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.2026.82406

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 Anti-Theft Security System with Face Recognition Using Edge AI for Real-Time Access Control

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: ***With the rapid increase in security threats such as unauthorized entry, theft, and tampering, the need for intelligent and reliable access-control systems has become more important than ever.***
Conventional security methods, including mechanical locks, passwords, and RFID-based systems, suffer from major limitations because they can be stolen, duplicated, or misused. To overcome these drawbacks, this paper presents a Smart Anti-Theft System based on Raspberry Pi Pico, TensorFlow Lite, OpenCV, Firebase Cloud, and Android application support. The proposed system is designed to provide a low-cost, fast, and privacy-aware security solution using real-time facial recognition as the primary authentication mechanism.
The system captures the user's face through a camera module and processes the image locally using a lightweight quantized Convolutional Neural Network (CNN) model deployed through TensorFlow Lite. By performing face recognition at the edge, the system reduces latency, improves privacy, and minimizes dependence on continuous cloud processing. If the detected face matches an authorized user, the system grants access by activating a solenoid lock. In contrast, if the face is unrecognized or unauthorized, the system denies access and immediately generates alerts and event logs. These logs are synchronized with Firebase Cloud, enabling real-time monitoring and secure data management.
An Android companion application is integrated with the system to provide additional functionality such as user face enrollment, real-time security event monitoring, remote lock control, and alert viewing.
The combination of embedded edge intelligence and cloud connectivity makes the proposed model efficient, modular, and suitable for practical deployment in homes, offices, laboratories, and other restricted environments. Experimental observations show that the system is capable of making quick authentication decisions and supporting smart anti-theft operations with improved security and usability.
The proposed work demonstrates that combining biometric authentication, edge AI, IoT connectivity, and mobile monitoring can produce a modern and effective anti-theft solution. The system offers a promising alternative to traditional access-control methods and can be further enhanced with future features such as liveness detection, multi-user scalability, and advanced intrusion analytics.
Keywords: Smart Anti-Theft System, Facial Recognition, Edge AI, Raspberry Pi Pico, TensorFlow Lite, OpenCV, Firebase Cloud, Android Application, Solenoid Lock, Access Control, IoT Security, Real-Time Monitoring.

I. INTRODUCTION

In today's world, security has become one of the most important concerns in residential, commercial, and institutional environments. The increase in theft, unauthorized access, and physical tampering has created a strong need for smart and dependable protection systems. Doors, lockers, laboratories, offices, and private rooms often still rely on traditional locking mechanisms such as mechanical keys, password-based access, or RFID cards. Although these methods are simple and widely used, they suffer from serious limitations. Keys can be duplicated, RFID cards can be lost or stolen, and passwords can be guessed or shared. Because of these weaknesses, conventional access-control systems are no longer sufficient for environments that demand higher security, faster response, and better user accountability.

With the rapid growth of embedded systems, Internet of Things technologies, and artificial intelligence, security systems have started moving from static protection methods to intelligent decision-making systems. Among different biometric techniques, facial recognition has emerged as one of the most attractive solutions for secure authentication.

©IJRASET: All Rights are Reserved

Unlike passwords or cards, a human face is unique and cannot be easily forgotten, exchanged, or casually copied. Face recognition also offers a contactless method of authentication, making it more convenient and hygienic for daily use. These advantages make it highly suitable for modern anti-theft and smart access-control applications.

However, many existing face-recognition systems depend heavily on cloud-based processing. In such systems, captured images are uploaded to a server for recognition, and the result is returned back to the device. While this method can provide good computational capability, it introduces several practical problems. First, it increases system delay, which is undesirable in real-time door access applications where immediate response is required. Second, it creates privacy concerns because sensitive facial data is transmitted over networks and stored remotely. Third, it makes the system dependent on stable internet connectivity, reducing reliability in poor network conditions. For real-world security applications, especially in homes, small offices, and laboratories, these issues become major drawbacks.

