iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VII **Month of publication:** July 2026

DOI: https://doi.org/10.22214/ijraset.2026.84278

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 VII July 2026- Available at www.ijraset.com

AI Facial Recognition Smart Locker Security System with Multi-Level Authentication

M. Nagakeerthi[1], Etamsetti Padma[2]
[1]*Associate Professor,* [2] *MCA Final Semester, Master of Computer Applications, Sanketika Vidya Parishad Engineering College, Vishakhapatnam, Andhra Pradesh, India*

Abstract: ***AI Facial Recognition Smart Locker Security System with Multi-Level Authentication is an intelligent AI-based security platform designed to provide secure, reliable, and keyless access control for lockers and restricted areas through multi-factor authentication techniques. In today's digital era, traditional locker systems that rely on physical keys, passwords, or RFID cards are vulnerable to theft, duplication, unauthorized access, and security breaches. This project addresses these limitations by offering a real-time, intelligent, and multi-level authentication mechanism using Artificial Intelligence and Machine Learning techniques.***

The system analyzes user authentication inputs such as facial features, behavioural patterns, voice commands, and One-Time Password (OTP) verification to accurately identify authorized users and prevent unauthorized access. It integrates modern technologies including Artificial Intelligence, Computer Vision, Machine Learning algorithms, biometric authentication methods, email-based OTP services, and database management systems to ensure security, efficiency, scalability, and real-time monitoring.

By combining facial recognition intelligence with multi-level authentication and intruder detection mechanisms, the AI Facial Recognition Smart Locker Security System aims to provide a secure, intelligent, and scalable access control solution suitable for banks, offices, smart vaults, and other restricted environments.

I. INTRODUCTION

Security plays a vital role in protecting valuable assets and personal information. However, one of the major challenges faced by traditional locker systems is the lack of secure and intelligent authentication mechanisms. Conventional systems that rely on physical keys, passwords, or RFID cards are vulnerable to theft, duplication, hacking, and unauthorized access.To overcome this problem, the AI Facial Recognition Smart Locker Security System with Multi-Level Authentication is developed as an AI-powered security platform that provides real-time and secure locker access using advanced authentication techniques. The system leverages Computer Vision and Machine Learning to identify authorized users through facial recognition and deliver secure access control.Based on this, the system incorporates additional security mechanisms such as Behaviour Authentication, Voice Authentication, OTP Verification, and PIN Backup to provide multi-level protection and prevent unauthorized access. The integration of Artificial Intelligence and Machine Learning techniques ensures improved security, real-time monitoring, and enhanced authentication accuracy.

II. EXISTING SYSTEM

The existing locker security systems primarily rely on physical keys, passwords, and RFID cards for authentication. [4]These approaches provide a basic level of security; however, they are not sufficient to meet the growing need for secure and intelligent access control. [2]Physical keys can be lost or duplicated, passwords can be shared or hacked, and RFID cards can be stolen or cloned. Similarly, traditional systems lack intelligent monitoring and are unable to verify the identity of users accurately.[1]Moreover, these conventional systems suffer from several limitations, including the absence of multi-level authentication, real-time monitoring, and intruder detection mechanisms. Most existing systems do not incorporate advanced technologies such as facial recognition, behaviour analysis, voice authentication, or OTP verification to ensure secure access. [6]As a result, they fail to provide reliable protection and are unable to effectively prevent unauthorized access to lockers and restricted areas.

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

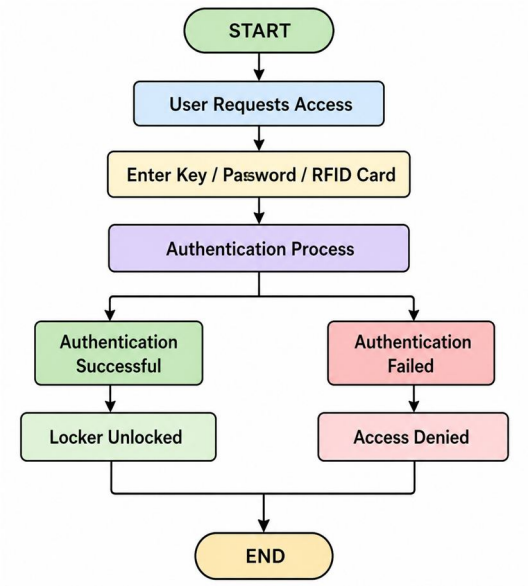


Figure : Flow Chat

A. Challenges

The major challenges identified in the existing locker security systems highlight the limitations of traditional authentication methods and the need for a more secure and intelligent access control solution.

- Lack of Multi-Level Authentication: Most existing locker systems rely on a single authentication method such as physical keys, passwords, or RFID cards. If these credentials are lost, duplicated, or stolen, unauthorized users can easily gain access. [7]The absence of multiple verification layers significantly reduces the overall security of the system.
- Limited Security and User Verification: Traditional systems do not accurately verify the identity of the user. [6]They lack advanced technologies such as facial recognition, behaviour analysis, and voice authentication, making it difficult to distinguish between authorized and unauthorized individuals. [9]This limitation increases the risk of security breaches and unauthorized access.
- No Real-Time Monitoring and Alerts: Existing systems do not provide real-time monitoring or instant notifications during suspicious activities. [11]In case of unauthorized access attempts, there is no mechanism to immediately inform the owner or capture evidence of the intrusion. [9]This reduces the effectiveness of security management and incident response.
- Lack of Intruder Detection Mechanisms: Conventional locker systems do not include intelligent intruder detection features. [12]They fail to capture images of unauthorized users, generate alerts, or perform additional verification procedures such as OTP authentication. [15]As a result, security incidents often remain unnoticed and unrecorded.
- Data Management and Scalability Limitations: Most existing systems do not efficiently manage user authentication records, security logs, and biometric information. [13]They lack intelligent data processing and scalable security mechanisms required for modern access control systems. Consequently, these systems cannot adapt to increasing security requirements and fail to provide reliable and efficient protection.

III. PROPOSED SYSTEM

The proposed system, AI Facial Recognition Smart Locker Security System with Multi-Level Authentication, is an AI-based security platform designed to provide secure and intelligent access control for lockers and restricted areas. It uses ad[14]vanced authentication methods to identify authorized users and prevent unauthorized access. [8]The system includes features such as Facial Recognition, Behaviour Authentication, Voice Authentication, OTP Verification, and Email Alerts. It integrates technologies like Artificial Intelligence, Machine Learning, Computer Vision, and Speech Recognition to ensure secure authentication and real-time monitoring. Overall, the system provides a secure, reliable, and scalable solution for modern smart locker security applications.

IV. ALGORITHM

The system uses **Artificial Intelligence, Machine Learning, and Computer Vision techniques** to process biometric inputs and perform secure user authentication. These algorithms help in recognizing patterns, making authentication decisions, and improving the accuracy of verification over time. [3]The system continuously processes authentication data and enhances its performance. By combining different authentication methods, it ensures better security and reliable access control. [2]Overall, algorithms play a key role in making the smart locker system intelligent and efficient.

1) Decision ProcessThe decision process involves analyzing biometric inputs and identifying meaningful patterns from the authentication data. Based on this analysis, the system grants or denies access to the locker. It helps in verifying user identity and providing secure authentication. This process forms the foundation for intelligent access control.
2) Error FunctionThe error function is used to evaluate how accurate the system's authentication results are. It compares the captured biometric data with stored information to identify mismatches. Based on this evaluation, the system measures performance and accuracy. [4] This helps in improving the quality of authentication over time.
3) Optimization ProcessThe optimization process focuses on improving the model's performance by adjusting its internal parameters. It reduces errors by continuously updating recognition models based on feedback. This iterative process ensures better accuracy with each authentication attempt. As a result, the system becomes more reliable and efficient.
4) Supervised LearningSupervised learning uses labeled biometric data to train the model for authentication and classification tasks. The system learns from known examples and improves its accuracy over time. It is useful for structured tasks where input-output relationships are defined. This method helps in delivering precise authentication results.
5) Unsupervised LearningUnsupervised learning works with unlabeled data to identify hidden patterns and relationships. It groups similar authentication data and discovers meaningful structures. This approach is useful for pattern analysis and anomaly detection. It enhances the system's ability to identify unusual activities.
6) Semi-Supervised LearningSemi-supervised learning combines both labeled and unlabeled data for training. It improves learning efficiency when labeled biometric data is limited. The system uses a small amount of known data to guide the analysis of larger datasets. This method balances accuracy and flexibility in authentication.

V. TECHNIQUE

The system uses various modern techniques to ensure secure authentication, intelligent user verification, and smooth communication between components. These techniques help in processing biometric inputs, generating authentication results, and managing security data effectively. They also improve system performance and reliability. By combining multiple techniques, the system delivers accurate and real-time authentication. Overall, these techniques play a crucial role in enhancing the functionality of the smart locker security system.

1) Facial RecognitionFacial Recognition is used to identify and verify users in a human-like manner. It analyzes facial images to identify facial features and compare them with stored biometric data. This helps the system provide secure and accurate authentication.
2) Multi-Level AuthenticationThe multi-level authentication technique provides additional security based on facial verification, behavioural analysis, voice verification, and OTP authentication. It analyzes multiple authentication factors to verify user identity. This helps users access the locker securely and prevents unauthorized access.
3) Email IntegrationEmail integration connects the frontend interface with email services and verification modules. It enables smooth data exchange and real-time processing of authentication requests. Through email services, the system sends OTP codes and security alerts efficiently.
4) Database ManagementDatabase management is used to store and organize user information, biometric data, and security logs in a structured format. It ensures data consistency, security, and easy retrieval of information. The system uses a database for scalability and reliability.

VI. METHODOLOGY

The methodology of the proposed system follows a structured process to ensure secure and intelligent authentication. Initially, users provide authentication inputs such as facial images, behavioural patterns, or voice inputs through the system interface. These inputs are captured in real time for verification.

Once the data is collected, it moves to the processing stage, where Artificial Intelligence, Machine Learning, and Computer Vision techniques are applied to analyze the biometric inputs. In this phase, the system extracts important features and prepares the data for authentication.

After processing, the information is sent to the verification module. [5] The system compares the captured data with stored biometric information and generates authentication results to grant or deny access to the locker.

A. Input

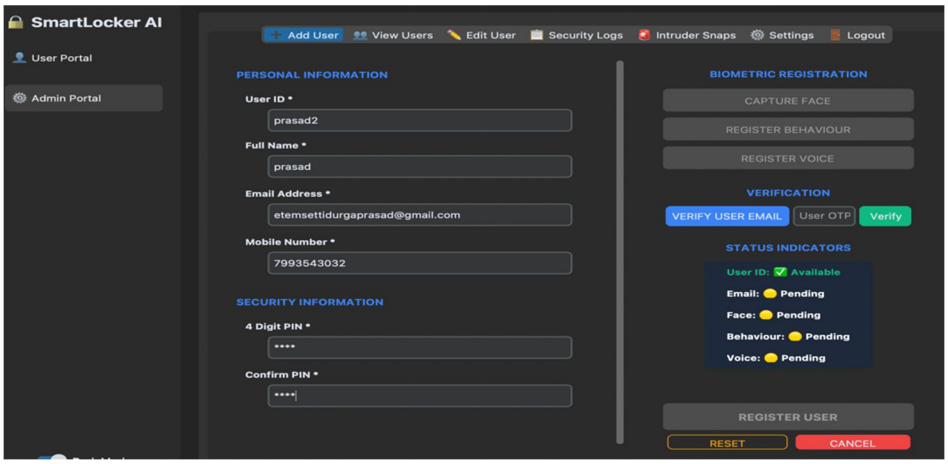


Figure 1: User Registration

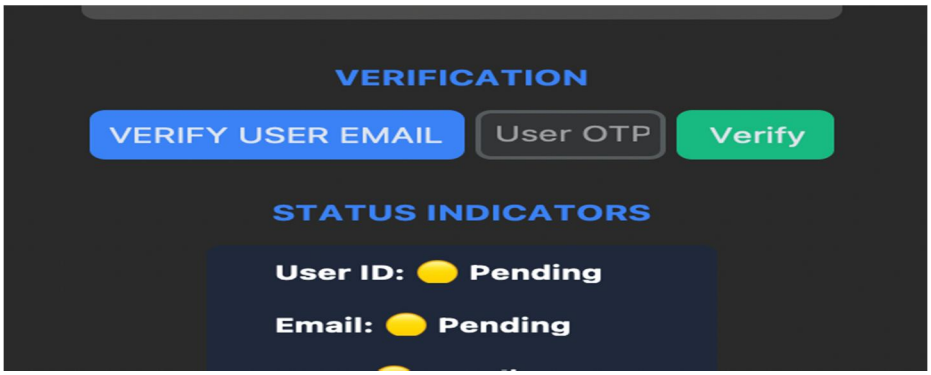


Figure 2 : Email OTP Verification

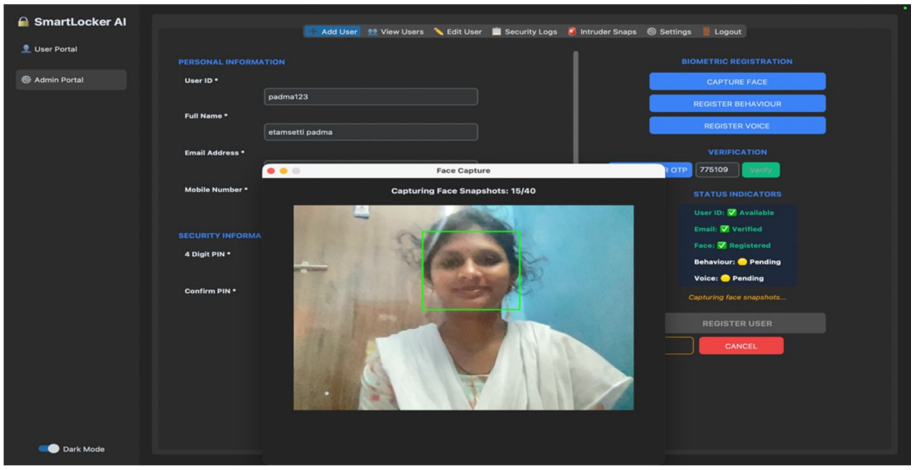


Figure 3 : Face Capture input page

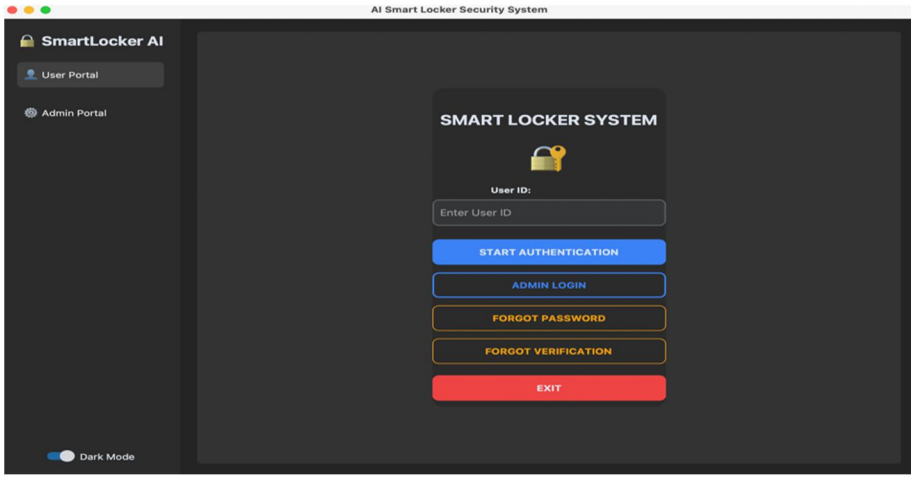


Figure 4 : Profile Input page

B. Output

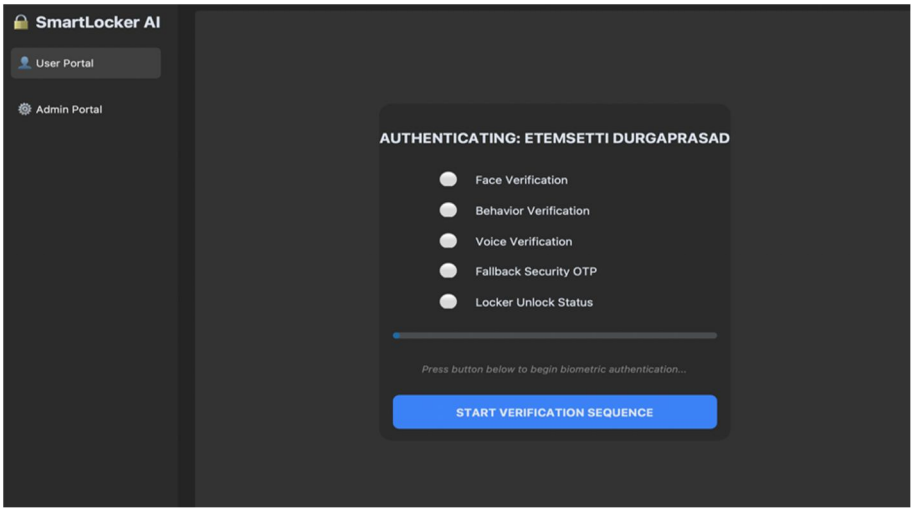


Figure 5 : Dashboard Output page

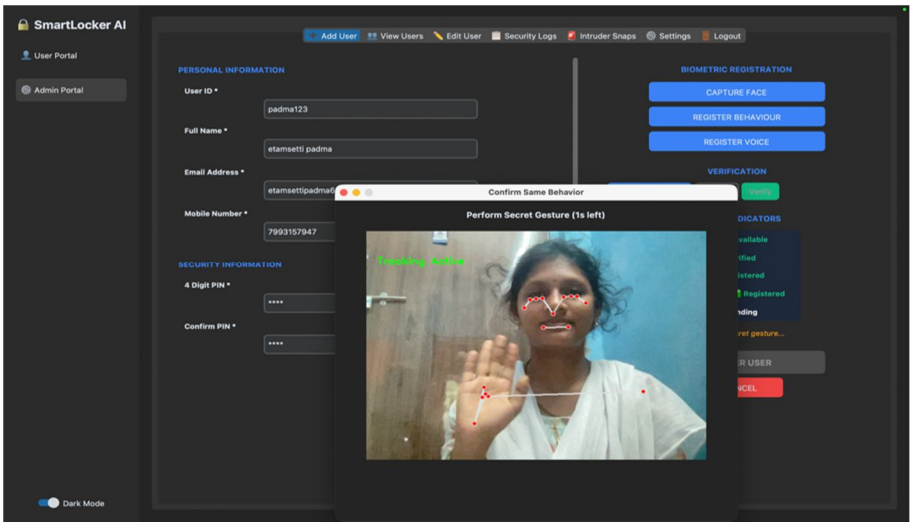


Figure 6: Ai Investment Advisor Output page

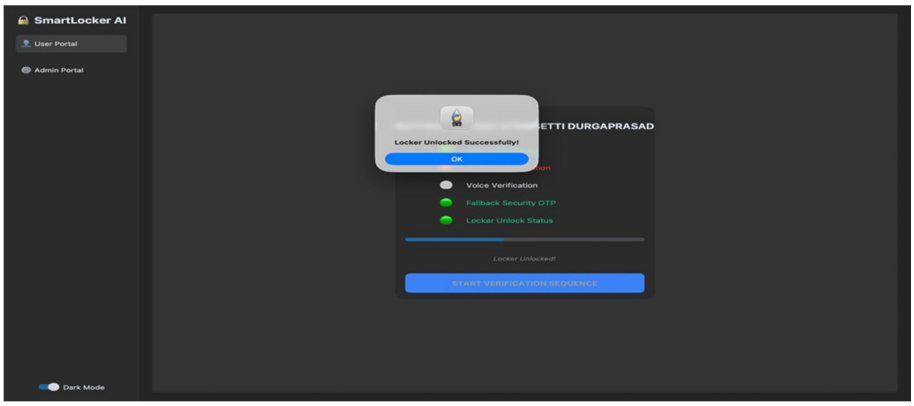


Figure 7: Chat History Output page

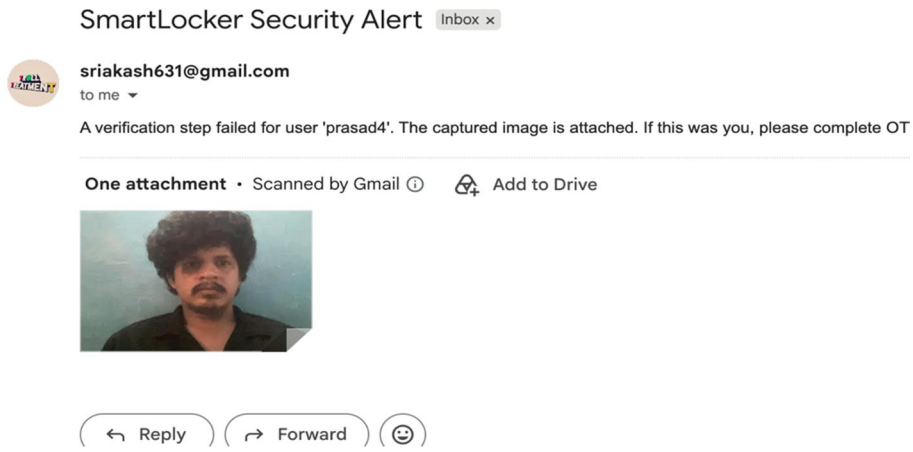


Figure 8: AI Visibility Score Output

VII. CONCLUSION

SmartLocker AI provides a secure and intelligent authentication system using facial recognition, voice verification, behavioural biometrics, and email OTP. The system enhances security, reduces unauthorized access, and offers efficient user authentication. Overall, it delivers a reliable and modern smart locker security solution.

REFERENCES

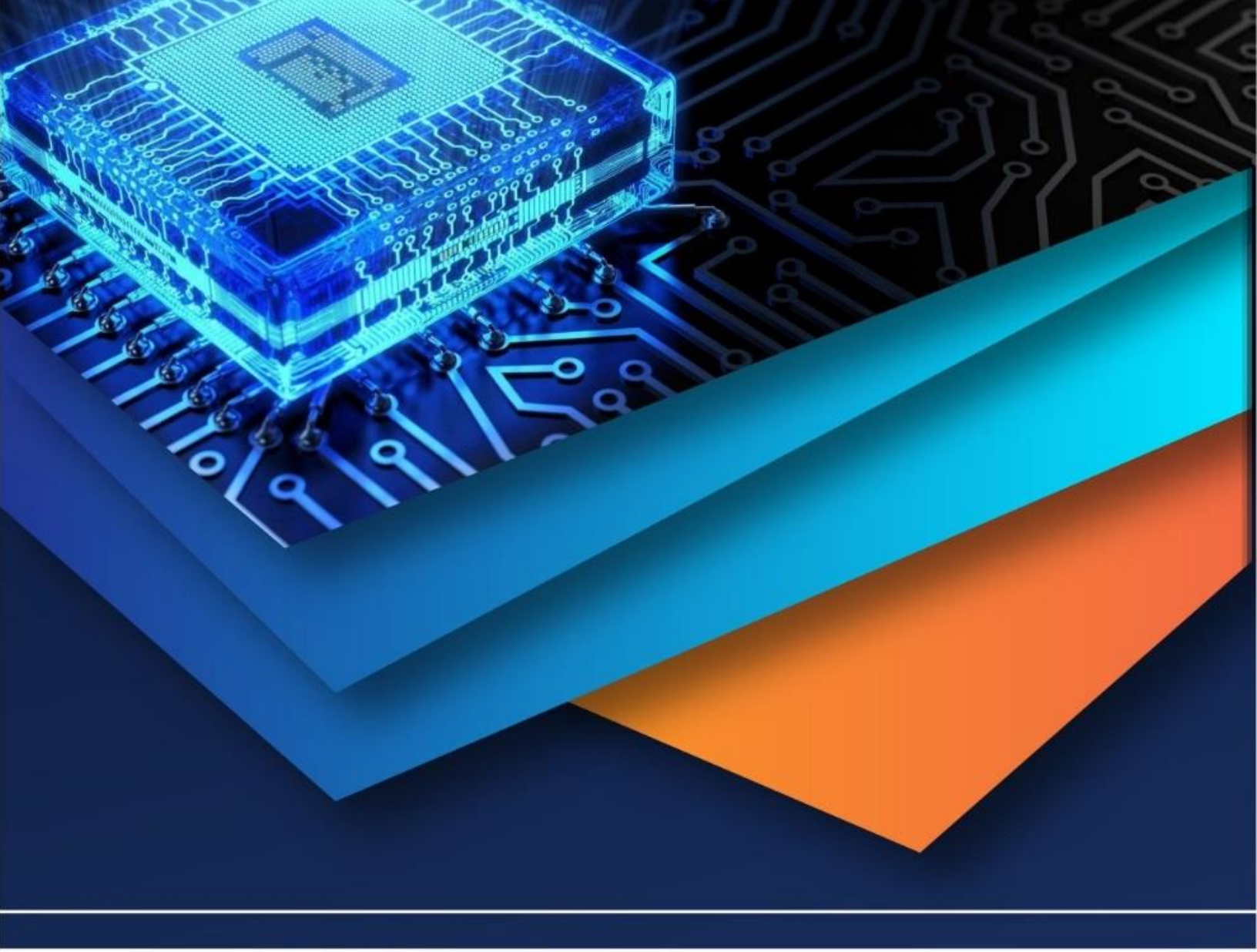
[1] Viola, P., & Jones, M. (2001). "Rapid Object Detection using a Boosted Cascade of Simple Features." *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 1, 511–518.
[2] Turk, M., & Pentland, A. (1991). "Eigenfaces for Recognition." *Journal of Cognitive Neuroscience*, 3(1), 71–86.
[3] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). "FaceNet: A Unified Embedding for Face Recognition and Clustering." *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 815–823.
[4] Zhang, K., Zhang, Z., Li, Z., & Qiao, Y. (2016). "Joint Face Detection and Alignment Using Multi-task Cascaded Convolutional Networks." *IEEE Signal Processing Letters*, 23(10), 1499–1503.
[5] Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
[6] Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. Springer.
[7] Bradski, G. (2000). "The OpenCV Library." *Dr. Dobb's Journal of Software Tools*.
[8] Zeng, W., & Zhao, Y. (2022). "Artificial Intelligence-Based Smart Security Systems: A Survey." *Journal of Information Security and Applications*, 65, 103091.
[9] Jain, A. K., Ross, A., & Nandakumar, K. (2011). *Introduction to Biometrics*. Springer.
[10] Daugman, J. (2004). "How Iris Recognition Works." *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 21–30.
[11] Rabiner, L. R., & Juang, B. H. (1993). *Fundamentals of Speech Recognition*. Prentice Hall.
[12] Howard, A. G., et al. (2017). "MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications." *arXiv preprint arXiv:1704.04861*.
[13] Szeliski, R. (2022). *Computer Vision: Algorithms and Applications* (2nd ed.). Springer.
[14] Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson.
[15] Sandhu, R., & Samarati, P. (1994). "Access Control: Principle and Practice." *IEEE Communications Magazine*, 32(9), 40–48.

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

BIBLOGRAPHY

Muppala Nagakeerthi working as an Assistant Professor in Master of Computer Applications in Sanketika Vidya Parishad Engineering College, Visakhapatnam, Andhra Pradesh, affiliated by Andhra University and approved with 'A' grade by NAAC and member in IAENG with 14 years of experience in computer science. Her areas of interests in C, Java, Data Structures, DBMS, Web Technologies, Software Engineering and Data Science.

Etamsetti padma is currently pursuing his final semester of Master of Computer Applications (MCA) at Sanketika Vidya Parishad Engineering College, which is accredited with an 'A' grade by NAAC, affiliated to Andhra University, and approved by AICTE. With a keen interest in Machine Learning and Artificial Intelligence, she has undertaken her postgraduate project titled "AI Facial Recognition Smart Locker Security System with Multi-Level Authentication" The project is carried out under the guidance of M.Nagakeerthi, assistant professor, svpe



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY