Block Chain Based Cloud Computing Model on EVM Transactions for Secure Voting

Sathya V[*], Arpan Sarkar[1], Aritra Paul[2], Sanchay Mishra[3]
[*]Assistant Professor, M E
[*123]Dept. of Computer Science
[123]SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu – IN 600089
Email: sathyakavi17@gmail.com, sarkararpan28@gmail.com[1], aritra9698@gmail.com[2], sanchaym811@gmail.com[3]

Abstract--- Voting is a tedious task in this nation. The highest amount of controversies and corruptions are involved along this path. A nation needs a fair and unbiased election for the masses to redeem their right to elect the leader of their choice. The latest trends of EVM (Electronic Voting Machine) hacking has taken over the ability to hold a clear and transparent election. In this paper, we discuss an innovative approach by imbibing the latest technologies with the traditional voting methods. The technology involves a secure data storage technique named as block chain which is used for cryptocurrencies and is proven [7] for its security. The votes which are recorded by the EVM will be updated with the cloud-based storage (SAAS). Any changes made to the voting panel or tampering with the votes will cause the hash to break the link and by detecting the manipulated votes, any discrepancy can be removed by marking them as NOTA, hence not affecting the polling by any means. Blockchain technology has a significant feature of Proof-of-Work which does not allow the continuous creation of data blocks hence protecting the rapid manipulation of data. Also, this system only requires uploading the hashes created along with the blocks which are stored in a hash table [12] on the cloud. The data of the EVM, when tallied with the hash table, can help in identifying the point of manipulation. Moreover, the areas with no broadband internet connection can also implement these techniques as it required only a few kilobytes of upload data rate to update the hash values. The already existing UIDAI based biometric system already adds an extra layer of security to the voting system. Each vote will be treated as a single block of data. Also, as added features of block chain technology, the P2P (Peer to Peer) network allows only communication between two already connected peers. Man-in-Middle attacks are impossible in this case as the blockchain proof-of-work does not allow mass updating of data at a time, hence reducing the rate at which votes can be manipulated, hence securing a country's political future.

Keywords--- *Blockchain Technology, Cloud computing, EVM, UIDAI, SAAS, Proof-of-Work, Election, Voting Machine.*

I. INTRODUCTION

Voting in this country is the most tedious job to be handled, involving all kinds of corrupted and illegal deeds. Elections in India are conducted exclusively using EVM's developed over the past two decades by a group of government-owned companies. These devices, known in India as EVMs, have been adopted greatly for their simple design, ease of conduct, and robustness. However, recently they have also been marked prey following widespread reports of election irregularities. Despite this criticism, many details of the mechanism have never been publicly discussed, and they have not been subjected to a stringent, independent security evaluation. We conclude that in spite of the machines' simplicity and [8] software trusted computing base, they are vulnerable to indigenous attacks that can modify election results and violate the law of the election commission. Most of the attacks done are physical, by changing the electricals, but if the machine is connected real time to a cloud server and involves an independent screen which shows the confirmation of choice symbolically before placing the final vote, it can help in detecting problems and maintain the integrity of the system. Blockchain technology [3] has primarily been used to store data and the major advantage of this technology is the inertia of the data. This technology was initially implemented by Satoshi Nakamoto [1] in 2008 to imbibe the concept of cryptocurrency (or) bitcoins as a medium of secure electronic exchange of money. According to this technology the data once stored, a hash is generated, the following block stores this hash so as to form a chain of links between the data blocks. The hash generated is calculated from the data and any change in data causes the hash to change. The Proof-of-Work technology which is a part of the Blockchain technology, helps in preventing the modification of data by limiting the hashing rate. Hence, only a certain limited number of blocks can be created or modified at a time, hence lowering the chances of corruption. Moreover, the hashing in this case requires to be done at every peer node individually to be accepted by all the peers else it is rejected.

978-1-5386-7808-4/19/$31.00 ©2019 IEEE

II. RELATED WORKS

1. Satoshi Nakamoto explained how Blockchains [1], could be used for secure transfer of data in between transactions for a new method for currency transfer but it is not good enough for other applications.
2. Yuan Yuan and his team [2] explained how Blockchain can help in an online voting system but doesn't explain implementation.
3. Arya Sahadevan and team [6] mentioned an IOT based approach for real time tackling of corruption at polling booths.
4. Yiderendra Kumar Yadav et. Al [11] mentioned an integrated and secure way to use biometrics to pulverise booths and affirming the voter but grieves potential.
5. Hui Yang [5] and team showed a way for future improvements in the 5G network wind. The fibre optics-based connection would help in zero latency upload and download of data for immediate action.

