IMPLEMENTATION ON E-VOTING SYSTEM USING BLOCKCHAIN TECHNOLOGY AND FINGERPRINT AUTHENTICATION

Sonali Malhari Tambe, Piyusha Vijaykumar Vhanakde,
Pratiksha Ashok Wagh, Shraddha Umesh Adhav, Prof. Pranita Ingale

DEPARTMENT OF INFORMATION TECHNOLOGY
JSPM'S
BHIVARABAI SAWANT INSTITUTE OF TECHNOLOGY & RESEARCH, NAGAR ROAD, WAGHOLI, PUNE-412207

---***---

Abstract - : *Increasing digital technology has revolutionalized the life of people. Unlike the electoral system, there are many conventional uses of paper in its implementation. The aspect of security and transparency is a threat from still widespread election with the conventional system (offline). General elections still use a centralized system, where in one organization manages it. Some of the problems that can occur in traditional electoral systems is with the organization that has full control over the database and system. It is possible to tamper with the database of considerable opportunities. Block chain technology is one of solutions, because it embraces a decentralized system and the entire database are owned by many users. Block chain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting block chain in the distribution of databases on e-voting systems one can reduce the cheating sources of database manipulation. This project aims to implement voting result using block chain algorithm from every place of election. Unlike Bitcoin with its Proof of Work, this will be a method based on a predetermined turn on the system for each node in the built of block chain.*

KEYWORDS: Blockchain, Voting System, Fingerprint, Authentication

1.INTRODUCTION

From the dawn of democratically electing candidates, the voting system has been based on pen and paper scheme. Replacing the traditional pen and paper scheme with a new election system is a new idea for researchers.

An E-voting system has to have heightened security in order make sure it is available to voters but protected against outside influences changing votes from being cast, or keep a voter's ballot from being tampered with.

Lately, electronic voting systems have begun being used in many countries. Estonia was the first in the world to adopt an electronic voting system for its national elections [1]. Soon after, electronic voting was adopted by Switzerland for its state- wide elections [2], and by Norway for its council election [3]. For an electronic voting system to compete with the traditional ballot system, it has to support the same criteria the traditional system supports, such as security and anonymity. An e- Voting system has to have heightened security in order make sure it is available to voters but protected against outside influences changing votes from being cast, or keep a voter's ballot from being tampered with. Many electronic voting systems rely on to hide the identity of voters [4]. However, this technique does not provide total anonymity or integrity since many intelligence agencies around the world control different parts of the Internet which can allow them to identify or intercept votes.

MOTIVATION

The proposed system can reduce the cheating sources of database manipulation. This project aims to implement voting result using block chain algorithm from every place of election.

PROBLEM DEFINITION

Proposed a E-voting using block chain Technology and fingerprint authentication for providing a facility to cast vote for critical and confidential. The flexibility to allow casting vote from any remote place.

II. PROPOSED SYSTEM

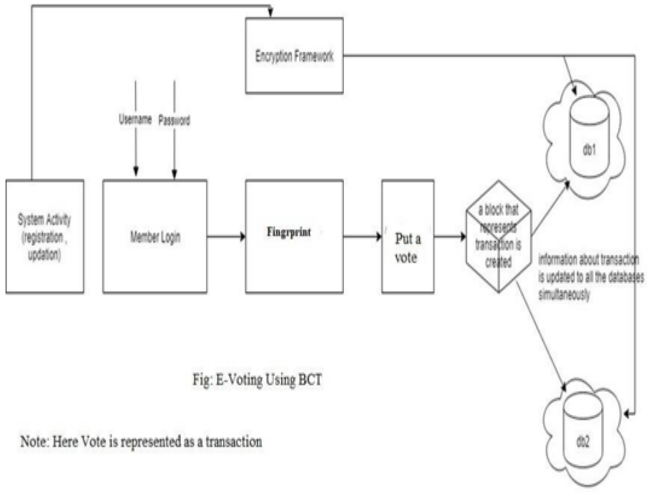

Encryption Framework
Username
Password
System Activity (registration , updation)
Member Login
Fingrprint
Put a vote
a block that represents transaction is created
information about transaction is updated to all the databases simultaneously
db1
db2
Fig: E-Voting Using BCT
Note: Here Vote is represented as a transaction

Fig 1. Proposed System

Whenever any transaction will occur in the system, the record of that transaction is maintained in the form of hash value in a block. Each next block will get attached to the previous block and in this way a virtual block chain will occur. The hash value of a current block is generated using the data of a current block and the hash of the previous block. In this way if any of the block is tempered the subsequent all the block's hash must be changed. Such multiple copies are maintained at different servers, which will assure the data security and confidentiality. As everything is through application interface, it will maintain the transparency in the voting system.

- Admin: admin can add candidate, voter, ward and election. He/she can perform update delete operation and declared result also.
- FingerPrint: Administrator (Election officer) sends share 1 to voter e-mail id before election and share 2 will be available in the voting system for his login during election. Voter will get the secret password to cast his vote by combining share 1 and share 2 using FingerPrint.
- User: Voter can vote only if he/she logs into the system by entering the correct password which is generated by merging the two shares (Black & White dotted Images)using Fingerprint scheme.
- Block Chain: Block chain is a distributed database that stores data records that continue to grow, controlled by multiple entities. Block-chain (distributed ledger) is a trustworthy service system to a group of nodes or non-trusting parties, generally block chain acts as a reliable third party to keep things together, mediate exchanges, and provide secure computing machines.

III. ALGORITHM USED

AES: AES is used to encrypt the database. The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data, the data to be encrypted. This array we call the state array.

STEPS:

- Derive the set of round keys from the cipher key.
- Initialize the state array with the block data (plaintext).
- Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation.
- Perform the tenth and final round of state manipulation.
- Copy the final state array out as the encrypted data (ciphertext).

SHA 256 : SHA-256 (secure hash algorithm, FIPS 182-2) is a cryptographic hash function with digest length of 256 bits. It is a keyless hash function; that is, an MDC (Manipu- lation Detection Code). A message is processed by blocks of 512 = 16 × 32 bits, each block requiring 64 rounds A cryptographic hash (sometimes called 'digest') is a kind of 'signature' for a text or a data file. SHA-256 generates an almost-unique 256-bit (32-byte) signature for a text.A hash is not 'encryption' – it cannot be de- crypted back to the original text (it is a 'one-way' cryptographic function, and is a fixed size for any size of source text). This makes it suitable when it is appropriate to compare 'hashed' versions of texts, as opposed to decrypting the text to obtain the original version.

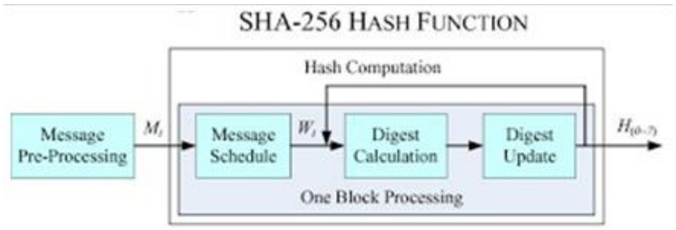
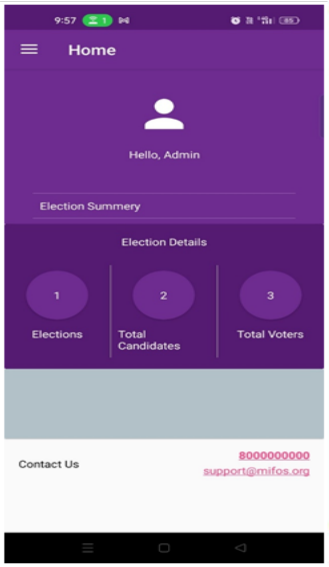


Figure 2: SHA 256 Diagram

IV. RESULT


9:57

Home

Hello, Admin

Election Summery

Election Details

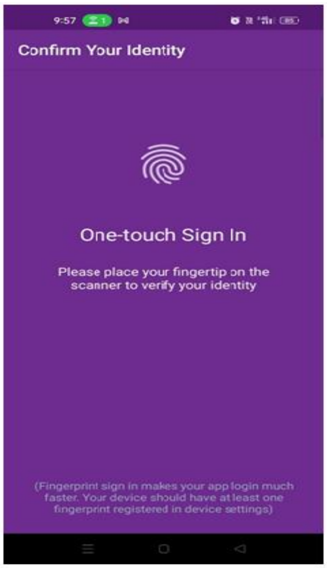
1 Elections

2 Total Candidates

3 Total Voters

Contact Us 8000000000 support@mifos.org

Fig 3: Admin Dashboard


9:57

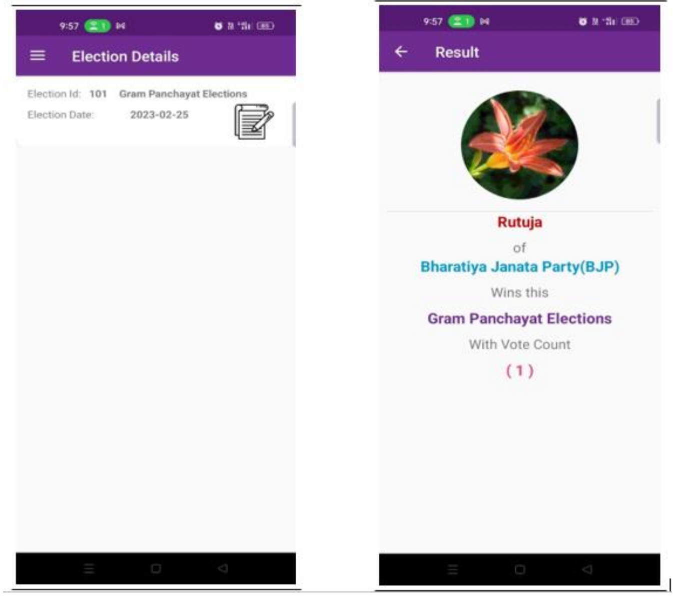
Confirm Your Identity

One-touch Sign In

Please place your fingertip on the scanner to verify your identity

(Fingerprint sign in makes your app login much faster. Your device should have at least one fingerprint registered in device settings)

Fig 3: User Dashboard


9:57

Election Details

Election Id: 101 Gram Panchayat Elections

Election Date: 2023-02-25

9:57

Result

Rutuja

of

Bharatiya Janata Party(BJP)

Wins this

Gram Panchayat Elections

With Vote Count

(1)

Figure 4: Election Results

V. CONCLUSION

The proposed system will be designed to provide a secure data and a trustworthy Evoting amongst the people of the democracy. Block chain itself has been used in the Bit-coin system known as the decentralized Bank system. By adopting block chain in the distribution of databases on e-voting systems one can reduce the cheating sources of database manipulation. This project aims to implement voting result using block chain algorithm from every place of election.

VI. REFERENCES

[1] Ahmed Ben Ayed,A Conceptual Secure Block Chain-Based Electronic Voting System,2017 IEEE International Journal of network & Its Applications(IJNSA),03 May 2017[1].

[2] RifaHanifatunnisa, Budi Rahardjo, Blockchain Based E-Voting Recording System Design,IEEE 2017[2]

[3] Kejiao Li, HuiLi,HanxuHou, KedanLi,Yongle Chen, Proof of Vote: A HighPerformance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain, 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems[3]

[4] Ali KaanKo, EmreYavuz, Umut Can abuk, GkhanDalkilic, Towards Secure E-Voting Using Ethereum Blockchain,2018 IEEE[4]

[5] Supriya Thakur Aras, Vrushali Kulkarni, Blockchain and Its Applications A Detailed Survey, International Journal of Computer Applications (0975 8887) Volume 180 No.3, December 2017[5].

[6] Freya Sheer Hardwick, ApostolosGioulis, Raja Naeem Akram,Konstantinos Markantonakis, E-Voting with Blockchain: An E-Voting Protocolwith Decentralisation and Voter Privacy,IEEE 2018,03 July 2018[6]