E-Voting System Using Block Chain

Aashay Motiwala[1]*, Parshva Timbadia[2], Teerth Upadhyay[3], Pankaj Kunekar[4]

[1,2,3]Student of Information Technology , Atharva College of Engineering,Mumbai University, India.
[4]Faculty of Information Technology , Atharva College of Engineering,Mumbai University, India.

Publication Info

Article history:
Received : 19 February 2019
Accepted : 26 May 2019

Keywords:
Blockchain, e-voting, Opencv

Corresponding author:
Aashay Motiwala
e-mail: *ashaymotiwala@gmail.com*

Abstract

In this paper, we have proposed a method where the users input is considered as a part of a vote. We are using block chain technology, the most secure technology which enables us to transfer data between two nodes, without manipulation from any untrusted sources. In our project, there are two peers, namely the voter and candidate for whom the voter casts a vote for. By casting votes as transactions, we can create a block-chain that keeps track of the tallies of the votes in the database which has restricted access. In this way, everyone can agree on the final count of the votes. In our project, we have used OpenCv, which uses image processing capturing pictures for facial recognition. There is also an involvement of trusted third parties.

1. INTRODUCTION

Block-chain is a peer-to-peer version which allows e-commerce payments, the building of smart cities, data sharing, copyright and royalty protection, etc. It is a decentralized system where there is no central node or server. We have built an e-voting system to overcome the problems such as low voter turnout in several states/ areas. To address this problem we have designed a voting system where every person could vote by simply logging online either through their mobile phones or their nearest available computer. Block-chain technology when being used with the e-voting system makes the voting process more secure and reliable. The traditional voting system leads to many frauds and forgery. The E-voting system overcomes all the problems that we face in the traditional system. In information security study the online voting system is viewed as an interesting subject. The electronic voting system provides the people to elect their preferred candidate and express their opinions on how they are to be governed[1]. The security community has declared the electronic machines as a flawed system based primarily on physical safety concerns. The machine can be scuppered by someone who has physical grant to the system and therefore affects all votes casted. A block- is a public ledger that is distributed, irreversible, incontrovertible[2]. Block-Chain is assisted by a distributed network and consists of several interconnected nodes. All the nodes in the network has its own copy of the distributed ledger which holds the comprehensive history of all transactions processed by the network. The acceptance of transactions is decided by the taking mutual decision of all the nodes present in the next and hence the larger the network, the stronger the chain becomes. This network allows users to remain anonymous [3].

2. LITERATURE SURVEY

In paper [1] “Online Voting System for India Based on AADHAAR ID” by Himanshu Agarwal, G.N. Pandey has described a model for an electronic voting system has been identified as much more reliable and effective than the conventional voting system. With this system we can prevent votes being manipulated and results being delayed. Identity Aadhar is the main subject of the showcased program. They have tried in this paper to create a safe online voting system, free of security breaches. The server aspects of the proposed framework have such authority distribution which would prevent the server from manipulating the votes. This new voting system can be considered much more reliable and transparent when being compared to the traditional voting system.

In paper [2] “block-chain-Based E-Voting System” by Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson have implemented a specific, block-chain-based voting system which helps to maintain the privacy of the user or the voter by making the use of smart contracts, also at the same time making sure it is safe and cost-efficient. The sole purpose of the paper was to illustrate how the block-chain technology can provide a new opportunity for democratic countries by making the use of computers which can provide enhanced security and at the same time something which is more transparent and budget-friendly as compared to pen and paper election processes. This system makes sure the vote from the voter gets counted from the correct district, even though the vote is submitted at any given district of their choice.

In paper [3] "ELECTRONIC VOTING SYSTEM USING BLOCK-CHAIN" by Raghavendra Ganji, Yatish BN, they have introduced a multi-chain, electronic voting method. They have shown the way to configure multi-chain to limit their transactions between voter and contestant to only one vote. A new, reliable third party agency TTP has been launched. TTP retains secrecy throughout the voting process. If this particular setup was missing, it would have been impossible to preserve privacy among voters and who the voters vote for. It sometimes happens that the Election Commission or the trusted part manipulate the data collected from the user. Saying so, this system helps to prevent data manipulation and forgery even from them. Ultimately, it was shown how auditing would guarantee integrity of the entire program.

In paper[4], "BLOCK-CHAIN- A PEER TO PEER CASH SYSTEM" by Santoshi Nakamoto, they have tackled the problem of double-spending required on third party authorization providers. In this paper they have proposed a method of which makes use of 'proof of work'. Proof of work means encoding the entire chain with hash and then adding any new transactions to the original chain such that the hash of the change changes every time it updates the chain. Because of this it becomes practically impossible for the attacker to penetrate and manipulate the created block chain. This solves the problem of double-spending.

