IJIS: Vol.1, Issue 10, November 2025 Page: 42-47 ISSN 3049-3277

International Journal of Integrative Studies (IJIS)

Journal homepage:www.ijis.co.in

Privacy Preserving E-Voting System Using Homomorphic Encryption

Dr. Rajeshwar[1], Dantala Siddartha[2], Kolakani Sanjay[3], Paleti Prem Kiran[4], Rachagiri Omkarnath[5]

Dr. Rajeshwar[1], Dantala Siddartha[2], Kolakani Sanjay[3], Paleti Prem Kiran4, Rachagiri Omkarnath5

[1]Associate Professor, Hyderabad Institute of Technology and Management, Medchal, Telangana

[2]UG Student, Hyderabad Institute of Technology and Management, Medchal, Telangana

[3]UG Student, Hyderabad Institute of Technology and Management, Medchal, Telangana

[4]UG Student, Hyderabad Institute of Technology and Management, Medchal, Telangana

[5]UG Student, Hyderabad Institute of Technology and Management, Medchal, Telangana

Abstract

With the rise of digital governance, secure and private electronic voting systems are becoming increasingly important. Traditional e-voting platforms often suffer from vulnerabilities such as vote tampering, lack of transparency, and weak identity verification. To address these challenges, this project introduces a secure online voting system that integrates Paillier homomorphic encryption with deep-learning-based facial recognition technology. Homomorphic encryption enables the aggregation of votes while they remain encrypted, ensuring that individual ballots stay completely confidential throughout the counting process. Facial recognition provides real-time voter authentication, effectively preventing proxy and duplicate voting.Throughout the voting lifecycle, ballot data is encrypted during both transmission and storage, eliminating opportunities for third parties to intercept or manipulate information. An administrator can access results only after the voting period concludes, and the system reveals only the final aggregate tally without disclosing individual choices. The proposed model is implemented using Python, Flask, OpenCV, and SQLite, offering a secure, scalable, and user-friendly solution suitable for small-scale elections in academic institutions and local organizations.The system includes an intuitive web interface, encrypted data storage, and secure communication mechanisms to enhance usability and reliability. By combining biometric authentication with advanced cryptographic techniques, the project delivers a robust, tamper-resistant voting framework that strengthens voter trust and ensures end-to-end privacy. Overall, this work demonstrates how modern cryptography and artificial intelligence can significantly improve the security and transparency of digital election systems, making it a strong foundation for future e-voting applications.

Keywords: Electronic Voting, Homomorphic Encryption, Paillier Cryptosystem, Facial Recognition, Deep Learning, Biometrics, Python Flask, Secure Voting, Digital Democracy, Encrypted Ballots.

1. Introduction

Electronic voting has emerged as a modern alternative to traditional paper-based and electronic machine voting, aiming to make the election process faster, more accessible, and more reliable. However, many existing online voting systems suffer from weak authentication methods and lack strong privacy protections, making them vulnerable to impersonation, data tampering, and unauthorized access. As a result, ensuring secure voter identification and maintaining complete confidentiality of votes remain major challenges in digital elections.

To overcome these issues, this project introduces a secure E-Voting System that integrates facial recognition for biometric voter authentication and homomorphic encryption for privacy-preserving vote processing. Facial recognition ensures that only valid, registered individuals can cast a vote, while homomorphic encryption guarantees that votes remain encrypted throughout the election process. Together, these technologies provide a robust, trustworthy, and user-friendly voting platform suitable for institutional and small-scale elections.

2. Litraturesurvey

R. Kumar et al. emphasize the effectiveness of homomorphic encryption in preserving ballot secrecy while enabling encrypted vote tallying without decryption. Paillier's additive homomorphic scheme is widely adopted because it supports accurate aggregation of encrypted votes and prevents insider tampering. Modern research also recommends distributing private keys among multiple authorities to eliminate single-point trust failures. Several studies highlight the need for client-side encryption, one-hot vote encoding, and publicly verifiable bulletin boards to enhance transparency. Recent work further integrates biometric authentication such as facial recognition to ensure voter legitimacy while keeping identity separate from vote data. Performance evaluations indicate that homomorphic schemes are efficient for small-to-medium elections and can be optimized for larger deployments. Emerging hybrid models combine homomorphic encryption with blockchain for greater auditability. Overall, the literature supports homomorphic-encryption-based e-voting as a strong foundation for privacy-preserving, tamper-resistant digital elections.

Mehta and Kaur (2022) propose a secure digital voting system that relies on deep-learning-based facial recognition to authenticate voters and eliminate impersonation risks. Their work demonstrates that CNN models such as FaceNet, VGG-Face, and ArcFace achieve high accuracy and stability even under varying lighting and pose conditions. The system captures a live facial image and compares it with stored templates to verify identity before ballot access. They emphasize that biometric authentication reduces proxy voting and multiple vote attempts. The study also stresses the importance of dataset quality, feature extraction, and threshold tuning. Results show facial recognition to be scalable and user-friendly for voter verification.

Zhan et al. (2024) propose an improved e-voting system leveraging homomorphic encryption for strong privacy protection across voting stages. Their design enhances the efficiency of Paillier-based additive operations, enabling faster vote encryption, aggregation, and tallying. Optimized algorithms and reduced ciphertext size make the system suitable for large-scale elections. Experimental results show improved performance, security, and resistance to manipulation or unauthorized decryption.

T. N. Aruna presents an online voting system that integrates facial recognition for secure voter authentication. Real-time face comparison with stored templates eliminates impersonation and repeated voting attempts. The study highlights higher accuracy and convenience compared to password- or OTP-based systems, and emphasizes encrypting facial data and secure communication.

Halidou et al. (2025) introduce a voter authentication system using an enhanced ResNet-50 with ArcFace loss, significantly improving feature discriminability and recognition accuracy even under challenging conditions. MTCNN-based detection improves end-to-end robustness, achieving accuracy exceeding 99% while minimizing error rates. The study stresses secure storage of face embeddings to safeguard biometric privacy.

Yuan and Sang (2023) propose a decentralized e-voting scheme leveraging Paillier homomorphic encryption to preserve ballot confidentiality while supporting secure encrypted tallying. Distributed key control eliminates centralized risks, and double-layer encryption protects against replay and tampering. Performance analysis shows strong efficiency and verifiability without compromising anonymity.

Schroff, Kalenichenko, and Philbin (2015) introduced FaceNet, a deep-learning model that learns a 128-dimensional facial embedding using triplet loss, improving accuracy and scalability in face recognition tasks. The approach achieves near-human performance on benchmark datasets such as LFW and YouTube Faces and forms the foundation of modern biometric authentication used in secure e-voting systems.

3. Existing System

Traditional voting mechanisms used in most regions still rely heavily on paper-based electoral processes, manual authentication, physical identity verification, and ballot casting at designated polling stations. These conventional systems often face several challenges, including long queues, limited accessibility for remote or disabled voters, and dependence on extensive manpower and logistics. Manual vote counting introduces risks of human error, delays, and potential manipulation. Additionally, transparency is often limited due to centralized vote handling, making auditability and trust difficult to achieve. Security vulnerabilities such as proxy voting, ballot tampering, duplicate voting, and the possibility of unauthorized influence further weaken the reliability of the current system. Overall, traditional voting methods lack efficiency, real-time monitoring, and sufficient protection against fraud, leading to reduced voter confidence and participation.

4. Proposed System

The proposed secure E-Voting System introduces a modern, technology-driven solution that integrates biometric authentication and homomorphic encryption to ensure secure and trustworthy election management. The system leverages deep-learning-based facial recognition to verify voter identity, preventing impersonation, proxy voting, and multiple submissions. Once authenticated, votes are encrypted using the Paillier Homomorphic Encryption scheme, allowing encrypted aggregation without decryption and ensuring complete secrecy of individual ballots.

The methodology for system development is systematic and modular, covering requirement analysis, system design, module creation, secure database management, interface development, and final deployment. The architecture includes an intuitive web interface, secure communication protocols, and encrypted storage to provide a user-friendly and tamper-resistant environment. Testing is performed to validate accuracy, performance, and security, while future enhancements can incorporate blockchain integration, improved scalability, and multi-factor authentication.

Overall, the proposed system strengthens voter trust by offering a transparent, privacy-preserving, and highly secure digital voting platform suitable for institutional and organizational elections.

5. SYSTEM Modelilding NLP Pipelines.)

The system design phase forms the foundational blueprint of the E-Voting System. It describes how various components of the application interact with each other, establishes the overall architectural structure, defines data flow mechanisms, and breaks the system into well-defined modules. A well-designed architecture ensures security, scalability, maintainability, and efficient system performance. The design is divided into four major categories: architecture-level design, module-level design, workflow design, and interface design.

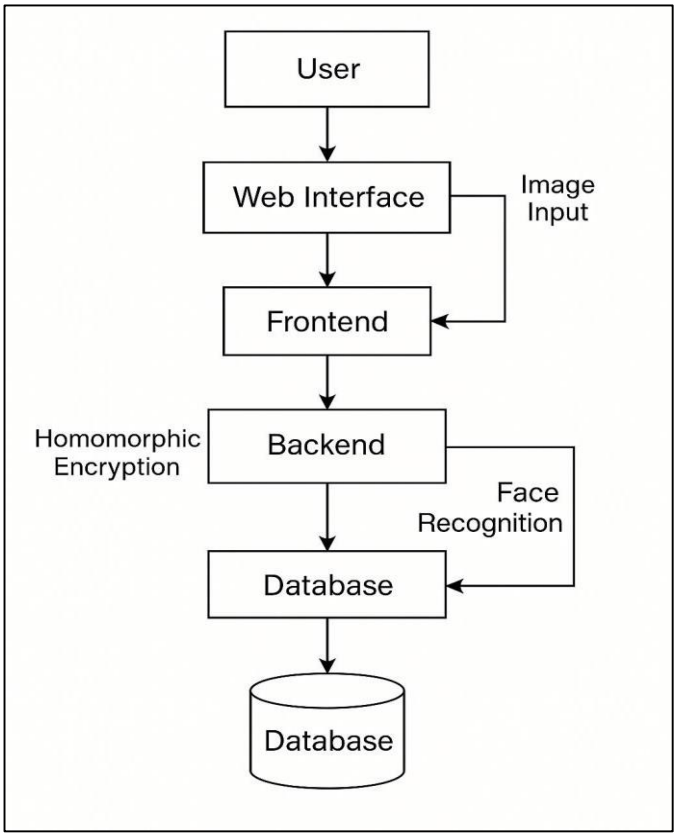

Fig 1. System Model

6. Implementation

The successful development and deployment of the E-Voting System requires a detailed understanding of both the hardware and software resources necessary to support biometric authentication, secure encryption, real-time processing, and web-based interface functionalities. This section outlines the complete set of requirements needed for implementation, including functional prerequisites, system specifications, software frameworks, libraries, and installation steps. By fulfilling these requirements, the system ensures optimal performance, compatibility, and scalability.

6.1 Modules

- Registration Module

Collects voter details and captures facial images, converting them into encoded feature vectors.

- Face Recognition Module
  Utilizes machine learning and deep-learning algorithms to verify voter identity in real-time.
- Voting Module
  Displays the list of candidates and allows authenticated voters to securely cast their vote.
- Encryption Module
  Encrypts each vote using homomorphic encryption algorithms to ensure ballot secrecy and tamper resistance.
- Database Module
  Securely stores encrypted votes, voter profiles, and facial encodings with controlled access.
- Admin Module
  Provides tools for monitoring election progress and retrieving encrypted results after voting concludes.

7. Results

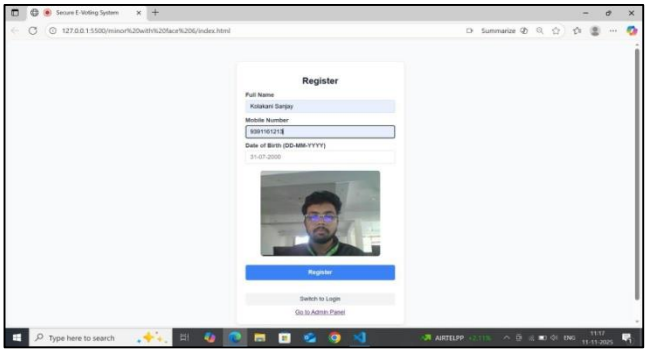

Fig7.1 Signup Page

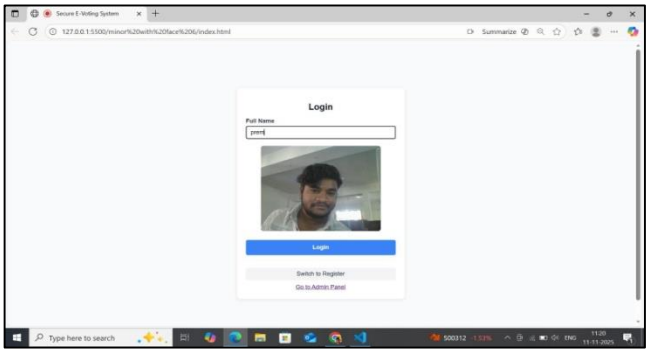

Fig7.2 Login Page

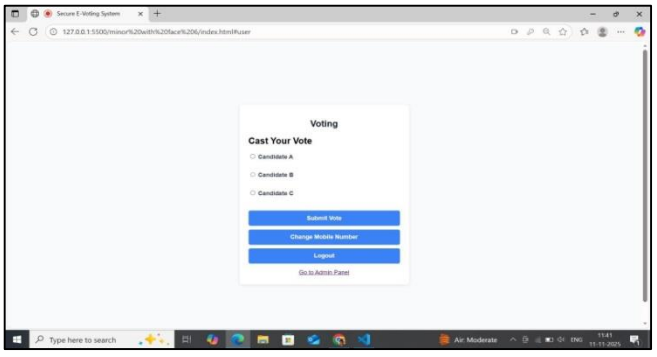

Fig 8.3 Voting Page

Fig 7.4 Admin Page

Fig 7.5 Results Page

Fig 7.6 Registered Users Page

8. Conclusion

The project demonstrates how combining facial recognition with homomorphic encryption can significantly enhance the security and integrity of electronic voting systems. Real-time biometric authentication prevents identity fraud and proxy voting, ensuring that only legitimate voters can participate. Homomorphic encryption protects vote confidentiality by keeping ballots encrypted throughout storage, transmission, and tallying. The system also improves accessibility and administrative efficiency through its user-friendly web interface and remote voting capability. Overall, this approach offers a practical, scalable, and trustworthy solution for modern digital elections, with strong potential for future large-scale adoption.

9. Future Enhancements

The system can be further enhanced by improving the user interface with accessibility features such as multi-language support, speech-guided navigation, and high-contrast visual themes to assist elderly and disabled voters. Real-time monitoring and an election analytics dashboard can be integrated to provide encrypted turnout statistics, progress tracking, and admin alerts for suspicious activities or repeated vote attempts. Future versions may support government-level integration by linking voter verification with national identity systems such as Aadhaar or digital e-ID, enabling large-scale authentication through secure identity APIs. Advanced face recognition models like ArcFace, FaceNet, and InsightFace can be incorporated to achieve higher accuracy, alongside adaptive thresholding to handle lighting variations and natural aging. Multi-factor authentication can be implemented by combining face recognition with OTP, PIN, or QR-based verification and employing role-based access control for administrators and auditors. Additionally, liveness detection mechanisms such as blink or smile prompts, head-movement checks, and AI-powered 3D depth analysis can be integrated to prevent spoofing using photos, videos, or masks, thereby strengthening protection against biometric attacks. Together, these enhancements can greatly improve security, scalability, and usability, supporting deployment at larger national and institutional levels.

References

1. Kumar, R., Verma, S., & Singh, P. (2021). Secure E-Voting Through Homomorphic Encryption and Privacy-Preserving Computation. IEEE Access. Available at: https://ieeexplore.ieee.org/document/9448381
2. Zhan, Y., et al. (2024). Efficient Electronic Voting System Based on Homomorphic Encryption.
3. Mehta, S. D., & Kaur, A. (2022). Face-Recognition Based Biometric Authentication for Secure Digital Voting. Springer LNNS. Available at: https://link.springer.com/chapter/10.1007/978-981-16-7617-5_39
4. Shrestha, A., Bajracharya, B., & Shakya, A. (2023). Blockchain-Integrated E-Voting Systems with Biometric Verification. Elsevier. Available at: https://www.sciencedirect.com/science/article/pii/S1084804523000025
5. Online Voting System Using Facial Recognition. (2023). IJNRD.
6. Halidou, A., Idrissi, M. K., & Hmina, N. (2025). Voter Authentication Using Enhanced ResNet-50 With ArcFace. MDPI. Available at: https://www.mdpi.com/2624-6120/6/2/25
7. Yuan, K., & Sang, P. (2023). An Electronic Voting Scheme Based on Homomorphic Encryption and Decentralization. MDPI. Available at: https://www.mdpi.com/2079-9292/12/1/190
8. Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering. CVPR. Available at: https://arxiv.org/abs/1503.03832
9. Parmar, P. V., Padhar, S. B., Patel, S. N., Bhatt, N. I., & Jhaveri, R. H. (2014). Survey of various homomorphic encryption algorithms and schemes. International Journal of Computer Applications, 91(8).
10. Lee, H., Alves-Foss, J., & Harrison, S. (2004). The use of encrypted functions for mobile agent security. In Proceedings of the 37th Annual Hawaii International Conference on System Sciences (pp.10–10). IEEE.
11. Kohno, T., Stubblefield, A., Rubin, A. D., & Wallach, D. S. (2004). Analysis of an electronic voting system. In IEEE Symposium on Security and Privacy.
12. Sakurai, K., & Takagi, T. (2002). On the security of a modified Paillier public-key primitive. In Information Security and Privacy. Springer Berlin Heidelberg.
13. Marhur, H., & Alam, Z. (2015). Analysis in symmetric and asymmetric cryptology algorithm. International Journal of Emerging Trends of Technology in Computer Science, 4(1).
14. Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In Advances in Cryptology – EUROCRYPT'99 (pp. 223–238). Springer Berlin Heidelberg.
15. Choinyambuu, S. (2009). Homomorphic tallying with Paillier cryptosystem. HSR Hochschule für Technik Rapperswil.