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.2026.79707

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

An AI-Enhanced Biometric Authentication Framework for Transparent Digital Elections

Mrs. J. Sowmya[1], K.Sai Krishna[2], D. Santhosh[3], M.Varshith Yadav[4]
[1]*Assistant Professor, Department of Computer Engineering, Methodist College of Engineering and Technology Abids, Hyderabad, Telangana, 500001, India*
[2, 3, 4]*Students, Artificial Intelligence And Data Science, Methodist College of Engineering and Technology Abids, Hyderabad, Telangana, 500001, India.*

Abstract: ***The proposed SmartVote system is based on the idea of improving the security and robustness of the voting process using an artificial intelligence-based approach with dual biometric verification. The proposed SmartVote system is based on an optical fingerprint sensor and artificial intelligence-based facial recognition technology to verify the voter's ID. Only verified individuals can cast their votes using the proposed SmartVote system. Advanced features such as live detection and duplicate vote checking have been included in the proposed SmartVote system to avoid any type of spoofing, impersonation, or other types of fraudulent activities. The proposed SmartVote system is implemented using a Python programming language as the core language. Other libraries used in the proposed SmartVote system are OpenCV for image processing, MediaPipe for facial recognition, TensorFlow/Keras for machine learning algorithms, and PyQt5 for the GUI interface. Biometric verification is implemented using fingerprint matching algorithms and facial embedding algorithms. MySQL/SQLite is used for storing data securely in the proposed SmartVote system.***

Keywords: Smart Voting, Biometric Authentication, Facial Recognition, Fingerprint Verification, Optical Fingerprint Sensor, Liveness Detection, Computer Vision, AI-Based Security, Electronic Voting System

I. INTRODUCTION

Electronic voting systems are increasingly being used to make voting processes faster, more efficient, and better managed. Despite all these benefits, many of the voting systems currently in use are facing severe problems, such as identity fraud, duplication of votes, impersonations, and poor verification processes. Voting systems based on single biometric verification, such as fingerprint or facial verification, are often facing severe problems of spoofing, poor image quality, and environmental conditions. These problems clearly indicate the need for a more reliable and intelligent voting system.

The proposed system will be able to overcome all these problems associated with voting processes by using a dual verification system based on fingerprint verification and artificial intelligence-based facial verification. This will make voting processes more secure, as voters will be verified using two different biometric characteristics. Artificial intelligence will also be used to make voting processes more secure by using advanced features such as liveness detection, prevention of spoofing, detection of masks or obstructions in faces, and behavioral analysis. This will ensure that voting processes are conducted by real individuals who are physically present, thereby reducing fraudulent activities.

In order to make this system more inclusive and user-friendly, it is implemented in multiple languages, such as Telugu, Hindi, and English. Furthermore, voice-based guidelines are included in this system to assist elderly people, people from rural areas, and people with less technical knowledge. In addition, a time slot-based voting system is included in this project. It helps manage the flow of voters, avoid overcrowding, and identify unauthorized or premature voting attempts. Once the biometric verification is done, a risk score is generated, dividing every voting attempt into Green, Yellow, or Red zones. These zones are used to identify voting activities, helping administrators to track voting activities and respond quickly in case of irregularities.

Apart from security, this system ensures a complete and transparent voting workflow. Verified votes are stored, and administrators are provided with a real-time dashboard, detailed logs, and AI-based post-election analysis. These features ensure a comprehensive workflow, providing valuable insights for a better voting process.

This project showcases how artificial intelligence, dual biometric verification, and workflow management come together to create a robust voting system. With security, inclusiveness, and transparency at its core, this proposed system is a scalable solution for voting systems in various scenarios..

II. MOTIVATION

The growing use of digital technologies in critical infrastructure has thus raised a pressing need for the development of secure electronic voting systems. In the past, voting processes have been largely manual, relying on the verification of voting papers. However, voting processes have been largely vulnerable to errors, delays, and security risks, including impersonation and duplication. Research studies have suggested that voting irregularities, which may amount to only 1-3% in less secure voting systems, could arise from inadequate identity verification and loopholes in the system. Although the percentage is seemingly small, the outcome could be significant in a closely contested election, thus sparking serious security concerns.

Considering the fact that there is a rapid advancement in the field of artificial intelligence and biometric systems, there is a huge scope of improving the security and transparency of the voting systems. Biometric systems, such as fingerprint recognition and facial recognition, can be a better solution for authenticating the identity of the voters compared to other traditional methods. However, it has been proven through research that biometric attacks can be launched with a probability of 10-20% if there is no implementation of live detection systems.

The major motivation for undertaking this project is to design a voting system that is not only secure and intelligent but can overcome the challenges currently experienced in voting processes using the integrated biometric technology with artificial intelligence. Through the use of fingerprint scanning technology and facial recognition technology, the proposed voting system is able to minimize fraudulent activities in the voting process and ensure that only eligible voters participate in the electoral process.

The other motivation for undertaking this project is to design a voting system that is not only efficient but also effective and user-friendly for real-world applications. Through the proposed voting system, the voting process is not only efficient but also effective in the sense that it is able to automate the voting process. Moreover, the proposed voting system is an example of how computational technology can be used to enhance democratic processes.

The motivation for undertaking this project is to design a voting system that is not only reliable but also secure and intelligent for future voting processes..

III. WORKING PRINCIPLE

Secure electronic voting involves verification of individuals' identities and prevention of fraudulent activities such as impersonation and duplication of votes. In a normal system, a single-factor verification system may not be sufficient to ensure security. The SmartVote system has been designed to overcome all the challenges in the voting process by using dual biometric verification coupled with artificial intelligence. This will ensure a secure and efficient voting system.

1) Development of Voter Enrollment and Registration Module

This involves a special module designed to enroll voters by capturing their personal information and biometric data such as fingerprint and facial images. This information will be processed and saved in an encrypted format to prevent unauthorized access.

2) Biometric Data Acquisition and Preprocessing

During the voting process, an optical fingerprint sensor and a web camera will be used to capture biometric data. Preprocessing of the acquired data will involve noise reduction, normalization, and alignment of features to enhance the accuracy of the input data.

3) Construction of Dual Biometric Authentication Using AI Models

The system uses fingerprint matching algorithms and AI-based facial recognition models for voter verification. Feature extraction methods are used for both biometric verification, and then the features are compared for accurate matching and authentication.

4) Application of Liveness Detection and Duplicate Vote Verification

The system also includes liveness detection, which verifies whether the biometric input comes from a real person or not. In addition, a duplicate vote verification mechanism checks if a voter has already voted or not.

5) Facilitating Secure Vote Process and Data Storage

Once the voter's verification process is successfully completed, he or she is granted access to vote. The vote is then securely stored in the database using appropriate encryption methods.

6) Incorporating Monitoring and Fraud Detection Mechanisms

The system includes a monitoring mechanism that tracks all user activities and detects suspicious activities. The system maintains a log of all activities, and notifications are sent in case of any suspicious activities.

Finally, all the modules, including voter registration, biometric acquisition, authentication, liveness check, voting, and monitoring, are integrated into a seamless whole within a Python environment with frameworks such as PyQt5 for the GUI and OpenCV, MediaPipe, and TensorFlow/Keras for biometric processing and artificial intelligence verification. The entire system is designed to allow for seamless interaction between the different components for real-time processing and decision-making. The database system is responsible for managing voter information, biometric data, and voting information in a secure manner. It is also responsible for integrity and fast retrieval of data. The proposed voting system is thus scalable for small-scale institutional elections.

IV. LITERATURE SURVEY

Gaurav Thakur, Pradeep Chouksey, Mayank Chopra, and Parveen Sadotra (2024) proposed a multi-factor authentication framework combining fingerprint verification and cryptographic algorithms to enhance e-voting security in India. Their study emphasized that the integration of biometric identity and encryption protocols effectively prevents duplication, impersonation, and tampering during electronic voting. This supports the inclusion of fingerprint-based authentication and AES-RSA cryptography modules in the proposed system for voter verification and secure data transmission. [1]

Ashish Dixit, Avadhesh Kumar Gupta, Gurmeet Kaur, Mradul Jain, Rahul Kumar Pandey, and Anubha Sharma (2024) explored the combination of biometric authentication and IoT-enabled infrastructure to enhance voting security and accessibility. Their findings show that real-time data communication and automated validation using IoT improve transparency and speed. This study informs the real-time monitoring and alert subsystem in the proposed model for detecting duplicate or suspicious votes. [2]

P. V. Sidharth, P. M. Nagarajan, Dany Geo Johnson, Aadith Anil Kumar, and KalakunnathNamitha (2024) introduced a two-phase authentication framework for e-voting systems to mitigate fraudulent access. Their work demonstrates that a layered verification process combining biometrics and secure access codes reduces identity spoofing risks. This inspires the dual biometric (fingerprint + face) verification layer integrated into the proposed AI-enabled system. [3]

Sanjay Kumar and Manpreet Singh (2013) designed an early secure voting system using fingerprint identification. While effective for unique voter identification, their system lacked modern encryption and AI-based anomaly detection. This motivates the proposed project's AI-driven liveness detection and cryptographic vote protection to overcome limitations of earlier biometric models. [4]

Kandan M., Devi K.D., Sri K.D.N., Ramya N., and Vamsi N.K. (2021) developed a smart voting system using face detection and recognition algorithms. Their research highlights the effectiveness of facial biometrics for quick voter verification but notes challenges in lighting conditions and spoofing attacks. This study supports the integration of AI-based face recognition with liveness and spoof detection for reliable and genuine voter participation. [5]

D. Ashok Kumar and T. UmmalSariba Begum (2011) presented a microcontroller-based fingerprint voting prototype, emphasizing hardware simplicity but lacking scalability and encryption. Their findings guide the hardware architecture and modular design of the proposed system, ensuring adaptability to larger election environments while maintaining security. [6]

Cranshaw et al. (2017) introduced Calendar.help, a workflow-based scheduling agent that integrates human intelligence with AI automation. Their work demonstrated that a "human-in-the-loop" approach allows the system to handle complex and unstructured constraints that purely automated systems fail to process. The study showed that users have higher trust and satisfaction when they retain final oversight of the AI's proposed schedules, supporting an agentic rather than fully autonomous model [7].

Abdelrazek, M., et al. (2022) investigated the visualization challenges in personal informatics dashboards. Their study shows that users frequently struggle with "data voids" and complex graphical representations that fail to convey immediate meaning or context. The authors suggest that simplified, actionable visualizations are essential for preventing abandonment and ensuring that users can derive value from their tracked data [8].

Dizon, G., and Tang, D. (2017) explored the comparative effectiveness of intelligent digital assistants versus paper flashcards for vocabulary acquisition. Their study demonstrates that digital tools encourage more frequent study sessions during short periods of downtime, such as commuting or waiting. The results showed that this utilization of "dead time" leads to higher cumulative engagement, validating the mobile-first approach for modern learning tools [9].

Alshehhi, Y. A., et al. (2022) surveyed the needs and challenges associated with mHealth tracking applications. Their work highlights a critical disconnect where health data is often isolated from the user's broader life context. The authors demonstrate that for tracking to be effective, systems must integrate physiological metrics with daily productivity and lifestyle context to provide holistic and actionable guidance [10]

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

V. METHODOLOGY

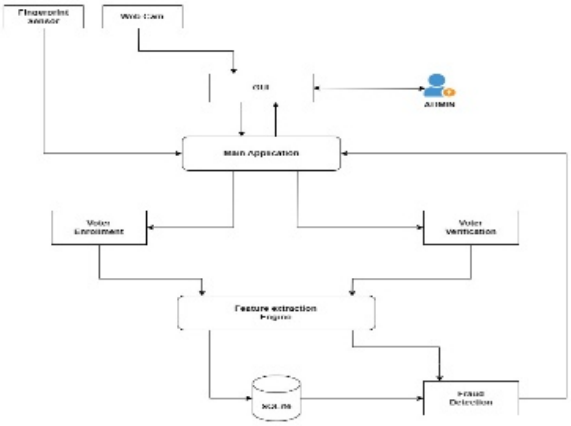


Fig.1: System Architecture

SmartVote uses a structured and systematic approach to design and develop a secure e-voting system using artificial intelligence and dual biometric verification. The methodology is based on accurate verification of voters, preventing fraudulent practices, and ensuring transparency during the entire e-voting process.

1) Data Collection and Voter Enrollment

The first step in the process is to collect voter information, which includes personal information as well as biometric information such as fingerprint and facial images. This information is collected using an optical fingerprint sensor and a web camera. The collected information is then processed and saved in the database in an encrypted format

2) Biometric Data Preprocessing and Feature Extraction

The biometric data obtained from the sensors is subject to preprocessing to ensure that it is of high quality. Feature extraction algorithms are then used to interpret the biometric data, allowing for a precise matching process.

3) Model Development and Integration

The artificial intelligence models are created using TensorFlow or Keras for facial recognition purposes. Fingerprint recognition uses minutiae-based matching algorithms. The models are then integrated to allow for efficient biometric authentication.

4) Authentication and Verification Process

After a voter has been authenticated, access to the voting system is granted. The voter then casts their vote

5) Monitoring and Fraud Detection

The system also monitors all activities. It logs all operations. There is a fraud detection mechanism that uses pattern analysis to detect suspicious activities such as repeated attempts. There are alerts for administrative review.

6) System Integration and Deployment

All modules, such as enrollment, authentication, voting, and monitoring, are combined under a single platform, all implemented through Python-based technologies. The interface is implemented using PyQt5, while OpenCV, MediaPipe, and AI models are used for biometric processing. The system is scalable, making it fit for deployment in real-world scenarios.

7) Results

The final output is presented as authenticated voting results, as well as voter verification status. The system allows for confirmation of successful or failed authentication through biometric verification. Administrative interfaces are provided to monitor voting statistics, as well as suspicious voting attempts. The output ensures transparency, prevents fraudulent voting, and facilitates decision-making for institutions or small-scale voting.

VI. TECHNOLOGIES USED

The development and implementation of the SmartVote system utilize a variety of artificial intelligence methods, biometric technologies, and supporting software tools in order to make it a secure and efficient system of electronic voting.:

1) **Python Programming Language:** Python is used as the core programming language for implementing system logic, backend processing, and integrating AI models due to its flexibility and rich ecosystem of libraries.
2) **Convolutional Neural Networks (CNNs) with ArcFace:** CNN-based models are used for facial recognition, with ArcFace providing highly accurate facial embeddings and improved identity verification performance.
3) **TensorFlow/Keras-Frameworks:** These deep learning frameworks are utilized for building, training, and deploying AI models for facial recognition and intelligent authentication processes.
4) **OpenCV-Library:** OpenCV is used for real-time image capture, preprocessing, and face detection, ensuring high-quality input for recognition models.
5) **Biometric-Feature-Extraction:** Feature extraction techniques are applied to both fingerprint and facial data to convert raw inputs into structured representations for accurate matching.
6) **Firebase_Authentication:** Firebase is used for managing user authentication, providing secure login, identity handling, and session management.
7) **Database_Management_(SQLite):** SQLite is used for storing voter information, biometric templates, and voting records securely, ensuring efficient data retrieval and integrity.
8) **PyQt5_Framework:** PyQt5 is used to design and develop the graphical user interface (GUI), enabling smooth and user-friendly interaction for both voters and administrators.
9) **Version_Control_(Git):** Git is used for version control, helping track changes, manage code efficiently, and support collaborative development.
10) **Image-Processing_Techniques:** Techniques such as normalization, noise reduction, and feature alignment are applied to enhance biometric input quality and improve model performance.

.

VII. FUTURE SCOPE

The SmartVote system is a good base for a secure and intelligent electronic voting system; however, the system can be further improved to make it suitable for larger-scale election environments. In the future, the system can be improved to make it suitable for larger-scale public elections using cloud computing infrastructure and distributed database management for efficient management of a large number of users.

The system can be improved using advanced biometric technologies like iris scan or multi-modal authentication for improved security. In addition, the system can be improved using blockchain technology for secure vote storage. The system can be improved to make it accessible to a larger population by using multi-language voice assistance and mobile application support for voting using smartphones. In addition, the system can be improved by integrating national identity platforms like Aadhaar for efficient voter verification.

The system can be improved using advanced AI models for efficient fraud detection using behavioral pattern analysis. In addition, the system can be improved using remote voting with secure authentication for efficient voting from different locations.

The future enhancements for the SmartVote system will make the system more scalable, secure, accessible, and suitable for practical use.

VIII. CONCLUSION

The SmartVote system has been successfully designed and implemented, demonstrating efficient and reliable performance across all modules. The integration of dual biometric authentication using an optical fingerprint sensor and AI-based facial recognition ensures accurate voter verification and significantly reduces the risk of impersonation and duplicate voting.

The inclusion of liveness detection further strengthens the system by preventing spoofing attempts and ensuring that only genuine users participate in the voting process.

All components of the system, including voter enrollment, biometric processing, authentication, vote casting, and monitoring, are seamlessly integrated to provide a smooth and secure workflow. The system operates in real time with minimal delay, offering a user-friendly interface and efficient data management. The voting process is carried out securely, with all votes stored safely in the database while maintaining confidentiality and integrity.

The results obtained from the implementation confirm that the system performs effectively and meets the intended objectives. The SmartVote system proves to be a robust, scalable, and practical solution for secure electronic voting. It can be successfully applied in institutional and small-scale elections, contributing to transparent, accurate, and trustworthy election management.

REFERENCES

[1] Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S. (2009). *Handbook of Fingerprint Recognition.* Springer. A foundational reference on fingerprint extraction, minutiae matching, and biometric security.

[2] Zhang, K., Zhang, Z., Li, Z., and Qiao, Y. (2016). "Joint Face Detection and Alignment Using Multi-task Cascaded Convolutional Networks (MTCNN)." *IEEE Signal Processing Letters*, 23(10), 1499–1503. A widely used model for fast, accurate face detection.

[3] Parkhi, O. M., Vedaldi, A., and Zisserman, A. (2015). "Deep Face Recognition." *British Machine Vision Conference(BMVC).*Introduces the VGGFace CNN model used in high-precision face recognition systems.

[4] Nikisins, O., and Petrovics, G. (2018). "Presentation Attack Detection in Biometric Systems: A Review." *IEEE Access*,6,13530–13549.Comprehensive review on liveness detection for anti-spoofing in face and fingerprint recognition.

[5] McCorry, P., Shahandashti, S. F., and Hao, F. (2017). "A Smart Contract for Boardroom Voting with Maximum Voter Privacy." *International Conference on Financial Cryptography and Data Security.* Discusses blockchain and cryptographic protocols relevant for secure vote storage and auditing.

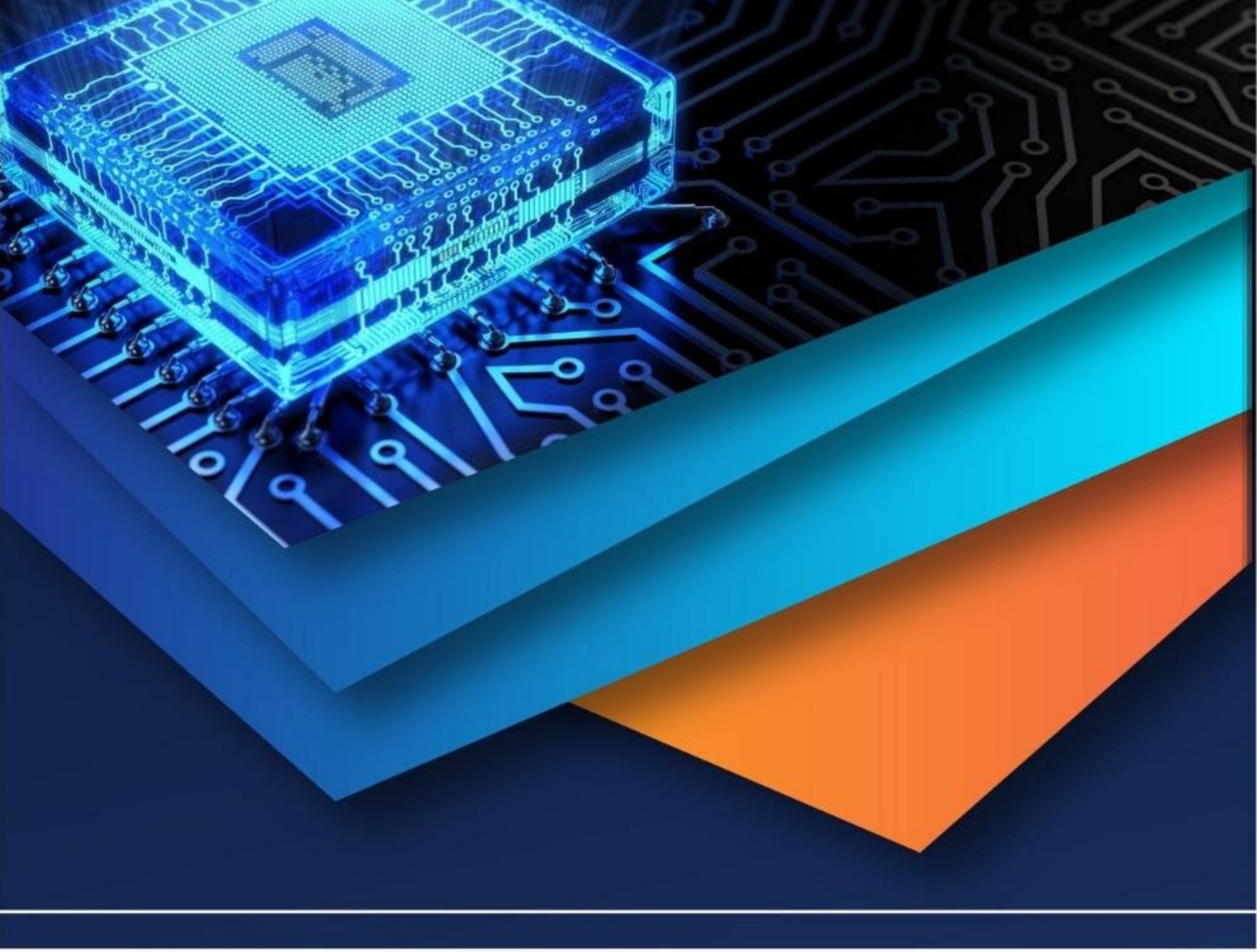
[6] Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice.* Pearson. Key reference for AES, RSA, hashing, message authentication codes, and secure communication.

[7] Ross, A., Nandakumar, K., and Jain, A. K. (2006). *Handbook of Multibiometrics.* Springer. Covers multimodal authentication systems such as combined fingerprint and face verification.

[8] Chollet, F. (2017). "Xception: Deep Learning with Depthwise Separable Convolutions." *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 1251–1258.CNN architecture used in high-performance face recognition and liveness detection models.

[9] Adida, B. (2008). "Helios: Web-based Open-Audit Voting System." *USENIX Security Symposium*, 335–348. A transparent and verifiable e-voting model, useful for understanding secure online election frameworks.

[10] Olaniyi, O. M., Folorunso, T. A., Ahmed, A., and Joseph, O. (2016). "Design of Secure Electronic Voting System Using Fingerprint Biometrics and Crypto-Watermarking Approach." *International Journal of Computer Applications.* Discusses fingerprint-based voting and encrypted watermarking for vote integrity.of Environmental Research and Public Health, 19(19), 12633.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY