

# Anchoring EVM Transactions using Blockchain: An Application of Cloud Computing

*Virtualization and Cloud Computing Project*

## Team Details

Himanshi (M21CS006)

Shubham Singh (M21CS016)

MTech CSE

## Background

Elections are the backbone of democracy, but is it disappointing when political Parties criticize the voting machines used for election? The current polling system EVM profoundly lacks in technology. The EVM used has the control unit(CU) and the balloting unit(BU). These units are linked with the help of a cable. The control unit(CU) of the EVM resides with the polling officer, and the balloting unit(BU) is kept inside the voting booth for citizens to cast their choices. This helps polling officers in verifying their identity. With the EVM, the polling administrator will press the Ballot Button, permitting voters to cast their choice. A record of candidates' names along with symbols will be available on the ballot with a blue button. The citizen can choose the candidate by pressing the blue button next to their name. No section of the current voting system is "networked". EVM voting machines are very simple, like pocket calculators[1]. Hence its consequences include Liability towards fraud, the time interim within the polling and calculating votes is large, which leads to tampering, and due to the physical convenience to the EVM, the third-party can intervene and modify the calculation of votes. Therefore the dilemma of the current voting system has a low level of security and authentication. The trust of current voting has been attacked, and this is why we move towards the Blockchain-based cloud voting system.[2]

Blockchain voting, as of now, is shaping the democratic process. Those in the army from West Virginia, USA, working overseas can choose by utilizing their cell phones for polling in their home elections. A combination of encryption and the blockchain registry counts and checks these votes. Crucial characteristics of Blockchain-based voting technology are High Availability, Transparency, Immutability, Decentralized, and Enhanced Security.[3]

## Problem Statement

In India, elections are conducted using EVM's (Electronic Voting Machine), which emerged in the preceding two decades by government-owned companies associations [4]. EVMs commit towards the more agile counting, vote fitting and distribution of votes on the results despite that the EVM machine receives input information from citizens or voters and generates results in a manner that external spectators and election officials cannot testify or witness[5]. Consequently, the EVM is lacking in transparency and integrity.

The Council of Europe's handbook on e-voting states, "It has become clear that e-voting systems cannot be introduced unless citizens and other stakeholders trust their political and administrative systems" [5]. The population requires a transparent and honest voting system to restore their rights to choose and elect the leader of their preference. The existing EVM has several allegations. There is a necessity to consider the issues and demands of Provable studies, which reduce malpractices [6] as hacking has taken over the ability to hold a clear and transparent election.

## Methodology

A Fair E-voting web app is created in which the voters can register themselves using their name, state and aadhaar card number, and get an exclusive voterId which is used to login to the app, and cast the vote. The system uses blockchain and cloud technology for authentication and to make the voting system transparent and integrated.

## Dependencies

Dependencies are concerned with the software components needed by the project to work as expected and to avoid runtime errors.

```
INSTALLED_APPS = [
    'django.contrib.admin',
    'django.contrib.auth',
    'django.contrib.contenttypes',
    'django.contrib.sessions',
    'django.contrib.messages',
    'django.contrib.staticfiles',
    'myapp',
]

MIDDLEWARE = [
    'django.middleware.security.SecurityMiddleware',
    'django.contrib.sessions.middleware.SessionMiddleware',
    'django.middleware.common.CommonMiddleware',
    'django.middleware.csrf.CsrfViewMiddleware',
    'django.contrib.auth.middleware.AuthenticationMiddleware',
    'django.contrib.messages.middleware.MessageMiddleware',
    'django.middleware.clickjacking.XFrameOptionsMiddleware',
    'django.middleware.csrf.CsrfViewMiddleware',
]
```

## Voting Procedure

Initially, the user registers to cast a vote by providing their Name, State and Aadhaar card number. In this step, we authenticate the user with the help of a PHP file by checking these details in the database situated on the AWS. If the entries are valid and have not been registered yet, only then the voterID is displayed.

Subsequently, we use the voterID to present our vote, through which the application tests if the voter's voterID has voted already and confers if the user has earlier cast a vote. The political party the voter has chosen is given a vote, a new block node is added to the blockchain, and the hash code of that block is stored in the database. Since every vote or transaction has a signature from a right pair, we can follow back any transaction to any voter of the application in the state of an inspection.

