Secure Electronic Voting System

Dr. Madhu Bhan
M.S.Ramaiah Institute of Technology, Bangalore India
Shubam Koundel
PG Student at M.S.Ramaiah Institute of Technology, Bangalore India

Abstract:

India conducts both state and federal elections using paperless electronic voting machines. Indian authorities have never allowed a meaningful, independent investigation of the security of the devices despite mounting fears of fraud. Blockchain is a technology that has gained a lot of attention recently because it uses an immutable distributed ledger to offer security and anonymity. In applications where trust is of the utmost significance, Blockchain is extensively used because of its reliable consensus mechanism and tamper-proof data storage. By combining all of the individually encrypted votes into one encrypted tally using the homomorphic property, you may obtain the separated-out tallies without compromising the privacy of individual votes. Homomorphic encryption methods are employed to work on the encrypted data without the knowledge of private key. If database data is lost, it may still be possible to recover it from the blockchain cloud. Data that has been encrypted can be operated on without having to first decrypt it. Data may be transferred and stored securely in cloud systems using Blockchain and Homomorphic mechanisms. In this paper we have explained the design, implementation and working of a dependable and trustworthy electronic voting application.

Keywords: Voting System, Blockchain, Homomorphic encryption, Security, Storage.

DOI Number: 10.14704/nq.2022.20.13.NQ88364 **Neuro Quantology 2022; 20(13):2924-2929**

1. Introduction

Due to inherent security concerns, many technologies are being used, however the current voting procedure has not been able to meet the integrity requirement of the voting system. The blockchain technology, which started to shine when Bitcoin entered the market and gained widespread support, has now become a popular idea in the modern software industry [1,2]. One of the significant industries that can be entirely safeguarded utilizing blockchain technology is electronic voting. The ideal alternative for electronic voting applications is blockchain technology since it is practical, scalable, and safe. Using the comparison of digital cash, the concept behind electronic voting using blockchain technology is presented in [3,4]. Votes can be casted as transactions, allowing us to build a blockchain that records vote totals. In this manner, everyone can concur on the final vote total since they can count the votes themselves and, thanks to the blockchain audit trail, which can confirm that no votes are altered, eliminated, or fraudulently added. Electronic voting is a complex and costly system [5,6]. In this paper, we describe a revolutionary election polling prototype that uses Internet connectivity, Blockchain storage, and homomorphic encryption. This system has two web-based apps, one for Election officers and the other for Booth managers and Users who are going to poll. The Election Officer will take on the role of administrator and will be responsible for configuration settings of election polling. Booth Managers are the local managers who are in charge of entering voter information into the system and who have access to a retrieval system that allows them to see voting results and contestant/candidate information. The ballots are transformed into encrypted data and kept on a blockchain.

2. Methodology

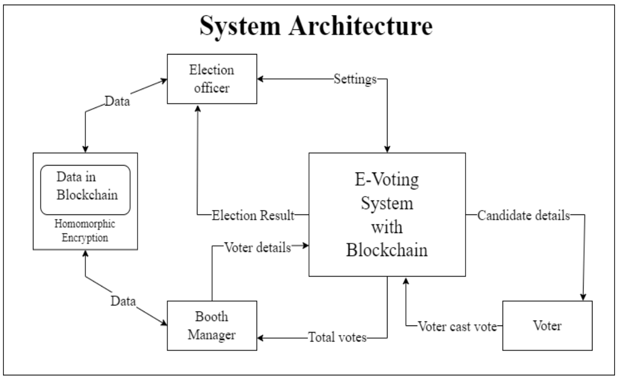

Figure 1: System Architecture

Figure 1 shows that there will be an Election Officer who will be able to see the election results as well as the votes casted against each candidate that has been registered. Also, he will be able to register new voters, Booth Managers and candidates. The Booth manager can open a voting window where the voter can enter his unique id like Aadhaar Number and cast a vote. The vote is then saved in the blockchain and data for candidates, voters and Booth Managers are stored in the MYSQL database [7,8].

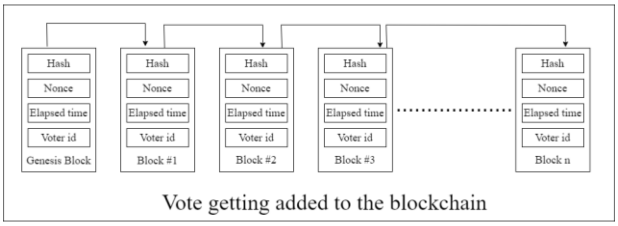

Figure 2: Structure Blockchain Architecture

Figure 2, shows the structure of a generated block in the Blockchain server when a voter clicks on the vote. First there will be a genesis block, a temporary block which is carrying a value 0. When a voter clicks on a vote button a new block is being added in the Blockchain server. Each block that is generated has a new hash value and a nonce which is a unique [9,10,12].

