E-Voting System Using Blockchain and Homomorphic Encryption

P Ramesh Naidu[1]
Department of CSE,
Nitte Meenakshi Institute of Technology, Yelahanka
Bangalore, India
ramesh.naidu@nmit.ac.in

Dileep Reddy Bolla
Department of CSE,
Nitte Meenakshi Institute of Technology, Yelahanka
Bangalore, India
dileep.bolla@gmail.com

Prateek G
Department of CSE,
Nitte Meenakshi Institute of Technology, Yelahanka
Bangalore, India
prateek.giridhar2000@gmail.com

Shreya A Hegde
Department of CSE,
Nitte Meenakshi Institute of Technology, Yelahanka
Bangalore, India
shreyahegde294@gmail.com

Sheetal S Harshini
Department of CSE,
Nitte Meenakshi Institute of Technology, Yelahanka
Bangalore, India
sheetalharshini09@gmail.com

Vallamkonda Venkata Sree Harsha
Department of CSE,
Nitte Meenakshi Institute of Technology, Yelahanka
Bangalore, India
harshavallamkonda@gmail.com

***Abstract*—Only about half of the elections are deemed to be free and fair, according to a study. Electoral fraud not just mutilates the nature of portrayal, but also has an impact on political, social, and monetary outcomes. A cutting-edge technology like blockchain can be utilized to ensure free and fair elections, and homomorphic encryption can be used to maintain data security. In this paper, we aim to allow only the eligible citizens to vote by automatically checking their eligibility status from a federally approved application. The , and the vote cast by the voter, is stored onto the blockchain. By doing this, statistical analysis can be performed on encrypted data without revealing voter identity and vote cast, which results in a unique set of insights that may otherwise remain unknown. The proposed system uses Ganache as the local blockchain, the vote cast related data is stored on the blockchain and the voter's data gets encrypted using the Paillier cryptosystem.**

Keywords— Security, Hashing, Blockchain, Privacy, Homomorphic Encryption, E-Voting, Ganache, Immutability.

I. Introduction

The right to vote is a constitutionally protected right that all citizens are granted, and it is the foundation of democracy [1]. A democracy is a popular form of government, i.e., popular sovereignty but limited by a constitution that guarantees individual freedoms (such as speech) and rights (such as a fair trial). However, through research, as per research conducted in [2] it has been found that only about half the elections are free and fair. Election record contorts portrayal quality, yet additionally affects political, social, and financial outcomes according to [3]. The drawbacks of the conventional voting systems include security threats, lack of transparency, centralization of authority and general difficulties faced by citizens to cast a vote [4]. To overcome these drawbacks, an electronic voting system could be introduced. The main aim of this paper is to propose a system that helps in conducting free and fair elections using cutting-edge technology. To achieve this, a federally approved E-voting application that only allow eligible voters to cast their vote. Homomorphic encryption is then used in securing the voter's data, statistical analysis can be performed on this encrypted data, which results in a unique set of insights that may otherwise remain unknown.

Blockchain is a conveyed record of data that is often used for keeping a tamper – proof system. The immutability of the records that have already been written in blocks is the fundamental principle of the blockchain. Chaining of blocks provides data integrity, which is ensured by advanced encryption. The type of network connectivity is another feature, client-client communication is the method used by network nodes. The genuine identity of the network user is maintained as unknown [5].

Decentralization, digitization, and consensus-based secure information storage mechanism which is perfect for the e-voting system according to [6]. As per [7], the main requirements of E-Voting are Privacy, Eligibility, Receipt Freeness, Convenience, and Verifiability. In [8], a secure system using Paillier Algorithm is proposed which uses non-deterministic property of the algorithm, this property is essential and being used in our proposed system.

Before adding transactions to the chain, the blockchain network verifies and validates them using consensus. The blockchain can be isolated into Public Blockchain and Private Blockchain, relying upon the kind of agreement instrument used. Any member node in a public blockchain can validate and contribute transactions. Bitcoin is a well-known example of this. Only a select few nodes are allowed to validate transactions on a private blockchain. There are four commonly used consensus algorithms that are ordinarily utilized in the blockchain. They are:

- Proof of work
- Practical Byzantine Fault Tolerant Algorithm
- Proof of stake
- Delegated proof of stake

II. Background work

We should be able to cast ballots, protect them, and have them counted on election day using an Electronic Voting Machine (EVM). Electronic voting devices that store the results are utilized in traditional EVM, there is no web association. To acquire the absolute number of votes cast for the competitor, the stall director should physically peruse the outcomes from each EVM and add them. Computers that are networked will be employed in certain other systems. It might be the internet or a local network. Data should be transferred carefully throughout the network to prevent vote tampering. Data must be encrypted before being transferred over a network using secure channels like SSL/TLS.

Through research conducted in [2], it has been found that approximately half the elections are free and fair. Electoral fraud not only affects the quality of representation, but it also has a negative impact on the economy, political, social effects. The major vulnerabilities faced by the voters as per [9][10] are:

- Validity of voters
- The integrity of the ballot
- Secure transmission of the ballot
- Transparency
- Centralized System
- Possibility to tamper with the databases.

Further, based on extensive research, in [11] it describes that blockchain technology when infused with various other technologies, as an instance of supply chain blockchain can be leveraged to perform better in a distributed manner to enhance the automation of process. For real world related applications, the existing testbed is extended by using the simulation models in blockchain [12][13]. Finally, based on the current research status, a secure model for medical and internet-based applications is feasible by fusing IoT (Internet of Things) and Blockchain is demonstrated in [14]. When homomorphic encryption integrated with a few specific blockchain concepts like Zero-Knowledge Proofs can help with maintaining security and privacy at the same time [15]. Furthermore, to enhance the security, protocol – based approach is more secure and an effective voting mechanism can be simulated [16]. Multi-add structure is implemented to support some real value inputs, exists in many of the prominent protocols [17].

III. System Design

The blockchain-based electronic voting system proposed in this paper can be used for all state and federal level elections to elect the representatives of the people. This system uses a consortium blockchain to store the votes cast by the citizens. There are two main roles in the proposed system: administrator and the voter. The voter details are included in the smart contract. The architecture contains the following components: blockchain, EPIC (Electronic Photo Identity Card) ID, poll creation interface, voting interface and results interface. The smart contract is used to process and evaluate the votes cast by the voters.

A. Admin Process

The administrator can access the admin options by logging into the system using the designated admin email and password. The admin functions are illustrated in Figure 1, upon successful verification and authentication of the administrator, the administrator can create a poll, declare the election results constituency wise and declare the overall election results in the admin options page. The admin can also encrypt the voter's data using Homomorphic encryption and export the data for statistical analysis.

B. Proposed Voter Process

The eligible voter logs into the system by entering his Name (as per VoterId), VoterId and Phone Number (linked with the VoterId). The system will verify the details and an OTP is sent to the registered phone number to authenticate the voter. Further, upon verification of the OTP the voter is authenticated and redirected to the voting page according to the voter's constituency, the voting page, would display registered candidates of the parties participating in the election of that constituency.

After the successfully voting of the voter, these details and information get stored into the blockchain and the vote gets successfully recorded. The security of voting process is based on blockchain technology, the vote of each voter is considered as a transaction inside the blockchain and the data inside the backend of the database as in Fig.1. To make sure the person is voting only once, the web application will notify that the voter has already voted and needs to wait for the next eligible election. Once the voting process is completed, the voter will be logged out and cannot log in to the voting page. This mechanism is present as a static security feature present in the application to preclude any possibility of a duplicate voting.

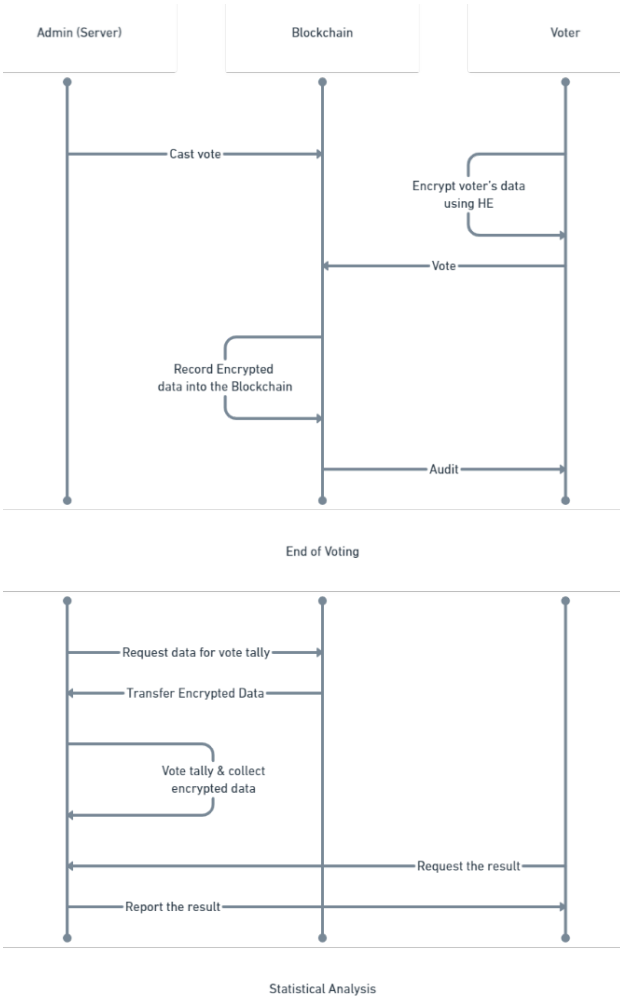

Fig.1: Sequence Diagram of proposed e-voting system

C. Homomorphic Encryption

Homomorphic Encryption in basic terms is that you can perform arithmetic operations on encrypted data, this feature helps perform statistical analysis without revealing voter data. The Paillier algorithm is used to encrypt the voter data along with the vote cast that was recorded on the blockchain, this encrypted data can be provided to the companies that perform statistical analysis. The arithmetic operations that are supported for performing statistical analysis are addition and multiplication.

D. Paillier Algorithm

1) Key Generation Process

Step 1: *Consider any two prime numbers p and q of equal size and independent of one other, where* $gcd(pq, (p-1)(q-1)) = 1$. *Both the primes are to be of the same length.*

Step 2: *Calculate* $n = pq \; and \; \lambda = lcm\,(p-1,\, q-1)$ *where* ***lcm*** *is the Least Common Multiple function.*

Step 3: *Pick random integer g where* $g \in \mathbb{Z}^{*}_{n^2}$

Step 4: *Ensure that n divides the order of g by checking if the modular multiplicative inverse is present:* $\mu = (L(g^{\lambda} \bmod n^2))^{-1}$ *mod n where function L is defined as* $L(x) = (x-1)/n$.

- ***Key (Public) is*** $(n,\, g)$ ***used for encryption.***
- ***Key (Private) is*** $(\lambda,\, \mu)$ ***used for decryption.***

2) Encryption Process

Step 1: *Suppose m is the message to be encrypted where* $0 \leq m < n$

Step 2: *Select random r where* $0 < r < n$.

Step 3: *Calculate ciphertext as:* $c = g^{m} r^{n} \bmod n^2$

3) Decryption Process

Step 1: *Suppose c be a ciphertext to decrypt, where* $c \in \mathbb{Z}^{*}_{n^2}$.

Step 2: *Compute the plaintext message as:*

$$m = L\left(c^{\lambda} \bmod n^2\right) . \mu \bmod n$$

IV. Evaluation and Results

To evaluate the application performance and developed system's efficiency, six test constituencies were created where citizens can vote to elect their representatives. The general objective was to test the speed, security, and usefulness of the proposed framework. The testing was conducted on Windows and Linux based operating systems, on Chrome Web Browser with JavaScript enabled and the Metamask plugin installed. The Metamask plugin provides a simple interface to interact with the local Ethereum network, which is used for testing the system. The local Ethereum test network was created using Ganache, and Ropsten test network helped create a real-time Ethereum test network.

A. System Specifications

The application was tested on a Linux-based system running Ubuntu operating system, the programming languages used are solidity and JavaScript for the developing the smart contracts and web application respectively. Ganache, a truffle framework-based tool, was used to simulate a local blockchain. The hardware specifications used to develop this project are:

- Processor: Intel i3
- Ram: 4 GB

B. Observations in Results

There are many observations that can be considered, whether it is the performance of encryption of the data or time taken for voting process in different blockchain test environments. A table is recorded for both, Table I is the time taken for the encryption of voter details varying based on the number of voter details being encrypted.

TABLE I: Time taken for Voter Details being Encrypted

Number of Voters	Time Taken (in ms)
1	1.25
5	3.76
10	8.6
15	12.35

Table II is the time taken for 3 epochs of automated voting of 5 votes every second in two different environments, namely Ganache for local simulation and Ropsten Test Network to simulate a live Ethereum-based network environment.

TABLE II: Time taken for a complete voting process in different simulated environments

Epochs (5 votes per second)	Time (in Seconds)	
	Ganache (Local)	Ropsten (Live)
1	7.02	15.56
2	6.98	15.3
3	7.2	16.21

The home page gives a brief introduction to the users of the benefit of using the application to cast the vote during the elections. The creation of a new poll functionality allows the admin to create and add a new constituency for which elections are to be conducted. The form accepts the candidate details for the particular constituency.

The voter is required to have a device which is connected to the internet to cast the vote. The voter can cast their vote through the Dapp, which is the website and the wallet account provide by the government. The voter is provided with a public and private key of an account of the registered user, the voting percentages in the cities is way less compared to rural and suburban areas of a locality. The other major issue with this existing system is rigging and coercion at the place of voting, which makes the system of voting not so secure and lessen the freedom of choice. To solve some of these problems there is a one-stop solution that is online voting system and supplementing it with blockchain makes the process to be carried out in a secured way. With the system of E-voting, voters neither need to worry about getting stuck in a long queue and waste their time to exercise their fundamental right nor get worked up about poll riggings and other malign

methods of coercion. They can sit at their place of comfort and cast their vote to the candidate of their choice. They just need a mobile phone or a computer having access to a wallet containing their voting account and a connection to the internet.

V. Conclusion

Online voting systems, in our opinion, have a security flaw that allows authority to commit fraud or manipulate the system in ways that are difficult to detect by other users. The various issues uncovered in these early attempts at online voting can be solved using blockchain. Homomorphic encryption now provides an irrefutable method of ensuring the correctness of each vote cast. Blockchain technology is one of the most secure ways to store the information. By opting for a decentralized method over a centralized and traditional voting system, the On – Stream voting system is made more secure. This implies that by switching from a centralized database to a peer network of blockchain that store data, the data/votes are safe and cannot be tampered with since the data in the blocks is immutable. It even assures that the election rules do not change because they are kept as a Smart Contract of the blockchain, so because of this online e voting system using blockchain will be very helpful towards the society. It will also be useful to the people as they can conveniently cast their vote from their place of comfort, they just require a mobile (or) a laptop which is connected to internet. And even for government, numerous resources and manpower will be saved because the officials of the Election Commission can be at one place. They can take a count of the number of votes of the particular region with more accuracy so that there will be no overhead in the voting process.

References

[1] S. Bishop and A. Hoeffler, “Free and fair elections: A new database,” Journal of Peace Research, vol. 53, no. 4, pp. 608–616, 2016, doi: 10.1177/0022343316642508.

[2] R. Hanifatunnisa and B. Rahardjo, “Blockchain-based e-voting recording system design” 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), 2017, pp. 1-6, doi: 10.1109/TSSA.2017.8272896.

[3] L. Carter and F. Bélanger, “Internet Voting and Political Participation: An Empirical Comparison of Technological and Political Factors,” SIGMIS Database, vol. 43, no. 3, pp. 26–46, Aug. 2012, doi: 10.1145/2351848.2351851.

[4] W. Tan, H. Zhu, J. Tan, Y. Zhao, L. D. Xu, and K. Guo, “A novel service-level agreement model using blockchain and smart contract for cloud manufacturing in industry 4.0,” Enterprise Information Systems (EIS), vol., no., pp. 1–26, 2021, doi: 10.1080/17517575.2021.1939426.

[5] K. M. Khan, J. Arshad, and M. M. Khan, “Secure digital voting system based on blockchain technology,” Int. J. of Electron. Gov. Res. (IJEGR), vol. 14, no. 1, pp. 53–62, 2018, doi: 10.4018/IJEGR.2018010103

[6] S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran and N. Guizani, “Securing Smart Cities through Blockchain Technology:Architecture, Requirements, and Challenges,” in IEEE Network, vol.34, no.1, pp. 8-14, January/February 2020, doi: 10.1109/MNET.001.1900178.

[7] H. Kim, K. E. Kim, S. Park, and J. Sohn, “E-voting system using homomorphic encryption and blockchain technology to encrypt voter data,” arXiv [cs.CR], 2021, doi: 10.48550/arXiv.2111.05096

[8] N. Kakade and U. Patel, “Secure Secret Sharing Using Homomorphic Encryption,” 2020 11th International Conference on Computing, Communication, and Networking Technologies (ICCCNT), 2020, pp. 1-7, doi: 10.1109/ICCCNT49239.2020.9225325.

[9] X. Li, H. Lee, M. Lee, and J. Choi, “A Study of Vulnerabilities in E-Voting System,” Advanced Science and Technology Letters Vol.95 (CIA 2015), May 2015, pp. 136–139. doi: 10.14257/astl.2015.95.25.

[10] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, “Blockchain-Based E-Voting System,” 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151.

[11] S. E. Chang and Y. Chen, “When Blockchain Meets Supply Chain: A Systematic Literature Review on Current Development and Potential Applications,” in IEEE Access, vol. 8, pp. 62478-62494, 2020, doi: 10.1109/ACCESS.2020.2983601.

[12] Z. Chen, S. Chen, H. Xu and B. Hu, “A Security Authentication Scheme of 5G Ultra-Dense Network Based on Block Chain,” in IEEE Access, vol. 6, pp. 55372-55379, 2018, doi: 10.1109/ACCESS.2018.2871642.

[13] H. Ewen, L. Mönch, H. Ehm, T. Ponsignon, J. W. Fowler and L. Forstner, “A Testbed for Simulating Semiconductor Supply Chains,” in IEEE Transactions on Semiconductor Manufacturing, vol. 30, no. 3, pp. 293-305, Aug. 2017, doi: 10.1109/TSM.2017.2713775.

[14] J. Indumathi et al., “Block Chain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User-Friendly, Unflappable, Unblemished, Unlimited Health Care Services (BC IoMT U6 HCS),” in IEEE Access, vol. 8, pp. 216856-216872, 2020, doi: 10.1109/ACCESS.2020.3040240.

[15] T. Nguyen and M. T. Thai, “zVote: A Blockchain-based Privacy-preserving Platform for Remote E-voting,” ICC 2022 – IEEE International Conference on Communications, 2022, pp. 4745-4750, doi: 10.1109/ICC45855.2022.9838690.

[16] X. Yang, X. Yi and A. Kelarev, “Secure Ranked Choice Online Voting System via Intel SGX and Blockchain,” 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2021, pp. 139-146, doi: 10.1109/TrustCom53373.2021.00036.

[17] C. -z. Gao, J. Li, S. Xia, K. -K. R. Choo, W. Lou and C. Dong, “MAS-Encryption and its Applications in Privacy-Preserving Classifiers,” in IEEE Transactions on Knowledge and Data Engineering, vol. 34, no. 5, pp. 2306-2323, 1 May 2022, doi: 10.1109/TKDE.2020.3009221.