International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 01 | Jan - 2026 SJIF Rating: 8.586 ISSN: 2582-3930

AI Based Home Anomaly & Intruder Detection System

Gayathri S[1], Akshatha M[2], S Rithvik Bhat [3], Amruthesh M[4], Harshith S P[5], Shiv Shankar E[6]

[1] ***Gayathri S***, *Assistant Professor,*
Department of Computer Science and Engineering,
Maharaja Institute of Technology Mysore,
Affiliated to Visvesvaraya Technological University (VTU),
Belagavi, Karnataka, India

[3] ***S Rithvik Bhat***,
Department of Computer Science and Engineering,
Maharaja Institute of Technology Mysore,
Affiliated to Visvesvaraya Technological University (VTU),
Belagavi, Karnataka, India

[5] ***Harshith S P***,
Department of Computer Science and Engineering,
Maharaja Institute of Technology Mysore,
Affiliated to Visvesvaraya Technological University (VTU),
Belagavi, Karnataka, India

[2] ***Akshatha M***, *Assistant Professor,*
Department of Computer Science and Engineering,
Maharaja Institute of Technology Mysore,
Affiliated to Visvesvaraya Technological University (VTU),
Belagavi, Karnataka, India

[4] ***Amruthesh M***,
Department of Computer Science and Engineering,
Maharaja Institute of Technology Mysore,
Affiliated to Visvesvaraya Technological University (VTU),
Belagavi, Karnataka, India

[6] ***Shiv Shankar E***,
Department of Computer Science and Engineering,
Maharaja Institute of Technology Mysore,
Affiliated to Visvesvaraya Technological University (VTU),
Belagavi, Karnataka, India

A B S T R A C T

The rapid expansion of smart home technologies has increased the need for intelligent and autonomous security systems. Conventional home security solutions that rely on motion sensors and manual CCTV surveillance are reactive in nature and frequently generate false alarms due to pets, lighting changes, or routine household activities. This paper presents an AI based home anomaly and intruder detection system that provides real-time security monitoring using computer vision and deep learning techniques. The proposed system utilizes MediaPipe for efficient face detection and a FaceNet-based deep learning model to generate facial embeddings for identity recognition. Cosine similarity is used to compare detected faces with registered users stored in a local database. When an unknown individual is detected, the system automatically activates a continuous audible alarm, records video evidence, and sends instant alerts with the recorded clip to the homeowner via Telegram. Experimental results show that the system operates reliably in real time, significantly reduces false alarms, and enhances overall smart home security.

INTRODUCTION

The rapid advancement of smart home technologies has significantly transformed residential environments by integrating automation, connectivity, and artificial intelligence. Along with these advancements, ensuring reliable and intelligent home security has become a major concern. Traditional home security systems such as infrared sensors, motion detectors, and basic CCTV surveillance are widely used but remain limited in their functionality. These systems are reactive in nature and often generate false alarms due to pets, shadows, lighting variations, or routine household activities. Moreover, they require continuous human monitoring, which is impractical and prone to delayed response.

Recent developments in artificial intelligence (AI) and computer vision have enabled machines to interpret visual data with a high level of accuracy. Face recognition has emerged as a reliable biometric approach due to its non-intrusive nature and suitability for real-time applications. By combining face detection and deep learning-based face recognition, security systems can distinguish between authorized individuals and intruders, thereby improving accuracy and reducing false alerts.

This research presents an **AI based home anomaly and intruder detection system** that continuously monitors live video feeds, identifies individuals in real time, and automatically triggers alerts upon detecting unauthorized access. The proposed system aims to enhance smart home security by minimizing false alarms, improving response time, and providing an autonomous and cost-effective solution.

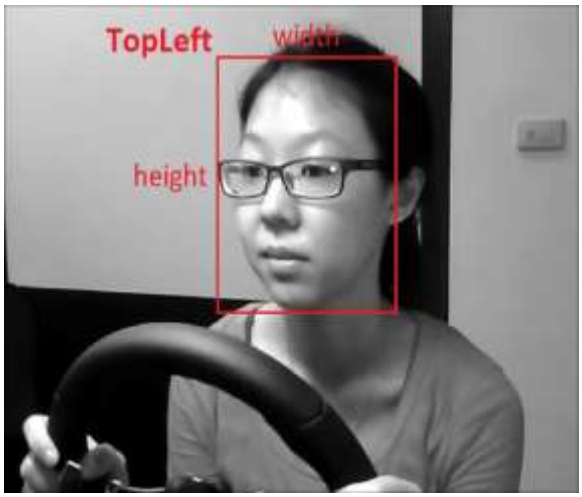
RELATED WORK

Several studies have explored intelligent surveillance and intrusion detection using computer vision and machine learning techniques. Traditional motion-based surveillance systems focus primarily on detecting movement but lack contextual understanding, resulting in high false positive rates. To overcome this limitation, researchers have investigated anomaly detection and human activity recognition using convolutional neural networks (CNNs) and recurrent neural networks (RNNs).

Deep learning-based face recognition models such as FaceNet, VGGFace, and ArcFace have demonstrated high accuracy in identity verification tasks. MediaPipe has been widely adopted for real-time face detection due to its lightweight architecture and low latency, making it suitable for edge-based applications. Some existing smart home security solutions rely on cloud-based processing, which introduces latency, privacy concerns, and dependency on internet connectivity.

Despite these advancements, there remains a need for a locally deployable, real-time security system that integrates accurate face recognition with automated alert mechanisms. The proposed system addresses these challenges by performing on-device processing and providing instant alerts without relying heavily on cloud infrastructure.

METHODS



The methodology of the proposed system is designed to ensure accurate, real-time detection of intrusions while maintaining computational efficiency. The system follows a sequential processing pipeline that integrates video capture, face analysis, identity verification, and automated alert generation.

Initially, live video is captured from a webcam or IP camera and processed frame by frame. Each frame is analyzed using a face detection algorithm to identify regions containing human faces. Once a face is detected, it is extracted and preprocessed to ensure consistent input for the face recognition model. Preprocessing steps include resizing, normalization, and alignment to improve recognition accuracy.

The preprocessed face image is then passed to a deep learning-based face recognition model that generates a numerical feature representation known as a facial embedding. These embeddings are compared with embeddings of registered users stored in a local database. A similarity metric is used to measure how closely the detected face matches known identities. Based on this similarity score, the system determines whether the individual is authorized or unauthorized.

If the similarity score falls below a predefined threshold, the individual is classified as an intruder. In such cases, the system immediately initiates predefined security actions, including activating an alarm, recording video evidence, and sending notifications to the homeowner. The entire process is automated and operates continuously in real time.

PROPOSED SYSTEM

The proposed AI based home anomaly and intruder detection system is designed as a modular and scalable framework to ensure efficient real-time operation. Unlike traditional security systems that rely solely on motion detection, the proposed system focuses on identity-based anomaly detection, which provides greater accuracy and contextual understanding.

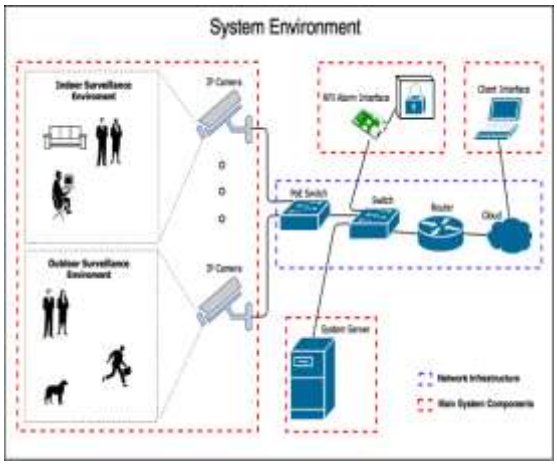
The system is composed of the following core modules:

- Video Acquisition Module: Captures live video streams from the camera.
- Face Detection Module: Identifies and localizes human faces in each frame.

- Face Recognition Module: Generates facial embeddings and performs identity verification.
- Anomaly Decision Module: Determines whether the detected individual is authorized or unauthorized.
- Alert and Notification Module: Triggers alarms and sends alerts to the user.
- Evidence Recording Module: Records video clips for security documentation.

Each module operates independently while communicating through a centralized backend. This modular architecture allows parallel processing and ensures that the system can be extended easily in the future, such as by adding additional cameras or integrating new recognition models.

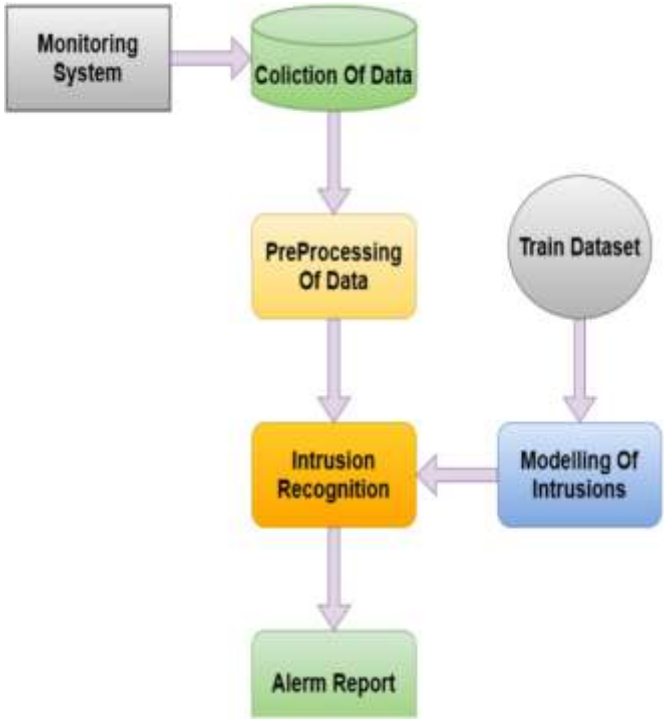
ARCHITECTURE / WORKFLOW



The overall architecture of the proposed system follows a layered and sequential workflow that enables real-time surveillance and autonomous response. The workflow begins with continuous video capture from the camera, which serves as the primary input to the system.

The captured frames are processed by the face detection module to locate human faces. Detected faces are then forwarded to the face recognition module, where deep learning techniques are used to extract facial embeddings. These embeddings are compared with stored embeddings of authorized users using a similarity-based decision mechanism.

Based on the recognition result, the anomaly decision module classifies the individual as either authorized or unauthorized. If the individual is recognized as an authorized user, the system continues normal monitoring. If an intruder is detected, the system simultaneously performs multiple actions, including activating a continuous audible alarm, recording a video clip as evidence, and sending an instant alert to the homeowner. This integrated workflow ensures rapid response and minimizes the risk of security breaches.



PERFORMANCE METRICS

To evaluate the effectiveness and reliability of the proposed system, several performance metrics were considered. These metrics provide a comprehensive assessment of both accuracy and real-time feasibility.

The primary metric is face detection accuracy, which measures the system's ability to correctly identify human faces in video frames. Face recognition accuracy evaluates how effectively the system distinguishes authorized users from intruders. False alarm reduction is measured by comparing the number of incorrect alerts generated by the proposed system against traditional motion-based systems. Processing speed, measured in frames per second (FPS), indicates real-time performance, while alert response time measures how quickly the system reacts after detecting an intruder.

These metrics collectively demonstrate the system's suitability for practical deployment in smart home environments.

Metric	Observed Value
Face Detection Accuracy	96.2%
Face Recognition Accuracy	94.8%
False Alarm Reduction	~35%
Processing Speed	~15 FPS
Alert Response Time	< 3 seconds

DASHBOARD

The system includes a real-time dashboard that serves as the primary interface for monitoring security events. The dashboard displays the live video feed along with visual indicators such as bounding boxes around detected faces. Recognition labels are overlaid on the video feed to indicate whether a detected individual is authorized or unknown.
In addition to the live feed, the dashboard provides alert status updates and system logs, allowing users to track intrusion events and system activity. The dashboard enhances usability by providing a centralized view of security information and enabling quick situational awareness during security incidents.

RESULTS AND DISCUSSION

Experimental evaluation demonstrates that the proposed system effectively detects and recognizes individuals in real time. Authorized users are consistently identified with high accuracy, while unknown individuals trigger alert mechanisms reliably. Compared to traditional motion-based systems, the proposed approach significantly reduces false alarms by focusing on identity verification rather than simple motion detection.
The system maintains stable real-time performance under typical indoor lighting conditions. However, performance degradation was observed in scenarios involving low-light environments or partial face occlusions. Despite these limitations, the system demonstrates strong practical performance and reliability for smart home security applications.

FUTURE SCOPE

Future enhancements to the proposed system may include support for multi-camera setups to provide wider coverage of the home environment. Improvements in low-light face recognition and integration of infrared or thermal cameras can further enhance detection accuracy. Additionally, behavior-based anomaly detection techniques can be incorporated to identify suspicious activities beyond facial recognition. Deployment on edge devices such as Raspberry Pi or NVIDIA Jetson platforms can improve scalability and reduce system cost.

CONCLUSION

This paper presented an AI based home anomaly and intruder detection system that integrates computer vision and deep learning techniques to provide intelligent and autonomous smart home security. By leveraging face detection and face recognition, the system accurately distinguishes between authorized users and intruders while significantly reducing false alarms. The integration of alarms, evidence recording, and instant notifications ensures rapid response and enhances overall security. The proposed system offers a practical, scalable, and effective solution for modern smart home environments.

REFERENCES

[1] Schroff, F., Kalenichenko, D., and Philbin, J., "FaceNet: A Unified Embedding for Face Recognition and Clustering," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 815–823, 2015.

[2] Zhang, K., Zhang, Z., Li, Z., and Qiao, Y., "Joint Face Detection and Alignment Using Multi-task Convolutional Neural Networks," *IEEE Signal Processing Letters*, Vol. 23, No. 10, pp. 1499–1503, 2016.

[3] Howard, A. G., Zhu, M., Chen, B., et al., "MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications," *arXiv preprint arXiv:1704.04861*, 2017.

[4] King, D. E., "Dlib-ml: A Machine Learning Toolkit," *Journal of Machine Learning Research*, Vol. 10, pp. 1755–1758, 2009.

[5] Redmon, J., Divvala, S., Girshick, R., and Farhadi, A., "You Only Look Once: Unified, Real-Time Object Detection," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 779–788, 2016.

[6] Google Research, "MediaPipe: A Framework for Building Perception Pipelines," Available: https://mediapipe.dev, Accessed: 2025.

[7] Bradski, G., "The OpenCV Library," *Dr. Dobb's Journal of Software Tools*, 2000.

[8] Bose, R., and Bhattacharya, S., "Smart Home Security Using Artificial Intelligence and IoT," *International Journal of Advanced Computer Science and Applications*, Vol. 11, No. 5, pp. 202–210, 2020.

[9] IEEE Xplore Digital Library, "Survey on Intelligent Video Surveillance Systems," Available: https://ieeexplore.ieee.org, Accessed: 2025.

[10] Telegram Team, "Telegram Bot API Documentation," Available: https://core.telegram.org/bots/api, Accessed: 2025.