IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 8, August 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

Secure E-Voting Using Block Chain with Protection against Selective Tampering

Alisha Erum K, Dr. Mohammed Tajuddin

PG Student, Dept. of CSE., Dayananda Sagar College of Engineering, Bangalore, Karnataka, India

Associate Professor, Dept. of CSE., Dayananda Sagar College of Engineering, Bangalore, Karnataka, India

ABSTRACT: Electronic means of casting votes is called as E-voting. E-voting has become popular last decade in many countries due to its cost and time saving effectiveness. Especially in bigger and population dense country like India, e-voting brings lot of benefits in terms of knowing the result earlier and reducing the election expenses. In India electronic voting has become a standard and it is being deployed for elections at all levels from nations to district levels. But recently there are many doubts in current e-voting process as the results are kept in the EVM (electronic voting machine) and there is doubts of EVM being tampered and results can be forged. This paper proposes a secure e-voting using the concept of block chain to prevent the results from being tampered and even if tampered, recovery of results from backup chains.

KEYWORDS: Peer 2 Peer, E-Voting, Block Chain, Cloud Computing, Selective Tampering.

I. INTRODUCTION

In democracy, voting is the method to select the ruling government by the people of the country. Voters cast their ballot to their selected candidate and candidate having the higher number of votes wins. Election is the process conducted in democratic countries using voting to select the ruling party. Elections traditionally were conducted using paper ballot. The paper ballot system is in efficient in terms of cost and time and resources needed for counting. Towards this end, electronic voting was proposed. Electronic voting can be online or offline. In online systems, people cast their voting using internet from their places. In offline systems, people must go to election booth and cast their vote in electronic voting machines. Offline voting using electronic voting machines has gained popularity in many countries in last 10 years due to reduction of election cost and results can be announced soon. Online voting is difficult in countries like India due to lack of internet coverage to many people. In offline voting system, the votes are saved in the electronic voting machines. During counting process, the votes in the electronic voting machines are counted and results are announced.

Recently there is widespread doubts about EVM being tampered and the votes in it are compromised to give false results. The benefits of using EVM are nullified with risk of tampering. Towards this end many solutions have been proposed for e-voting resilient against the risk of tampering. In this paper, a secure e-voting using blockchain is proposed for resiliency in offline voting systems. Blockchain is based on distributed ledger technology (DLT). It synchronizes the ledgers replicated among multiple nodes by using community validation, which is adopted to serve as the public transaction ledger of the crypto-currency Bitcoin. In this work, block chain is exploited to avoid forgery of votes. The work also implements authentication and non-repudiation using elliptic key cryptography. Anonymity is an important requirement in voting process, In the proposed solution, since the votes are kept in the block chain, to provide anonymity, voter id obfuscation using pseudonym is done to traceability of voter from the votes. With combined use of concepts of cryptography, block chain and cloud backup the proposed solution can provide a scalable secure e-voting resilient against forgery attacks.

II. RELATED WORK

A review of security solutions for e-voting is presented in this section.

[1] In this paper the researches have implemented a public permission less block chain technology to overcome the mechanism of the security breach and provide some advanced applications such as the bulletin board as these were the favourite selections to implement in the majority of the recent blockchain based e-voting scheme which mainly focuses on the DLT. But the disadvantage with the mechanism was that the Block chain did not eliminate the need for external trust presenters or the miners.

[2] In this paper the researchers propose an e-voting system that exploits the use of the blockchain as a transparent box. The system has been designed to stick to essential e-voting properties also to bid a degree of decentralization and permit the voter to change/update their vote according to their choices (within the permitted threshold period). This paper also highlights the advantages and disadvantages of using blockchain for such an application from a real-world point of view in both progress/positioning and usage circumstances.

[3] In this paper the researchers present a complete analysis of e-voting system by watching the challenges. The paper also reviews the huge amount of security requirements named within the works that permits researcher to design a secure system. They have also analysed several the e-voting systems that are found within the world and therefore also the relevant literature. They also put forth their ideas on how an e-voting system are often usable by different research conducted on the e-voting system and summarizes on diverse cryptographic tools in creating an e-voting system.

[4] In this paper the researchers propose blockchain based on a decentralized e-voting system, without the presence of a reliable third party. They also provide numerous possible allowances and improvements that meet the needs in some exact voting situations. it might be agreeable if some facts of the e-voting procedure might be further optimized and applied. for example, due to intended transparency of blockchain, it seems tough to satisfy coercion-resistance (voters shouldn't be prepared to evidence how they voted.) without they implement access control using permissioned blockchain mechanism.

[5] In this paper the researchers propose Additional procedures for articulating the society applicants' determination. Additionally, beyond inconvenience, there could also be genuine explanations for not having the capability to involve portion within the voting process, e.g. being organized overseas in military or presence on another official assignment. during this they present methods, the way to make internet e-voting system secure by means of blockchain concept.

[6] In this paper the researchers propose electronic voting systems which depend upon some of the electronic technology for his or her accurate functionality. Several of them are subjected to such technology for the announcement of election data. counting on one or additional communication channels to run election process with many technical challenges with reference to verifiability, reliability, safety, secrecy, and confidence. Altering the way during which people vote has many public and politically aware implications. The role of election commissioners and (autonomous) viewers is basically diverse when multipart expertise is intricate within the method.

[7] E-voting can take many methods: using the web or a dedicated, remote network; demanding voters to appear at a voting place or permitting unofficial voting; using present devices, like android phones and laptops, or demanding professional kit. To remain trusting chief ruling classes to accomplish elections or to use blockchain technology to dispense an open voting record among citizens. Many authorities agree that e-voting would need innovative progresses in security systems. the talk is whether blockchain will characterize a transformative or just incremental progress, and what its consequences might be for the extended period of consensus.

[8] In this paper the researchers present feature-oriented classification for viable electronic voting machines, which mainly focuses on usability aspects. maintained this analysis, they extant a “Just-Like-Paper” (JLP) classification method which classifies five broad classes of e-voting interface. They cover the classification to enquiry its application as an indicator of voting competence and classify a worldwide ten-step process encircling all probable voting steps across the twenty-six machines studied. Experimental study accomplishes that multi-functional and liberal interfaces are likely to be more effectual against multi-modal voter-activated machineries.

[9] In this paper the researchers presented procedure established on blockchain technology. The underlying technology exploited in the electoral system may be an imbursement scheme, which offers secrecy of communications, a characteristic not seen in blockchain proprieties so far. The projected procedure offers secrecy of voter communications, while keeping the communications isolated, and thus the election transparent and secure. The underlying imbursement procedure has not been adapted in any way; the voting procedure just offers an alternative usage instance.

[10] In this paper the researchers they emphasized the complication of the distribution of e-voting systems and therefore the characteristic security issues that arise from the underlying distributed system. The projected system has successfully addressed many issues in e-voting and has recognized the issues associated to veracity, recording and verification especially. the need to resolve identification and anonymity, on one hand, and verifiability and anonymity on the reverse hand could also be the clincher within the broader adoption of e-voting. The challenge is to take care of the veracity of the self-governing process by securing eligibility and avoiding corruption and compulsion. Furthermore,

the lack of election authorities to make sure the safety and dependability of isolated machines may cast uncertainty on the viability of electronic voting and must favour the distribution of hybrid classifications.

III. PROPOSED ALGORITHM

The secure e-voting system proposed in this work is an offline e-voting system with Block chain and cloud at backend for storing the votes. The architecture of the system is given below

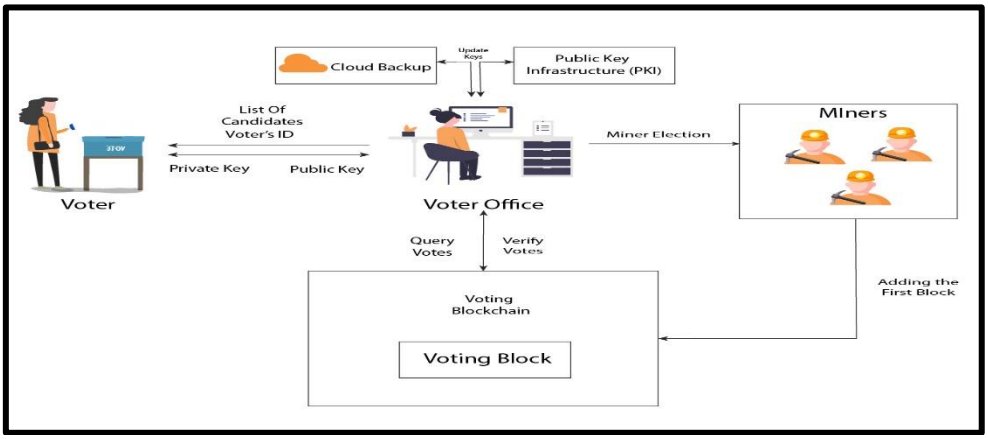

Figure 1: Architecture of the E-voting System using Blockchain

Each time a voter casts his vote, a vote block is created, the vote block has following contents

Voter's ID	It is pseudonym derived from voter's actual id
Vote	Voters chosen candidate
Voter signature	Voter uses his private key to sign the hash of vote which is used to judge the authenticity of the vote
Timestamp	Submission time of the vote
Hash of previous block	SHA- 256 hash value of previous block.

Table 1: Terminologies In E-voting Process

The private key for signing the vote is found using Elliptic key cryptography. The voter must have created his public and private keys. Private key is an integer denoted by d_A. The public key is a curve point $Q_A = d_A \times G$, where $\times$ is the elliptic curve point multiplication. The voting algorithm is given below:

1. SHA-256 algorithm is used to create the hash value "V" = Hash (ID + Vote + Timestamp) by the voter.
2. By using the private key of an individual voter, the signature "U" is created for the hash value "V".
3. All the data that is stored on a vote block like the voter ID, casted Vote, Timestamp, signature "U" are all sent by the voter to the miner.
4. Public key from the PKI is retrieved by the miner on receiving the vote block based on the voter ID.
5. SHA-256 algorithm is used to create the hash value of "V" = Hash (ID + Vote + Timestamp) by the miner.
6. Public key is used to verify the signature "U" and get the hash value "V`" by the miner.
7. The hash value generated by the voter "V" and the hash value generated by the miner "V`" are compared. If both the values are the same, the signature "U" is accepted. Else, it is discarded.
8. Through this the miner concludes if the voter has already voted enough times or if the voter has a right to vote.

The Hash in the above algorithm refers to SHA 256 algorithm. The flow chart of the SHA 256 algorithm is given below

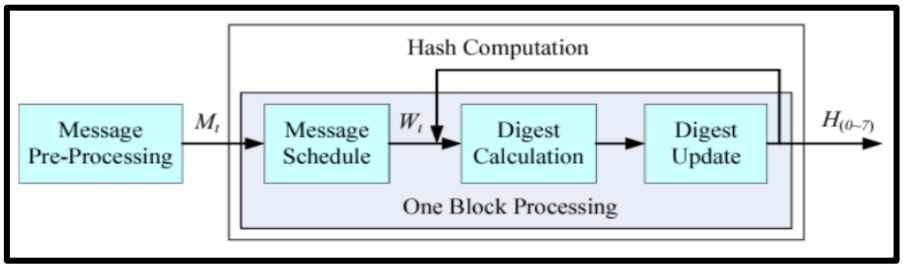

Figure 2:Flow chart of SHA 256 algorithm

The signature generation process is represented as flowchart and given below

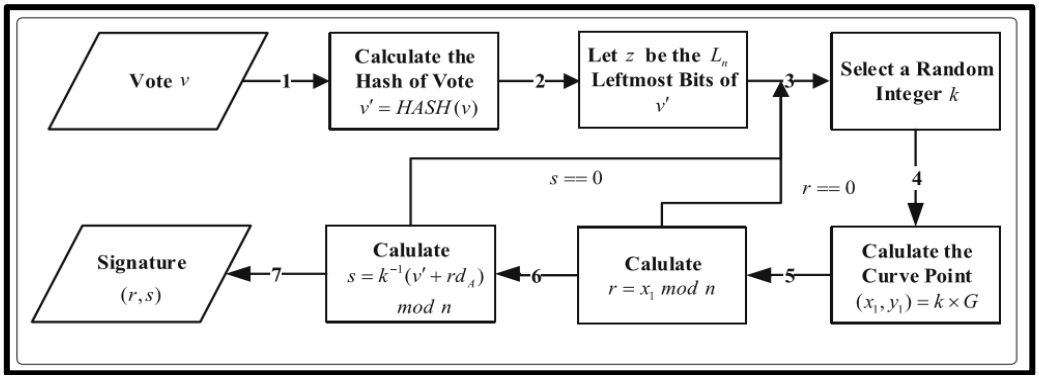

Figure 3: Flow chart of Signature Generation Process

During the counting process, signature is again computed and verified with the signature stored in block to detect if the block is selectively tampered while transmitted in the network. If the block is detected as tampered, the corresponding associated content for it is received from cloud by using the pseudonym present in the block and checking it the cloud. From it, the vote of the block is retrieved from the cloud and block is recovered. The recovered block is then used for counting. The flow chart for counting process is given in figure 2.

IV. IMPLEMENTATION AND RESULTS

The proof of concept of proposed solution is implemented in Java with Ethereum blockchain and amazon s3 cloud for backup. The solution is implemented into three subsystems

1. P2P chain
2. Voter application
3. Vote office application

P2P chain module stores the block into Ethereum block chain and cloud. Voter application create the vote block containing the voter pseudonym and casted candidate information. The created blocks are sent to P2PChain for storage in block chain and cloud. Vote office application queries the block chain and in case of forgery detection also queries cloud to recover the blocks, counts votes and presents the results.

The P2P chain is first started. The app listens at TCP port 5000 for blocks as shown in figure 4. After this the vote casting application is started as shown in figure 5.

Figure 4: P2P Application Interface after starting server

Figure 5: Voting Application Interface

The figure 5 shows the voting interface which has a tab to enter the valid voter ID and a drop-down list with several candidates to vote. It has two buttons one for casting the vote and the other for recasting. It also has a Space to display the status of the voter's vote. The voter can enter a valid ID and select one candidate to whom he wishes to vote as shown in the figure 6. The voter id is converted to pseudonymfor maintaining the anonymity of each individual and stored with other data as a block and stored on the cloud and the database for local storage. The vote block is sent to P2P chain and block is saved in Ethereum block chain and cloud as shown in figure 7.

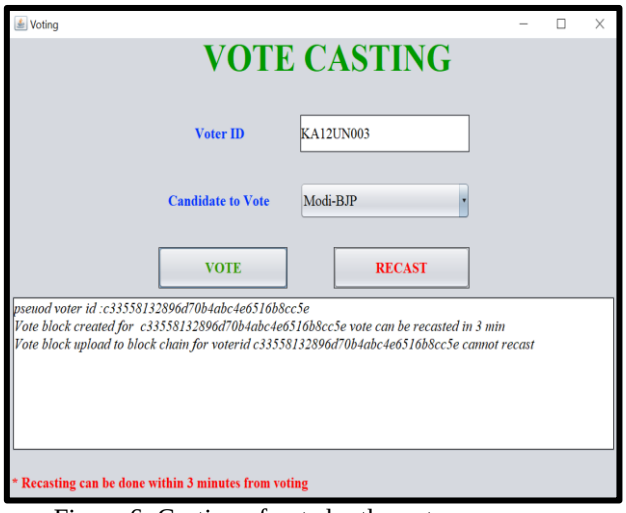

Figure 6: Casting of vote by the voter

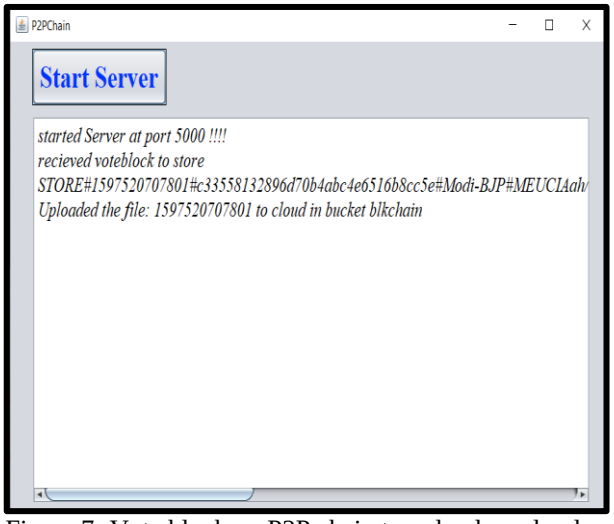

Figure 7: Vote block on P2P chain to upload on cloud

The figure 7 shows the acknowledgement of the uploaded block to the chain in the cloud which displays the pseudo random number of the voter ID and the name of the candidate to whom the voter has casted the vote. The below figure shows the actual storage of the vote on the cloud.

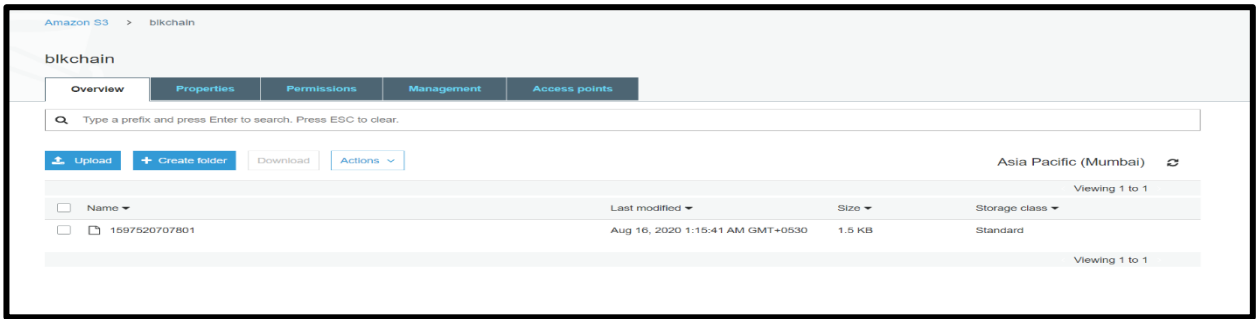

Figure 8: Vote storage on Cloud

The voting office interface is for the administrative purpose and it is final step of the E-voting system, where the admin or the voting officer who is the head of the entire voting process uses this interface to query the votes and display the end results to the public. This module has 2 steps one is the admin login and the other is the vote query.

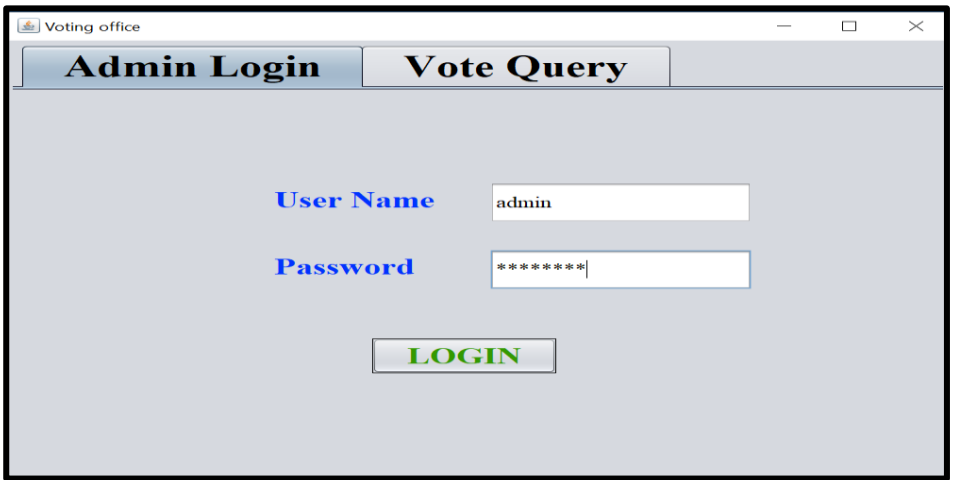

Figure 9: Voting Office interface shows the admin page for authentication

If the admin authentication is successful, then the query button is enabled on the vote query page and the voting officer can click on the query button to check the voting results, the vote counting process is designed as shown in the figure 10.

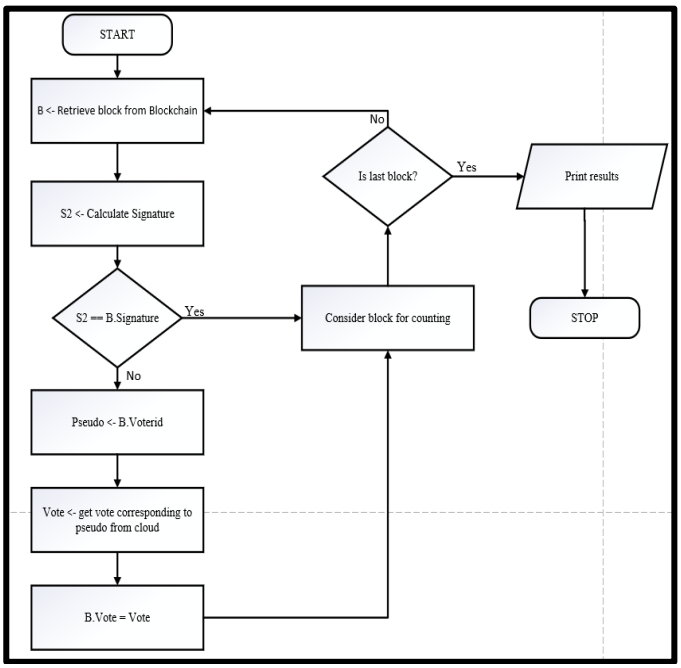

Figure 10: Flow Chart of Vote Counting Process

Querying can be done in two modes – without recovery and with recovery.

1. Querying without recovery:
   In without recovery mode, block corruption is detected, but it cannot recovery from the information in the blocks as shown in figure 11.

2. Querying with recovery:
   In with recovery mode, block corruption is detected, and block content is recovered from the information in the cloud. After recovery, counting is done, and result is displayed as shown in figure 12.

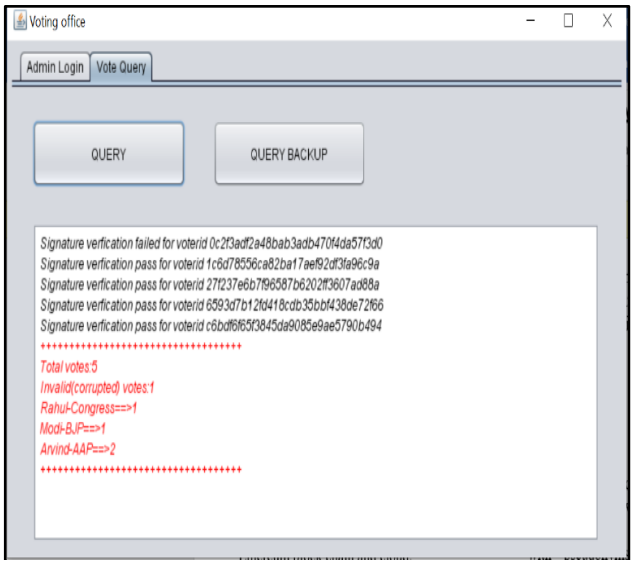

Figure 11: Querying without Recovery.

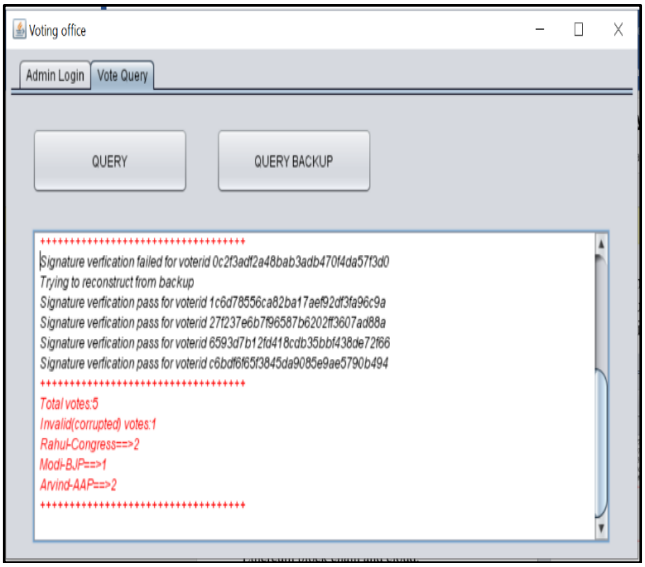

Figure 12: Querying with Recovery

We measure the time for counting for different number of votes and the result is given below. The time for counting in presence of recovery at 10% forgery is measured and the result is compared to solution proposed in [11].

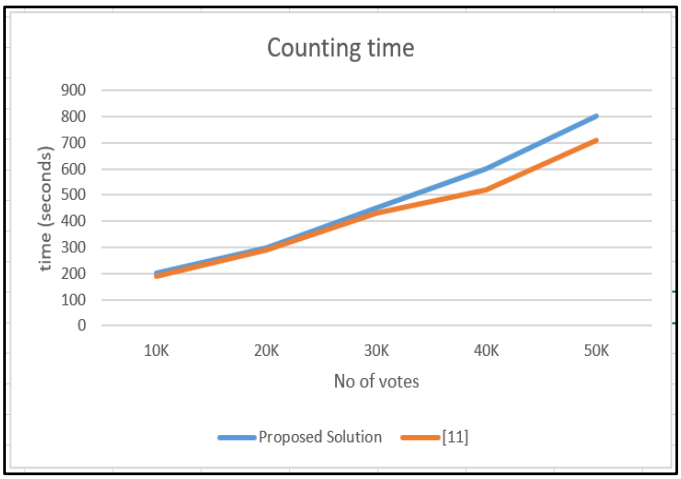

Figure 13: Simulation analysis of time taken for the counting process

Compared to solution proposed in [11], the time is little bit high due to time taken for accessing the cloud and recovering the block content from cloud. The time is justified, considering, recovering from forgery and providing accurate result is more important than the additional time taken for counting in the proposed solution.

V. CONCLUSION AND FUTURE WORK

A secure block chain-based E-voting system is proposed in this work. The system uses cloud for forgery assistance. Anonymity of votes is preserved with pseudonyms. Authentication and non-repudiation is ensured with use of Elliptic key cryptography. The system is full proof against forgery and even in case blocks can be tampered selectively while transportation on network, with cloud backup, recovery can be done to find the original content of the block. As a future work, prevention of e-voting systems from quantum computer attacks can be investigated.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

REFERENCES

1. King-Hang Wang, Subrota K. Mondal, Ki Chan, XiaohengXie, "A review of contemporary e-voting: Requirements, technology, systems and usability", Data Science and Pattern Recognition, vol. 1, no. 1, pp. 31- 47, [2017].
2. J. P. Gibson, R. Krimmer, V. Teague, and J. Pomares, "A review of E-voting the past, present and future", Annals of Telecommunications, pp. 18, [2016].
3. MacNamara, Paul Gibson, and Ken Oakley, "The ideal voting interface: Classifying usability", Journal of eDemocracy and Open Government, vol. 6(2), [2014].
4. Rachid Anane, Richard Freeland and Georgios Theodoropoulos, "E-voting requirements and implementation", in the 9th IEEE CEC/EEE 2007. IEEE, pp. 382-392, [2007].
5. Sven Heiberg, Ivo Kubjas, JannoSiim, and Jan Willemson, "On Trade-offs of Applying Block Chains for Electronic Voting Bulletin Boards", IACR-[2018].
6. Pavel Tarasov and Hitesh Tewar, "THE FUTURE OF E-VOTING", IADIS International Journal on Computer Science and Information Systems Vol. 12, No. 2, pp. 148-165, ISSN: 1646-3692, [2017].
7. Yi Liu and Qi Wang, "An E-voting Protocol Based on Blockchain"; ACM, [2010].
8. Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralization and Voter Privacy"; arXiv: 1805.10258v2 [cs.CR] 3 Jul [2018].
9. Philip Boucher, "What if blockchain technology revolutionised voting?" EPRS- EuropianParlimentaryReasech Services, PE-581.91, [2016].
10. Ivo Kubjas, "Using blockchain for enabling internet voting", January 6, [2017].
11. HaiboYi, "Securing e-voting based on block chain in P2Pnetwork", YiEURASIP Journal on Wireless Communications and Networking,2019.

BIOGRAPHY

Alisha Erum K completed her B.E in Computer Science and Engineering from Visvesvaraya Technological University, Karnataka. She is currently pursuing her MTech at Dayananda Sagar College of Engineering, Bengaluru, Karnataka in Computer Science and Engineering. Her areas of interest include Could Computing, Network Security, Web Application Development,Machine Learning and Artificial Intelligence.

Dr. Mohammed Tajuddinis an Associate Professor at Dayananda Sagar College of Engineering, Bangalore, Karnataka. Bearing an experience of 23 years. His areas of interest include Network Security and Biometrics. He is also a member of the ISTE.

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details