In paper[5] "E-Voting with block-chain: An E-Voting Protocol with Decentralisation and Voter Privacy'' by Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis claimed that electronic voting can be helpful in luring the young generations and techies to cast a vote for the democratic nation and also increase their interests in political matter, thereby voting the perfect leader for the nation. However, the paper discusses several flaws of the e-voting system like lack of privacy and data stealing or manipulation from an untrusted source. To solve the above issue they also propose a mechanism(block-chain technology) to prevent these flaws and still stick to electronic voting. This paper showcased how to implement the decentralized network effectively and at the same time maintain the transactions among different voting booths. Their proposed system also makes the use of hash technology to prevent data manipulation and indeed maintain the data integrity.

3. PROPOSED SYSTEM

Our proposed system includes the following modules.

3.1. Nodes

Node is nothing but the entities present in the system. Here we will consider different polling booths as the nodes in our network. When the voters visit the polling booth and cast for a vote. The additional vote gets reflected into each and every system, as the vote gets stored into a distributed network.

3.2. Data Structure

3.2.1. Unique ID/(Aadhar Number):

Each voter will have a unique identity number or Aadhar number(Authentic Proof by the Government of India) which will be used to allow the user to login after successful registration and cast a vote.

3.2.2. Block Structure:

Block Structure for our system is described in the Fig

A block structure used in our proposed system contains components such as given below:

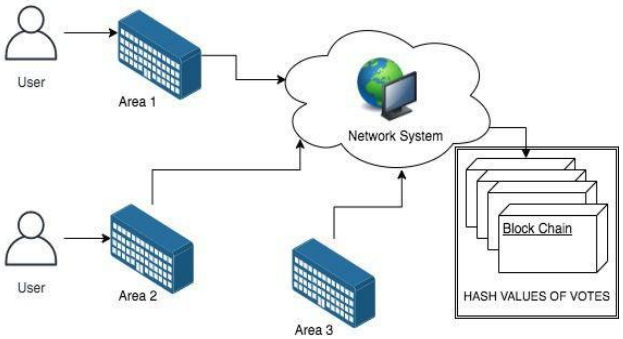

Figure 1: Our Proposed System

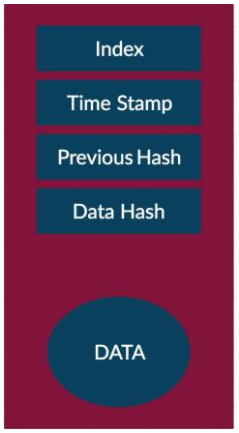

Figure 2: Block Structure

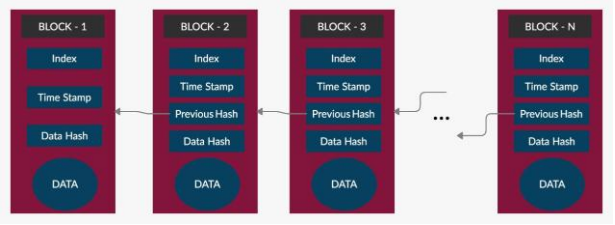

Figure 3: Block-Chain Structure

 2010-2019 S-JPSET : Vol. 11, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

- Indexing helps to keep the track of the number of blocks created.
- Timestamp which gives the amount a time required for the creation of the block.
- It contains the Data, which in our case includes the name of the voter, Unique Identity Number, and the vote given to the prefered candidate.
- Hash of the entire block, which changes if there is any manipulation made in the data.
- The hash value of the previous block gets stored into the PreviousHash and this helps to keep maintain the chain. If there are any changes made in the hash value the entire chain breaks.

3.2.3. BlockChain Structure:

Entire Block-chian of our proposed system can be represented as above and there are also some terms that should be noted, which are as follows:

- The block with Index 0 is nothing but the very first block called, the Genesis Block.
- Previous DataHash is pointed by the next block's hash pointer.
- Data integrity is maintained by comparing the DataHash and PreviousHash.

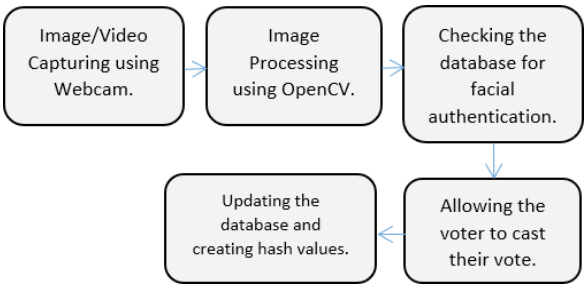

Figure 4: Block Diagram

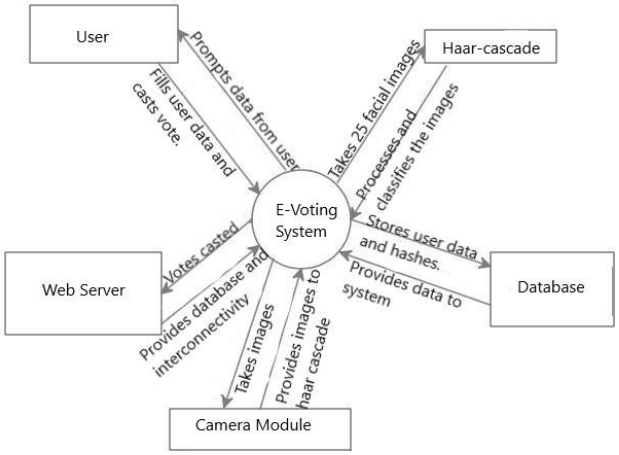

Figure 5: UML Diagram

- On creation of the new block the system recalculates to search for the last block. So that when a new block is introduced in the system it can point to the very last block.

3.3. Block Diagram

The block diagram shown above explains the flow of the process of how our system works. User's image is first captured in the form of frames by the webcam which sends it to OpenCV which processes the image and returns the coordinates of the object. The next time when the voter visits his/her image would have already been stored in the database. Using this stored image in the database we will

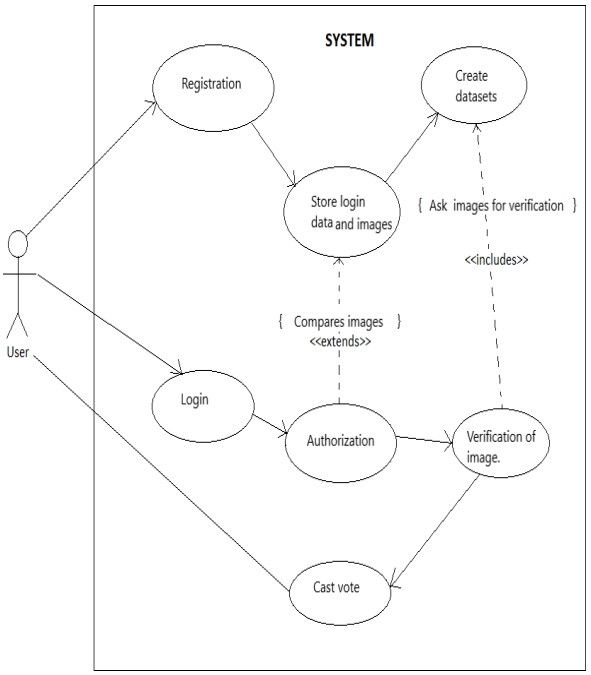

Figure 6: Use Case Diagram

```
def vote(self):
    conn = sqlite3.connect("db.db")
    cursor = conn.execute("SELECT ID, HASHBLOCK FROM VOTETABLE")
    conn.commit()
    for row in cursor:
        id = row[0]
        previous_block = row[1]

# Creating new block and hashing it
hash_block = str(previous_block) + str(id + 1)
hash_object = hashlib.md5(hash_block.encode()).hexdigest()

conn = sqlite3.connect("db.db")

# Storing new block
conn.execute("INSERT INTO VOTETABLE (HASHBLOCK,PREVIOUSBLOCK,VOTE,AADHAR) VALUES (?,?,?,?)",
    (str(hash_object), str(previous_block), self.comboBox.currentIndex(), "123456789"))
conn.commit()
self.openWindow()
QtWidgets.QMessageBox.information(MainWindow, "Message", "Vote Casted")
```

Figure 7: Code Snippet Showing DB Connection and applying Hash Function

2010-2019 S-JPSET : Vol. 11, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)

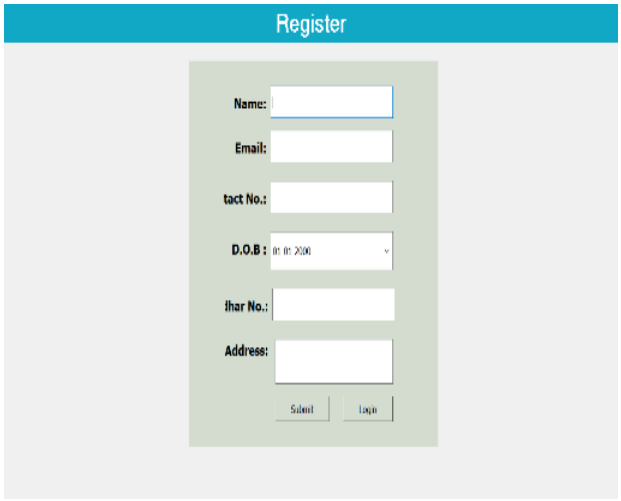

Figure 8: Registration Module

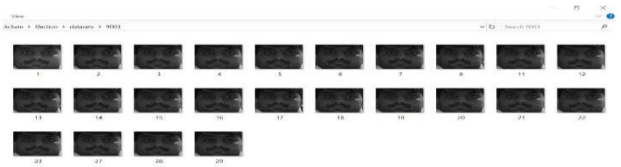

Figure 9: Illustration of how facial images are captured

Figure 10: Login Module

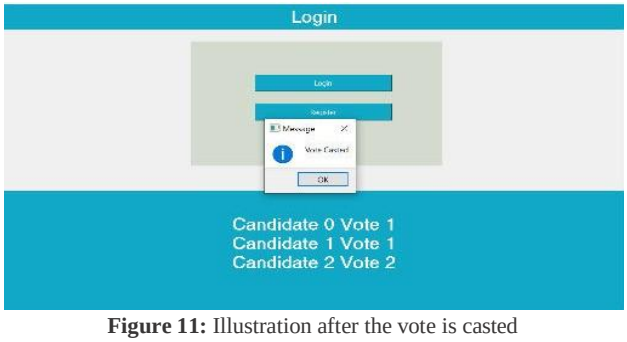

Figure 11: Illustration after the vote is casted

verify the user and allow him/her to call for a vote. This vote will be stored in each database using the block chain technology which is immutable due to 'proof of work' with the other system's database. The larger the network, the stronger and robust it becomes against the attacker.

3.4. Use Case

Here the use case diagram is quite self explanatory.

It is basically collecting the input data from the user during the registration time and further using that data for verifying the user during the voting data. On successful verification the user will be permitted to the voting module where they can cast a vote for their preferred candidate. It also illustrates all the modules used in our proposed project and connection done between them.

3.5. Code Snippet

We have incorporated the 'SHA' algorithm to create hash value using the 'hashlib' library.

In the above fig., we are appending an hash value to the previous block stored in the database and then updating the database.

In this function 'hash_block.encode().hexdigest()' generates a 32 bit hash value which is stored in the blockchain which can not be manipulated.

4. EXPERIMENTAL RESULTS AND DISCUSSION

This is the registration module of our proposed system. Here the voter has to provide the basic information related to his/her identity and the information will be stored. Further, this module also takes in the picture of the voter for enhanced security.

Next time the user visits during the voting day. He/She would be directly routed to the login page where they can cast for vote. During the login module, the user has to provide with the unique identity detail which was entered previously at the time of registration. Apart from that, the system will also check the authenticity of the user using the facial detection, Machine Learning feature. So basically the system provides a 2 step verification process.

Once the user is able to login successfully, he/she can cast a vote for their preferred candidate. As we are using Blockchain technology we don't have access to the database. So for our system, that is for Admin, we have displayed below to whom the voter caste the vote for. Note: It is only used to check the correctness of the code.

5. CONCLUSION

Our proposed system is an e-voting system which uses blockchain for security and confidentiality. In our project we have shown how blockchain can be configured in the field of Voting to grant a safer system than the others. A new entity called as TRUSTED THIRD PARTY is introduced inorder to keep the voting private. With the help of our system, it is possible to maintain the identity of the voter a secret.

6. REFERENCES

[1] Agarwal, H., & Pandey, G. (2013). Online voting system for India based on Aadhar ID. *IEEE*.

[2] Ganji, R., & BN, Y. (2018). ELECTRONIC VOTING SYSTEM USING BLOCKCHAIN. *DELL EMC*.

[3] Satish Kumar Nalluri, Venkata Krishna Bharadwaj Parasaram, Varun Teja Bathini. (2020). Secure Automation Frameworks for Smart Manufacturing Using Blockchain-Assisted Traceability. International Journal of Research & Technology, 8(2), 47–53. Retrieved from https://ijrt.org/j/article/view/879

[4] Hardwick, F., Gioulis, A., Akram, R. N., & Markantonakis, K. (2019). E-Voting with blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. *IEEE*.

[5] Hjálmarsson, F. Þ., & Hreiðarsson, G. K. (2018). "Blockchain-Based E-Voting System". *IEEE*.

[6] Nakamoto, S. (2009). "Bitcoin- A PEER TO PEER CASH SYSTEM. *bitcoin.org*.

2010-2019 S-JPSET : Vol. 11, Issue Supplementary-1, ISSN : 2229-7111 (Print) and ISSN : 2454-5767 (Online)