iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: V Month of publication: May 2025

DOI: https://doi.org/10.22214/ijraset.2025.70612

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

EagleAI: AI Powered Real Time Restricted Area Surveillance

Jahith Sai Krishna Varma[1], K Pallavi[2], Darshan R[3], K Prashanth Kumar[4], Associate Prof. Dr. Phanindra Reddy K[5]
Dept Of AIML Ballari Institute of Technology and Management Ballari, India

Abstract: Traditional security measures often fail to provide accurate and efficient monitoring, leading to vulnerabilities in restricted areas. This project implements an advanced real-time facial recognition-based surveillance system to enhance security and address these shortcomings.
The system uses facial recognition technology for live monitoring, identifying authorized personnel and detecting unauthorized individuals. Attendance is recorded automatically in an Excel file, with timestamps for entry and exit. For unauthorized access, the system triggers multiple actions, including capturing and saving the individual's image, uploading it to Azure Blob Storage, sending email alerts with timestamps and image URLs, and activating a buzzer alarm alongside an on-screen warning. By integrating automated facial recognition with real-time alerts and cloud storage, the system significantly improves surveillance accuracy and efficiency, providing a robust solution for preventing unauthorized access in restricted areas.

I. INTRODUCTION

The project's motivation is to strengthen security measures and ensure effective access management, thereby reducing vulnerabilities in sensitive areas. Traditional approaches, which rely on manual checks and static monitoring systems, often lead to inefficiencies, delays, and errors. These shortcomings can compromise the safety of personnel, data, and infrastructure. This project aims to address these issues by introducing an intelligent system that automates monitoring, reduces manual dependency, and provides real-time responses to potential threats.

The traditional access control model has difficulty adapting to modern security requirements. Fixed processes and human error often do not immediately detect unauthorized access. EagleAI provides a dynamic approach to ensuring immediate attention to potential breaches by identifying and recording authorized individuals while flagging unauthorized individuals. This proactive system not only enhances security but also simplifies attendance tracking, which is extremely valuable in educational institutions, corporate settings, and industrial settings.

The primary goal lies in protecting limited areas through effective monitoring and timely warnings. Secure Vision ensures that unauthorized access is marked and reacted to quickly, minimizing risks of violations or disturbances. In addition to security, the project also has the potential to improve operational efficiency by automating attendance registration and simplifying access control. This project combines innovation and vigilance to pave the way for a more secure future. By setting the benchmark in access control and surveillance, it envisions a world where sensitive areas are protected with intelligence and reliability, providing a model for others to implement similar advances.

Objectives

This research focuses on the following goals of the study:

1) Design a real-time automated surveillance system to ensure continuous, efficient monitoring of sensitive premises without manual intervention.
2) Accurately identify and classify authorized personnel within restricted zones to maintain secure access control and prevent unauthorized entry.
3) Implement real-time alert mechanisms to instantly detect and notify about trespassing incidents, enhancing situational awareness and rapid response.
4) Enable automated, timely notifications to administrators to ensure immediate attention to potential security breaches and streamline decision-making.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

II. RELATED WORKS

A. Literature Survey

1) Face Detection and Recognition Using OpenCV (2021) by R. T. H. Hasan and A. B. Sallow

: Explores OpenCV as a computer vision library with modules for face detection and recognition using Haar Cascade, LBPH, and Eigenfaces; highlights integration with Python, C++, and Java, along with applications in emotion, age, and gender recognition. Discusses OpenCV's cost-effective use on devices like Raspberry Pi, while addressing drawbacks like lighting sensitivity, classifier limitations, and mobile dependency.

2) Intra Student Surveillance System: Detection and Identifying Unauthorized Wandering (2024) by D. Sattibabu et al.

:Proposes a student surveillance system using HOG and dlib for face recognition, ensuring real-time alerts when students enter unauthorized zones. Demonstrates higher accuracy over previous CNN models via HOG descriptors and SVM classifiers, yet notes scalability and environmental challenges in large deployments with poor lighting or occlusion.

3) Development of Deep Learning Algorithms for Improved Facial Recognition in Security Applications (2023) by A. S. Bein and A. Williams

:Introduces advanced facial recognition using CNNs, RNNs, VAEs, and MTCNN to improve accuracy under challenging conditions like expression changes, lighting, and head rotation. While effective for high-security applications, limitations include computational demands, dataset dependency, and constraints on mobile or real-time usage due to energy consumption and ethical concerns.

4) Optimizing Face Detection Performance with Cloud Machine Learning Services (2024) by K. Virendra et al.

: Evaluates face detection using cloud-based models (MTCNN, SSD, YOLO) on AWS, balancing accuracy, latency, and cost. MTCNN offers the highest accuracy, YOLO the lowest latency, and SSD a middle ground. Cloud tools like SageMaker and Lambda aid deployment, but model complexity, cost variability, and resource requirements present barriers for large-scale or budget-sensitive implementations.

III. PROPOSED METHOD

The proposed solution enhances the security and operational efficiency of restricted areas by integrating AI-driven surveillance, real-time facial recognition, and automated alert systems.

1) To ensure continuous monitoring, a real-time automated surveillance system is developed using computer vision and face recognition technologies.
2) To classify access, the system identifies and distinguishes authorized personnel through face encoding comparisons with a secure database.
3) For immediate breach response, real-time alerts and visual/audio warnings are triggered upon detecting unauthorized individuals.
4) To maintain prompt communication, the system automatically sends notifications and captured evidence to administrators via email.

IV. METHODOLOGY

This project adopts a two-phase methodology for automated face recognition -based monitoring and access control. In phase 1 (feature recording of the face), the characteristics of the face are extracted from the input image and stored in the database. This includes a face detection by prey in subsequent signs using a benchmark or geometric measurement detection. The extracted data is securely saved. Phase 2 (Model Training and Monitoring) uses this stored data to train a machine learning model. This trained model is then used to analyze real-time video surveillance footage. Facial features are extracted from the image and compared to captured data: if a match is found, the individual is identified and appropriate action is taken. If no match is found, a warning is triggered, including visual and auditory alerts, email notifications, and cloud storage of alert information. This two-phase approach enables accurate and efficient facial recognition for enhanced security and access management.

A. Facial Feature Recording Phase

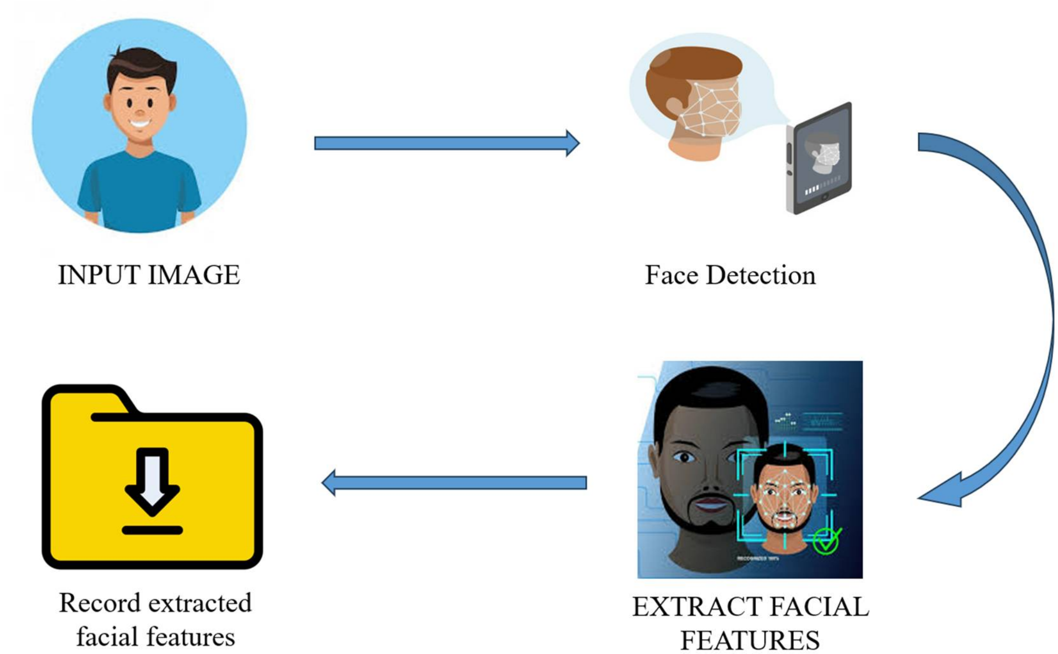

Fig 1 Facial features recording phase

B. Model Training and Surveillance Phase

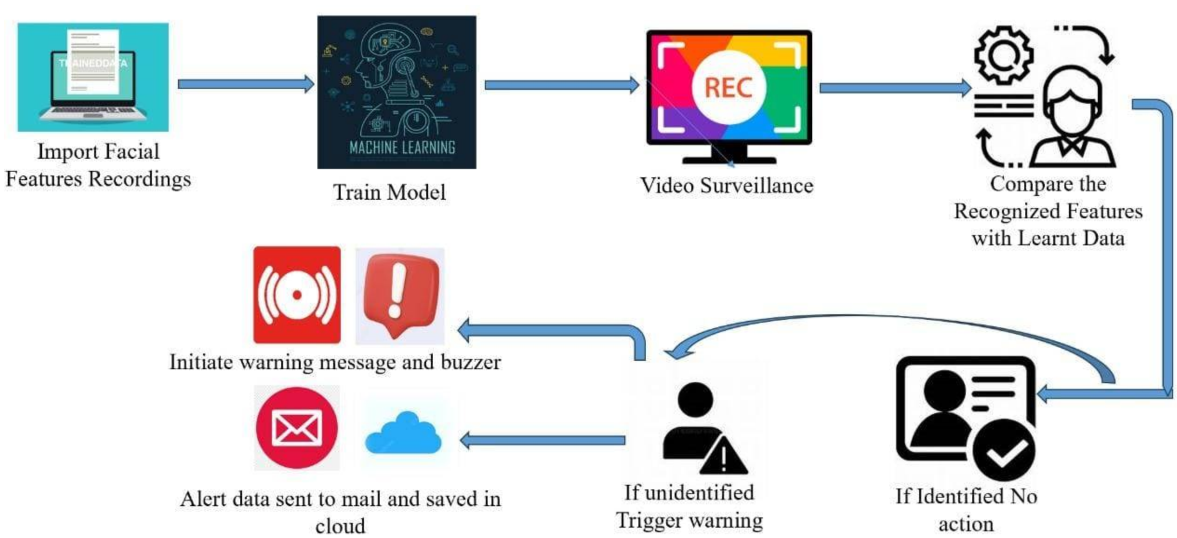

Fig 1Model training and surveillance phase

1) Data Collection

The system collects facial images of authorized individuals, organized in person-named folders. This data is used to create a structured dataset stored in the Augmented Data directory for training the facial recognition model.

2) Data Processing

Each image undergoes preprocessing using the Face Recognition library to extract and encode facial features. Encodings are stored with associated names in a pickle file. Metadata is maintained to avoid duplicate processing, and failed image logs are recorded to track errors.

3) Data Augmentation

To enhance model accuracy, the Albumentations library is used to generate five variations of each image through cropping, flipping, brightness, and contrast changes. Augmented images are stored in a structured directory to improve recognition across diverse real-world conditions.

4) Surveillance Initialization

The system initializes a real-time webcam feed, loads facial encodings, and prepares storage directories and attendance logs. MTCNN is employed for robust face detection, even under variable lighting or angles.

5) Face Recognition and Encoding

Faces detected in the video feed are encoded and compared with stored encodings to identify individuals. This enables classification as either authorized or unauthorized in real-time.

6) Attendance Tracking

Authorized individuals' attendance is automatically recorded using the openpyxl library. Time-ins and time-outs are logged with time gap handling to manage multiple entries and exits within a day.

7) Notification System

If an unknown face is detected, a timer is triggered. On prolonged presence, the system captures a warning image, uploads it to Azure Blob Storage, and sends an email alert with the image and timestamp to concerned authorities.

8) Automated Alert and Email Generation

Alerts are sent using the smtplib library, including a local image snapshot and a cloud access link. Audible alarms provide immediate on-site alerts during security breaches.

9) Continuous Monitoring

The system operates continuously, processing video frames in real-time until manually terminated with a designated key, ensuring reliable surveillance in high-traffic or sensitive environments.

C. Use Case Diagram

In the context of an AI-powered restricted area surveillance system, two main actors are involved:

- Admin: Inputs images, extracts facial features, and trains the model.
- System: Captures live video, performs face recognition, matches faces with the database, and triggers alerts (email, buzzer, image capture) for unknown individuals.

Fig 3 depicts this interaction, highlighting real-time monitoring and rapid response for enhanced security.

