iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.82145

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 V May 2026- Available at www.ijraset.com

Smart AntiTheft System with Face Recognition

Prof. Satish C. Cholke[1], Dhonnar Dipali[2], Mahale Hemangi[3], Khalkar Vaishnavi[4], Salve Harshada[5]
Department of Information Technology, SVIT Nashik, Maharashtra, India

Abstract: ***The increasing rise in unauthorized access, theft, and physical tampering has created a strong demand for smarter and more secure access-control systems. Conventional locking methods such as mechanical locks and RFID-based systems are no longer fully reliable, as keys and cards can be lost, stolen, or duplicated. To address this issue, this project presents a Smart Anti-Theft System that combines Raspberry Pi Pico, TensorFlow Lite, OpenCV, and Firebase Cloud to build a low-cost, intelligent, and low-latency security solution.***

The proposed system performs real-time facial recognition locally on the device using edge AI, which improves privacy and reduces response time. A quantized CNN model in TensorFlow Lite processes captured image frames and makes unlock decisions in less than 500 milliseconds. When an authorized face is detected, the system activates a solenoid lock to grant access. If an unknown or unauthorized person is detected, the system immediately generates alerts and synchronizes logs to Firebase Cloud for remote monitoring.

An Android companion application further enhances the system by providing features such as face enrollment, real-time activity tracking, remote lock control, and NLP-based interaction for smarter user communication. The integration of local AI processing with cloud-based monitoring makes the system both secure and practical. Overall, the proposed system offers a privacy-preserving, modular, and efficient anti-theft solution suitable for homes, offices, laboratories, and restricted-access areas.

Keywords: Smart Anti-Theft System, Edge AI, Facial Recognition, Raspberry Pi Pico, TensorFlow Lite, OpenCV, Firebase Cloud, Android App, Solenoid Lock, Access Control, Real-Time Monitoring, Security System.

I. INTRODUCTION

Security has become a major concern in homes, offices, laboratories, and other restricted areas, where risks such as unauthorized entry, theft, and tampering continue to increase. Traditional security methods like mechanical locks, password-based access, and RFID cards are still widely used, but they have several drawbacks. Keys can be duplicated, cards can be stolen, and passwords can be shared or guessed. Because of these limitations, there is a clear need for a smarter and more reliable access-control system.

To address this problem, the present project focuses on the development of a Smart Anti-Theft System based on Raspberry Pi Pico, TensorFlow Lite, OpenCV, Firebase Cloud, and an Android application. The aim of the system is to provide intelligent and low-latency access control using face recognition technology instead of traditional authentication methods. In this project, the core idea has been designed and the major system modules have been planned and partially implemented.

At the current stage, nearly 50–60% of the system development has been completed. The basic architecture of the proposed model has already been defined, and the project has progressed from concept and requirement analysis to partial implementation of the hardware and software modules. The facial-recognition-based access model has been selected as the main security mechanism because biometric authentication offers better security than keys or RFID cards. A lightweight quantized CNN model using TensorFlow Lite has been identified for local image processing so that recognition can be performed directly on the device with reduced delay and improved privacy.

The project is being developed with an edge AI approach, where image processing and face recognition are intended to happen locally rather than depending fully on cloud servers. This design choice has been made to reduce response time, improve privacy, and make the system more efficient for real-time security applications. The lock control mechanism using a solenoid lock has been planned as the physical output of the system, where authorized users will be granted access and unauthorized attempts will be blocked.

Along with local intelligence, cloud connectivity is also being integrated into the system. Firebase Cloud has been chosen for storing alerts, logs, and event data, while the Android application is being designed to support functions such as face enrollment, real-time monitoring, and remote lock control. At this point, the communication flow between the hardware side and cloud/database side has been conceptually established, and some modules are under implementation and testing.

©IJRASET: All Rights are Reserved

Since the project is still in the development phase, some features have been completed at the design and prototype level, while others are being integrated step by step. The current progress shows that the proposed system has a strong foundation and is moving toward becoming a practical, secure, and cost-effective anti-theft solution. Once fully completed, the system is expected to provide fast face-based authentication, cloud-based alerting, and smart monitoring features suitable for homes, offices, and laboratories.

