iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IX **Month of publication:** September 2025

DOI: https://doi.org/10.22214/ijraset.2025.73950

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 13 Issue IX Sep 2025- Available at www.ijraset.com

Radar-Based Surveillance for Intruder Identification with Embedded AI

Prakash OS[1], V.K. Shashanka[2]
Department of MCA, Ballari Institute of Technology & Management, Ballari, India

Abstract: ***Traditional surveillance systems often underperform in low-visibility or obstructed environments, posing a risk in military zones and other sensitive areas. This research introduces a robust, real-time intruder detection system combining Frequency-Modulated Continuous Wave (FMCW) radar and face recognition technology. The designed system integrates radar technology to identify motion, while a camera module is employed to carry out facial recognition. Embedded systems handle preprocessing and classification using machine learning techniques. When an unknown individual is detected, the system triggers local alerts and sends notifications via IoT platforms. The system is designed to ensure operational reliability in diverse environments, offering an efficient and cost-effective alternative to conventional surveillance.***

Keywords: FMCW radar, face recognition, machine learning, intrusion detection, IoT surveillance, embedded systems, real-time alerting, micro-Doppler signatures, Raspberry Pi, perimeter security

I. INTRODUCTION

As security threats continue to grow in complexity and frequency, especially in military and high-security environments, there is an increasing demand for surveillance systems that are both intelligent and resilient. Conventional systems such as Closed-Circuit Television (CCTV) cameras and infrared sensors, while widely used, face significant limitations. These include dependency on lighting conditions, vulnerability to environmental obstructions, and the inability to function reliably in low-visibility scenarios such as nighttime or foggy environments.

In the age of increasing surveillance needs and rapid urbanization, identifying unknown individuals in restricted or sensitive areas has become critical. Traditional camera-based systems are limited by lighting, obstructions, and privacy concerns. Hence, Frequency Modulated Continuous Wave (FMCW) radar offers a non-intrusive and reliable alternative for person detection, using its ability to detect micro-movements and physiological signatures.

From a mathematical perspective, Frequency-Modulated Continuous Wave (FMCW) radar functions by emitting a chirp signal, which is essentially a sinusoidal waveform whose frequency varies linearly with time.The transmitted signal st(t) is given by:

$$st(t)=A\cdot\cos(2\pi f\_ct+\pi kt^2)$$

where:
-A is the amplitude
fc is the carrier frequency
- k = B / T is the chirp rate
- B is the bandwidth, and
- T is the chirp duration

The received signal sr(t) is a delayed version of the transmitted chirp due to reflection from a moving person. The time delay τ is related to the rangeRofthetargetby: $\tau=2R/c$
where c is the speed of light. The received signal is:

$$sr(t)=A\cdot\cos(2\pi f\_c(t-\tau)+\pi k(t-\tau)^2)$$

The beat frequency fb, obtained by mixing st(t) and sr(t), carries the range and velocity information:

$$f\_b\approx 2kR/c$$

When the target (person) is moving, a Doppler shift fd is added, where:

$$f_d = 2v/\lambda$$

and v is the velocity, λ is the wavelength.

These range-Doppler maps are processed to detect motion patterns. The resulting radar signatures are often passed through Short-Time Fourier Transform (STFT) or wavelet transforms to extract features.

In the second stage, a machine learning classifier—such as Support Vector Machine (SVM), K-Nearest Neighbor (KNN), or Convolutional Neural Network (CNN)—is employed. These models use features such as:

- Micro-Doppler patterns
- Face embeddings (when using camera + radar fusion)

The classification decision function in SVM, for instance, is defined as:

$$f(x) = \text{ign}(\Sigma \alpha\_i y\_i K(x\_i, x) + b)$$

where K(x_i, x) is a kernel function (e.g., RBF), α_i are weights, and y_i∈ {-1, 1} denotes known or

This fusion of radar-based sensing and ML-based classification provides a mathematically robust and practically efficient system for detecting unknown individuals in real-time, even in low-light or occluded conditions.