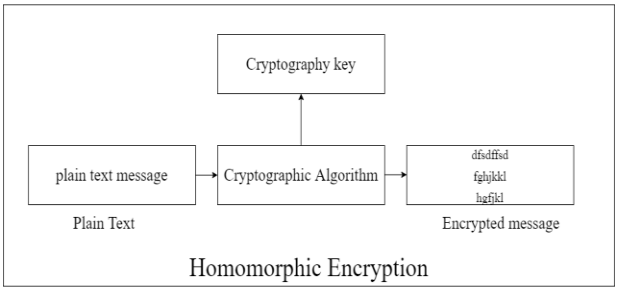

Figure 3: Homomorphic Encryption

Data is transformed into ciphertext via homomorphic encryption so that it can be analyzed and worked with as if it were still in its original format. Complex mathematical processes can be carried out on encrypted data without breaking the encryption. Because homomorphic encryption allows mathematical operations to be made directly on the encrypted data, it varies from conventional encryption techniques and can increase the security of third party's handling of user data. Homomorphic encryption is designed to create an encryption algorithm that enables an infinite number of additions to encrypted data[15]. There is a secret key present and it cannot be seen by a user each time voting is done and vote being added to blockchain. But when it comes to vote-count that is when counting of vote begins the homomorphic encryption is already in place. It has already encrypted the votes when voters were voting. On clicking the vote button, it creates an encrypted layer where votes are being kept safe and now when counting is done it decrypts it without the use of any public key as there is only one secret key which does this all work [11,14,]

3. Implementation

The implementation of the prototype has been carried out in a controlled environment [13]. The application is developed using pyhton language and its libraries, while the front end is developed using tkinter and in order to run the application in multiple systems we have used socket programming which allows us to run the application for multiple users at the same time. Haslib is another library which makes use of SHA algorithm and provides better security for the passwords. Libraries like Blockchain have also been used to create a blockchain architecture. Among other various number of libraries that are used, a module from Cryptography, Cryptography.fernet is used which is specific and relevant to homomorphic encryption. Platform requirements include Heidsql to see the database and windows operating system.

4. Working

This prototype has the following functionalities for the Election Officer. The Election officer can login to this application by entering his username and password for accessing the menu. Voter registration is made by entering voter details like voter ID, Aadhaar Number, Email ID and other details. Voter ID should be unique. Details are saved in MySQL database. Contestants/candidates are registered by Election officer. Each contestant/candidate is assigned with the pin code and party details. Election officer is responsible for assigning Booth Managers for different pin code. Booth manager is assigned with username and password to login to application. Election officer can get count of votes from Blockchain server for a specific pin code. Results are displayed in Election Officers window.

The functionalities for Booth Manager include logging to application using username and password provided by officer. Voting window automatically opens for pin code assigned by officer. In voting window voter can enter his voter ID and Aadhaar Number for voting. Voter will be validated if details are valid. Once voter details are validated, an OTP is generated and sent to voter's email ID. Voter has to enter OTP received in his mail. If voter enters wrong OTP in 3 attempts, voting is cancelled. Vote casted by the voter is encrypted for security reason before saving it in Blockchain server. Cryptography.fernet function is used for encrypting votes. Encrypted votes are sent to Blockchain server through socket. Once votes are saved in Blockchain, a reply is sent by Blockchain server. Booth manager can get count of all the votes casted from his polling booth. A request is sent to Blockchain server to get count. Blockchain server returns count of total votes. When the Election Officer sends request for count of votes for a given pin code, Blockchain server gets all the votes and finds count of votes for each candidate. Candidate details like name and party along with count of votes is sent back to officer as reply. All the votes saved in Blockchain are encrypted. Votes are decrypted by Blockchain server and counting is done.

Figure 4: Blockchain Server Running

Figure 4 shows that the Blockchain server is running before the voter is going to vote.

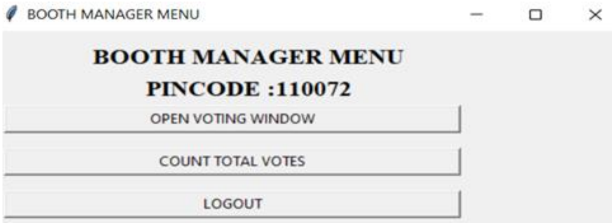

Figure 5: Booth Manager Menu

Figure 5 shows the Booth Manager menu and how the Booth Manager will open the voting window to vote. By clicking on the open voting window, the new page will open which is shown in the Figure 6.

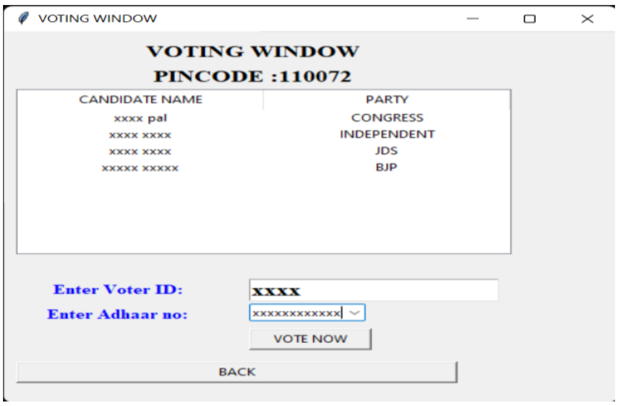

Figure 6: Booth Manager opens a voting window

Figure 6 shows all candidates and how a voter will select a candidate. Voter will enter his unique voter id and Aadhaar Number and then click on vote.

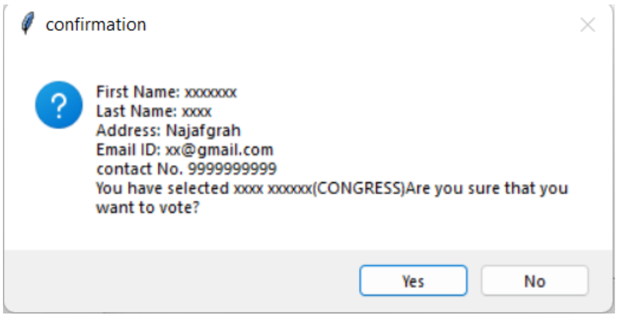

Figure 7: Confirm Voter Details

The system after verification of voter id displays the details of voter details as shown in Figure 7. The voter can now proceed and click on yes.

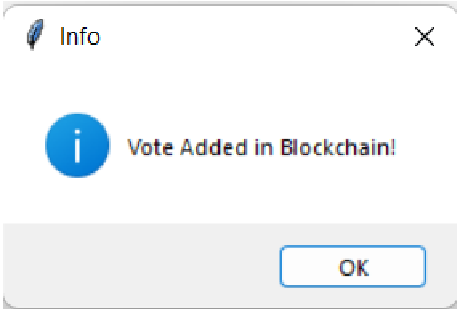

Figure 8 : Vote is in Blockchain

Figure 8 shows that the vote has been added to the Blockchain.

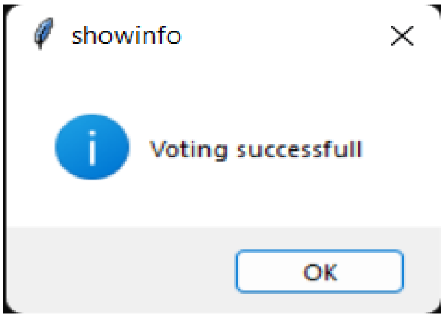

Figure 9 : Voting Successful

Figure 9 shows a pop up that indicates voting is successful.

Figure 10: New Block added in Blockchain

Figure 10 shows that the vote has been to the Blockchain. The hash of the block header that was mined needs to be less than the target. If it is higher, it will not be taken into account. Block size needs to be within reasonable bounds. A block generally can be of 2 MB in size. The block's timestamp must be less than two hours in future.

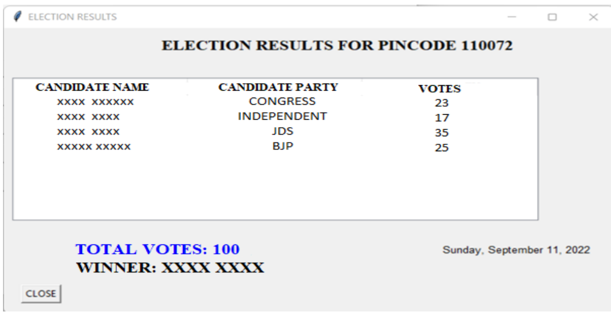

Figure 11: Overall results seen by Officer

Figure 11 shows the voting results which can be seen by the officer in the officer menu.

5. Conclusion and future enhancements

Many applications where security and transparency are crucial are favored by Blockchain technology. But the institutions in charge of holding elections have not extensively adopted it as a voting method. As stated in our application, we can develop a reliable Electronic Voting System that will change the way elections are conducted in the future if we combine blockchain technology with homomorphic encryption. Not only will it protect the data, but it will also increase voting process openness. Election costs will be reduced as it doesn't require any upkeep from a centralized body. Additionally, it will boost voter turnout, maintaining the democratic ideals of democracy. When data is kept in the cloud, homomorphic encryption will help to further improve the integrity of the data.

6. Future Enhancement

The creation of this prototype provided a wealth of knowledge about the current user and voting-based system, as well as its potential for improvement as time and technology advance. To create a suitable system, efforts have been made using the tools, resources, and approaches available today. Blockchain is growing and there are chances that by 2025 it will be used in major voting processes and other areas. This prototype has huge potential to grow and integrate additional features from Data Science and Machine Learning. The prototype can also become an android app. Features like real-time identity verification and dashboard can be further added for smooth and efficient working of the application.

References

1. Bela Shrimali, Hiren B. Patel. *Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities.* Journal of King Saud University - Computer and Information Sciences, 34(9), pp. 6793-6807, 2022. DOI: 10.1016/j.jksuci.2021.08.005
2. HuaqunGuo, XingjieYu. *A survey on blockchain technology and its security*. Blockchain: Research and Applications, 3(2), 2022. DOI: 10.1016/j.bcra.2022.100067
3. Francesco Fusco, Maria Ilaria Lunesu, Filippo Eros Pani, Andrea Pinna. *Crypto-voting, a Blockchain based e-Voting System*. In proceedings of 10th International Conference on Knowledge Management and Information Sharing. DOI: 10.5220/0006962102230227.
4. R. Hanifatunnisa and B. Rahardjo. *Blockchain based e-voting recording system design*. In proceedings of 11th International Conference on Telecommunication Systems Services and Applications (TSSA), pp. 1-6, 2017. DOI: 10.1109/TSSA.2017.8272896.
5. J. Thakkar, N. Patel, C. Patel and K. Shah. *Privacy-Preserving E-voting System through Blockchain Technology*. In proceedings of IEEE International Conference on Technology, Research and Innovation for Betterment of Society (TRIBES), pp. 1-6, 2021. DOI: 10.1109/TRIBES52498.2021.9751618.
6. K. Patidar and S. Jain. *Decentralized E-Voting Portal Using Blockchain*. In proceedings of 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1-4, 2019. DOI: 10.1109/ICCCNT45670.2019.8944820.
7. Y. Abuidris, A. Hassan, A. Hadabi and I. Elfadul. *Risks and Opportunities of Blockchain Based on E-Voting Systems.* In proceedings of 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, pp. 365-368, 2019. DOI: 10.1109/ICCWAMTIP47768.2019.9067529.
8. K. Teja, M. Shravani, C. Y. Simha and M. R. Kounte. *Secured voting through Blockchain technology*. In proceedings of 3rd International Conference on Trends in Electronics and Informatics (ICOEI), pp. 1416-1419, 2019. DOI: 10.1109/ICOEI.2019.8862743.
9. Uzma Jafar, Mohd Juzaiddin Ab Aziz, and Zarina Shukur. *Blockchain for Electronic Voting System—Review and Open Research Challenges.* Sensors 21(17), 5874, 2021 DOI: 10.3390/s21175874
10. Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan. *Secure Digital Voting System based on Blockchain Technology.* International Journal of Electronic Government Research 14(1), pp. 53-62, 2018. DOI: 10.4018/IJEGR.2018010103
11. Tannishk Sharma. *E-Voting using Homomorphic Encryption Scheme.* International Journal of Computer Applications 141(13), pp. 14-16. DOI: 10.5120/ijca2016909652
12. B. K. Nirupama and M. N, "Network Intrusion Detection using Decision Tree and Random Forest," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), 2022, pp. 1-9, doi: 10.1109/ACCAI53970.2022.9752578.
13. Saad Moin Khan, Aansa Arshad, Gazala Mushtaq, Aqeel Khalique and Tarek Husein, *Implementation of Decentralized Blockchain E-voting.* EAI Endorsed Transactions on Smart Cities 4(10):164859, 2018. DOI: 10.4108/eai.13-7-2018.164859.
14. K. R. Swetha, N. M, A. M. P and M. Y. M, "Prediction of Pneumonia Using Big Data, Deep Learning and Machine Learning Techniques," 2021 6th International Conference on Communication and Electronics Systems (ICCES), 2021, pp. 1697-1700, doi: 10.1109/ICCES51350.2021.9489188.

15. R, Raghavendra; M, Dr. N -"Web Information Extraction methods using Web Content Mining (WCM) for Web Applications" International Journal of Computing and Digital Systems, ISSN: 2210-142X 2022, 11(1), pp. 609–623 DOI: https://dx.doi.org/10.12785/ijcds/110149