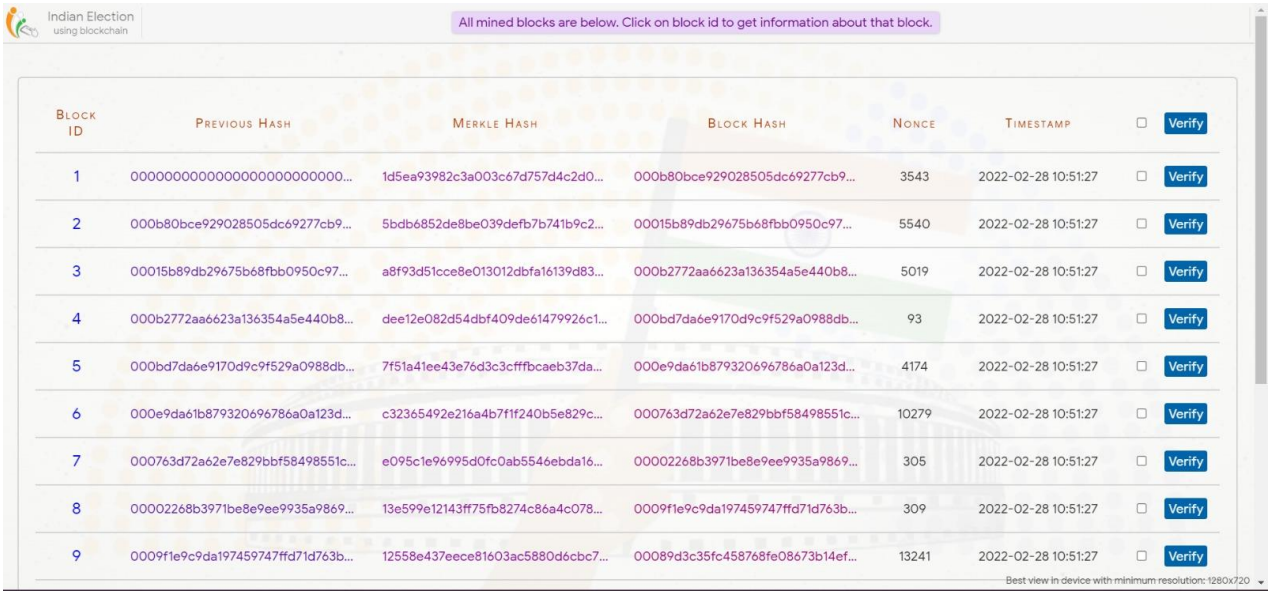
The process of the whole system includes certain parts; the first one is the user interface of the application, which also requires front-end security. It is critical because the user enters his credentials on that interface, so it should be secure and simple. The system provides full and fair access to every user during voting activity. It also provides traceability after casting of vote. The voter registers in the system by his credentials. VMS uses the ID details of voters and verifies them with online records of IA to register the voter in the system. The user receives a unique OTP to log in to the system. An OTP is generated each time the voter wants to login into VMS. All the detail of the voter is saved in VMS. After successfully registering in the system, One Voting Coin (VC) is added to the wallet of each voter. To prevent voters from voting twice, each voter is given only one VC.


Indian Election
using blockchain
Please Enter your Aadhar Card Number to Authenticate yourself in order to cast your pricelsess vote.
Enter Your Aadhar Card Number (UIDAI Number)
xxxx xxxx xxxx
Authenticate
Best view in device with minimum resolution: 1280x720


← Back
Indian Election
using blockchain
Dummy Data
Show Votes Count
Mine Blocks
Block Chain
Admin
Please Enter your Aadhar Card Number to Authenticate yourself in order to cast your pricelsess vote.
Enter Your Aadhar Card Number (UIDAI Number)
xxxx xxxx xxxx
Authenticate
Best view in device with minimum resolution: 1280x720

**1.**


Indian Election
using blockchain
Vote count.
Sr. No.
Party Symbol
Party Name
Vote Count
1
Communist Party of India
4
2
Indian National Congress
3
3
Bhartiya Janta Party (BJP)
2
4
DMK
0
Best view in device with minimum resolution: 1280x720

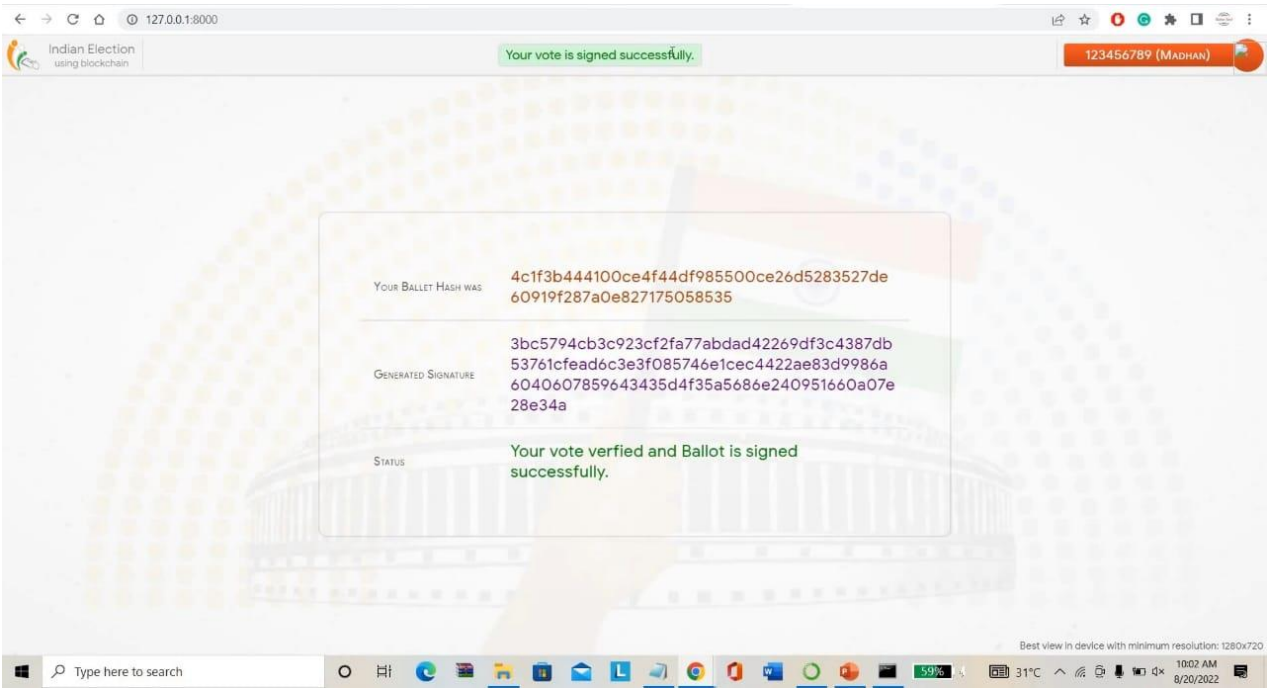



For4mulates DDoS detection as a sequence classification problem and uses RNN (LSTM, BiLSTM) and fully connected layers. show that models redu 1 to conventional machine learning approaches. ɔ increase the diversity system settings to test our model's robustness in different environments. 1ne comparison will also include otner snallow macnine learning models.

**REFERENCES:**

[1] V. D. Gligor, "A note on denial-of-service in operating systems," IEEE Transactions on Software Engineering, vol. 10, no. 3, pp. 320–324, 1984.
555FGHB2]

**5. RESULTS:**




**6. CONCLUSION:**

The purpose of proposing a blockchain-based solution for the voting system was to build trust between government and voters to make-believe that their voting integrity is kept safe. The blockchain-based voting is also make the voting process transparent and trustworthy. The amount of money spent on voting activity in any country is very high for the traditional voting system, whereas the proposed solution for using the blockchain voting systems to make the voting process cheaper, faster and trustworthy. It helps to enhance people's relations with their democratic state, as they get a transparent system on which they can rely and trust. The framework elaborates on the feature, services and role of official authorities using blockchain in the voting system which is highly in need to improve the level of the electoral system and its reliability, traceability and trust. The verification of each vote makes it

immutable. The use of hash assures the privacy of voters and the concept of public and private keys allows the authorities to control the process precisely. The traceability of the voting system assists in preventing hackers from modifying or viewing the voting information. It assures that one voter only votes one vote. The usability of this system performs well by using the more effective approach of implementing a flexible consensus algorithm to reduce extensive computing resources in the blockchain. This transparent behavior of the system tends to be promising for voters to rely and trust. The Chain Security Algorithm is also added, which automatically verifies the validity of the chain each time a new block is added to it. Smart Contracts play an important role to prevent any incomplete and malicious transactions in the blockchain voting system.

The proposed system is a secure, transparent, and reliable platform for the authorities, and voters. The proposed framework has a promising output based on the performance evaluation of blockchain technology in VMS. The experiment shows that the system keeps processing efficiently while processing a large number of transactions in the blockchain.

**REFERENCES:**


1. Raghav Chhabra, Uday Vohra, Vishrant Khanna, Aditya Verman, Poonam Tanwar, Brijesh Kumar, The Next Gen Election: Design and Development of E-Voting Web Application, Issue 10-12 June 2020, IEEE
2. Mrunal Annadate, Online Voting System Using Biometric Verification, Issue April 2017, ResearchGate
3. C. K. Adiputra, R. Hjort and H. Sato, "A proposal of blockchain-based electronic voting system", Proc. 2nd World Conf. Smart Trends Syst. Secur. Sustainability (WorldS), pp. 2227, Oct. 2018.
4. G. Rathee, R. Iqbal, O. Waqar and A. K. Bashir, "On the design and implementation of a blockchain enabled E-Voting application within IoT-oriented smart cities", IEEE Access, vol. 9, pp. 34165-34176, 2021.
5. D. Chaum, A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. Sherman, et al., "E-voting 40 scantegrity: End-to-end voter-verifiable optical-scan voting", IEEE Secur. Privacy, vol. 6, no. 3, pp. 40-46, May 2008, [online] Available: https://www.computer.org/security/. [6] G. H. Baker, "A vulnerability assessment methodology for critical infrastructure sites," in DHS symposium: R and D partnerships in homeland security, 2005.