ISSN: 2456-8503

International Journal for Development of Science and Technology (IJDST)

Homomorphic encryption electronic voting system

RESEARCH

Iswarya[1], Monisha[1], Praveena[1], Senthil Prakash[1]*

Abstract

This paper presents a secure and privacy-preserving electronic voting system using homomorphic encryption. In traditional electronic voting systems, ensuring data security, voter anonymity, and result integrity remains a major challenge. The proposed system addresses these issues by encrypting votes at the time of casting and allowing computations to be performed directly on encrypted data without decryption. Homomorphic encryption ensures that sensitive information is never exposed during processing, thereby enhancing security and privacy. The system also prevents vote tampering, unauthorized access, and data manipulation. This approach provides a transparent, efficient, and reliable voting mechanism suitable for modern digital elections. The proposed model ensures accuracy, confidentiality, and trust in the electoral process.

Keywords: *Homomorphic encryption, electronic voting, security, privacy, cryptography.*

1. Introduction

Electronic voting systems have become an essential component of modern democratic processes. They provide faster vote counting and improved accessibility compared to traditional paper-based systems. This paper presents a secure and privacy-preserving electronic voting system using homomorphic encryption [1]. Traditional electronic voting systems face challenges in ensuring data security, voter anonymity, and result integrity. The proposed system encrypts votes during casting and allows computation on encrypted data without decryption.

To overcome these limitations, homomorphic encryption has emerged as a promising solution. It allows computations to be performed on encrypted data without revealing the original information. By applying this concept to electronic voting, it is possible to ensure that votes remain confidential throughout the entire process while still enabling accurate result computation. This paper proposes a secure electronic voting system that leverages homomorphic encryption to enhance privacy, transparency, and trust in digital elections.

2. Background and related work

2.1. Homomorphic Encryption

Homomorphic encryption allows operations to be performed on encrypted data without decryption [2]. This makes it suitable for secure applications like electronic voting. It reduces the risk of data leakage and ensures privacy during processing.

[1]Department of Computer Science and Engineering, Shree Venkateswara Hi-Tech Engineering College (Autonomous), Tamilnadu, India.

[2]Department of Computer Science and Engineering, Shree Venkateswara Hi-Tech Engineering College (Autonomous), Tamilnadu, India.

[3]Department of Computer Science and Engineering, Shree Venkateswara Hi-Tech Engineering College (Autonomous), Tamilnadu, India.

[4]Professor, Head of the Department, Department of Computer Science and Engineering, Shree Venkateswara Hi-Tech Engineering College (Autonomous), Tamilnadu, India.

**Corresponding Author: jtysp14@gmail.com*

Figure 1: Homomorphic encryption

The homomorphic encryption process is illustrated in (Figure 1). In this approach, the input data (plaintext) is first encrypted into ciphertext using an encryption algorithm. Operations are then performed directly on the encrypted data without decrypting it. Finally, the processed ciphertext is decrypted to obtain the correct result. This ensures data privacy throughout the computation process.

2.2. Electronic Voting Systems

Traditional electronic voting systems rely on centralized servers and require decryption of votes for counting. Electronic voting systems use digital platforms for casting and counting votes [3]. However, traditional systems require decryption during counting, which introduces security risks.

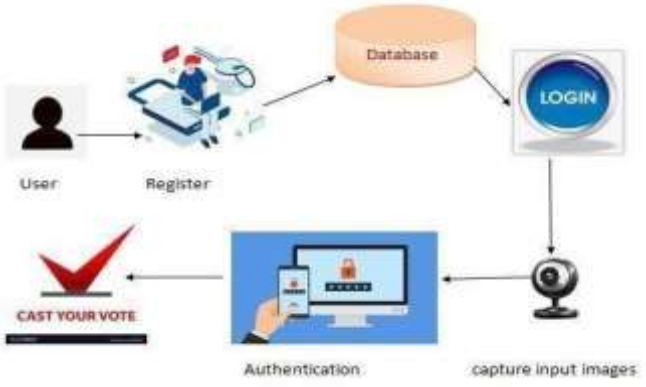

Figure 2: Electronic voting system

The electronic voting system process is illustrated in (Figure 2). It begins with voter authentication, where the user logs into the system using secure credentials. After successful verification, the voter casts their vote, which is then encrypted to ensure privacy and security. The encrypted vote is stored in a secure database, preventing unauthorized access or tampering. During the counting phase, votes are processed and the final result is generated accurately. This system ensures transparency, efficiency, and reliability in the voting process.

2.3. Need for secure voting

Secure voting systems are necessary to ensure privacy and prevent fraud in elections [4]. Homomorphic encryption provides a strong solution by maintaining confidentiality while enabling accurate vote computation. Homomorphic encryption provides a strong foundation for building such systems by ensuring that votes remain confidential while still enabling accurate computation of results.

3. Proposed system architecture

The proposed electronic voting system is designed to ensure security, privacy, and efficiency. The proposed system includes voter authentication, vote casting, encryption, secure storage, and result computation modules [5]. Votes are encrypted using homomorphic encryption before storage. When a voter casts a vote, the system encrypts the vote using homomorphic encryption techniques. The encrypted votes are stored securely in the database. During the counting process, operations are performed directly on the encrypted votes without decrypting them. Only the final result is decrypted by an authorized authority. The system ensures that individual votes remain confidential while allowing accurate computation of the final result. During counting, operations are performed on encrypted votes without decryption. The architecture is designed to ensure seamless integration between security and performance, enabling efficient handling of encrypted

voting data.

Table 1: Key components of proposed architecture

Component	Function	Benefit
Voter Authentication	Verifies user identity using login credentials	Prevents unauthorized access
Voting Interface	Allows user to cast vote	Easy and userfriendly voting
Encryption Module	Encrypts votes using homomorphic encryption	Ensures data privacy and security
Secure Database	Stores encrypted votes	Prevents data tampering
Vote Processing Unit	Performs operations on encrypted votes	No need for decryption during count
Result Decryption Module	Decrypts final result only	Maintains confidentiality

(Table 1) presents the key components of the proposed electronic voting system architecture. Each component plays a vital role in ensuring secure and efficient voting. The integration of encryption and secure processing modules enhances data privacy, prevents tampering, and ensures accurate result generation. The proposed architecture ensures a secure and reliable voting process by integrating multiple functional components. Each module is designed to handle a specific task, from user authentication to final result generation. The use of homomorphic encryption in the encryption module and vote processing confidential even during computation additionally, the secure database prevents unauthorized modifications, thereby maintaining data integrity. Overall, the system provides a robust framework for conducting transparent and trustworthy electronic elections. In modular design of the proposed system improves scalability and flexibility, allowing new features to be integrated easily without affecting existing components.

The separation of functionalities ensures better system management and fault isolation. By combining security mechanisms with efficient processing techniques, the architecture minimizes risks associated with data breaches and unauthorized access. This structured approach not only enhances system performance but also builds user trust in the electronic voting process.

Table 2: Comparison with conventional system

Feature	Proposed Homomorphic Voting System	Conventional Voting System
Computation	Performed on encrypted data	Performed on decrypted data
Data Security	Very High	Moderate to Low
Privacy	Fully preserved	Partially preserved
Risk of Tampering	Minimal	High
Transparency	High	Moderate
Accuracy	High	Depends on system

(Table 2) presents a comparative analysis between the proposed homomorphic encryption based electronic voting system and conventional voting systems. The proposed system performs computations directly on encrypted data, thereby ensuring that sensitive information is never exposed during processing. In contrast, conventional systems require decryption for vote counting, which increases the risk of data breaches and manipulation. The elimination of intermediate data exposure improves overall system security and reliability. In addition, the automated nature of the system increases processing efficiency and accuracy when compared to traditional methods that involve manual intervention.

Table 3: Performance advantages

Parameter	Improvement Achieved
Energy Efficiency	Faster vote processing and counting
Data Integrity	Prevents unauthorized modifications
Scalability	Handles large number of voters effectively
Transparancy	Increases trust in the voting system
Data Privacy	Votes remain confidential throughout the process

The performance advantages of the proposed electronic voting system are summarized. The system provides high security by encrypting votes and maintaining confidentiality throughout the process. It improves accuracy by eliminating manual errors and ensures reliable result generation. As shown in (Table 3). The proposed system achieves better efficiency and scalability compared to traditional systems. The use of homomorphic encryption enhances data integrity and prevents unauthorized access, making the system suitable for secure and large-scale voting applications. These advantages demonstrate that the proposed system is more efficient, secure, and reliable than conventional voting methods.

Table 4: Memristor crossbar parameters

Parameter	Description
Encryption Key	Used to encrypt and decrypt voting data
Ciphertext	Encrypted form of the vote
Homomorphic Property	Allows computation on encrypted data
Computation Time	Time taken for encrypted operations
Security Level	Strength of encryption used

The key parameters of the homomorphic encryption used in the proposed voting system are presented in (Table 4). These parameters define how data is encrypted, processed, and secured within the system. The encryption key and ciphertext ensure confidentiality, while the homomorphic property enables computation without decryption. As shown in Table 4, these parameters play a crucial role in maintaining security, efficiency, and reliability of the electronic voting system.

4. Implementation methodology

The implementation of the proposed system involves several steps to ensure secure and efficient voting [6].

- *User Authentication:* Voters log in using secure credentials to verify their identity.
- *Vote Casting:* The voter selects their preferred candidate.
- *Encryption:* The vote is encrypted using homomorphic encryption before being stored.
- *Secure Storage:* Encrypted votes are stored in a secure database.
- *Vote Counting:* Mathematical operations are performed on encrypted votes to compute the result.
- *Result Decryption:* Only the final result is decrypted by authorized personnel.

The system follows steps such as authentication, vote casting, encryption, secure storage, and result decryption. Votes are encrypted immediately after casting to ensure privacy. The proposed electronic voting system based on homomorphic encryption follows an integrated approach that combines secure data processing, encryption techniques, and efficient vote computation to achieve reliable election results. Before being processed by the system, voter inputs such as selected candidate choices are validated and formatted to ensure consistency and correctness. This preprocessing step includes user authentication, input validation, and session management to maintain system integrity.

Once the vote is cast, it is immediately converted into an encrypted format using homomorphic encryption algorithms. This encryption ensures that the vote remains confidential and protected from unauthorized access. The encrypted votes are then mapped to a secure database, where each entry corresponds to a specific encrypted value. Unlike conventional systems, the proposed method does not require decryption during intermediate stages, thereby minimizing the risk of data exposure. Secure databases store encrypted votes and prevent unauthorized access [7]. The final result is decrypted only by authorized users, ensuring data protection. The final result is decrypted only by an authorized authority, ensuring that individual votes remain confidential while the overall election outcome is accurately determined. Additionally, the system minimizes human intervention, reducing the possibility of errors and manipulation. The integration of encryption, secure storage, and automated processing enhances the overall efficiency and reliability of the voting system.

5. Results and discussion

The proposed homomorphic encryption based electronic voting system demonstrates promising performance in terms of security, privacy, and efficiency. The system was evaluated based on key parameters such as data confidentiality, accuracy of results, processing efficiency, and resistance to unauthorized access. The results indicate that the system effectively maintains voter privacy by ensuring that all votes remain encrypted throughout the voting and counting process. The system demonstrates improved security, privacy, and efficiency compared to traditional voting methods. Votes remain encrypted throughout the process, ensuring confidentiality [8]. In the experimental evaluation, the system successfully performed vote aggregation directly on encrypted data without requiring intermediate decryption. This significantly reduces the risk of data exposure and ensures that sensitive information is never revealed during computation.

The final results obtained after decryption were found to be accurate and consistent with the expected outcomes, demonstrating the correctness of the homomorphic operations applied during the counting phase. The system also shows improved efficiency compared to traditional voting methods. Automated vote processing reduces manual intervention, thereby minimizing human errors and increasing reliability. Additionally, the time required for vote counting is considerably reduced, making the system suitable for real-time election scenarios. The secure database ensures that encrypted votes are stored safely preventing any unauthorized modification or tampering. Encrypted vote processing reduces data exposure and improves accuracy. The system also provides faster vote counting and better scalability for large-scale elections [9]. Furthermore, the use of encryption techniques enhances data integrity, ensuring that votes cannot be altered once they are recorded. Compared to conventional voting systems, the proposed model provides better security, reduced risk of fraud, and improved transparency. The ability to process encrypted data directly offers a significant advantage in maintaining confidentiality while ensuring accurate result computation. Overall, the results confirm that the proposed system is a reliable and efficient solution for secure electronic voting. Future evaluations can focus on optimizing computational performance and testing the system with larger datasets to further validate its effectiveness in real-world applications [10].

6. Challenges and future scope

Despite its advantages, the system faces certain challenges. Homomorphic encryption requires high computational resources, which may affect performance. Implementing such systems on a large scale requires optimization and infrastructure support. Homomorphic encryption requires higher computational resources compared to traditional methods, which may affect performance.

