International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

E-VOTING SYSTEM USING BLOCKCHAIN TECHNOLOGY AND SEMI-HOMOMORPHIC ENCRYPTION

I. Kavitha C S[1], Ruchitha S[2], Sagar M J[3], Shoban Kumar C M[4], Vishwas Reddy S[5]

[1]Associate Professor, Department of Information Science and Engineering, MVJ College of Engineering, Bangalore, Karnataka, India.
[2,3,4,5]Undergraduate Scholar, Department of Information Science and Engineering, MVJ College of Engineering, Bangalore, Karnataka, India.

ABSTRACT :

Voting represents a crucial element of any democratic society, but conventional systems frequently encounter challenges such as inefficiency, human error, and transparency issues that ultimately undermine credibility. Our goal was to develop a demonstration of an electronic voting system that utilizes blockchain technology along with homomorphic encryption to overcome these challenges. The proposed system aims to enhance the transparency, reliability, and effectiveness of electoral processes in order to rebuild trust. Blockchain technology enables a transparent record and an efficient database, leading to the effective execution of public elections and instilling trust in the accuracy of the results. Homomorphic encryption ensures secure voting by using encrypted data calculations, addressing worries about voter confidentiality. This approach also guarantees maximum privacy for individual votes, ultimately reducing costs as physical ballots or polling stations are no longer necessary for elections.

Keywords: E-voting system, Blockchain technology and Semi-Homomorphic encryption

Introduction :

The act of voting is fundamental to democracy and serves as the foundation for how a country is governed. As technology continues to advance and influence the younger population, there is an urgent need to update the traditional voting methods. The existing electoral system has faced numerous issues, making it essential to introduce technological innovations to improve the current process. Conventional voting systems like paper ballots are susceptible to human errors and can be quite time-consuming. Electronic voting is being highlighted for its potential to lower costs and ensure the integrity of the electoral process through privacy, security, and compliance. Manual ballot counting can be burdensome and prone to errors, impacting election outcomes.

Electronic voting systems offer a more efficient and accurate way of casting and tallying votes, reducing errors and enhancing transparency in the process. However, concerns about transparency with current electronic voting methods persist. Furthermore, ensuring authenticity in the government's execution of vote recounting presents challenges in guaranteeing a credible electoral process for voters due to lack of external influence oversight. Blockchain technology provides a promising solution to the transparency issue in electronic voting. Utilizing blockchain has the potential to offer clear and verifiable documentation of the electoral process, enhancing its integrity and credibility. Implementing blockchain-based electronic voting systems can help assure voters of the fairness of the electoral process, leading to a more transparent and reliable democratic system. Semi-homomorphic encryption is a cryptographic approach that enables computations to be performed on encrypted data without the need for decryption.

It plays an important role in electronic voting (e-voting) technology, where maintaining privacy and security are crucial considerations. In e-voting systems that make use of blockchain technology, homomorphic encryption can be utilized to safeguard the confidentiality of votes while still allowing specific computations to be carried out on the encrypted data. The integration of Semi-homomorphic encryption and blockchain technology can establish a secure and transparent platform for electronic voting systems to conduct electoral processes.

2. Literature Review :

The preliminary study conducted prior to this research provides an understanding of the concept of blockchain technology, as well as the distribution of publications on relevant topics. The analysis shows that there is a lack of comprehensive coverage on certain subjects: blockchain as a managerial innovation, smart contracts, business models, entrepreneurial opportunities and challenges, and blockchain as a universally beneficial technology. The authors further note that the existing literature predominantly focuses on potential benefits of the innovation with limited discussion on how it can add value within organizations. While much attention is given to potential use cases if blockchain becomes widely adopted, there is insufficient exploration into value creation processes related to blockchain. We should instead explore reasons for employing blockchain technology to address issues and what value it brings to the organizations using it. The entrepreneurial aspect of blockchain presents a developmental challenge similar to that in new development economics; requiring coordination beyond just monetary value over complementary uses and opportunities.

System Architecture

The architectural framework proposed in Figure 3.1 consists of three essential modules: the Election Officer, the Booth Manager, and the Voters. The Election Officer module is responsible for integrating candidate details, managing booth managers, allocating booths, and verifying election outcomes. The Booth Manager module authenticates voter information during the voting process. Each voter is assigned a specific identification number that allows them to log in to the voting system using a One Time Password and cast their vote for their chosen candidate.