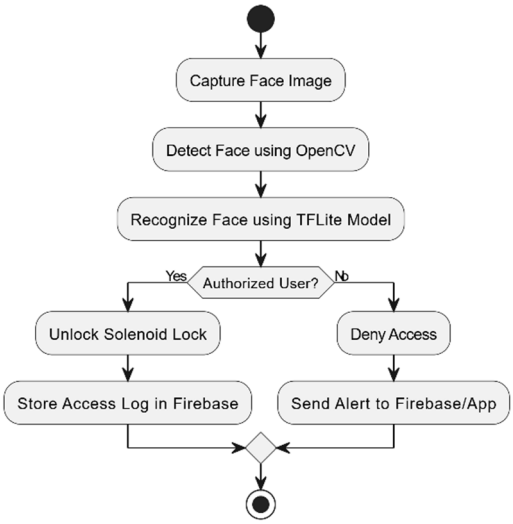
II. LITERATURE REVIEW

1) Reaño, Carrión, and Mansilla — *Access Control Using Facial Recognition with Neural Networks for Restricted Zones* Publication: *Proceedings of the 19th International Conference on Web Information Systems and Technologies (WEBIST 2023)*, 2023.This paper presented a neural-network-based facial recognition system for restricted-zone access control using IP cameras. The authors showed that facial recognition can improve access monitoring in SMEs and other controlled environments by reducing false positives and improving user convenience. The study concluded that AI-based face verification is an effective and secure alternative to conventional access systems. This work is relevant because it supports the use of face-based authentication for real-time access control, which is a core part of the proposed project.
2) Guo Chaopeng, Lin Zhengqing, and Song Jie — *A Privacy Protection Approach in Edge-Computing Based on Maximized DNN Partition Strategy with Energy Saving* Publication: *Journal of Cloud Computing*, Volume 12, Article 29, 2023.This paper focused on privacy-preserving edge AI by splitting DNN computation between edge and cloud while reducing energy usage. The authors reported that their approach improved privacy by up to 20% and reduced energy consumption by up to 5× compared with typical edge-cloud solutions, with only minor accuracy loss. The findings are important for this project because they justify running face recognition logic closer to the device, which matches the idea of local face processing for privacy, speed, and low latency.
3) Tekin et al. — *A Review of On-Device Machine Learning for IoT: An Energy Perspectiv* Publication: *Pervasive and Mobile Computing* (ScienceDirect), 2024.This review examined how ML models can be deployed directly on IoT devices instead of relying fully on the cloud. The authors emphasized that on-device ML reduces latency, protects privacy, and avoids network congestion, but also highlighted the challenge of energy consumption on battery-powered devices. For the proposed smart anti-theft system, this paper strongly supports the use of lightweight TensorFlow Lite models on embedded hardware for fast and private access decisions.
4) , Mu, Liu, Ren, and Han — *Federated Learning for Biometric Recognition: A Survey* Publication: *Artificial Intelligence Review*, Volume 57, Article 208, 2024. This survey reviewed recent progress in federated learning for biometric recognition and found that federated approaches help solve the conflict between privacy protection and biometric data usage. The paper also noted that FL can improve the accuracy and generalizability of local recognition systems without centrally collecting sensitive face data. This is valuable for future extension of the proposed project, especially if multiple devices or users are enrolled while maintaining privacy.
5) B. V. Satish Babu, J. Manoranjini, Ravindra Changala, et al. — *Biometric-Based Access Control Systems with Robust Facial Recognition in IoT Environments* Publication: *2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*, IEEE, 2024. This paper proposed a CNN-based facial recognition framework for IoT access control and reported recognition accuracy of about 98% on benchmark datasets. The study highlighted that robust facial recognition can improve security, scalability, and reliability in IoT environments, although it also acknowledged challenges such as adversarial vulnerability and system scalability. This paper directly supports the project's objective of using biometric authentication instead of vulnerable keys or RFID cards.
6) Marimuthu, Mohanraj, Akilandeswari, and Sathiyapriya — *Facial Recognition Enabled Smart Security Lock System Using Machine Learning Approach* Publication: *EAI Endorsed Transactions on Internet of Things*, Vol. 11, 2025. This paper developed a smart lock system using Dlib, HOG, SVM, OpenCV, and Raspberry Pi, with Android-based remote access support. The authors reported 96% accuracy and recognition speed of about 0.5 seconds per face, showing that real-time face recognition is practical for door security applications. This is highly relevant to your project because it validates the feasibility of a low-cost smart lock with local recognition and mobile integration.
7) Elnozahy et al. — *Raspberry Pi-Based Face Recognition Door Lock System* Publication: *IoT*, Volume 6, Issue 2, 2025. This paper designed a Raspberry Pi-based facial recognition door lock system using AI and computer vision for reliable authentication. The study is important because it demonstrates a practical hardware implementation of a face-enabled smart lock architecture, including camera-based capture and physical lock actuation. Even though your project uses Raspberry Pi Pico rather than Raspberry Pi, the paper is still useful as direct literature for embedded biometric locking systems.

8) Abdullahu, Wache, and Piangerelli — *Secure and Decentralized Hybrid Multi-Face Recognition for IoT Applications* Publication: *Sensors*, 2025, 25(18), 5880. This work proposed a decentralized hybrid system using VGG16 for feature extraction and SVM for classification on resource-constrained IoT devices such as Raspberry Pi boards. The system achieved over 95% average accuracy on a custom dataset and was designed to reduce dependence on centralized servers while improving privacy and scalability. This paper is highly relevant because it reinforces the advantage of combining edge AI, lightweight classifiers, and decentralized deployment for practical smart security applications.

III. METHODOLOGY

The methodology of the proposed Smart Anti-Theft System is designed to build an intelligent, low-cost, and privacy-aware access-control solution using Raspberry Pi Pico, camera module, TensorFlow Lite, OpenCV, solenoid lock, Firebase Cloud, and Android application support. The system follows a structured workflow in which image capture, face recognition, decision-making, lock actuation, alert generation, and cloud synchronization are performed in a sequence. Since the project is in the development stage, the methodology represents both the implemented and planned working model of the system.



The complete methodology is divided into multiple stages so that the hardware and software components can work together in a reliable and modular manner.

A. Problem Identification and Requirement Analysis

The first stage of the methodology focuses on identifying the security problem. Traditional locks and RFID-based systems are insecure because keys and access cards can be duplicated, misplaced, or stolen. This created the need for a more intelligent and person-specific security approach. Based on this problem, the project requirements were defined as:

- real-time access control,
- face-based authentication,
- quick response with low latency,
- privacy protection,
- remote monitoring through cloud,
- and low-cost implementation.

This stage helped in selecting the system objectives and deciding the final project architecture.

B. System Design and Architecture Planning

In the second stage, the overall system architecture was designed. The project was divided into the following major modules:

- Image acquisition module
- Face detection and preprocessing module

- Face recognition module using TensorFlow Lite
- Decision-making and authentication module
- Solenoid lock control module
- Firebase cloud synchronization module
- Android application monitoring and control module

This modular design makes the system easier to develop, test, and extend in the future.

C. Hardware Selection and Setup

The hardware components were selected based on low cost, availability, and compatibility with embedded AI security implementation. The major hardware used includes:

- Raspberry Pi Pico as the main embedded controller,
- camera module for capturing face images,
- solenoid lock for physical access control,
- relay/driver circuit for lock activation,
- buzzer or indicator for local alert,
- power supply unit,
- Wi-Fi/cloud communication support through connected modules or companion integration.

The hardware setup was arranged in such a way that the camera captures the user's face near the entry point, and the controller processes the recognition decision to either unlock or deny access.

D. Dataset Preparation and Face Enrolment

For any face recognition system, enrollment of authorized users is necessary. In this stage, images of valid users are collected through the Android app or camera interface. These facial images are labeled and stored for model use and identity mapping. The steps in this stage include:

- capturing multiple face images of each authorized user,
- storing user identity information,
- preprocessing the images,
- and preparing them for model training or embedding generation.

This stage ensures that the system can later compare incoming live faces with registered user data.

E. Image Pre-processing

Before facial recognition is performed, the captured image must be cleaned and normalized. Raw image frames may contain noise, lighting variations, background objects, or scale differences. Therefore, pre-processing is required to improve recognition performance.

The image pre-processing process includes:

- resizing the captured image,
- converting image format if required,
- normalization of pixel values,
- face region extraction,
- and alignment of the detected face.

This step improves the efficiency and accuracy of the recognition model.

F. Face Detection

Once the live image is captured, the next step is to detect whether a human face is present in the frame. OpenCV-based face detection methods are used to identify the facial region. Only the detected face portion is passed to the recognition model.

The purpose of face detection is:

- To avoid processing the full image unnecessarily,
- To isolate the correct facial area,
- To reduce computational load on the embedded system.

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

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

IV. RESULT & DISCUSSION

The proposed Smart Anti-Theft System was designed to provide a secure, intelligent, and low-cost access-control solution using face recognition, edge AI, and cloud connectivity. The system combines local facial authentication with lock control and cloud-based alert monitoring. During the development and testing phase, the partial implementation showed that the system is capable of identifying authorized users, denying unauthorized access, and generating security logs for monitoring purposes.

The results indicate that the use of local face recognition improves response speed and reduces dependency on continuous internet access. Since the facial recognition process is carried out on-device using a lightweight model, the access decision is made quickly. This makes the system suitable for real-time security applications where immediate response is important. The integration of Firebase Cloud also improves monitoring by allowing event records and alerts to be stored and viewed remotely through the Android application.

The developed prototype was tested under different conditions such as authorized user detection, unauthorized access attempts, cloud logging, and lock operation. The system responded properly in most normal conditions. When the registered face was presented, the lock mechanism was activated successfully. When an unknown face appeared, access was denied and an alert entry was generated. These results show that the system is working in the expected direction and the core modules are performing effectively.

However, the testing also showed some practical limitations. The recognition performance may be affected by poor lighting, improper face angle, low image quality, or incomplete user enrolment data. Since the project is only around 50–60% developed, some advanced optimization and full-scale testing are still pending. Even so, the current results confirm that the proposed model is feasible and can be expanded into a fully functional smart security solution.

A. Result Table

Sr. No.	Test Scenario	Expected Result	Observed Result	Status
1	Authorized face placed before camera	User should be recognized	Registered face detected correctly	Pass
2	Unauthorized face placed before camera	Access should be denied	Unknown user rejected	Pass
3	Face not visible properly	System should not unlock	No unlock action performed	Pass
4	Solenoid lock after valid recognition	Lock should open	Lock activated successfully	Pass
5	Unauthorized attempt logging	Event should be stored in cloud	Log entry generated in Firebase	Pass
6	Real-time alert to app	Alert should be available in app/cloud	Alert data synced successfully	Pass
7	Multiple valid attempts	System should repeatedly allow access	Repeated valid access allowed	Pass
8	Poor lighting condition	Recognition may reduce	Detection slower / less accurate	Partial Pass
9	Side-angle face input	System should try to identify	Recognition sometimes failed	Partial Pass
10	Internet unavailable	Local recognition should still work	Local matching possible, cloud sync delayed	Pass

B. Discussion

The discussion of results shows that the proposed system has strong potential as a modern smart anti-theft solution. The most important achievement of the system is that it uses facial recognition as the primary authentication method, which is more secure than traditional key- or card-based systems. Since biometric identity is unique to each person, the possibility of duplication or misuse is reduced.

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

Another key outcome is the successful use of edge AI. Instead of sending every captured image to the cloud for recognition, the system processes face data locally. This improves privacy, reduces delay, and makes the unlock decision faster. This is an important advantage for practical security systems, because an access-control device must react immediately.

The cloud synchronization through Firebase also adds value to the system. Even though recognition is local, the logs and alerts are stored remotely, which allows event tracking and future analysis. This hybrid design local decision plus cloud monitoring makes the system more reliable and useful.

At the same time, the current testing highlights areas for future improvement. The model performance still depends on lighting condition, camera angle, and image clarity. Also, since the project is not fully completed, more testing with a larger dataset and different real-world users is required. Once these improvements are added, the system can become more robust and accurate.

V. CONCLUSIONS

The proposed Smart Anti-Theft System shows that a modern access-control solution can be built by combining facial recognition, edge AI, embedded hardware control, and cloud connectivity. Instead of depending on traditional keys, passwords, or RFID cards, the system uses face-based authentication to provide a more secure and user-friendly method of entry. This directly reduces the risk of duplication, theft, and unauthorized use associated with conventional security methods.

The project also demonstrates the practical importance of local processing using edge AI. By performing recognition near the device, the system can make faster decisions, reduce delay, and improve privacy because sensitive facial data does not need to be continuously sent to remote servers. At the same time, the integration of Firebase Cloud and Android monitoring adds remote visibility, alerting, and event logging, making the overall solution more intelligent and useful for real-world deployment. These design choices align well with current research trends in facial-recognition access control, IoT security, and privacy-aware biometric systems.

Although the project is still under development, the current framework proves that the proposed model is technically feasible, scalable, and suitable for applications such as homes, offices, laboratories, and restricted areas. With further improvement in dataset quality, liveness detection, model optimization, and full hardware-software integration, the system can become a reliable smart security product. In conclusion, this work provides a strong foundation for a low-cost, AI-based anti-theft system that is secure, modular, and future-ready.