Additionally, implementing such systems on a large scale its requires careful optimization and infrastructure support. Future work can focus on improving the efficiency of encryption algorithms and reducing computational overhead. Future improvements include enhancing encryption efficiency and integrating blockchain for better security and transparency. Integration with blockchain technology can further enhance transparency and security. The system can also be extended to support mobile-based voting applications.

7. Conclusion

The homomorphic encryption electronic voting system provides an effective and secure solution to the limitations of traditional electronic voting systems. The proposed electronic voting system using homomorphic encryption provides a secure and reliable solution to traditional voting challenges. It ensures vote privacy, prevents tampering, and improves transparency. This project overcomes these issues by implementing homomorphic encryption, which ensures that votes remain encrypted throughout the voting and counting processes. The system demonstrates how advanced cryptographic techniques can enhance trust in digital elections. By allowing vote tallying on encrypted data, the system removes the need to decrypt individual votes, thereby guaranteeing complete voter privacy. By enabling computation on encrypted data, the system enhances trust in digital elections. This approach proves that secure and privacy-preserving electronic voting systems are achievable using modern cryptographic techniques. The integration of intelligent components such as NLP-based interaction, emotion aware responses, and ethical AI safeguards further improves system usability and reliability. Overall, this project proves that secure, privacy preserving, and intelligent electronic voting systems are achievable using modern web technologies and cryptographic methods. The developed system is suitable for academic, organizational, and small scale election environments and lays a strong foundation for future large-scale implementations.

Conflict of interest statement: The author declares that there is no conflict of interest regarding the publication of this research paper.

Funding information: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Data availability statement: The data used in this study are generated within the system and are not publicly available. However, relevant data can be provided by the author upon reasonable request.

Ethical approval statement: This study does not involve any human participants, animals, or sensitive personal data. Therefore, ethical approval was not required for this research work.

Acknowledgement: The author sincerely thanks the Shree Venkateshwara Hi-Tech Engineering College, Gobi, for providing academic support and a conducive research environment for the completion of this study.

References

1. Adida B, Helios: Web-based open-audit voting, in proc., USENIX security symposium helios is a web-based electronic voting system that provides open-audit functionality, It improves transparency and allows voters to verify the correctness of election results. 2008, 335-348
2. Benaloh J, Verifiable secret-ballot elections, in proc., USENIX security symposium, verifiable secret-ballot election systems ensure that votes remain confidential while allowing verification, this improves both security and trust in electronic voting systems. 2006, 1-14

3. Boneh D, Goh E, Nissim K, Evaluating 2-DNF formulas on ciphertexts, in LNCS, cryptographic techniques such as evaluating encrypted data enable secure computations without revealing actual information, this is useful in maintaining vote privacy during counting. 2005, 325-341
4. Chaum D, Secret-ballot receipts: True voter-verifiable elections, IEEE Security Privacy, voter-verifiable receipt systems allow users to confirm that their vote has been counted correctly, these systems enhance transparency without compromising anonymity. 2004, 38
5. Cramer R, Gennaro R, Schoenmakers B, Secure multiparty computation, secure multiparty computation enables multiple participants to compute results without revealing their individual inputs, this technique is important in secure vote tallying. 1997, 103-118
6. Elissa K, An overview of cryptography, cryptography plays a major role in securing electronic voting systems, It ensures data confidentiality, integrity, and authentication throughout the voting process. 2005, 1-10
7. Fujioka T, Okamoto K, A practical secret voting scheme for large scale elections, Journal of Cryptology, secret voting schemes for large-scale elections are designed to handle a large number of voters efficiently, these methods maintain privacy while ensuring accurate results. 1992, 244-251
8. Paillier P, Public-key cryptosystems based on composite degree residuosity classes, EUROCRYPT, public-key cryptosystems such as paillier encryption support secure and private voting, they allow operations on encrypted data, making them suitable for electronic voting systems. 1999, 223-238
9. Smart NP, Vercauteren F, Fully homomorphic encryption with relatively small key and ciphertext sizes, PKC, fully homomorphic encryption enables computations on encrypted data without decryption, this technology enhances privacy and security in electronic voting systems. 2010, 420-443
10. Gentry, Fully homomorphic encryption using ideal lattices, STOC. 2009, 169-178