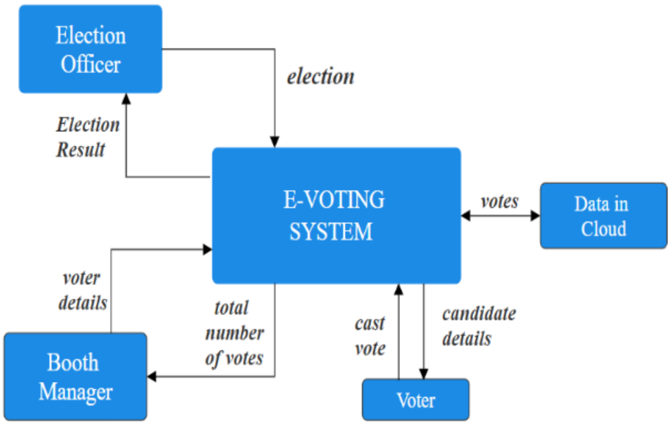

Figure 3.1 System Architecture

Methodology

The Paillier cryptosystem uses a specific methodology, involving key generation, encryption, addition, and decryption. Key generation starts with choosing the key bit length and certainty value. Then large prime numbers are retrieved to calculate the modulus and its square. A generator value is assigned, followed by determining the lambda value using a formula with the prime numbers. The adequacy of the generator is then confirmed. Encryption involves applying a specific formula to create ciphertext from plaintext message and random value. Homomorphic addition of ciphertexts is enabled through this process where decryption factor and plaintext sum are computed together. Decryption finally recovers initial plain text from encrypted text leading to secure communication while preserving homomorphic properties inherent in the Paillier cryptosystem.

4.1 Method for Key generation.

This method is used for generating a public-private key pair for the Paillier cryptosystem, which is a public-key cryptosystem used for encrypting and decrypting data.

4.2 Method for Paillier Encryption.

he Paillier encryption system is a cryptographic technique that provides homomorphic features, allowing computations to be conducted on encrypted data without the need for decryption. This method involves encrypting data with a randomly selected integer and a public key to generate ciphertext. Decryption of the ciphertext can only occur using the corresponding private key.

4.3 Method for Paillier Addition which is used for viewing total votes.

This technique is used to conduct homomorphic addition on two encrypted messages within the Paillier cryptosystem. Homomorphic addition enables the combining of two ciphertexts without the need for decryption beforehand.

4.4 Method for Paillier Decryption.

This approach is used to decrypt a given ciphertext in the Paillier cryptographic system. The decryption algorithm takes an input ciphertext c and produces the corresponding decrypted plaintext message.

Implementation

The incorporation of blockchain technology, Advanced Encryption Standard, and homomorphic encryption in the development of an electronic voting (e-voting) system creates a secure and transparent platform for conducting elections. This assures the integrity of the voting process while also safeguarding voter privacy. The fundamental concept behind this design relies on integrating blockchain technology, which functions as a persistent and decentralized record composed of interconnected blocks. Each block contains an encrypted set of votes, ensuring that once a vote is recorded on the blockchain, it remains unchangeable and resistant to tampering, thereby upholding the credibility of election results. The inclusion of Advanced Encryption Standard encryption in the ballot provides an additional layer of security, making it challenging for unauthorized entities to manipulate or access vote data. AES is used as a robust encryption algorithm to ensure both confidentiality and accuracy in voting processes. By applying AES encryption to the ballot, the system incorporates an extra level of security that makes it tough for unauthorized entities to alter or gain access to vote data. By the use of homomorphic encryption helps maintain voter confidentiality by enabling mathematical operations to be performed on encrypted data without the need for decryption. This cryptographic method allows mathematical operations to be carried out on encrypted data without requiring decryption. When applied in an e-voting system, this feature enables the combination of encrypted votes on the blockchain while preserving the secrecy of individual votes. The combined AES and homomorphic encryption-secured vote is then transformed into a block. This approach ensures that the votes remain confidential and secure as voters' actual preferences are not revealed. The electoral process begins with an Election officer initiating the election, giving eligible voters access to the voting interface. Voter legitimacy is verified using an authentication process incorporating a One-Time Password mechanism. After accessing the voting interface successfully, voters are prompted for their credentials, typically including a unique identification number.

Afterwards, the system verifies the initial credentials and generates a unique OTP. This OTP is then sent to the voter's registered mobile number and email address for validation. Only individuals with valid credentials and access to the registered contact information are allowed to proceed with voting. Upon receiving the OTP on their mobile device and in their email inbox, voters enter it into the specified field within the voting interface. The system validates this input by comparing it against the earlier generated OTP. If they match, indicating successful authentication, the voter is authorized to vote. Booth managers play a vital role in managing the voting process by adding voters to their respective booths and monitoring total votes cast within their designated areas. This empowers them to ensure accurate and legitimate conduct of the voting process; however, due to encryption and privacy-preservation measures, the specific details of votes or which candidate garnered more votes remain undisclosed to booth managers.

Evaluation and Result

The graphs illustrate a comparative examination of the time taken for encryption and decryption using three prominent encryption techniques: RSA, ElGamal, and Paillier. The horizontal axis represents the number of blocks, while the vertical axis indicates the duration of execution in seconds.

After examining the graph illustrating encryption time in Figure 6.1, it is clear that the Paillier encryption algorithm consistently performs better than the other two methods in terms of encryption time. As the number of blocks increases, the Paillier encryption method demonstrates exceptional efficiency, with encryption time remaining relatively stable and minimal. This efficiency is particularly beneficial in situations where numerous blocks need to be encrypted quickly and securely. In contrast, the ElGamal encryption algorithm shows slightly higher encryption times than the Paillier method but still outperforms RSA. As the number of blocks increases, ElGamal's encryption time gradually rises, indicating a linear relationship. Although not as efficient as the Paillier method, ElGamal remains a viable option for scenarios involving a moderate number of blocks.

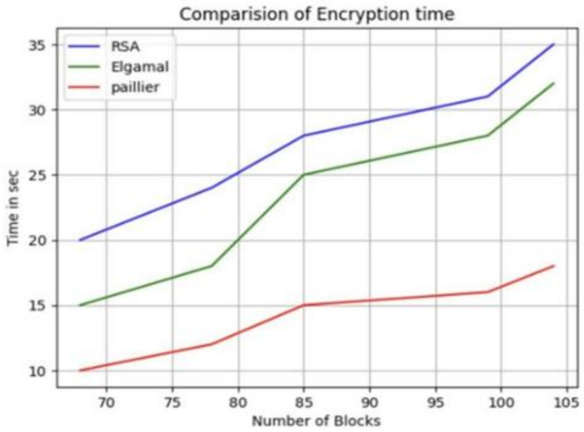

Figure 6.1 Encryption time

In terms of decryption time, Figure 6.2 illustrates that the Paillier encryption algorithm stands out as the most efficient once again. The decryption time for Paillier remains consistently low across all numbers of blocks, highlighting its suitability for quick and secure decryption processes. ElGamal shows similar performance with slightly higher decryption times than Paillier, but significantly lower than RSA. In contrast, RSA encryption exhibits the highest encryption and decryption times among the three algorithms, especially for a larger number of blocks. As the number of blocks increases, RSA encryption and decryption times experience a notable increase, making it less favourable for applications requiring fast processing or real-time operations. The graph results indicate that the Paillier encryption algorithm is best suited for achieving efficient encryption and decryption processes. The graphs provided demonstrate a comparative analysis of the encryption and decryption times of three prominent methods: RSA, ElGamal, and Paillier. The x-axis represents block quantity while the y-axis indicates execution duration in seconds.

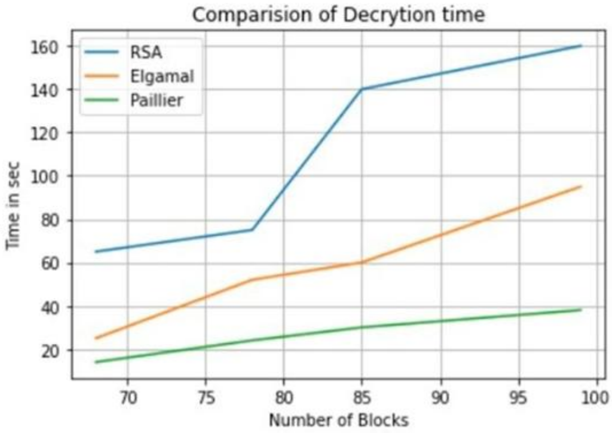

Figure 6.2 Decryption Time

Conclusion

This advanced method builds trust and confidence in the electoral process, addressing concerns about tampering and privacy violations. By combining these technologies, a secure environment is established to ensure the integrity, authenticity, and confidentiality of election results. The use of blockchain technology and Semi-homomorphic encryption enables secure result analysis while safeguarding voter privacy and system transparency. Precise statistical calculations can be carried out without revealing individual voting preferences. The integration of AES, Semi-homomorphic encryption, and blockchain technology in e-voting systems creates a strong environment that ensures the confidentiality, authenticity, and integrity of election outcomes—instilling trust in the electoral process. Despite challenges faced with scalability, efforts towards creating secure implementations will significantly promote widespread adoption of blockchain-based e-voting systems and foster trustworthiness, integrity, and fairness in democratic processes. For future implementation we can add facial recognition using artificial intelligence, fingerprint recognition.

REFERENCES :

[1] “Blockchain Technology and Cryptocurrencies” by Siddharth Rajput, Archana Singh, Smiti Khurana, Tushar Bansal, Sanyukta Shreshtha IEEE 2019.

[2] “Application of Blockchain for the Security of Decentralized Cloud Computing” by Nazmun Nahar, Farah Hasin and Kazi Abu Taher IEEE 2021.

[3] “A Homomorphic Encryption Approach in a Voting System in a Distributed Architecture” by Segundo Moisés Toapanta Toapanta , Luis José Chávez Chalén , Javier Gonzalo Ortiz Rojas , Luis Enrique Mafla Gallegos 2020 IEEE.

[4] “Secure Remote E-Voting using Blockchain” by Divya Rathore, Virender Ranga IEEE 2021.

[5] “A Blockchain-Based Authentication Method with One-Time Password” by Mingli Zhang, Liming Wang, Jing Yang IEEE 2019.