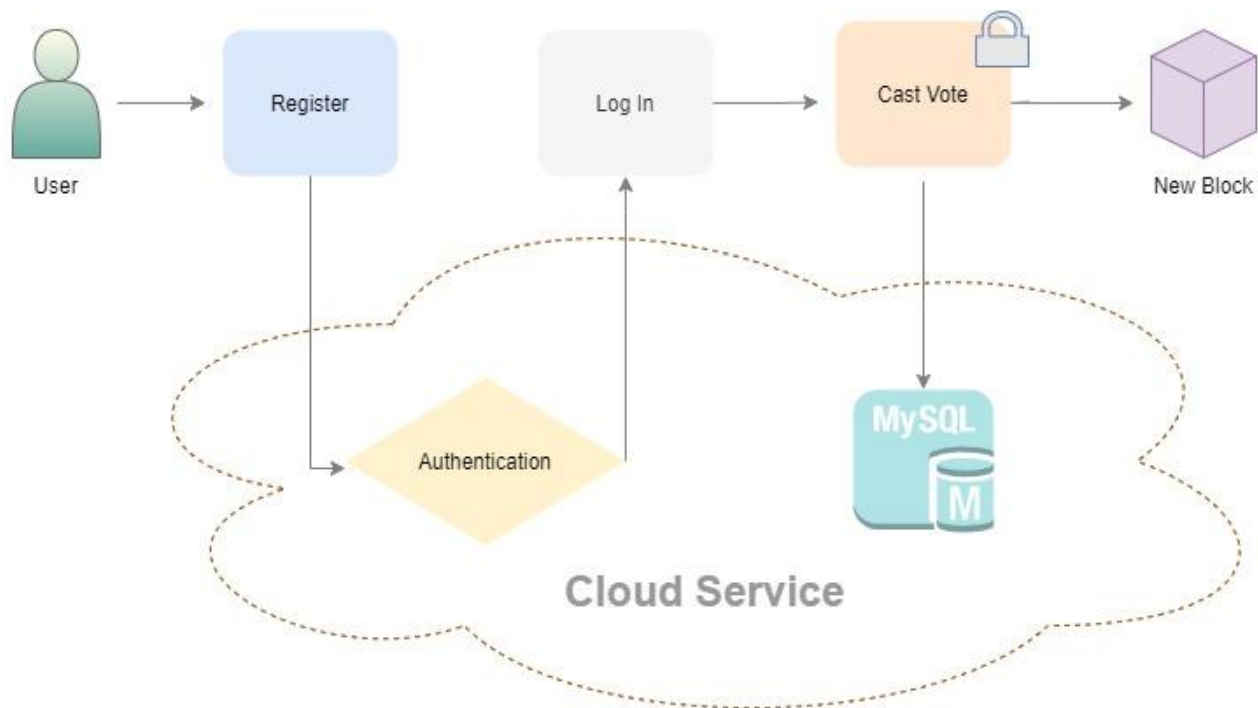


Fig.1: Voting process

The above image shows the flow of the web application in the registration phase: voters get the voterID to vote only if the user is found authenticated, and after voting securely a new block is created, and hash code is stored in the database on the AWS.

## Network Connection

The web application is connected with Cloud services using PHP files. Two PHP files are created, one to authenticate the user and the second to store the hash values of the block along with respective voter details.

## Backend used

We use the Django framework to provide the whole functionality to the webpage. Django makes the entire process of transmitting data over the Internet more straightforward and faster. The Django server maintains information pretty well and also manages the Speed.

## Analysis

Our proposed system involved collecting the ballot information as a block for every voter and transferring the hash over the internet to cloud storage. After every hash entry, we analysed the updated time to interpret the error rate between the proposed method and the base paper's error detection rate as shown in Fig. 2.

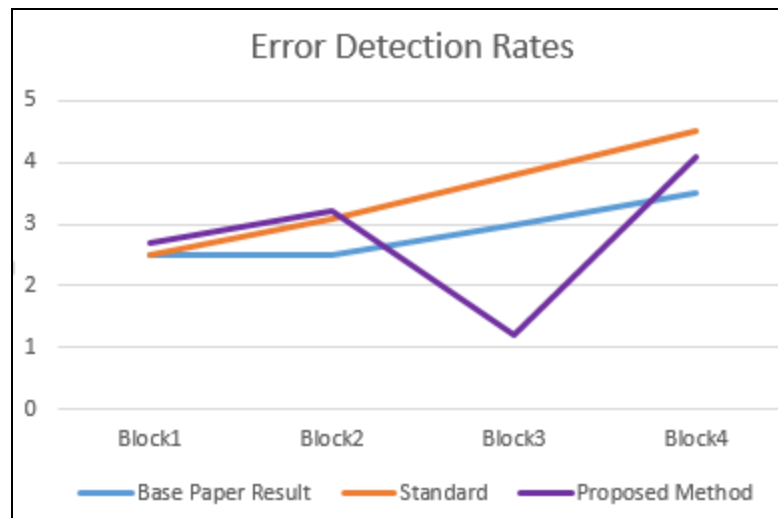


Fig. 2 Error Production Rates (in ms)

## Result and Comparison

We tried to implement the base paper and to enhance its functionality. The method currently used for polling has been widely believed best, but the reality is there is no transparency and hence simply hackable. Executing cloud and blockchain-based solutions will improvise the security of the ballot that is received. Hence, the base research paper illustrates a way to devise the political future in the country, especially India. We enhanced its security by adding an authentication layer so that only valid users have the right to cast the vote.

## Future Directions

- 1) Better networks or channels can be used for high-speed storing and evading more network vulnerabilities.
- 2) Kubernetes service can be used to create clusters and deploy containers. A Kubernetes cluster allows us to securely handle the resources that we require to deploy, update, and scale applications.
- 3) For the enhancement of security, end-to-end voting systems can use advancements of cryptography to secure the integrity of the elections.

## References

1. <https://www.ijert.org/research/secure-voting-system-using-blockchain-IJERTV8IS110414.pdf>
2. <http://www.ijies.net/finial-docs/finial-pdf/270318333.pdf>
3. <https://www.dailyo.in/technology/blockchain-evm-voting-polls-politics/story/1/24073.htm>
4. V Sathya, Arpan Sarkar, Aritra Paul and Sanchay Mishra, "BlockChain Based Cloud Computing Model on EVM Transactions for Secure Voting", *Third International Conference on Computing Methodologies and Communication (ICC WC 2019)*, pp. 1075-1079, 2019.
5. "E-voting Handbook: Key Steps in the Implementation of E-enabled Elections", Council of Europe.
6. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3871197](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3871197)
7. <https://stackoverflow.com/questions/50532591/how-to-create-a-blockchain-network-on-a-lan-with-other-computers-as-nodes-or-par>
8. <https://dzone.com/refcardz/getting-started-with-ethereum-private-blockchain?chapter=1>