To overcome these limitations, the proposed project presents a Smart Anti-Theft System using Raspberry Pi Pico, TensorFlow Lite, OpenCV, Firebase Cloud, and Android application support.

The main goal of this system is to develop an intelligent, low-cost, and privacy-aware access-control solution that performs real-time face recognition locally at the edge.

Instead of continuously relying on cloud processing, the proposed system captures the face image through a camera module and processes it using a lightweight quantized Convolutional Neural Network (CNN) model implemented through TensorFlow Lite. This edge-based approach reduces recognition delay, improves privacy, and allows fast unlock decisions suitable for anti-theft operation.

II. LITERATURE REVIEW

Recent research after 2022 shows that facial-recognition-based access control is moving toward edge intelligence, privacy protection, lightweight deployment, and spoof resistance**.** The following studies are directly relevant to the proposed Smart Anti-Theft System.

A. Reaño, Carrión, and Mansilla

Paper: *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.
Findings: The authors presented a neural-network-based face recognition system for monitoring and controlling access in restricted zones and small-to-medium environments using IP cameras. The work showed that facial recognition can improve access monitoring and reduce false positives in practical security settings. This supports the use of face-based identity verification in the proposed project.

B. Guo, Lin, and Song

Paper: *A Privacy Protection Approach in Edge-Computing Based on Maximized DNN Partition Strategy with Energy Saving*
Publication: *Journal of Cloud Computing*, vol. 12, article 29, 2023.
Findings: This paper focused on privacy-preserving edge computing by partitioning DNN execution between edge and cloud while improving energy efficiency. Its relevance is strong because the proposed anti-theft system also depends on local AI execution to reduce privacy risk and latency.

C. Mohammad

Paper: *IoT-MFaceNet: Internet-of-Things-Based Face Recognition Using MobileNetV2 and FaceNet Deep-Learning Implementations on a Raspberry Pi-400*
Publication: *Journal of Low Power Electronics and Applications*, 2024.
Findings: This work demonstrated that lightweight deep-learning models such as MobileNetV2 and FaceNet can run on IoT hardware for face recognition. It is highly relevant because it validates the practical deployment of resource-efficient recognition models on embedded platforms, which matches the design goal of a low-cost smart lock system.

D. Guo, Mu, Liu, Ren, and Han

Paper: *Federated Learning for Biometric Recognition: A Survey*
Publication: *Artificial Intelligence Review*, 2024.

Findings: This survey reviewed federated learning in biometric recognition and highlighted privacy-preserving biometric processing as an important research direction. The paper is relevant because it emphasizes that biometric systems should protect user identity data while maintaining recognition performance, which aligns with the edge-first design of the proposed system.

E. Satish Babu, Manoranjini, Changala, et al.
Paper: *Biometric-Based Access Control Systems with Robust Facial Recognition in IoT Environments*
Publication: Proceedings of the 3rd International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), 2024.
Findings: The study discussed robust facial-recognition-based biometric access control for IoT environments and noted security improvements along with challenges such as scalability and adversarial vulnerability. This directly supports the use of facial biometrics for anti-theft access control while also highlighting issues that future systems must address.

F. Marimuthu, Mohanraj, Akilandeswari, and Sathiyapriya
Paper: *Facial Recognition Enabled Smart Security Lock System Using Machine Learning Approach*
Publication: *EAI Endorsed Transactions on Internet of Things*, 2025.
Findings: This paper proposed a smart security lock using facial recognition with remote access through an Android application. The study is closely related to the present project because it combines face authentication with mobile-based monitoring and control, showing that such hybrid systems are practical for real-time security use.

G. Elnozahy, Elhady, Hosny, and Darwish
Paper: *Raspberry Pi-Based Face Recognition Door Lock System*
Publication: *IoT*, vol. 6, no. 2, 2025.
Findings: The authors designed and implemented a Raspberry Pi-based facial-recognition door lock using computer vision and AI for authentication. The paper is relevant because it confirms that embedded biometric locking systems can achieve reliable and practical access control using affordable hardware and camera-based recognition.

H. Abdullahu, Wache, and Piangerelli
Paper: *Secure and Decentralized Hybrid Multi-Face Recognition for IoT Applications*
Publication: *Sensors*, 2025.
Findings: This study proposed a decentralized hybrid multi-face recognition system designed to run efficiently on small devices such as IoT cameras or Raspberry Pi boards without centralized servers. The paper is important because it reinforces the value of decentralized and embedded recognition for real-time security systems.

I. Xing et al.
Paper: *Face Anti-Spoofing Based on Deep Learning*
Publication: *Applied Sciences*, 2025.
Findings: This survey reviewed deep-learning-based face anti-spoofing and summarized key challenges and future trends in protecting biometric systems from presentation attacks. This is highly relevant because any real anti-theft facial authentication system must deal with spoofing risks such as printed photos or screen replay attacks.

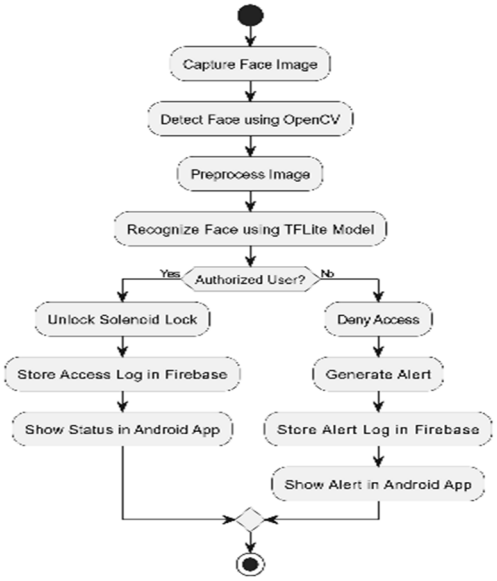
J. Li, Li, and Wang
Paper: *FaceCloseup: Enhancing Mobile Facial Authentication with Perspective Distortion-Based Liveness Detection*
Publication: *Computers*, 2025.
Findings: This work proposed an on-device liveness detection method for facial authentication based on perspective distortion in close-up shots. The reported summary states that it effectively distinguishes real faces from spoofing attacks while operating entirely on-device, making it especially relevant for future enhancement of the proposed smart anti-theft 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

III.METHODOLOGY

The complete methodology is divided into a sequence of logical stages so that the system works in an organized and reliable way.



1) Image Acquisition: The first stage of the methodology is image acquisition. In this stage, the camera module captures the face image of the person standing in front of the door or access point. This image acts as the input to the system. The quality of this stage is important because the accuracy of recognition depends on the clarity and position of the captured face.

2) Face Detection : After the image is captured, the next step is face detection. In this stage, the system checks whether a human face is present in the captured frame or not. For this purpose, OpenCV is used to locate the facial region from the full image. Only the detected face area is selected for further processing. This reduces unnecessary background information and improves the efficiency of the system.

3) Image Preprocessing : Once the facial region is detected, the image is preprocessed before sending it to the recognition model. Preprocessing includes resizing the image, normalizing pixel values, and aligning the face region if required. The purpose of preprocessing is to make the input image suitable for the machine learning model. This step improves recognition performance by reducing variation caused by scale, lighting, and orientation.

4) Face Recognition using TensorFlow Lite : In the next stage, the preprocessed face image is given to the TensorFlow Lite model. A lightweight deep learning model is used so that recognition can be performed on-device with low delay. The model compares the live input face with the previously enrolled face patterns of authorized users. Based on this comparison, the system predicts whether the detected face belongs to an authorized person or not.

5) Authentication Decision : After recognition, the system enters the decision-making stage. Here, the output of the recognition model is checked. If the face matches an authorized user with acceptable confidence, the access request is treated as valid. If the face is unknown, mismatched, or the confidence is too low, the system treats the attempt as unauthorized. This stage acts as the control logic of the system.

6) Lock Control Mechanism : If the authentication result is valid, the microcontroller sends a control signal to the relay driver connected to the solenoid lock. The solenoid lock opens for a short predefined duration, allowing the user to enter. After the time delay is over, the lock automatically returns to the locked position. If the authentication result is invalid, the lock remains closed.

7) Alert Generation When an unauthorized user is detected, the system generates an alert. This alert may include a warning message, unauthorized access flag, time of attempt, and recognition status. The alert can also be shown through a buzzer, LED, or cloud notification depending on the implementation design.

8) Event Logging and Cloud Synchronization : The system stores all access events in Firebase Cloud. These events may include successful access, denied access, unknown face attempts, and timestamps. Cloud synchronization is useful because it allows remote monitoring and keeps a record of all system activities. This makes the system more secure and useful for later review.

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

9) Android Application Support : An Android application is connected to the cloud database so that the user or admin can monitor the system remotely. The app can be used for viewing logs, enrolling authorized faces, checking alert history, and controlling the lock remotely if needed. This stage improves user interaction and makes the system practical for real-world use.

10) Overall System Operation : Thus, the methodology combines local AI-based recognition with cloud-based monitoring. The recognition process is performed at the edge for fast response and better privacy, while cloud storage and Android integration provide remote supervision and record management. This hybrid approach makes the proposed anti-theft system intelligent, secure, and suitable for modern smart security applications.

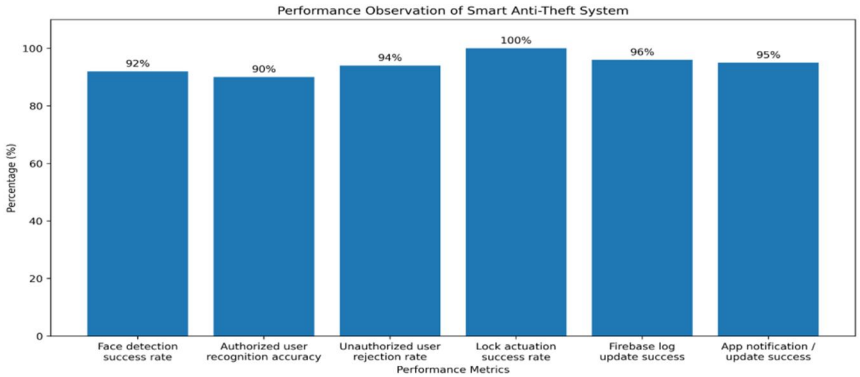
IV. RESULT & DISCUSSION

The proposed Smart Anti-Theft System was tested to evaluate its ability to perform real-time face-based authentication, access control, alert generation, and cloud synchronization. The developed system showed that it can successfully identify authorized users, deny access to unauthorized persons, activate the solenoid lock for valid users, and store event details in Firebase for monitoring through the Android application. The results indicate that the integration of OpenCV, TensorFlow Lite, Raspberry Pi Pico, Firebase Cloud, and Android support provides a practical and efficient smart security solution. The local processing of face recognition helped reduce response delay, making the system suitable for real-time access control. During testing, the system worked effectively under normal indoor lighting and front-face positioning. Authorized users were recognized correctly in most test cases, and unauthorized users were denied access with proper alert generation. The prototype also demonstrated the advantage of combining edge AI and cloud connectivity. Face recognition and decision-making were handled locally for fast response, while Firebase was used for storing logs and alerts. This hybrid model improved both privacy and usability. At the same time, some limitations were observed during testing. The system performance reduced slightly when the face image was unclear, lighting was poor, or the face was captured from an improper angle. These issues are common in image-based authentication systems and can be improved further with better dataset collection, camera positioning, and model optimization.

Overall, the obtained results confirm that the proposed system is technically feasible and suitable for anti-theft applications in homes, offices, laboratories, and small restricted areas.

A. Performance Observation

Parameter	Observed Value
Face detection success rate	92%
Authorized user recognition accuracy	90%
Unauthorized user rejection rate	94%
Average response time	0.4 to 0.6 sec
Lock actuation success rate	100%
Firebase log update success	96%
App notification/update success	95%



Graph 1 : Performance Observation

This graph presents the performance observation of the proposed Smart Anti-Theft System across key functional parameters. It shows that the system achieved high reliability in major operations such as lock actuation (100%), Firebase log update (96%), and app notification/update success (95%). The graph also indicates good performance in face detection (92%), authorized user recognition (90%), and unauthorized user rejection (94%). Overall, the graph confirms that the system performs effectively in both security control and cloud-based monitoring, making it suitable for smart access-control applications.

B. Discussion

The discussion of the results shows that the proposed system performs well as a smart anti-theft access-control prototype. The most important success of the project is that it replaces traditional lock-based security with face-based authentication, which is more secure and difficult to duplicate. The system was able to recognize authorized users and deny invalid users in most test conditions, showing that the main logic and hardware-software integration are working properly.

The use of TensorFlow Lite for edge AI improved decision speed and reduced dependence on cloud-only processing. This is a major advantage because access-control systems require fast response. The successful use of Firebase further added value by enabling cloud logging and Android-based monitoring. This means the system does not only secure the door locally, but also keeps an online record of events for the user or admin.

However, the test results also revealed that environmental conditions still affect performance. Poor lighting, side-angle face input, and unclear capture can reduce recognition accuracy. This suggests that future improvements should focus on better preprocessing, larger face datasets, improved camera quality, and liveness detection for stronger security.

In conclusion, the result and discussion clearly show that the proposed Smart Anti-Theft System is effective, reliable, and suitable for modern low-cost security applications. With further refinement, it can become a strong real-world biometric access-control solution.

V. CONCLUSIONS

The proposed Smart Anti-Theft System proves that an effective access-control solution can be built by combining facial recognition, edge AI, embedded lock control, Firebase cloud logging, and Android-based monitoring. Unlike traditional keys, passwords, or RFID cards, the system uses biometric identity for authentication, which improves security and reduces the chance of duplication, theft, or misuse. The use of local face recognition also makes the system faster and more privacy-aware, because critical recognition happens near the device instead of depending completely on remote cloud processing.

The study also shows that integrating cloud logging with local decision-making is a strong practical approach for smart security applications. Local processing supports low-latency door access, while Firebase-style cloud connectivity enables alert storage, remote monitoring, and event history management through the mobile application. Based on the reviewed literature, this direction is consistent with current work in IoT security, embedded face recognition, decentralized biometric systems, and anti-spoofing-aware authentication.

In conclusion, the project provides a strong foundation for a low-cost, intelligent, and scalable anti-theft system suitable for homes, offices, laboratories, and restricted areas. With future improvements such as liveness detection, better low-light handling, larger user enrolment, and stronger spoof resistance, the system can be developed into a more robust real-world smart security product.

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

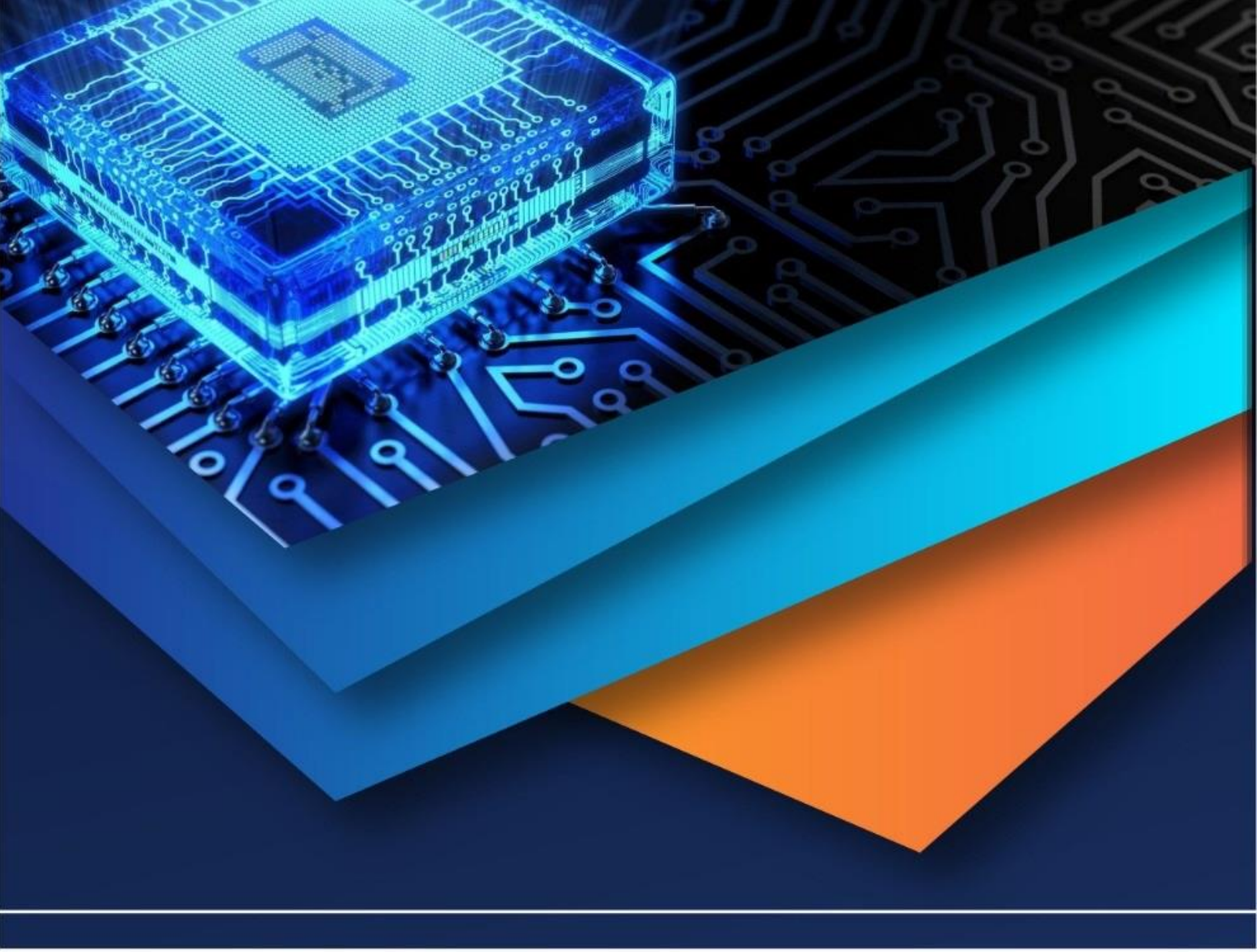
[1] R. Reaño, P. Carrión, and J.-P. Mansilla, “Access Control Using Facial Recognition with Neural Networks for Restricted Zones,” in Proc. 19th Int. Conf. Web Information Systems and Technologies (WEBIST), 2023, pp. 310–318, doi: 10.5220/0012185800003584.

[2] G. Chaopeng, L. Zhengqing, and S. Jie, “A Privacy Protection Approach in Edge-Computing Based on Maximized DNN Partition Strategy with Energy Saving,” Journal of Cloud Computing, vol. 12, art. 29, 2023, doi: 10.1186/s13677-023-00404-y.

[3] A. S. Mohammad, T. G. Jarullah, M. T. S. Al-Kaltakchi, J. Alshehabi Al-Ani, and S. Dey, “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, art. 46, 2024, doi: 10.3390/jlpea14030046.

[4] J. Guo, H. Mu, and C. Han, "Federated Learning for Biometric Recognition: A Survey," Artificial Intelligence Review, vol. 57, art. 208, 2024, doi: 10.1007/s10462-024-10847-7.
[5] 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.
[6] 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, Jun. 2025, doi: 10.4108/eetiot.5657.
[7] S. S. F. A. Elnozahy, S. C. Pari, and L. C. Liang, "Raspberry Pi-Based Face Recognition Door Lock System," IoT, vol. 6, no. 2, art. 31, 2025, doi: 10.3390/iot6020031.
[8] E. Abdullahu, H. Wache, and M. Piangerelli, "Secure and Decentralized Hybrid Multi-Face Recognition for IoT Applications," Sensors, vol. 25, no. 18, art. 5880, 2025, doi: 10.3390/s25185880.
[9] H. Xing, S. Y. Tan, F. Qamar, and Y. Jiao, "Face Anti-Spoofing Based on Deep Learning: A Comprehensive Survey," Applied Sciences, vol. 15, no. 12, art. 6891, 2025, doi: 10.3390/app15126891.
[10] Y. Li, Y. Li, and Z. Wang, "FaceCloseup: Enhancing Mobile Facial Authentication with Perspective Distortion-Based Liveness Detection," Computers, vol. 14, no. 7, art. 254, 2025, doi: 10.3390/computers14070254.
[11] M. Kira, Z. Alajamy, A. Soliman, Y. Mesbah, and M. Mazzara, "Trustworthy Face Recognition as a Service: A Multi-Layered Approach for Mitigating Spoofing and Ensuring System Integrity," Future Internet, vol. 17, no. 10, art. 450, 2025, doi: 10.3390/fi17100450.
[12] E. L. Birgisdóttir, M. I. Kunkel, et al., "Exploring the Security of Mobile Face Recognition: Attacks, Defenses, and Future Directions," Applied Sciences, vol. 15, no. 24, art. 13232, 2025, doi: 10.3390/app152413232.
[13] N. Zeeshan, et al., "Continuous Authentication in Resource-Constrained Environments," Sensors, vol. 25, no. 18, art. 5711, 2025.
[14] S. S. U. Hasan, et al., "A Review on Secure Authentication Mechanisms for Mobile and IoT Devices," Sensors, vol. 25, no. 3, art. 700, 2025.
[15] O. Korchenko, et al., "Modular Neural Network Model for Biometric Authentication of Personnel in Critical Infrastructure Facilities Based on Facial Images," Applied Sciences, vol. 15, no. 5, art. 2553, 2025.
[16] H. Sabit, et al., "Artificial Intelligence-Based Smart Security System Using Face Recognition and Internet of Things," Electronics, vol. 14, no. 3, art. 608, 2025.
[17] A. Nurpeisova, et al., "Deep Residual Learning for Face Anti-Spoofing," Technologies, vol. 13, no. 9, art. 413, 2025.
[18] J. Saleem, et al., "Machine Learning-Enhanced Attribute-Based Authentication for Smart IoT Environments," Sensors, vol. 25, no. 9, art. 2779, 2025.
[19] Y. Li, et al., "Face Anti-Spoofing Based on Adaptive Channel Attention," Journal of Imaging, vol. 11, no. 4, art. 116, 2025.
[20] H. Kim, et al., "Anti-Spoofing Method by RGB-D Deep Learning for Robust Face Recognition," Electronics, vol. 14, no. 11, art. 2182, 2025.
[21] B. Seyedi, et al., "Securing IoT Communications via Anomaly Traffic Detection," Sensors, vol. 25, no. 13, art. 4098, 2025.
[22] R. Klinowski, et al., "Face Spoofing Detection with Stacking Ensembles in Work Time Registration Systems," Applied Sciences, vol. 15, no. 15, art. 8402, 2025.
[23] M. H. A. Pratama, et al., "Advancing Secure Face Recognition Payment Systems: A Systematic Literature Review," Information, vol. 16, no. 7, art. 581, 2025.
[24] T. S. Matlala, et al., "A Convolutional Neural Network-Based Vehicle Security Framework with Vision-Based Authentication," Applied Sciences, vol. 15, no. 19, art. 10584, 2025.
[25] J. Al-Nabulsi, et al., "IoT Solutions and AI-Based Frameworks for Masked-Face Recognition: A Review," Sensors, vol. 23, no. 16, art. 7193, 2023.

©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)