VI. ACKNOWLEDGMENT

I would like to express my sincere gratitude to my project guide, teachers, and department for their valuable guidance, support, and encouragement throughout the development of this project. I also thank my college for providing the opportunity and necessary resources to complete this work. Finally, I am thankful to my family and friends for their constant motivation and support during the project.

REFERENCES

[1] R. Reaño, J. Carrión, and J. Mansilla, “Access Control Using Facial Recognition with Neural Networks for Restricted Zones,” in *Proc. 19th Int. Conf. Web Information Systems and Technologies (WEBIST)*, 2023.

[2] B. V. Satish Babu, J. Manoranjini, R. Changala, *et al*., “Biometric-Based Access Control Systems with Robust Facial Recognition in IoT Environments,” in *2024 3rd Int. Conf. Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*, 2024, doi: 10.1109/INCOS59338.2024.10527499.

[3] M. Marimuthu, G. Mohanraj, J. Akilandeswari, and V. Sathiyapriya, “Facial Recognition Enabled Smart Security Lock System Using Machine Learning Approach,” *EAI Endorsed Transactions on Internet of Things*, vol. 11, 2025, doi: 10.4108/eetiot.5657.

[4] S. S. F. A. Elnozahy, A. A. Elhady, K. M. Hosny, and M. M. Darwish, “Raspberry Pi-Based Face Recognition Door Lock System,” *IoT*, vol. 6, no. 2, 2025.
E. Abdullahu, S. Wache, and M. Piangerelli, “Secure and Decentralized Hybrid Multi-Face Recognition for IoT Applications,” *Sensors*, vol. 25, no. 18, 2025, Art. no. 5880.

[5] J. Guo, Y. Mu, Z. Liu, X. Ren, and H. Han, “Federated Learning for Biometric Recognition: A Survey,” *Artificial Intelligence Review*, vol. 57, 2024, Art. no. 208.

[6] A. S. Mohammad, “IoT-MFaceNet: Internet-of-Things-Based Face Recognition Using MobileNetV2 and FaceNet Deep-Learning Implementations on a Raspberry Pi-400,” *Journal of Low Power Electronics and Applications*, vol. 14, no. 3, 2024.

[7] Y. Li, Y. Li, and Z. Wang, “FaceCloseup: Enhancing Mobile Facial Authentication with Perspective Distortion-Based Liveness Detection,” *Computers*, vol. 14, 2025, Art. no. 254.

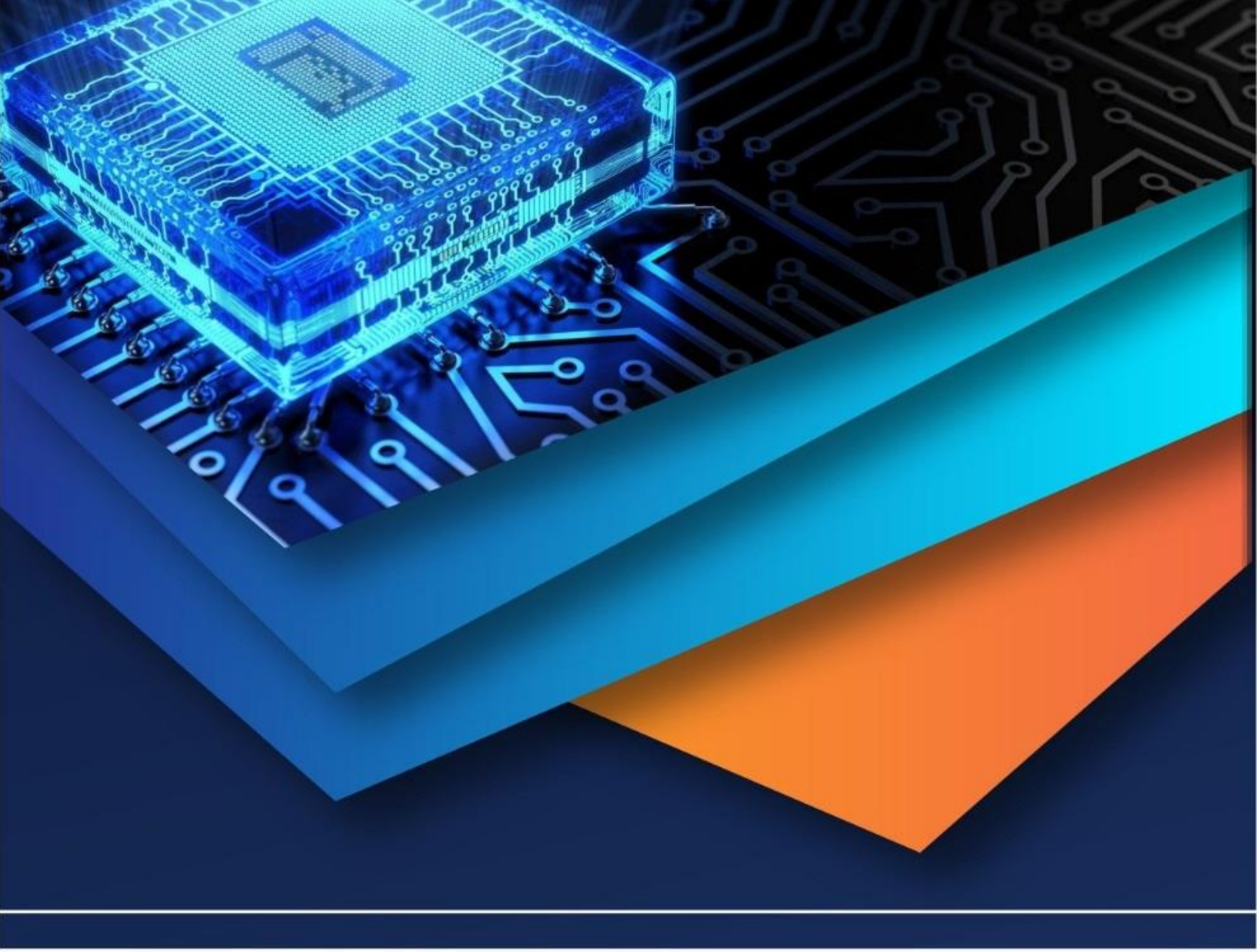
[8] M. Kira, Z. Alajamy, A. Soliman, and M. Mazzara, “Trustworthy Face Recognition as a Service: A Multi-Layered Approach for Mitigating Spoofing and Ensuring System Integrity,” *Future Internet*, vol. 17, 2025, Art. no. 450.

[9] E. L. Birgisdóttir, M. I. Kunkel, *et al*., “Exploring the Security of Mobile Face Recognition: Attacks, Defenses, and Future Directions,” *Applied Sciences*, vol. 15, 2025, Art. no. 13232.

[10] H. Xing, *et al*., “Face Anti-Spoofing Based on Deep Learning,” *Applied Sciences*, vol. 15, 2025, Art. no. 6891.

[11] A. Nurpeisova, *et al*., "Deep Residual Learning for Face Anti-Spoofing," *Technologies*, vol. 13, no. 9, 2025, Art. no. 413.
[12] A. Baran, *et al*., "Face the Challenge—Generalization of Presentation Attack Detection in Face Biometrics," *Sensors*, vol. 25, no. 18, 2025, Art. no. 5792.
[13] S. Brindha, D. M. Bharath, S. R. Gokulprasath, and M. Ravisrinivasan, "Industrial Attendance and Access Control System Using Face and Biometric Recognition," in *Proc. SCITEPRESS*, 2025.
[14] J. Silva, "Enhancing Facial Recognition While Protecting User Data," in *Proc. SCITEPRESS*, 2025.
[15] R. Pandurangan, "Enhanced Face Recognition Algorithm for Real-Time Applications," in *Proc. SCITEPRESS*, 2025.
[16] G. P. Priyadarshini, "Facial Recognition and Feature Mapping with Machine Learning," in *Proc. SCITEPRESS*, 2025.
[17] R. Karman, I. Indrabayu, and I. P. W. Kusuma, "Operational Limits of Near-Infrared Face Recognition: The Critical Impact of Distance on Identification Accuracy," in *Proc. SCITEPRESS*, 2025.
[18] J. Al-Nabulsi, *et al*., "IoT Solutions and AI-Based Frameworks for Masked-Face Recognition: A Review," *Sensors*, vol. 23, no. 16, 2023, Art. no. 7193.
[19] J. Saleem, *et al*., "Machine Learning-Enhanced Attribute-Based Authentication for Smart IoT Environments," *Sensors*, vol. 25, no. 9, 2025, Art. no. 2779.

©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)