III. TECHNIQUES AND ALGORITHMS

The given system uses a secure data storage system called as block chain technology. It involves storing data into blocks and securing them with a hash. Our proposed system involved storing the ballot information as a block for each and every voter and transfer the hash over internet to cloud based storages, which when tallied with the EVM can discretely identify the manipulated votes.

A. Voting Algorithm (Proposed)

Step 1: Collect the ballot information from the EVM and send it to Blockchain generator.

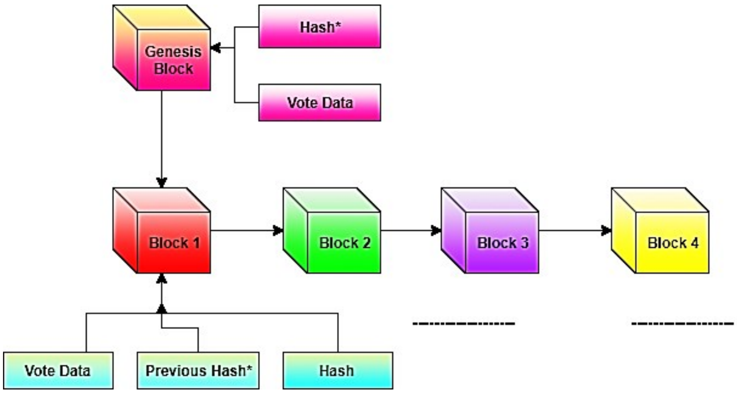
Step 2: Blockchain generator generates the blocks with data and hashes as well as connects to the previous hash.

Step 3: Hash value is sent to the cloud service for remote transfer using low bandwidth internet.

Step 4: The receiver station receives the data as Publish-Subscribe model and stores it in a hash table.

Step 5: The hash of the blocks is compared with the hash table, if any discrepancies are found, it is rejected and marked as NOTA.

Fig. 1 Block Chain Schema



```
Algorithm Secure_Vote

Input: Ballot_info
Output: Hash

While true
Loop
Hash=Hash (Ballot)
If (Hash= =NULL)
Then
Break
Else
Create_block(hash)
End if
End loop
```

B. Code Snippet (Python 3.x)

The above diagram [Fig.1] shows how the ballot information can be encrypted and stored in a hash table on the cloud, which is updated after every entry. Any changes made to the information on the EVM changes the hashes, hence discreetly identifying the faulty blocks.

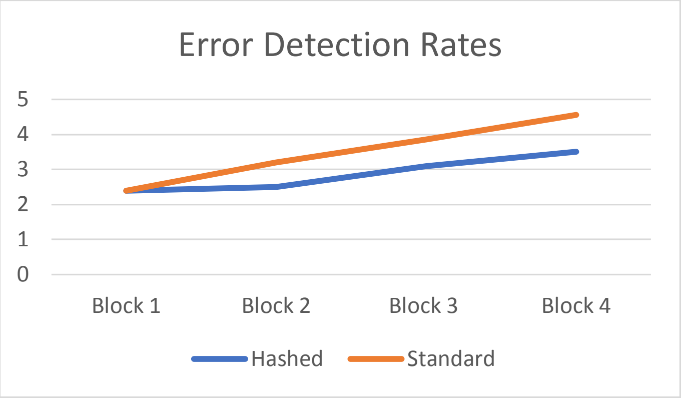


Fig. 2 Error Production Rates (in ms)

IV. BLOCKCHAIN BASED VOTING SCHEMA

The innovative voting systems consists of four parts:

1. EVM
2. Block Chain Software
3. Cloud Storage
4. Receiver Station

The polling booth has a direct uplink with the cloud service and it continuously uploads data to server using a low bandwidth connection. The data that is sent is the hash which is 16 bits long. It might be numeric or alpha numeric depending upon the algorithm used. SHA1, SHA256, md5 can be used for based comparison.

The receiving end also has a system set up which consists of the hash table. The data stored on the cloud server is continuously read by the system and stored on the table. The hash then is compared on the day of vote counting, with the ones in the EVM. If they match the votes are calculated else, they are marked as NOTA such as to favour no particular political party.

1. EVM:

Also known as the electronic voting machine, stores the vote entered by a voter in a secure latch-based storage system.

2. Block Chain Software:

Initially developed for cryptocurrency, but soon has gained popularity for its security features.

```
import uuid
import hashlib

def  hash_password (password):
    # uuid is used to generate a random number
    salt = uuid.uuid4().hex
    return hashlib.sha256 (salt.encode() +
password.encode()).hexdigest() + ':' + salt
    # random number is concatenated for added security
def check_password (hashed_password,
user_password):

    password, salt = hashed_password.split(':')
    return  password  ==  hashlib.sha256(salt.encode()  +
user_password.encode()).hexdigest()
```

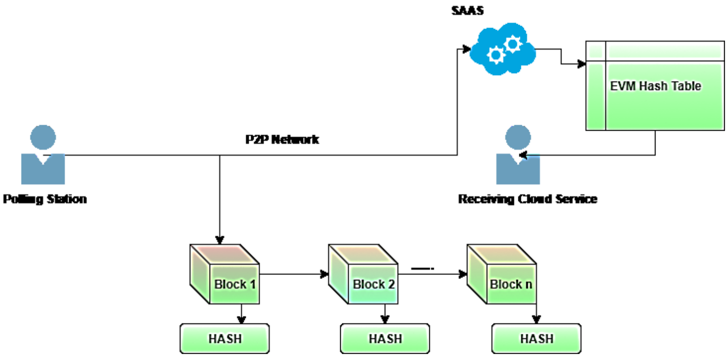


Fig. 3 Blockchain Schema

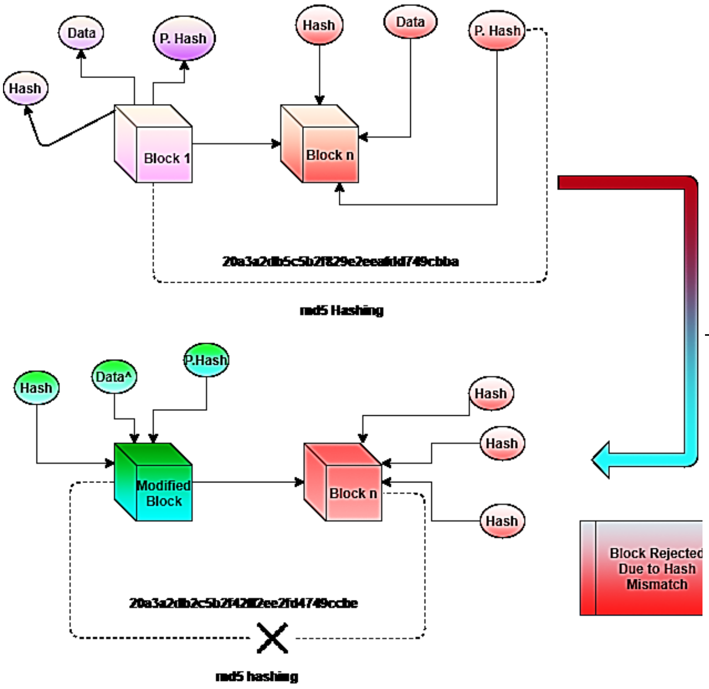
3. Cloud Storage:

Cloud storage service offered by Google or Amazon are fast enough to store data at the required rate.

4. **Receiver Station:**

A general server or a computer which can fetch data from the cloud and store it in a data structure like a table or a database.

Fig. 4 Tampered Block Example



The above diagram [Fig.4] shows the effect of tampering with the data on the block. The Purple block is the initial data which is chained to the red block. Later by some means the purple block is manipulated, represented here by green. The hash linked to the block changes as well as the link from the red block to the green block breaks as it is not the same. At this point we can identify the manipulation and mark the vote as NOTA. The received data can also be classified as private block chain as it involves P2P connections. Any possibilities for man in the middle attacks are ruled out as the system id for the Peer will be the same as the receiving Peer. Any other Peers need the same system id to receive the blocks and to decode them. Also, the hashes will not be the same at different Peers.

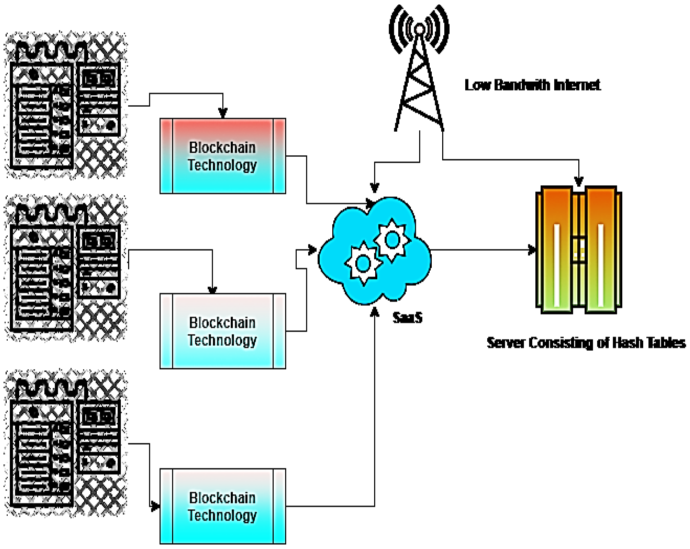


Fig. 5 Voting System Implementation

Also, further down the line, UIDAI based Aadhar numbers/ VID can also be hashed along with the voter's choice to identify each and every vote uniquely. This can help in further improving redundancy rather than the current inking systems used.

The cloud can be connected to a database on the server as it has to store large amounts of data in case of a national level polling. The proposed python code for cloud implementation is given below:

```
import mysql.connector

mydb = mysql.connector.connect
(
  host="localhost",
  user="yourusername",
  passwd="yourpassword",
  database="mydatabase"
)

mycursor = mydb.cursor()

mycursor.execute("CREATE TABLE customers
(name VARCHAR(255), address
VARCHAR(255))" #this consists the SQL
statement
```

V. CONCLUSION

The current system used for voting has been blindly trusted to be the best, but has no transparency and hence easily hackable. This increases the chances of corruption and immorality which leads to an unstable government and unhappy public. Implementing cloud-based solutions as well as blockchain for security will improvise on the transparency for the critics and also improve the security on the ballot information that is collected. Hence, the paper successfully demonstrates a way to improvise the political future in the country especially India.

VI. FUTURE ENHANCEMENTS

- Better networks can be used for faster storing and avoiding further network vulnerabilities.
- Cryptocurrency security is increasing day by day and hence improved security qualities will enhance the system.
- EVM(s) can be equipped with a screen to confirm the vote symbolically. As a large mass of voters are uneducated, double tap system should be implemented, where first press requires a second confirmation after the party is symbolically confirmed on the screen.

REFERENCES

[1] Satoshi Nakamoto,"Bitcoin: A Peer-to-Peer Electronic Cash System"

[2] Yuan Yuan, Yanyan Hu, Shaohua Huang, Shengjiao Cao, Anuj Chopra,"A Privacy-Preserving Voting Protocol on Blockchain", 2018 IEEE 11th International Conference on Cloud Computing

[3] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, Gísli Hjálmtýsson ,"Blockchain-Based E-Voting System", 2018 IEEE 11th International Conference on Cloud Computing

[4] Dina MOLOJA, Noluntu MPEKOA,"Securing M-voting Using Cloud Intrusion Detection and Prevention System: A New Dawn", ST-Africa 2017 Conference Proceedings

[5] Hui Yang, Haowei Zheng, Jie Zhang, Yizhen Wu, Young Lee, Yuefeng Ji,"Blockchain-based Trusted Authentication in Cloud Radio over Fiber Network for 5G", 2017 16th International Conference on Optical Communications and Networks (ICOCN)

[6] Arya Sahadevan, Deepa Mathew, Jairam Mookatana, and Bijoy A. Jose,"An Offline Online Strategy for IoT using MQTT", 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing

[7] Shifa Manaruliesya Anggriane, Surya Michrandi Nasution, Fairuz Azmi,"Advanced E-Voting System Using Paillier Homomorphic Encryption Algorithm", 2016 International Conference on Informatics and Computing (ICIC)

[8] Mark A. Will, Brandon Nicholson, Marc Tiehuis and Ryan K L Ko,"Secure Voting in the Cloud using Homomorphic Encryption and Mobile Agents", 2015 International Conference on Cloud Computing Research and Innovation

[9] Quentin MONNET, Youcef HAMMAL, Lynda MOKDAD, Jalel BEN-OTHMAN,"Fair Election of Monitoring Nodes in WSNs"

[10] Haijun Pan, Edwin Hou, Senior Member, and Nirwan Ansari, Fellow,"M-NOTE: A Multi-part Ballot based E-voting System with Clash Attack Protection", IEEE ICC 2015 - Communication and Information Systems Security Symposium

[11] Yirendra Kumar Yadav, Saumya Batham, Mradul Jain, Shivani Sharma,"An Approach to Electronic Voting System using UIDAI", 2014 International Conference on Electronics and Communication Systems (ICECS -2014), Feb. 13 -14, 2014, Coimbatore, INDIA

[12] Friðrik Þ. Hjálmarsson , Gunnlaugur K. Hreiðarsson . Mohammad Hamdaqa , Gísli Hjálmtýsson. "Blockchain-Based E-Voting System", 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2-7 July 2018, San Francisco, CA, USA.