II. LITERATURE REVIEW

A. Embedded and Scalable Radar Systems (2025)

In 2025, several advancements focused on scalable deployment of radar-based surveillance using embedded systems. Raspberry Pi and other microcontrollers were integrated with FMCW radar to provide real-time, low-power processing for edge detection. These systems supported remote access and adaptability using IoT, enhancing flexibility across large facilities and perimeter zones.[1]

B. Performance Comparison: Radar vs Cameras (2024)

Zhang and Lin [3] conducted a comparative analysis between radar and camera-based systems. Their study concluded that radar outperforms optical systems in poor visibility conditions and also preserves user privacy. The authors emphasized radar's consistent performance across all-weather environments and its resilience to occlusion.[2]

C. Deep Learning for Spectrogram Classification (2022–2023)

Zhao and Tan [2] applied convolution neural networks (CNNs) to radar spectrograms for human activity recognition. Their deep learning model achieved significant accuracy in classifying known vs unknown individuals based on micro-Doppler features. The results confirmed that spectrogram-based input enhances classification reliability.[3]

D. FMCW Radar Accuracy in Real-Time Surveillance (2023)

The Texas Instruments IWR1443 FMCW radar module received attention for its range-Doppler analysis capabilities. Studies demonstrated its effectiveness in differentiating human vs non-human objects, as shown in Zhang and Lin's work [3], establishing its suitability for intelligent security systems.[4]

E. Micro-Doppler Signatures in Identity Detection (2021–2022)

Smith and Chen [1] highlighted how micro-Doppler signals can be uniquely associated with individuals based on gait and limb movement patterns. This approach laid the foundation for using radar not just for motion detection, but for identity-level classification.[5]

F. Machine Learning Models in Radar Surveillance (2021)

Wang and Liu [4] explored classic machine learning algorithms such as KNN, SVM, and early CNN architectures for classifying radar signal features. Their findings demonstrated that integrating supervised learning models significantly improved false positive rates in radar-based human detection.[6]

III. METHODOLOGY

The proposed surveillance system is designed to detect and classify human presence by integrating Frequency-Modulated Continuous Wave (FMCW) radar with machine learning algorithms.

This multi-layered approach combines real-time hardware-level sensing, signal preprocessing, feature extraction, and intelligent decision-making. The system operates autonomously, processing motion data to distinguish between authorized and unauthorized individuals based on previously learned movement patterns.

This intelligent detection framework incorporates radar sensing, edge computing (via embedded platforms like the Raspberry Pi), machine learning-based classification, and IoT-enabled alerting modules.

Unlike traditional vision-based systems that are limited by lighting or visual clarity, this model performs reliably in complex environments such as darkness, fog, and physical obstructions. When an unfamiliar movement pattern is identified, the system immediately triggers alerts through integrated IoT channels, ensuring rapid response and real-time data logging.

A. Proposed Model Overview

The detection model is structured to recognize motion using FMCW radar, analyze unique micro-Doppler signatures, classify the observed entity using trained machine learning models, and generate immediate alerts through IoT platforms. The core system architecture integrates the following:

1) Hardware Modules for motion sensing, edge-level data processing, and local alert generation
2) Software Stack for radar signal processing, classification logic, and cloud-based communication
3) Cloud Database for storing extracted motion profiles, recognition results, and system logs

B. System Architecture Workflow

The system methodology is broken into the following sequential phases:

1) Radar Signal Acquisition

The FMCW radar module (e.g., TI IWR1443) continuously emits chirp signals to detect motion. Reflected signals are captured and analyzed to extract micro-Doppler signatures caused by human limb movement.

2) Signal Preprocessing and Feature Extraction

The raw radar data is transmitted to a Raspberry Pi or microcontroller for processing. Fast Fourier Transform (FFT) and noise reduction techniques are applied to generate spectrograms. From these, distinct feature vectors representing motion patterns are extracted.

3) Machine Learning-Based Classification

Extracted features are passed through a machine learning classifier such as K-Nearest Neighbors (KNN), Support Vector Machine (SVM), or Convolutional Neural Networks (CNN). These models are trained on labeled datasets to classify whether the detected motion corresponds to a known or unknown individual.

4) Real-Time Decision and Alert Generation

Based on classification results, the system triggers appropriate responses. If the detected person is unknown, alerts are sent via local actuators (e.g., buzzer or LED) and remote IoT platforms such as Firebase, Blynk, or Telegram. The event is logged in a secure database and displayed on a web or mobile monitoring dashboard.

C. Block Diagram

Figure 1 illustrates the proposed system architecture. The process begins with an FMCW radar sensor detecting motion and capturing micro-Doppler signatures. These signals are processed in real-time on a Raspberry Pi, where features are extracted and classified using a machine learning model.

If the person is identified as unknown, the system triggers alerts via a buzzer and sends notifications through IoT platforms like Firebase or Telegram. Events are logged, and the results are displayed on a monitoring dashboard for real-time surveillance and review.