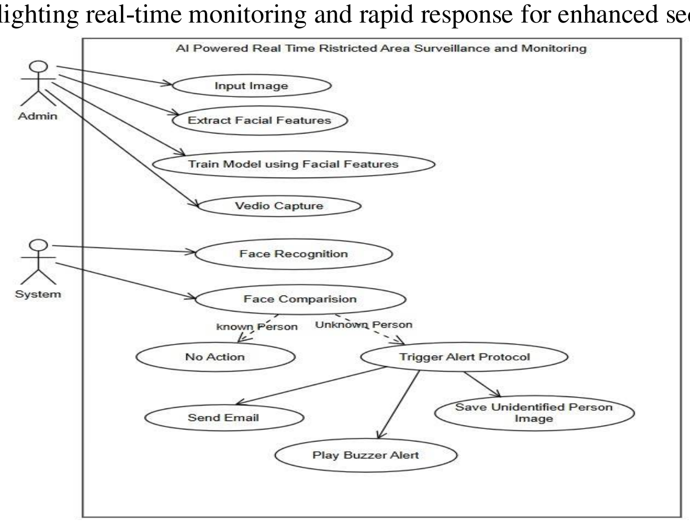

Fig 3 Use-Case Diagram

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

D. Sequence Diagram

A sequence diagram represents the order of interactions between system components over time. It's a dynamic UML model used to visualize how and when objects communicate, typically one per use case.

In Fig 4, the sequence diagram for the Eagle AI project illustrates the flow of actions during security monitoring:

- The webcam captures video when someone enters a restricted area.
- The system performs facial recognition using AI.
- If the person is recognized, their attendance is marked.
- If unknown, a countdown begins, a buzzer is triggered, and a warning image is captured.
- The image is uploaded to Azure Blob Storage and an email alert is sent to the admin with the image link.

This sequence ensures timely alerts and accurate access tracking for enhanced area security.

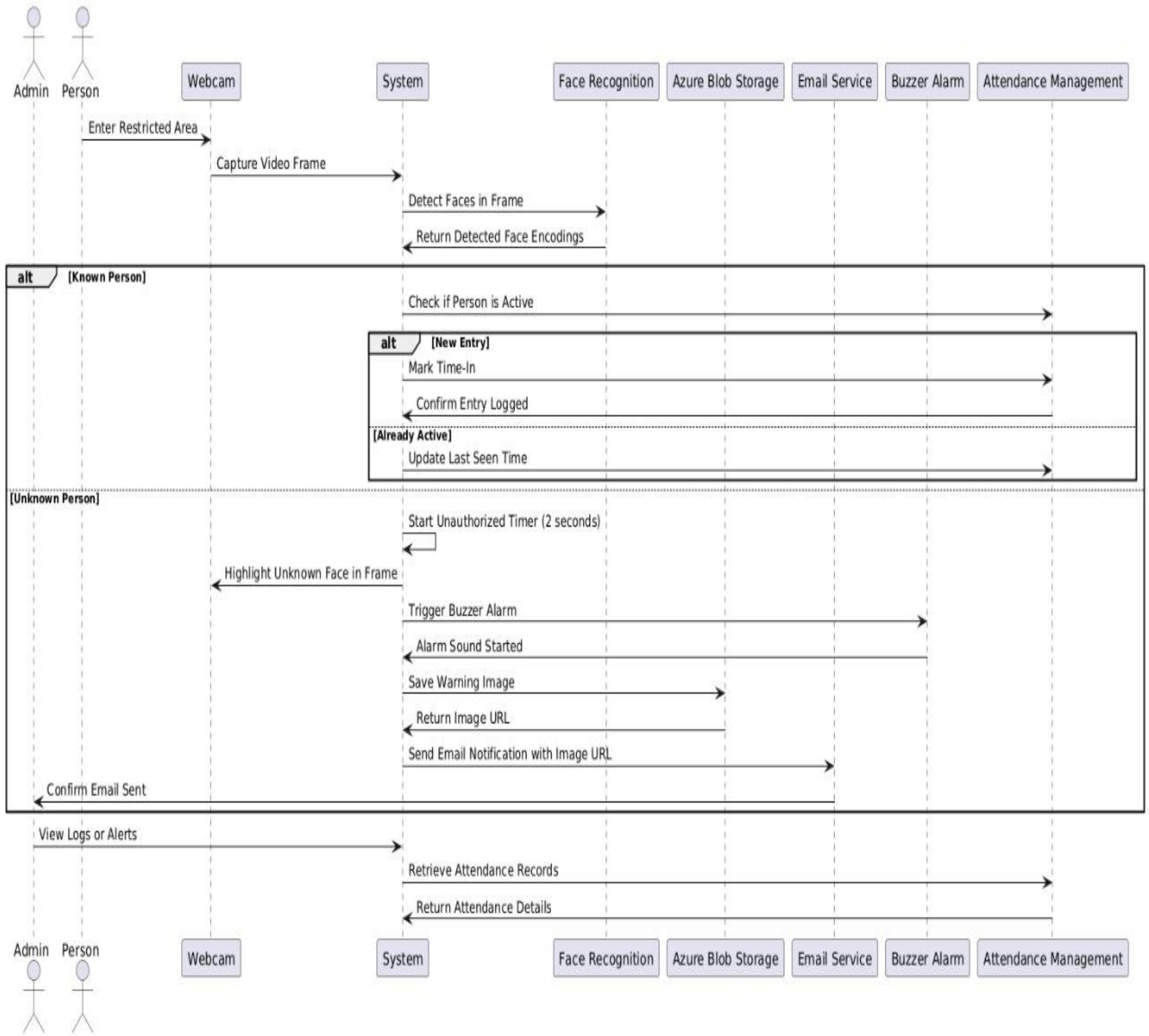

Fig 4 Sequence diagram

E. Data Flow Diagram

A Data Flow Diagram (DFD) visually maps how data moves through a system, showing sources, processes, storage, and outputs. It aids communication between analysts and stakeholders and helps define system boundaries.

Fig 5 illustrates a Level-0 DFD for the AI-Powered Restricted Area Surveillance System:

- Actors: Admin and Azure/Local Storage.
- Process: AI-driven surveillance monitors real-time video, detects faces, and distinguishes between known and unknown individuals.

- Data Flow:
- Admin inputs configurations.
- System sends alerts to the admin upon detecting unknown persons.
- Captured images are stored in both local and cloud storage for analysis.

This high-level diagram outlines efficient monitoring and secure data handling within the surveillance system

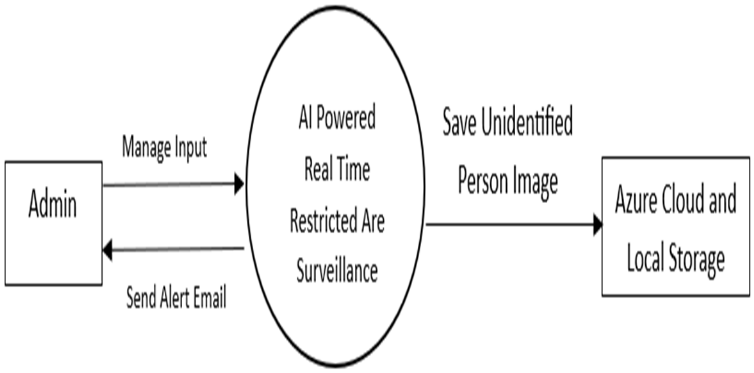

Fig 5 Level-0 DFD

V. RESULTS AND DISCUSSION

The outcomes of the EagleAI: AI Powered Real-Time Restricted Area Surveillance and Monitoring Project are elaborated in this section. Using advanced facial recognition, image processing, and AI-based surveillance, the system tracks authorized personnel efficiently, detects unauthorized access, and comes with automated alerts. Azure Blob Storage allows data to be securely handled while allowing real-time notifications for enhanced security response. The figures below show core features of attendance management, live monitoring, and unauthorized person detection, thereby demonstrating the system's capability to ensure high security in restricted areas.

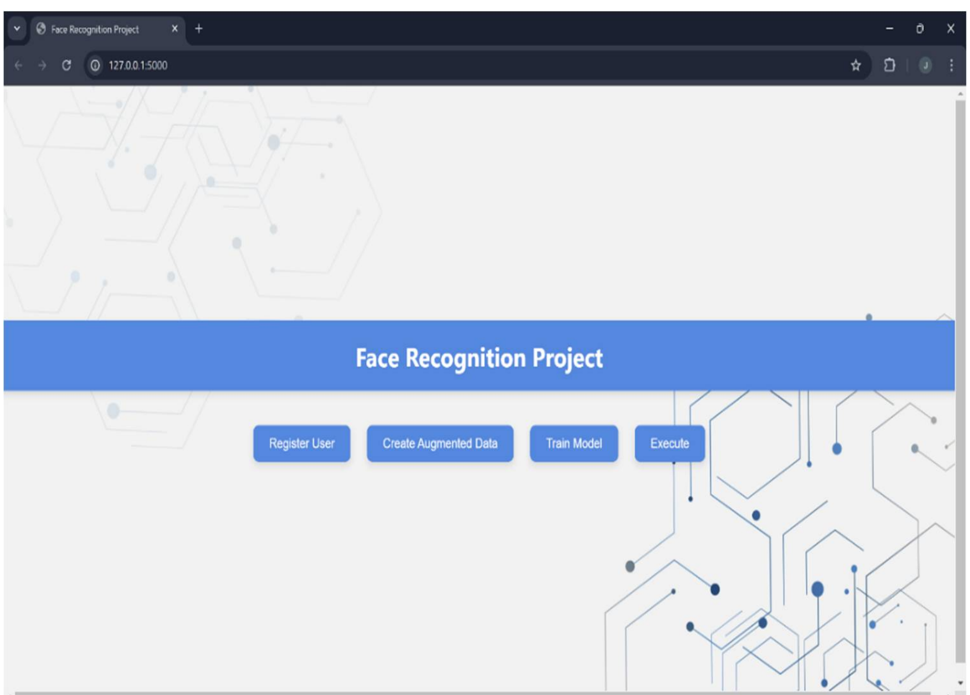

Fig 6 Output after successful login

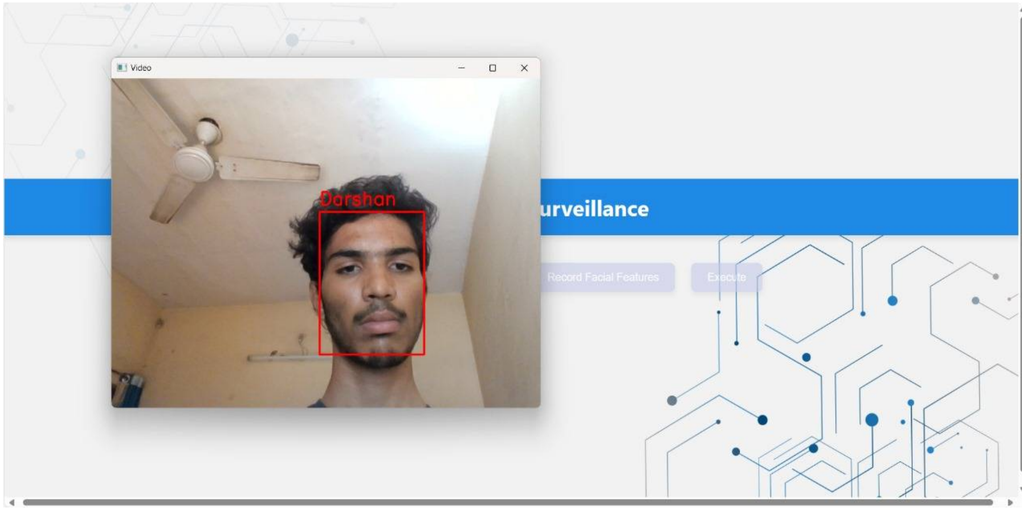

Fig 7 Output when Identified person is found

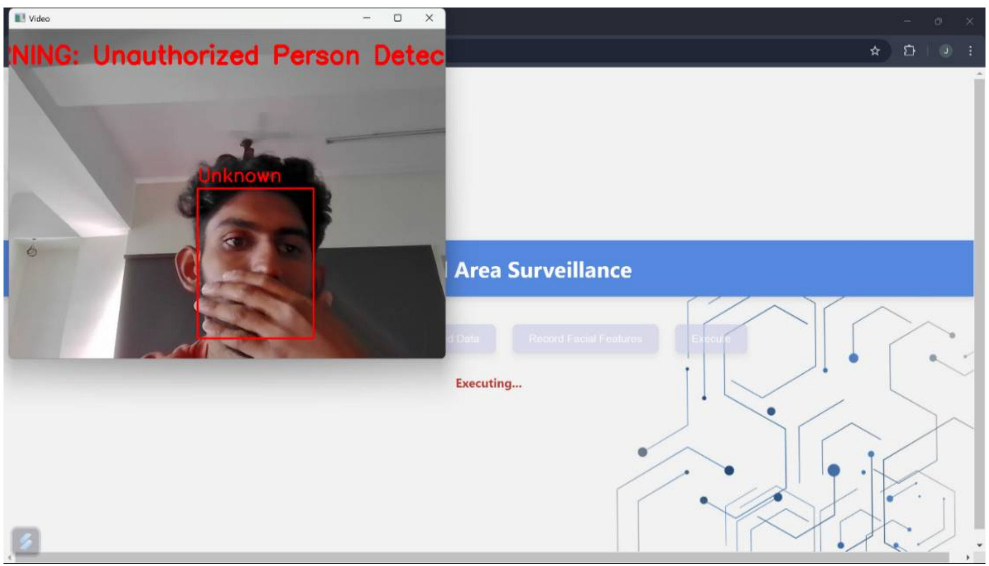

Fig 8 Output when unidentified person is found

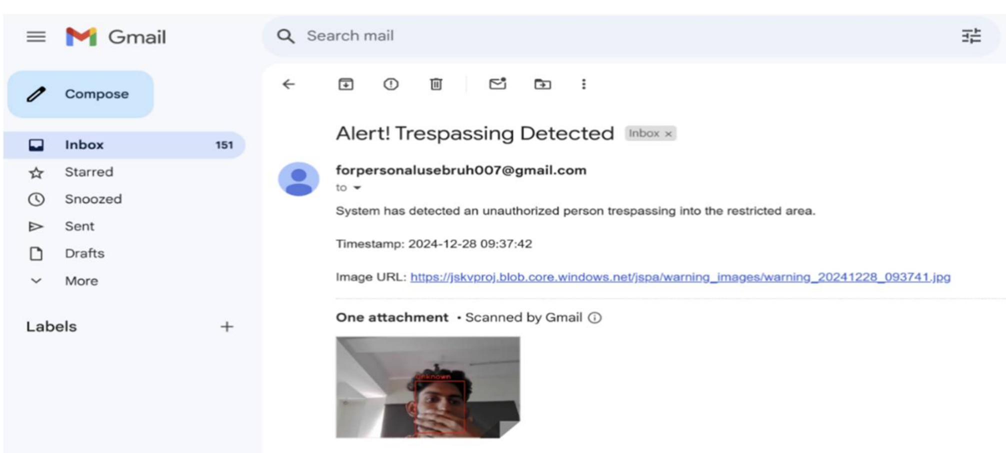

Fig 9 Email alert when trespasser is detected

VI. FUTURE SCOPE

1) Multi-Factor Authentication: Integrate biometric or OTP-based MFA for secure admin login and protection of sensitive system operations.
2) Automated Lock Control: Enable smart locking systems that automatically restrict access during unauthorized entry, enhancing on-site security.
3) Low-Light Detection Enhancement: Use IR or thermal imaging with pre-processing techniques to improve facial recognition in low-light conditions.
4) High Frame Rate Optimization: Implement GPU acceleration and multi-threading to achieve real-time performance with faster frame processing.
5) Multi-Camera Scalability: Expand system support for multiple synchronized cameras across various locations like campuses or industrial zones.

VII.ACKNOWLEDGMENT

We extend our sincere gratitude to everyone who contributed to the successful completion of this project,*EagleAI: AI Powered Real Time Restricted Area Surveillance*.Wearealso deeply grateful to the Head of the Department for their encouragement and valuable suggestions, which played a crucial role in shaping our work.

We are also deeply grateful to the Head of the Department for their encouragement and valuable suggestions, whichplayedacrucialroleinshaping our work.

REFERENCES

[1] R. T. H. Hasan and A. B. Sallow, “Face Detection and Recognition Using OpenCV,” Journal of Soft Computing and Data Mining, vol. 2, no. 2, pp. 86–97, Oct. 2021, doi: 10.30880/jscdm.2021.02.02.008.

[2] D. Sattibabu, S. Yacoob, P. Tanuja, B. M. Koushika, K. V. Babu, and Ch. J. Kumar, “Intra Student Surveillance System: Detection And Identifying Unauthorized Wandering,” 2024, pp. 1201–1208. doi: 10.2991/978-94-6463-471-6_115.

[3] A. S. Bein and A. Williams, “Development of Deep Learning Algorithms for Improved Facial Recognition in Security Applications,” IAIC Transactions on Sustainable Digital Innovation (ITSDI), vol. 5, no. 1, pp. 19–23, 2023.

[4] K. Virendra, M. Kumar Bagwani, V. Kumar Tiwari, D. Kumar Chouhan, and A. Jain, “Optimizing Face Detection Performance with Cloud Machine Learning Services,” 2024.

.