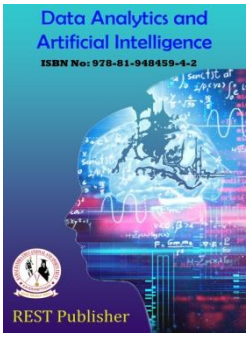
Data Analytics and Artificial Intelligence

Vol: 3(1), 2023

REST Publisher; ISBN: 978-81-948459-4-2

Website: http://restpublisher.com/book-series/daai/

DOI: https://doi.org/10.46632/daai/3/1/13



Online E-Voting System Using Blockchain Technology

***S. Kavitha, Praveen. R, Ragavendrar. M.A, Vishwa**

veltech hightech dr.rangarajan dr,sakunthala engineering college, Chennai,Tamil Nadu, India.

*Corresponding Author Email: kavithaarunachalam58@gmail.com

Abstract: *A secure method of counting and voting votes using electronic means, with the intent of improving the performance ofvoting systems, is known as electronic voting (electronic voting). Current electronic voting mechanisms face challenges such as confidentiality, integrity, verifiability, transparency, non-repudiation and trustworthiness. The e-voting system uses blockchain to ensure vote integrity and security, and machine learning models to detect intrusions into voting datacenter's and e-voting stations. Both encryption and decryption ensure voter integrity and confidentiality to prevent counterfeiting and other forms of election fraud. Voter data is encrypted with the state elections office's elliptical publickey. Public blockchains are used to maintain the integrity of voters' personal data by storing root hashes derived from the Merkle hash tree and revealing voting station results once the voting process is complete.*

Keywords: *Blockchain, Merkle Root, ECC, Intrusion Detection, SVM.*

1. INTRODUCTION

A Extensive research has been completed on digital vote casting structures that permit citizens to vote at their comfort the use of a cell phone, laptop or another digital device. Still, none of that technology had been included on a bigger scale because of inherent protection threats/worries that those structures may pose to the integrity of the vote casting process. An online e-voting system using block chain technology is a promising approach to secure and transparent electronic voting. In a blockchain-based e-voting system, each voter is assigned a unique digital identity, and their vote is recorded as a transaction on the blockchain. This allows for secure voter identification and prevents voter fraud. Additionally, the decentralized nature of the blockchain allows for a transparent and auditable voting process, as all transactions are recorded on multiple copies of the blockchain, making it difficult for any individual to tamper with the voting results. The use of blockchain technology in online e-voting systems can also improve voter turnout, as it allows for remote voting and eliminates the need for physical polling stations. Block chain technology is a decentralized system which means that no single entity controls the network, this can help to prevent manipulation of the voting process. Block chain technology creates a tamper-proof and transparent record of the voting process, allowing voters to verify that their vote was included in the final tally without revealing their vote to anyone. By storing the vote on a blockchain,the vote cannot be tampered with and is resistant to hacking. The use of cryptographic techniques such as encryption and decryption can further enhance the security of the system. The use of blockchain technology makes it possible to conduct a full audit of the voting process, making it easier to detect and prevent fraud. Blockchain technology can be used to ensure voter anonymity by encrypting the vote and storing it on the blockchain in such a way that it cannot be linked to a specific voter. A Merkle tree stores all the transactions in a block by producing a digital fingerprint of the entire set of transactions. It allows the user to verify whether a transaction can be included in a block or not. Merkle trees are created by repeatedly calculating hashing pairs of nodes until there is only one hash left. The proposed blockchain-based e-voting system offers transparency, treasury, confidence and prevents intrusion into the information exchange network. However, implementing a blockchain-based e-voting system can be technically challenging and requires a significant investment in infrastructure and resources.

2. RELATED WORKS

An online voting system is a method of voting in which eligible voters can cast their ballots electronically via the internet. This can include voting via a website, mobile app, or other digital means. Online voting systems can be used for a variety of elections, including political elections, corporate shareholder meetings, and even internal company elections. The key benefits of online voting are increased accessibility, convenience, and efficiency, as well as the abilityto quickly and

accurately count and report results. However, there are also concerns about the security and integrity of online voting systems, such as the potential for hacking and voter fraud. To address these concerns, online voting systems must incorporate strong security measures, such as encryption and voter verification processes. Some distinctive work has been done in this field already which has been referred for gaining the general idea and grasp a few key concepts required for this study.We referred to conference paper [1] to gain an overall idea on how the author tried to solve a similar problem using Ethereum as a blockchain network. Trustworthy Electronic Voting Using Adjusted Blockchain Technology - Basit Shahzad Raju, Jon Crowcroft in the year2019:This paper suggests a system that makes use of appropriate hashing methods to ensure data security. This paper introduces the concept of block-creation and block sealing. The implementation of a block sealing principle helps to make the blockchain flexible to meet polling process requirements.

3. MATERIALS & METHODS

Merkle Hash Tree: Merkle tree is a fundamental part of blockchain technology. It is a mathematical data structure composed of hashes of different blocks of data, and which serves as a summary of all the transactions in a block. It also allows for efficient and secure verification of content in a large body of data. It also helps to verify the consistency and content of the data. BothBitcoin and Ethereum use Merkle Trees structure.

How Do Merkle Hash Trees Work: A Merkle tree stores all the transactions in a block by producing a digital fingerprint of the entire set of transactions. Itallows the user to verify whether a transaction can be included in a block or not. The Merkle Tree maintains the integrity of the data. If any single detail of transactions or order of the transaction's changes, then these changes reflected in the hash of that transaction. This change would cascade up the Merkle Tree to the Merkle Root, changing the value of the Merkle root and thus invalidating the block. So everyone can see that Merkle tree allows for a quick and simple test of whether a specific transaction is included in the set or not.

4. ALGORITHM FOR MERKLE ROOT

Block Head Key Generation using Merkle Root
// Input: Vote Attributes VATR
// Output: Head Key HK
Function: head Key Generator (VATR) 0: Start
1: HK =Ø
2: MKEY=MERKLE(VATR)
3: N=MKEY MOD 7
4: If N<7, then 5: P=N+1
6: for i=0 to HK length < 7 7: i=i+P
8: if i < HK length, then
9: HK = HK + MK [i]
10: = rotate (MK)
11: end if
12: else
13: i=0
14: end for
15: end if
16: return HK
17: Stop

Ecc Algorithm: Ethereum is an open supply platform primarily based totally on blockchain innovation standards. The most important benefit of Ethereum is that it lets in builders to gather and put up fixed applications. Ethereum uses nodes to update manor woman cloud compounds and servers demanded via way of means of vital Internet services. These nodes are managedvia way of means of volunteers. The system is likewise providing the person to create very own desire of polls, selectingvery own candidate. While utilizing a clever contract. In our work, for every certified candidate or the candidate chosenwith the aid of using a regular person, a bearing on the character wallet can be created.

Input: Voter ID
Output: Sliced Encrypted Ballot

(1) Begin
(2) If Voter Id in Voter List Id then//Check Voter
(3) Get the voter Token, set the password
(4) else not an eligible voter exit
(5) if (voter Id in registered voter list) then//check registered Voter

(6) Check Token and Password
(7) else not registered voter exit
(8) if not voted (token and password) then
(9) chose Candidate ID
(10) Ecc Data = key derivation(Candidate ID)//data encryption
(11) C_Ballot = Secret Share Slicer (Ecc Data) //data share
(12) send C_ballot to blockchain nodes
(13) else failed login exit
(14) END

Intrusion Detection: The positioning of the Intrusion Detection System (IDS) is also very important to protect the E-voting network. One needs to find the correct location for the IDS so that it can make accurate predictions. The maximum number of attacks to protect the E-voting station from intrusions as well as the Datacenter (from which each E-voting station has access tothe data) should be discussed. We placed the IDS at the border for our data center to detect distributed denial of service(DDoS) attacks more precisely and for the E-voting station at the center of the voting station network so that it could observe more traffic to protect the system more precisely. The data set we used contains the attack instances of Dos, so that Dos attacks can be detected at the citizen data center where the E-voting centers request data for registration purposes. Similar models can be used to detect intrusions within the E-voting station network. Once the intrusion detection detects the intrusion, we can look into the counter-measures that we intend to address in the future.

5. SYSTEM ARCHITECTURE

The block chain-based e-voting scheme is public, distributed, and decentralized. It can record votes from voters across manymobile devices and computers. The block chain-based e-voting scheme allows the voters to audit and verify the votes inexpensively. The database of votes is managed autonomously and is using a distributed server of timestamp on a peer-to peer network Voting on block chain is a workflow where voters regarding data security is marginal, which removes the characteristic of infinitereproducibility from e-voting. The following diagram shows the Block diagram of Block Chain of e-voting using Elliptive curve cryptography, An online voting system may have multiple weak spots. Cybersecurity risks can come from the system itself, the authentication mechanisms it deploys, the mobile devices used by voters, and the mechanisms responsible for protecting stored and transferred data. We started with block chain and the underlying mechanism of how it works and wrote our first smart contract and a case study around electronic voting using blockchain here. The blockchain along with the smart contracts provides a platform for the development of safer, cheaper, secure, more transparent, and easy-to-use e-voting systems. Due to its consistency and widespread use along with the provision of smart contracts logic, Ethereum and its network is one of the most suitable platforms for e-voting via the blockchain.

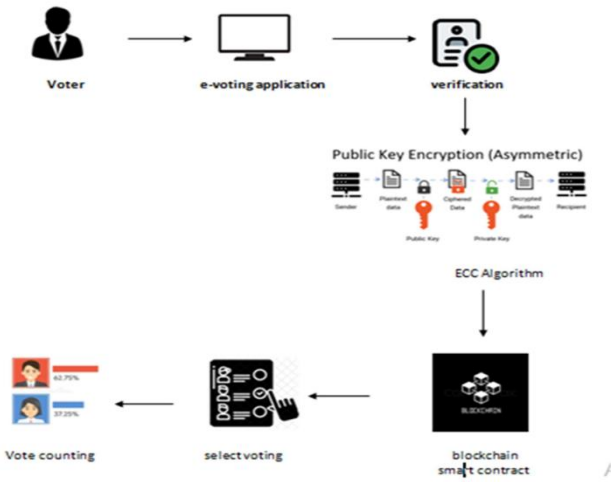


FIGURE 1: Block diagram of BlockChain e-Voting using Elliptive Curve Cryptography.

6. RESULTS AND DISCUSSION

As noted above, we need to detect various attacks, in particular the DOS attack on the data center, where the citizen record is stored, as well as other attacks within the network of the E-voting station, in order to protect the voting system from external threats by adding the IP attackers to the blacklist. These attacks can sabotage the voting process and can have an impact on the backbone of democracy. The concept of machine learning is used to demonstrate the identificationof such attacks. The Machine Learning Classifier is designed to predict attacks by monitoring network traffic. We usedthe USNWNB15 [29] data collection to train our machine learning model. The data set contains a large number of regular traffic instances as well as traffic attacks. Regular traffic helps to identify zeroday attacks. Using this data set, we have trained support vector machine (SVM) classifier models with different kernel settings to detect intrusions usingtraining data. To train the model, we first pre-process the data and select the required features, then feed the data to themodel for training purposes. The accuracy and the area under the curve for both of these models are calculated in order to evaluate and compare the models. The results for both of these models are shown in Table I, where we can see that SVM linear took more time while training the model but has better accuracy than SVM Coarse Gaussian. The positioningof the Intrusion Detection System (IDS) is also very important to protect the E-voting network. One needs to find the correct location for the IDS so that it can make accurate predictions. The maximum number of attacks to protect the E-voting station from intrusions as well as the Datacenter (from which each E-voting station has access to the data) shouldbe discussed. We placed the IDS at the border for our data center to detect distributed denial of service (DDoS) attacksmore precisely and for the E-voting station at the center of the voting station network so that it could observe more traffic to protect the system more precisely. The data set we used contains the attack instances of Dos, so that Dos attackscan be detected at the citizen data center where the E-voting centers request data for registration purposes. Similar models can be used to detect intrusions within the E-voting station network. Once the intrusion detection detects the intrusion, we can look into the counter-measures that we intend to address in the future.

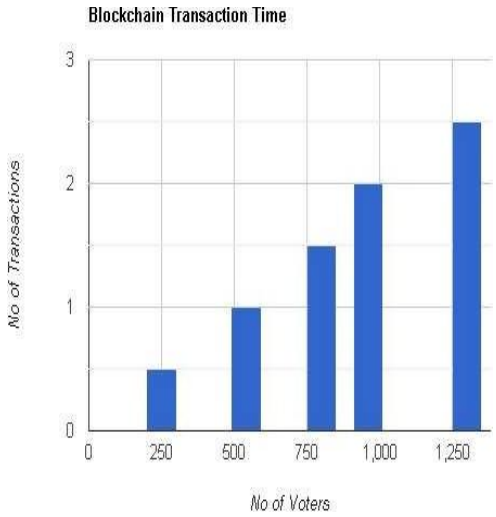


FIGURE 2: An Analysis of numbers of voters and Transactions

7. CONCLUTION

We put up an electronic voting system based on blockchain that satisfies all necessary criteria. The blockchain links each vote cryptographically, block by block. When two blocks have the same timestamp, the block with the highest signature value is chosen over the others. The voter has the option to select candidates from the list or any additional candidates they so choose. The voting process is typically open to the public, hence the results are not encrypted. The blockchain-based electronic voting system can be used for a range of elections and other purposes. Blockchain employsECC public key cryptography, despite the fact that it is a secure system. increased security when votes are cast throughencrypted channels. Low setup costs because voting simply requires the cost of an internet connectionWe used two machine learning models with a different set of settings. One is the Gaussian Vector Support Machine, and the other is the linear Vector Support Machine. A comparison is made between these two classifiers by measuring their accuracy and AUC (area under the curve). The idea of a smart contract is used to register voters and to receive votes as well. Where the Merkle root algorithm has been used to get the root hash to ensure the integrity of the data stored at the citizen's data centre. We believe

that this voting architecture can be extended as an I (internet voting) where users can vote through a secure application or secure web servers. We did not focus servers generating addresses for users that weuse to register and process blockchain that could be part of our future projects towards an efficient smart voting systemusing blockchain and machine learning. In addition, in the future, we will be able to look at the counter-measures of thevarious attacks once we have detected them.

REFERENCES

[1] Advances in Intelligent Systems and Computing, vol 1035. Springer, Cham. https://doi.org/10.1007/978-3-030-29035-1_54 Li, Y., Susilo, W., Yang, G., Yu, Y., Liu, D., Du, X., & Guizani, M. (2020).

[2] Michael Backes et al. “Ring Signatures: Logarithmic-Size, No Setup - from Standard Assumptions”. In: Advances in Cryptology - EUROCRYPT 2019. Vol. 11478.LNCS. Springer, 2019, pp. 281–311.

[3] Nikos Chondros et al. “Distributed, end-to-end verifi-able, and privacy-preserving internet voting systems”.In: Comput. Secur. 83 (2019), pp. 268–299. DOI: 10.1016/j.cose.2019.03.001. URL:https://doi.org/10.1016/j.cose.2019.03.001.

[4] Veronique Cortier, Pierrick Gaudry , and St´ephane´Glondu . “Belenios: A Simple Private and Verifiable Electronic Voting System”. In: Foundations of Security,Protocols, and Equational Reasoning - Essays Dedicated to Catherine A. Meadows. Vol. 11565. LNCS.Springer, 2019, pp. 214–238.

[5] K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019

[6] K. Garg, P. Saraswat, S. Bisht, S. K. Aggarwal, S. K. Kothuri and S. Gupta, "A Comparitive Analysis onE-Voting System Using Blockchain," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-4, doi: 10.1109/IoTSIU.2019.8777471

[7] Y. Zhang, Y. Li, L. Fang, P. Chen and X. Dong, "Privacy-protected Electronic Voting System Based on Blockchin and Trusted Execution Environment," 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 2019, pp. 1252-1257, doi: 10.1109/ICCC47050.2019.9064387

[8] T. M. Roopak and R. Sumathi, "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology," 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 2020, pp. 71-75, doi: 10.1109/ICIMIA48430.2020.9074942.

[9] J. Li, X. Wang, Z. Huang, L. Wang, and Y. Xiang, “Multi-level multi-secret sharing scheme fordecentralized e-voting in cloud computing,” Journal of Parallel and Distributed Computing, vol. 130, pp. 91- 97, 2019. [Online]. Available:http://www.sciencedirect.com/science/article/pii/S074373151930262X

[10] Y. Li, W. Susilo, G. Yang, Y. Yu, D. Liu, and M. Guizani, “A blockchainbased self-tallying voting scheme in decentralized iot,” arXiv preprint arXiv:1902.03710, 2019.

[11] S. Osken, E. N. Yildirim, G. Karatas, and L. Cuhaci, “Intrusion detection systems with deep learning: A systematic mapping study,” in Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT). IEEE, 2019

[12] Y. Li et al., “A Blockchain-based Self-tallying Voting Scheme in Decentralized IoT,” arXiv preprint., arXiv:1902.03710, 2019.

[13] Mukesh Soni, Dileep Kumar Singh, Blockchain-based security & privacy for biomedical and healthcare information exchange systems, Mater. Today: Proc., 2021, ISSN 2214-7853,https://doi.org/10.1016/j.matpr.2021.02.094.