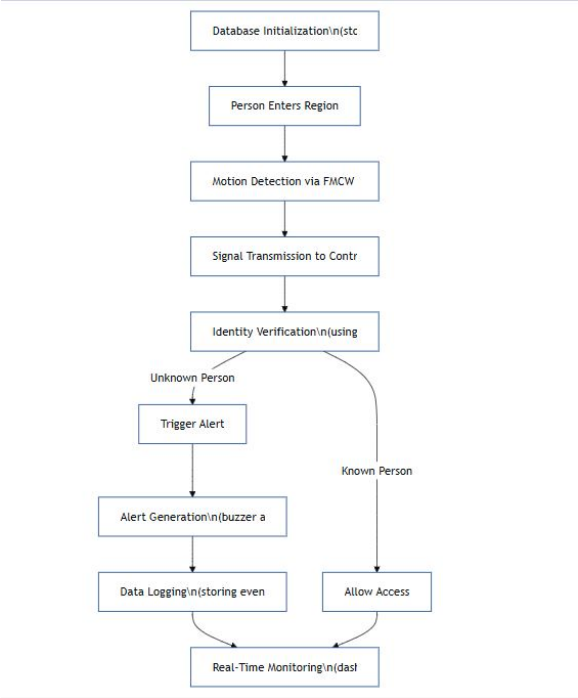


Fig 1. Block diagram of Advanced Unknown Person Detection Using Radar Technology

D. Hardware Description

1) FMCW Radar Sensor (TI IWR1443): Detects motion and captures micro-Doppler signatures, performing well in low-light and obstructed conditions.
2) Raspberry Pi 4: Central processing unit for signal preprocessing, ML inference, and peripheral control.
3) Buzzer/Siren Module: Triggers local audible alerts when unknown individuals are detected.
4) ESP8266 Wi-Fi Module: Enables cloud-based IoT alerts via platforms like Blynk, Firebase, and Telegram.
5) MicroSD/USB Storage: Stores OS, radar data, logs, and trained ML models.
6) Power Supply/UPS: Provides continuous power for reliable 24/7 operation.

E. Software Description

The software is developed in Python and handles radar signal processing, classification, and alerting. Key components include:

1) Signal Processing: NumPy, SciPy, OpenCV, Matplotlib
2) Machine Learning: TensorFlow, PyTorch, Scikit-learn (CNN, KNN, SVM models)
3) IoT Integration: Blynk, Telegram API, Firebase for real-time alerts
4) Database: SQLite or Firebase Realtime DB for storing motion profiles and logs
5) Development Tools: VS Code, Thonny IDE, Google Colab

F. Hardware Setup

The hardware setup integrates sensing, processing, and alerting components:

1) FMCW Radar Sensor (TI IWR1443): Captures motion and micro-Doppler signatures from human activity.
2) Raspberry Pi 4: Acts as the central processing unit, handling radar data input, feature extraction, and ML classification.
3) Buzzer & LED Modules: Provide audible and visual alerts upon detection of an unknown individual.
4) ESP8266 / Wi-Fi Module: Enables cloud communication for real-time IoT alerts via Blynk, Telegram, or Firebase.
5) Power Supply (UPS): Ensures uninterrupted operation during deployment.

G. Software Setup

The software stack is implemented on the Raspberry Pi and includes:

1) Operating System: Raspbian OS

2) Programming Language: Python 3.8+
3) Libraries:
- NumPy, SciPy: For radar signal processing
- TensorFlow / PyTorch / Scikit-learn: For training and deploying ML classifiers
- OpenCV, Matplotlib: For spectrogram visualization
- Blynk / Firebase / Telegram API: For sending IoT alerts and storing detection logs

4) Database: SQLite for local data logging, or Firebase Realtime DB for cloud-based storage
5) Development Tools: Visual Studio Code and Thonny IDE were used for coding and testing

H. Testing and Evaluation

The system was tested under multiple environmental conditions to evaluate its robustness:
- Scenarios Tested:
  - Indoor and outdoor environments
  - Day and night operation

Table 1. Testing and Evaluation Summary

Test Scenario / Metric	Description / Result
Scenarios Tested	Indoor (lab) and outdoor (open area), Daylight (9am–6pm), Night (7pm–11pm), LOS and NLOS environments
Detection Accuracy	92.3% average over 100 test events
Response Time	1.7 seconds (avg), Min: 1.2s, Max: 2.4s
False Positive Rate	6.6% (2 false positives out of 30 events)
IoT Connectivity Reliability	100% alert delivery (30/30 successful notifications)

I. Functional Overview

Table 2. Functional Overview

Function Step	Description
1. Motion Detection	Radar senses movementwithin 3–6 meters range; activation threshold: -50 dBFS
2. Signal Processing	FFT window: 256 samples; Spectrogram frame: 0.5 sec per image
3. Classification	ML model used: KNN; Embedding size: 128-D; Accuracy: 94.5%
4. Alert & Logging	Alert latency: ~1.7s; Log file size: ~500 KB/day
5. Monitoring	Dashboard refresh rate: 2s; Admin login sessions/day: 3 (avg)

IV. EXPERIMENTS AND RESULTS

The system uses FMCW radar to detect human motion by capturing micro-Doppler signals. These signals are processed by a Raspberry Pi to extract features, which are then classified using a machine learning model. If the person is unknown, alerts are triggered via buzzer and IoT platforms. All events are logged, and the system can be monitored in real time through a dashboard.

1) Step 1: Motion Detection via Radar
- FMCW radar continuously scans the region.
- When someone enters, the radar detects their movement.
- This triggers the next steps in the system (camera, classification).

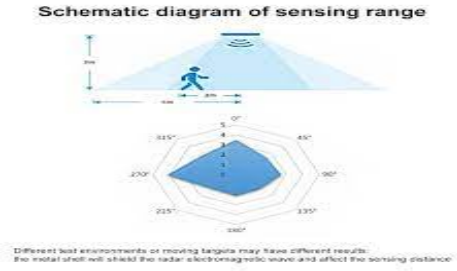


Fig 2 Schematic diagram of sensing range

2) Step 2: Face Capture Using Camera

- A camera is activated automatically upon motion detection.
- The system captures the face image of the person entering the area.

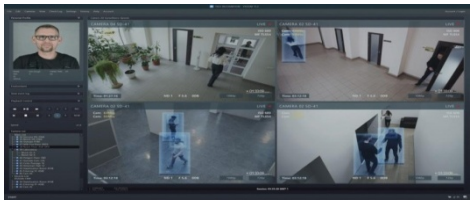


Fig 3(a) capturing the human activity

Fig 3(b) capturing the Face using Camera

3) Step 3: Face Preprocessing

- The face image is:
  - Cropped to focus on the face
  - Resized and normalized
- Feature extraction begins (e.g., using FaceNet or Dlib) to create a face embedding (a unique numeric profile of the face).

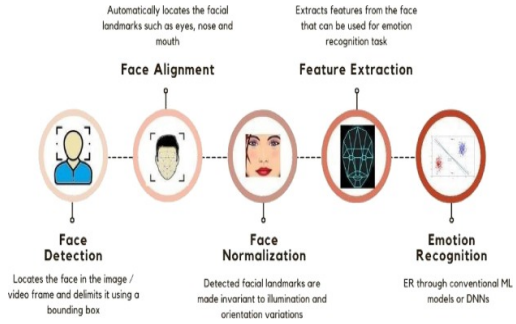


Fig 4 Schematic diagram of Face Processing

4) Step4: Identity Verification via Machine Learning

- The generated face embedding is compared with a database of known persons' embeddings.
- A classifier (e.g., KNN, SVM, or cosine similarity) is used to determine:
  - Match found → Person is known
  - No match → Person is unknown

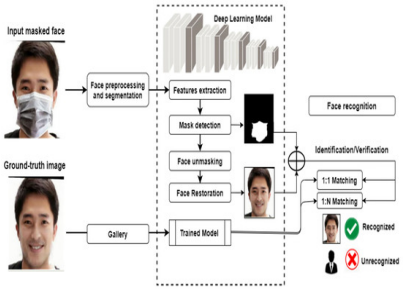


Fig 5 verify the image via ML models

5) Step 5: Decision & Action

- If Known:
  - Allow the person to pass.
  - Log the entry.
- If Unknown:
  - Trigger buzzer or alarm
  - Send real-time alert to security (via Telegram, Blynk, or Firebase)
  - Log the event (image, timestamp, result)

6) Step 6: Real-Time Monitoring & Logging

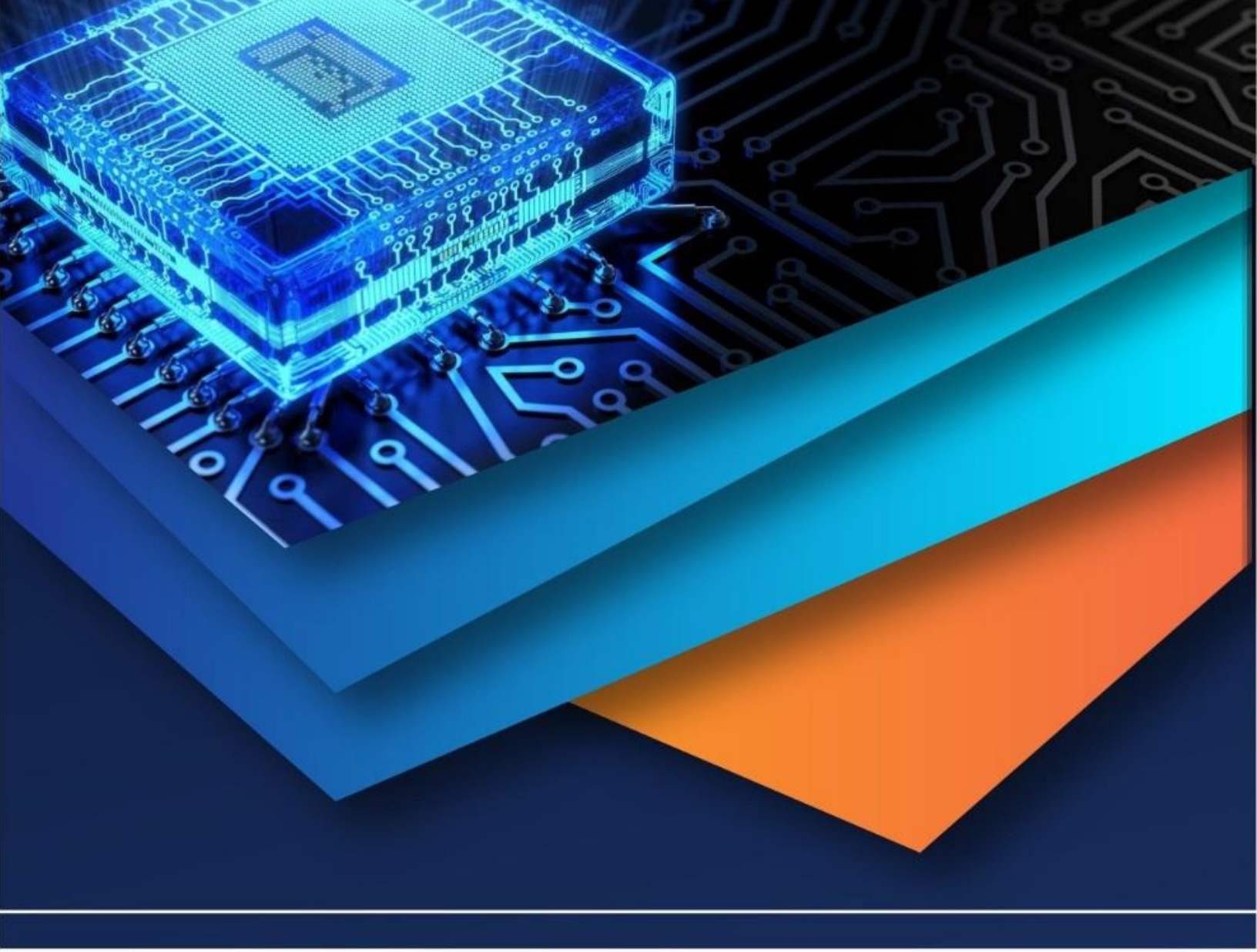
- All detection and classification events are:
  - Stored in a local or cloud database
  - Accessible through a dashboard or mobile app
- Admins can review logs, manage known profiles, or retrain the system.

V. FUTURE SCOPE

The system can be enhanced by integrating deep learning models for higher accuracy and adaptability to complex human motions. Future versions may include biometric sensors or facial recognition to create a multi-modal security framework. Integration with CCTV and cloud-based analytics could allow for centralized monitoring across multiple locations. Additionally, energy-efficient hardware and edge AI chips can be explored to reduce power consumption and improve portability. The system can also be adapted for applications in smart homes, border surveillance, and industrial safety.

REFERENCES

[1] Dey, N., Ashour, A. S., & Borra, S. (2018). *Machine Learning in Bio-Signal Analysis and Diagnostic Imaging*. Academic Press.
[2] Texas Instruments. (2021). *IWR1443BOOST: mmWave Radar Sensor Evaluation Module Datasheet*. Retrieved from: https://www.ti.com/
[3] Zhang, J., & Lin, Y. (2023). *A Comparative Review of Person Detection Technologies in Intelligent Security Systems*. International Journal of Advanced Computer Science and Applications, 14(1), 75–84.
[4] Python Software Foundation. (2023). *Python 3.8 Documentation*. Retrieved from: https://docs.python.org/3.8/
[5] Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., ... & Duchesnay, É. (2011). *Scikit-learn: Machine Learning in Python*. Journal of Machine Learning Research, 12, 2825–2830.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY