iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.81605

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Quantum Key Voting System

Nallabothula Amarachinneswari[1], Dhulipalla Tejaswi[2], Jangala Manjusri[3], Mathi Neelima[4]
[1, 3, 4]*Department of computer science and engineering (AIML), Bapatla Women's Engineering College, Bapatla, India*
[2]*Assistant Professor, Department of computer science and engineering (AIML), Bapatla Women's Engineering College, Bapatla, India*

Abstract: ***Recent research in 2024 emphasizes post- quantum security techniques to safeguard voting systems from future quantum-based attacks. At the same time, improvements in deep learning-based face authentication have enhanced the accuracy and reliability of voter verification under real-world conditions. Hybrid security models that combine cryptographic methods with face authentication provide stronger protection against unauthorized access and fraud. These systems focus on essential properties such as voter anonymity, data integrity, and end-to-end verifiability.However, challenges including high computational cost, scalability, and real-time implementation continue to be important areas for further research.Moreover, researchers are exploring optimized algorithms to reduce processing time and improve system efficiency. Efforts are also being made to enhance dataset management for accurate face storage and retrieval. Cloud-based implementations are being considered to support large-scale voting environments. These advancements indicate the growing importance of developing practical and scalable secure voting solutions.***

Keywords: ***The system uses Quantum Key Distribution (QKD) for secure communication and encryption of voting data. Face authentication verifies voter identity by matching live facial data with stored records. Voter ID mapping and encryption ensure data security, privacy, and prevention of fraud in the voting process.***

I. INTRODUCTION

In recent years, electronic voting systems have gained significant attention due to their ability to improve the efficiency and speed of the electoral process. However, traditional digital voting systems face serious challenges related to security, voter authentication, data integrity, and privacy. Issues such as identity fraud, multiple voting, and cyberattacks reduce trust in these systems and highlight the need for more secure and reliable solutions.

To address these challenges, advanced technologies such as quantum cryptography and face authentication are being explored. Quantum Key Distribution (QKD) offers a highly secure method for generating and sharing encryption keys based on the principles of quantum mechanics. This ensures that any unauthorized attempt to intercept or alter the communication can be detected, thereby providing strong protection against cyber threats.

In addition to secure communication, accurate voter verification is essential for a trustworthy voting system. This work introduces a face authentication mechanism in which each voter's facial data is captured and stored in a database during registration. During the voting phase, the system compares the live facial image with the stored data to verify the voter's identity. A strict one-to-one mapping between voter ID and facial data ensures that each individual can vote only once, effectively preventing duplication and impersonation. The integration of quantum key-based security with face authentication enhances both the confidentiality and reliability of the voting process. It eliminates the limitations of password-based systems and provides a more robust, tamper-resistant framework. This approach aims to build a secure, transparent, and efficient digital voting system that can meet the demands of modern electoral processes while maintaining voter privacy and trust. The rapid growth of digital technologies has transformed many sectors, including the electoral process, leading to the development of electronic voting systems. These systems aim to improve efficiency, reduce manual effort, and provide faster result generation. However, despite these advantages, traditional electronic voting systems face significant challenges related to security, voter authentication, data integrity, and privacy. Common issues such as identity theft, multiple voting, unauthorized access, and cyberattacks reduce the reliability and trustworthiness of existing systems, making secure voting a critical area of research.

To overcome these limitations, advanced security mechanisms are required that can ensure both secure communication and accurate voter verification. Quantum cryptography has emerged as a promising solution in this domain. In particular, Quantum Key Distribution (QKD) provides a secure method for generating and sharing encryption keys based on the principles of quantum mechanics. Unlike classical encryption techniques, QKD can detect any eavesdropping attempt during key exchange, thereby ensuring a highly secure communication channel for transmitting sensitive voting data.

©IJRASET: All Rights are Reserved

In addition to secure communication, reliable voter authentication plays a crucial role in maintaining the integrity of the voting process. This work focuses on face authentication as a robust method for verifying voter identity. During the registration phase, each voter's facial image is captured and processed to extract unique facial features, which are then stored in a database as encoded representations. A strict one-to-one mapping is maintained between the voter ID and the corresponding face encoding, ensuring that each voter is uniquely identified. During the voting phase, the system captures the live facial image of the user and compares it with the stored data to verify authenticity. If the match is successful, the voter is allowed to proceed; otherwise, access is denied.

Furthermore, the integration of face authentication with quantum key-based encryption creates a multi-layered security framework. This approach not only prevents unauthorized access and impersonation but also ensures that the transmitted voting data remains confidential and tamper-proof. The system also enforces constraints such as one vote per voter, thereby eliminating duplicate voting and enhancing fairness in the election process.

Compared to conventional voting systems that rely on passwords, ID cards, or manual verification, the proposed system offers a more secure, automated, and efficient solution. It minimizes human intervention, reduces the chances of error, and improves overall transparency. Additionally, the system preserves voter anonymity by ensuring that the identity of the voter is not linked to their vote.

II. LITERATURE SURVEY

In 2023, significant advancements were made in secure electronic voting systems by integrating emerging technologies such as quantum cryptography and face recognition. Researchers focused on enhancing security and preventing unauthorized access in digital voting platforms. One study proposed an electronic voting system using deep learning-based face recognition techniques, where facial features are extracted and matched with stored data to verify voter identity. The system achieved high accuracy and demonstrated that face authentication can effectively reduce identity fraud and enable remote voting.

Another line of research in 2023 explored the application of Quantum Key Distribution (QKD) in secure communication systems. QKD enables the generation of encryption keys based on quantum principles, ensuring that any interception attempt can be detected. This approach laid the foundation for integrating quantum security into voting systems, providing strong protection against cyberattacks and data breaches.

In 2024, research shifted towards combining multiple advanced technologies to further strengthen voting systems. A quantum-enhanced secure voting protocol was introduced, utilizing quantum computing principles such as superposition and entanglement along with digital signatures. The system ensured important properties such as voter anonymity, vote integrity, and verifiability, demonstrating improved security over traditional cryptographic methods.

Additionally, a hybrid blockchain-based electronic voting system was proposed in 2024, incorporating post-quantum cryptography and deep learning-based face verification. This system addressed key limitations of traditional voting systems by enhancing transparency, scalability, and resistance to cyber threats. The integration of face authentication improved voter validation, while blockchain ensured tamper-proof storage of votes.

Overall, the literature from 2023 and 2024 highlights a clear trend toward integrating quantum cryptography and face authentication techniques in electronic voting systems. These approaches aim to overcome the limitations of conventional systems by improving security, preventing fraud, and ensuring reliable voter verification. However, challenges such as system complexity, computational cost, and real-time implementation remain areas for further research.

Furthermore, recent studies in 2024 have explored the use of hybrid security models that combine advanced cryptographic techniques with intelligent authentication mechanisms to strengthen electronic voting systems. Researchers have investigated the integration of post-quantum cryptography with face authentication to ensure long-term security against emerging quantum computing threats. These systems focus on achieving key properties such as end-to-end verifiability, voter anonymity, and resistance to attacks such as spoofing and replay attacks. In particular, improvements in deep learning-based face recognition have increased accuracy and robustness under varying lighting and pose conditions, making face authentication more reliable for real-world deployment. Despite these advancements, challenges such as high computational cost, scalability issues, and the need for efficient real-time processing continue to be areas of active research, indicating the necessity for optimized and practical implementations in future voting systems.

III. PROPOSED SYSTEM ARCHITECTURE

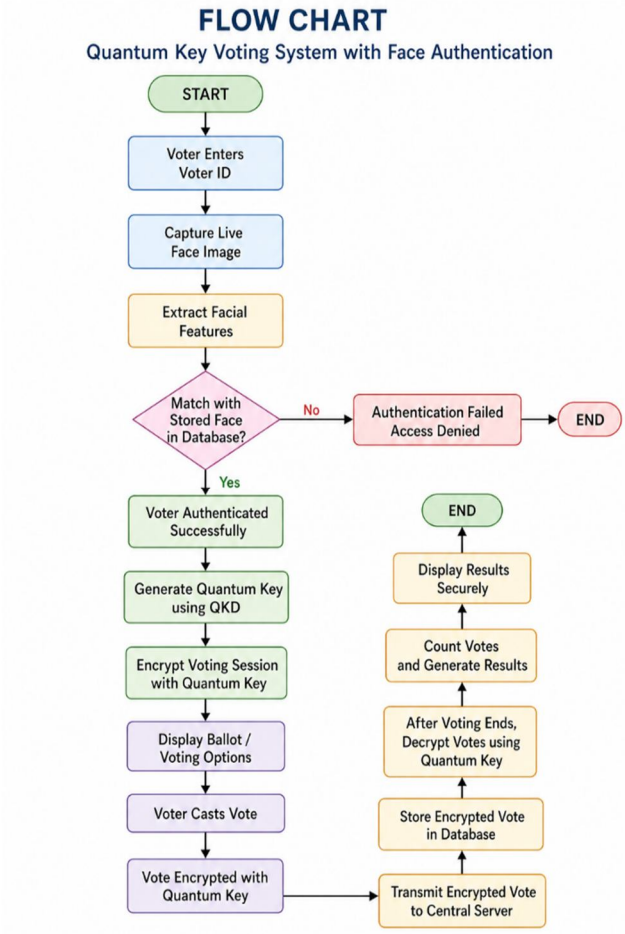
The proposed Quantum Key Voting System with face authentication is designed using a layered architecture to ensure security, efficiency, and reliability. The system consists of five main components:the User Interface, Face Authentication Module, Database Server, Quantum Key Security Module, and Voting & Result Management Module.The process begins at the User Interface layer, where the voter enters their voter ID and initiates the voting process.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

In the Face Authentication Module, the system captures the live facial image using a camera and extracts facial features. These features are compared with the stored facial encodings in the database to verify the voter's identity. Only when the face matches the registered voter ID is the user allowed to proceed.

The Database Server stores voter details, voter ID, and corresponding face encodings in a secure format. It ensures a strict one-to-one mapping between voter ID and face data to prevent duplication and unauthorized registration.The Quantum Key Security Module generates encryption keys using Quantum Key Distribution (QKD). These keys are used to encrypt all voting data during transmission, ensuring that the information cannot be intercepted or modified by attackers.

Finally, the Voting and Result Management Module allows authenticated users to cast their votes securely. The votes are encrypted, transmitted, and stored in the central server. During result generation, the encrypted votes are decrypted and counted, ensuring accuracy, transparency, and integrity of the election process.



IV. METHODOLOGY

The proposed Quantum Key Voting System with face authentication is designed to provide a secure and reliable voting process through a combination of quantum cryptography and facial verification. The methodology is divided into multiple phases, including system initialization, voter registration, face dataset creation, authentication, secure vote casting, and result generation.

In the system initialization phase, the election authority sets up the voting environment by generating system parameters and establishing secure communication channels. Quantum Key Distribution (QKD) is used to generateencryption keys, ensuring secure transmission of data between voters and the server.

During the voter registration phase, each voter provides their unique voter ID along with personal details. The system captures the voter's facial image using a camera and processes it using face recognition algorithms. The extracted facial features are converted into numerical encodings and stored in a database. A strict one-to-one mapping is maintained between the voter ID and the corresponding face encoding to ensure that each voter is uniquely identified.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

In the face dataset creation phase, all registered facial encodings are organized and stored securely. The dataset is continuously updated with new registrations while ensuring that duplicate or mismatched entries are not allowed. If a voter attempts to register with a face that already exists under a different voter ID, the system rejects the registration to prevent impersonation.

During the authentication phase, when a voter attempts to vote, their live facial image is captured and processed. The system extracts facial features and compares them with the stored dataset. If a match is found corresponding to the given voter ID, the voter is authenticated; otherwise, access is denied. This ensures that only legitimate voters can proceed to vote.

In the secure voting phase, once authentication is successful, the voter is allowed to cast their vote. The vote data is encrypted using the quantum-generated key before being transmitted to the central server. This ensures confidentiality and prevents tampering during transmission.

Finally, in the result generation phase, all encrypted votes are securely decrypted and counted by the election authority. The system ensures that votes remain anonymous and cannot be linked back to individual voters. The final results are generated accurately while maintaining transparency and integrity.

This methodology ensures end-to-end security by combining quantum key-based encryption with strict face authentication, effectively preventing unauthorized access, duplicate voting, and data manipulation.

V. SYSTEM IMPLEMENTATION

The system implementation focuses on developing a secure digital voting platform by integrating facial recognition with a unique VoteID-based authentication mechanism. The application is built using a Python-based backend with a Streamlit interface to enable user interaction and real-time processing. During registration, each user provides their assigned VoteID and captures facial data through a camera interface. The captured image is processed using computer vision techniques, where facial features are extracted and converted into numerical encodings.

These encodings are then compared with previously stored data to ensure a strict one-to-one mapping between VoteID and face. If a match is found with the same VoteID, the system permits registration; however, if the face is associated with a different VoteID or if the VoteID is already linked to another face, the system rejects the registration to prevent duplication or impersonation. Upon successful validation, the facial image is stored in a structured dataset, and its corresponding encoding is saved in a serialized file for efficient future comparisons. This implementation ensures data integrity, enhances voter authentication, and significantly reduces the possibility of fraudulent activities.

VI. CONCLUSION

The proposed Quantum Key Voting System with face authentication presents a secure and reliable approach to modern electronic voting. By integrating Quantum Key Distribution (QKD) with face-based identity verification, the system effectively addresses major challenges such as unauthorized access, identity fraud, and data tampering. The use of face authentication ensures that each voter is uniquely identified through a one-to-one mapping between voter ID and facial data, thereby preventing duplicate and fraudulent voting.

Additionally, the application of quantum cryptography enhances the confidentiality and integrity of the voting process by securing data transmission against potential cyber threats. Unlike traditional voting systems that rely on passwords or manual verification, this system provides a more advanced and automated solution while maintaining voter anonymity.

Overall, the proposed system improves transparency, trust, and efficiency in the electoral process. Although challenges such as implementation complexity and computational requirements exist, the approach demonstrates significant potential as a future-ready voting solution. Further research and optimization can enhance scalability and real-time performance, making it suitable for large-scale deployment in real-world elections.

VII. ACKNOWLEDGEMENTS

We would like to express our sincere gratitude to our project guide and faculty members for their continuous support, valuable guidance, and encouragement throughout the development of this research work. Their insights and suggestions greatly contributed to the successful completion of this project.

We also extend our thanks to our institution for providing the necessary resources and environment to carry out this work effectively. We are grateful to our friends and peers for their support and constructive feedback during the development process.

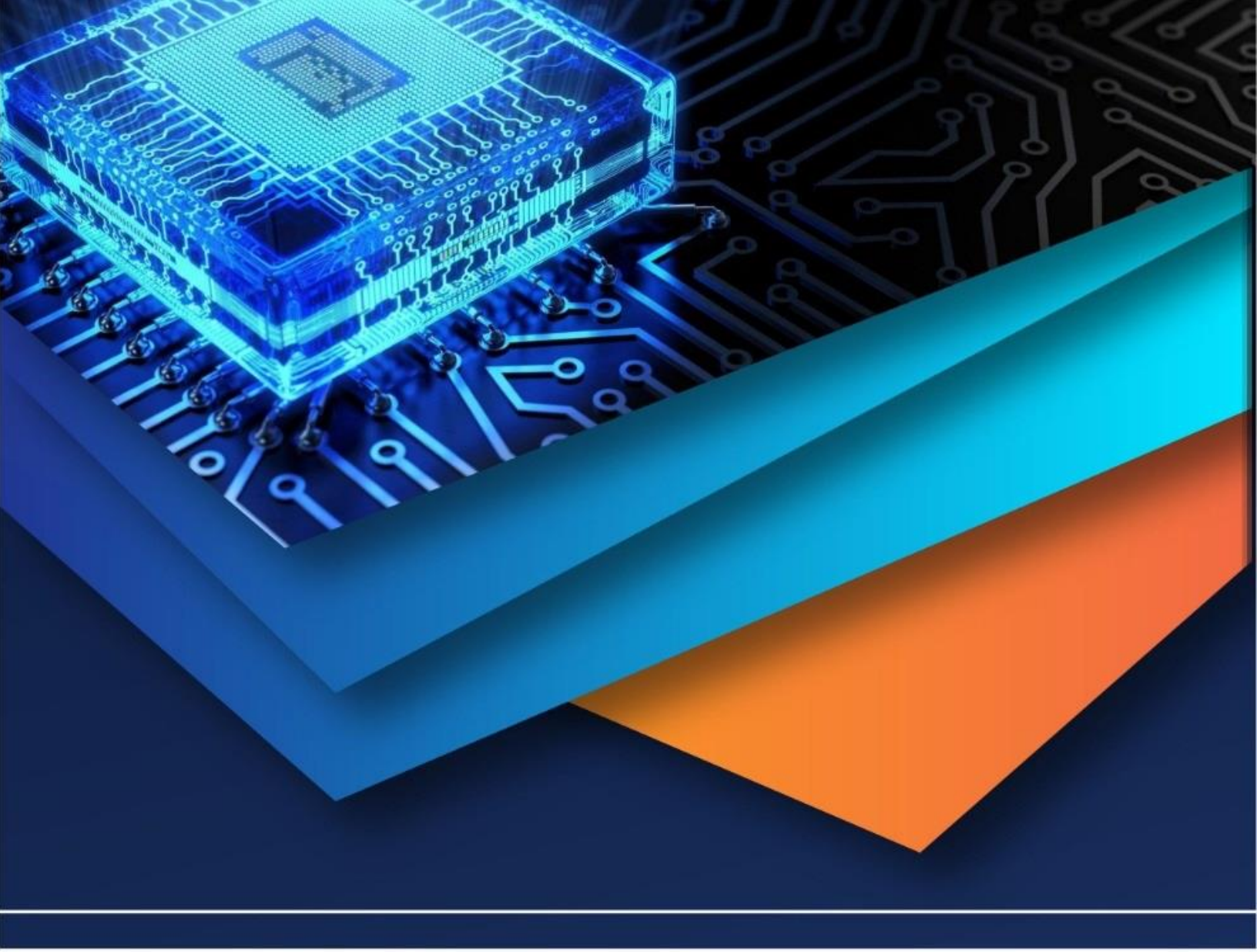
Finally, we would like to thank our family members for their constant encouragement and motivation, which helped us complete this work successfully.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

REFERENCES

[1] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing.
[2] Quantum Key Distribution – Overview and principles. Available at: Wikipedia
[3] Face Recognition – Concepts and algorithms. Available at: IEEE Xplore
[4] Sharma, R., & Singh, A. (2023). Secure E-Voting System Using Face Recognition and Deep Learning. International Journal of Computer Applications.
[5] Kumar, P., & Verma, S. (2023). Enhancing Voting Security Using Quantum Cryptography Techniques. Journal of Information Security.
[6] Zhang, Y., et al. (2024). A Secure Quantum-Based Voting Protocol with Privacy Preservation. arXiv.
[7] Patel, D., & Mehta, K. (2024). Blockchain-Based Secure Voting System with Face Authentication. International Journal of Advanced Research in Computer Science.
[8] OpenCV Documentation – Face detection and recognition techniques.
[9] Face Recognition Library Documentation – Facial encoding and comparison methods.
[10] National Institute of Standards and Technology (NIST). (2023). Digital Identity Guidelines.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)