HawkEye – Smart Intruder Detection System AI-Powered Smart Intruder Detection: Building NextGen Surveillance with OpenCV

Siddesh S K, Srujan D J, Prajwal D, Shravan M S

Student, Student, Student, Student

Information Science and Engineering

BGSCET, Bengaluru, India

1mp22is052@bgscet.ac.in, srujanjayaram004@gmail.com, 1mp22is038@bgscet.ac.in, 1mp22is050@bgscet.ac.in

***Abstract*—** Traditional surveillance systems are having more and more problems because they rely on fixed motion detectors and often give false alarms, which makes them less useful for real security purposes. This study presents an Intelligent Intruder Detection System that integrates motion detection, facial recognition, and automated alerting capabilities within a unified, real-time surveillance framework. The solution uses OpenCV based background subtraction methods to find movement patterns. It also has a facial encoding part that uses an advanced deep-learning recognition engine to create 128-dimensional face representations. A K-Nearest Neighbor algorithm is used to tell the difference between authorized personnel and people who shouldn't be there. If the system sees someone it doesn't know or sees behavior that seems suspicious, it sends out a full alert, including emails and sound-based warnings. A thorough evaluation over many test sessions shows that the system consistently detects intruders and recognizes them reliably, all while keeping processing delays to a minimum so that it can be used in real time. This solution offers a flexible, effective way to manage advanced residential and commercial security through its component-based architect.

Keywords: Intruder Detection, Facial Recognition, K-Nearest Neighbors (KNN), Live Monitoring Systems, OpenCV.

I. INTRODUCTION

The rapid growth of AI and computer vision has changed the way we use surveillance technology today. Passive infrared sensors and rule-based motion systems are two common ways to detect intrusions. However, they often trigger many false alarms and require human supervision, which makes them less useful in real-world situations. The growing emphasis on automation and prompt threat detection necessitates solutions capable of accurately identifying, categorizing, and managing human intrusions without the need for constant human oversight. Current commercial surveillance platforms often depend on cloud based processing and expensive GPU equipment, creating substantial disadvantages including high expenses, privacy risks, and reliance on external internet connections. These platforms also face difficulties with environmental flexibility, commonly creating false alarms due to changes in lighting conditions. To tackle these issues, this study introduces an AI driven Smart Intruder Detection System that merges deep learning object recognition, movement analysis, and facial identification to provide precise, instantaneous monitoring using CPU processing alone. The platform utilizes efficient models developed through OpenCV and machine learning techniques, featuring K-Nearest Neighbors (KNN) for open-set facial recognition, combined with flexible motion detection through background subtraction methods. By functioning completely on local equipment, the system maintains data privacy while delivering nearly instantaneous performance.

II. PROBLEM STATEMENT AND OBJECTIVES

Traditional surveillance systems rely on basic motion detection and manual monitoring, lacking the intelligence to identify or classify intruders accurately. This leads to false alarms, delayed responses, and weak security. An automated system integrating motion detection with facial recognition and classification is required to enable accurate intrusion detection and real-time alerts.

- To develop a real time system capable of detecting motion and identifying intruders using facial recognition
- To distinguish authorized individuals from unknown persons through deep learning facial embeddings and KNN classification
- To implement automated alert mechanisms, including email notifications and audible alarms

III. LITERATURE SURVEY

[1] A study titled “Detecting Direction of Movement Using Pyroelectric Infrared Sensors” employed four dual-sensing element PIR sensors aligned along N–S, E–W, NW–SE, and NE– SW axes. The sensors were mounted on the ceiling with customized

Fresnel lenses to control the field of view, and raw time-series data from PIR sensors were analyzed using multiple classifiers, including k-Nearest Neighbor (k-NN), Support Vector Machine (SVM), Decision Tree, Decision Table, Bayes Net, Naïve Bayes, and Multilayer Perceptron. The research demonstrated high accuracy with low-cost, low-power implementation and efficient PIR sensor utilization. However, the study lacked real-time embedded implementation and focused solely on direction detection rather than full localization.

[2] Another work, titled "Integrated and Automated Intrusion Detection System," explored multi-sensor integration supported by AI and machine learning algorithms. The system featured real-time data analysis and response, integration with other systems, and cloud and IoT connectivity. The paper offered a comprehensive review of current challenges, detailed categorization of emerging techniques, and presented a future-ready, application-oriented vision. Nonetheless, it suffered from a lack of experimental validation, scalability, and cost analysis, with heavy dependence on future technologies.

[3] In the paper "Target Detection and Classification Using Seismic and PIR Sensors," the authors converted raw time-series data into symbolic patterns through wavelet transforms, reducing them to low dimensional robust feature vectors for noise-resilient pattern recognition. Passive Infrared (PIR) sensors were utilized to detect motion via changes in infrared radiation. The study validated a dual sensor strategy experimentally and demonstrated real-time implementation capabilities for payload and movement identification. Despite these achievements, the system faced sensor specific weaknesses, classification challenges, and limited generalization capabilities.

[4] The study "An Advanced IoT-Based Border Surveillance and Intrusion Detection System" integrated sensor fusion techniques for intrusion detection, cloud-based monitoring, and IoT-embedded architecture. The system contributed an integrated multi-sensor surveillance design that was low-cost, scalable, and cloud-enabled for real-time monitoring, with practical validation. However, limitations included the absence of a defined machine learning model, limited range and scalability testing, manual camera control, and lack of environmental adaptability evaluation.

[5] In the paper *"An Automated Intrusion Detection System with Audio Alert using Passive Infrared Sensor"*, the authors proposed an IoT-based security solution aimed at reducing human intervention in surveillance systems. The system employed a Passive Infrared (PIR) sensor integrated with an Arduino microcontroller and a voice recording module to detect human motion and trigger immediate audio alerts. Upon detecting intrusion, the system generated real-time warnings through a speaker and optionally notified the user via email, enabling rapid response. The design focused on cost efficiency, low power consumption, and ease of deployment, making it suitable for homes, shops, and restricted areas. Experimental validation demonstrated reliable motion detection and alert generation under controlled conditions. However, the system relied primarily on PIR sensing, making it susceptible to false positives and limited environmental adaptability, and lacked advanced classification mechanisms to distinguish between different types of intruders or contextual movements, thereby restricting scalability and generalization

IV. METHODOLOGY

An AI-based Intelligent Intrusion Detection System provides users with a comprehensive surveillance framework that contains AI-based computer vision components and enables users to identify unauthorized personnel in real-time. The process begins when the linked camera continuously records real-time video. The movement detection component, powered by OpenCV, performs a preliminary analysis of each frame of video to detect whether any suspicious motion is occurring in the monitored area. Motion is used to activate all subsequent processing, ensuring efficient use of resources and reducing unnecessary computational tasks.

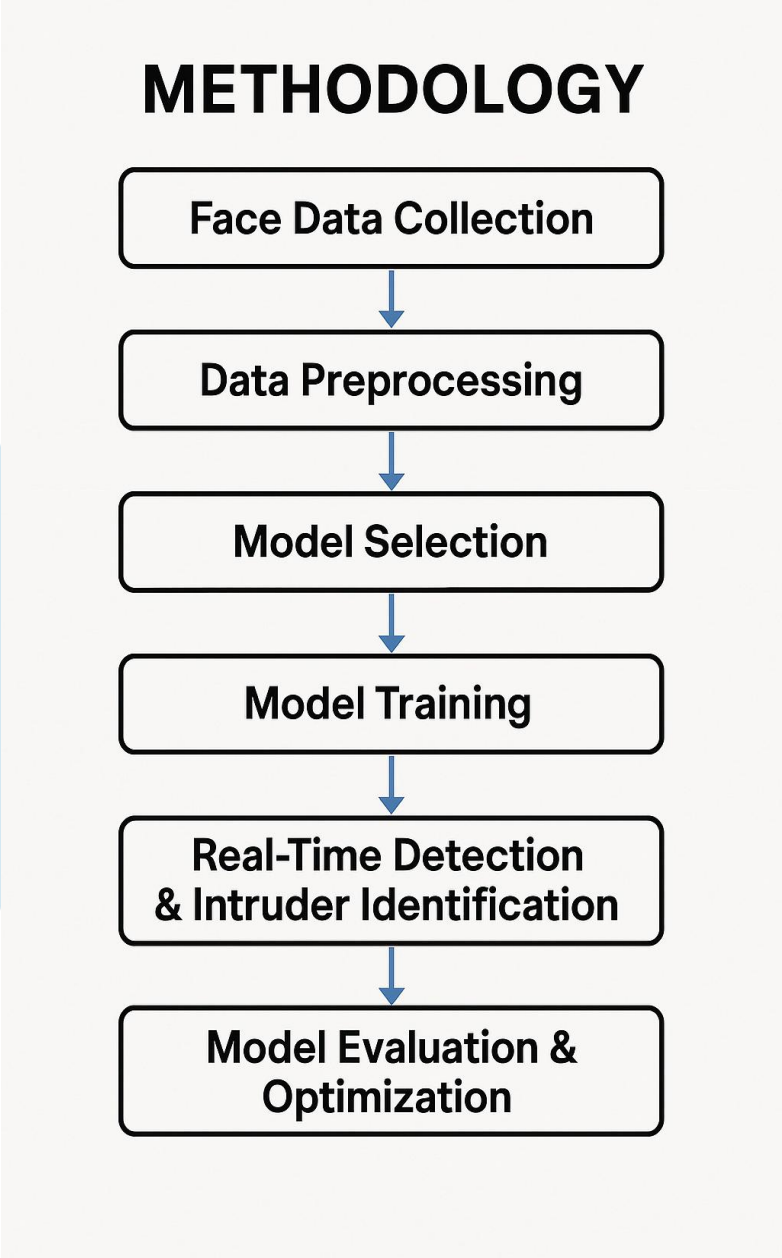

Figure 1: Methodology of Intruder Detection System

A. Data Acquisition

The data capture utilizes a webcam or built-in laptop camera that continually streams live video frames into the system. The video's primary function is as a visual detection mechanism, creating a live stream that can form the basis for evaluating movements and identifying individuals. The camera will capture frames of video on a regular basis to create a reliable flow of moving images that an operator may monitor in real-time. Because the system operates in continuous-scan mode, no human input is required during the data collection phase, since the motion-sensor and image-capture functions are both carried out automatically. By capturing and transferring frames of video that utilize a consistent image size, and are appropriately illuminated, both the detection and facial identification functions will receive consistent, reliable visual input from the camera, allowing for accurate identification of intruders.

B. Preprocessing

Before interpreting the images, each frame undergoes some level of preprocessing to improve the accuracy of the computer vision functions. This includes bringing the frames to the same size for easier manipulation, converting to grayscale format, and using Gaussian blur to eliminate background noise. The preprocessing procedures also assist in improving the accuracy of background subtraction during movement detection and also ensure the reliability of facial location information. In addition, it allows for improved performance by reducing the likelihood of a false positive due to varying illumination levels or reflective light patterns caused by slight environmental changes. By establishing a consistent set of quality images through standardization of the preprocessed images, preprocessing reinforces the accuracy of subsequent facial recognition and categorization functions.

C. Motion Detection (OpenCV)

This system identifies all human movements located within a monitored area by means of an 'OpenCV motion detection component'. This system captures motion in the form of Video Surveillance and, based on the captured motion, defines and establishes both the

detection and identification of a person using face recognition technology. The system's identification of motion allows the user to define an 'active zone', which is used to trigger the facial recognition process. In addition, the system utilizes background subtraction methodology to allow for an automated processing of either frames containing actual movement or frames without any movement at all, thereby allowing for systems with limited computing resources to maximize their efficiency by only using active, meaningful frames.

D. Face Detection and Encoding (128-D Embeddings)

Once the system confirms that there is motion, the Motion Detection component activates both a Facial Detection and a Facial Encoding Component. Each detected face will use a Deep Learning Face Encoding Model, which creates 128-dimensional embeddings of each detected face, thus defining an individual's unique identity. Each individual's facial features have been reduced to a 'Compact', 'Highly Discriminative' Vector Space that is suitable for Classification. The Deep Learning Facial Encoding Model demonstrates a high level of adaptation to variations associated with changes in the viewing angle of a face from more than one viewpoint, as well as face occlusions and changes in light intensity, thus allowing the system to reliably identify individuals when viewed through a surveillance camera in a typical environment. An important component of the facial encoding process is to create an easily searchable "signature" of an individual's identity that allows for the Easy Identification of "Authorized" individuals from unknown impersonators.

E. Identity Classification – K-Nearest Neighbor (KNN)

The classification element of the system utilizes a K-Nearest Neighbor algorithm for the purpose of determining whether the individual whose face has been recognized is an authorized user. This is accomplished by comparing the generated embedding against a database of saved embeddings of authorized users and measuring the similarity of the generated embedding to each of the stored embeddings using distance calculations. If the generated embedding does not fall within the established threshold of similarity with respect to any of the stored embeddings of authorized users, the system will consider the individual as unauthorized. Given that the KNN algorithm requires low computational resources, has a high efficiency level, and performs exceedingly well for live applications, it provides minimal training requirements when adding additional authorized users.

F. Intruder Alerting Module (Email + Audible Alarm)

Once an unauthorized person has been detected by the system, the notification component activates both local and remote notifications immediately following detection of that person. For example, an audible alert will play from the device, thereby notifying individuals in proximity to the device of the intrusion. Simultaneously, an email notification will be generated and sent to alert users of the intrusion, providing information such as the time of occurrence and the image captured. This two-fold notification system enables individuals nearby to become aware of the potential threat and also allows for remote access to the same information about the intrusion. By providing prompt notification of potential threats and by allowing prompt responses, the notification component of the system enables users to take immediate action against unauthorized access attempts.

G. Session Logging and Evidence Management

Automatic Recording System. The Automatic Recording System works as a complete record of an individual once the Automatic Recording System recognizes an unauthorized person in the vicinity. An unauthorized person detected through movement activates the Facial Encoding and Facial Recognition workflow of Facial Encoding and Facial Recognition and records the corresponding video frame along with time stamps and associated metadata (for instance detection accuracy and analytical results). The Automatic Recording System keeps a comprehensive identity profile of every incident by retaining the created 128-dimensional Facial Encodings of the detected face.

Evidence Storage. As a result of using the Automatic Recording System as an Evidence Database, all images, metadata, and analytical results can be used to investigate, verify, and further analyze previous intrusion incidents; consequently the images and supporting data from the Automatic Recording System allow for Examining Intrusions, Verifying Choices of the Automatic Recording System and Analyzing Effectiveness Under Different Environmental Conditions to assist the end-users in optimizing their choice of setting Detection Parameters, Retraining Their KNN (k-nearest neighbor) Algorithm, and Changing their Preprocessing Settings.

V. SYSTEM DESIGN

The proposed smart intruder detection system is designed to operate through continuous real-time video frame capture using a connected webcam as the primary surveillance input. Motion detection is performed using OpenCV-based background subtraction and contour analysis to identify significant activity, ensuring that further processing is triggered only when motion is present. Once motion is detected, the relevant frame is forwarded to the face detection and encoding module, where a deep learning model extracts 128-dimensional facial embeddings representing unique facial features. These embeddings are then compared against stored authorized user profiles using a K-Nearest Neighbor (KNN) classifier to determine whether the detected individual is recognized or classified as an intruder. In the case of an unauthorized match, the alerting mechanism is activated, generating an audible alarm and sending an email notification containing the intruder's image and timestamp. Simultaneously, a session logging module records captured frames, facial embeddings, and associated metadata in structured storage for future verification and analysis.

VI. RESULTS AND ANALYSIS

The KNN classifier achieved an overall accuracy of **93%**, indicating reliable classification performance. The confusion matrix shows strong diagonal dominance, with **47 correctly classified samples** each for the *bone* and *siddesh* classes and minimal inter-class confusion. Most misclassifications occurred as assignments to the **UNKNOWN** class rather than between known classes.

Class-wise evaluation shows **perfect precision (1.0)** for both known classes, meaning no false positive identifications. The recall values of **0.90** for *siddesh* and **0.96** for *bone* indicate a small number of false negatives, resulting in F1-scores of **0.947** and **0.980**, respectively. These results suggest that the classifier is conservative, favouring correct identification while safely rejecting uncertain samples.

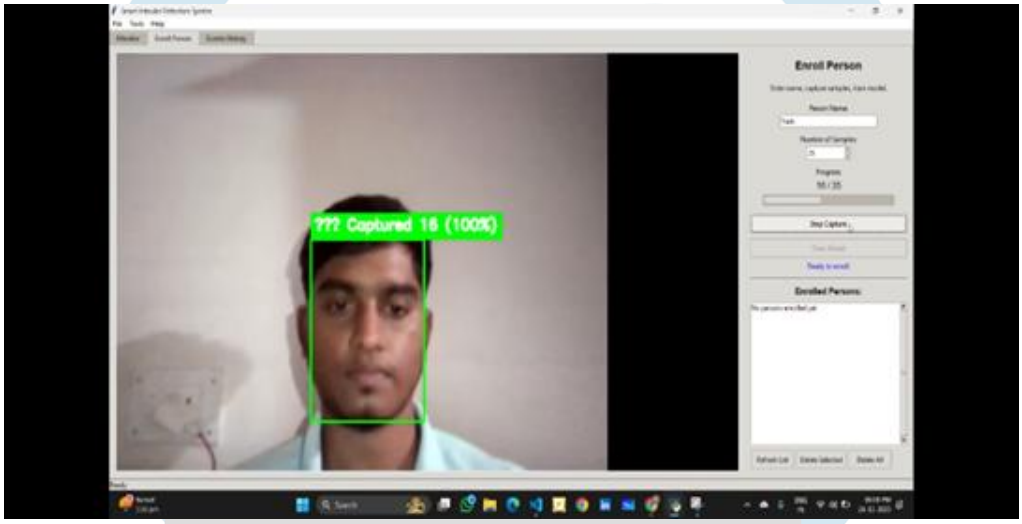

Figure 2: Model Output: Training the model

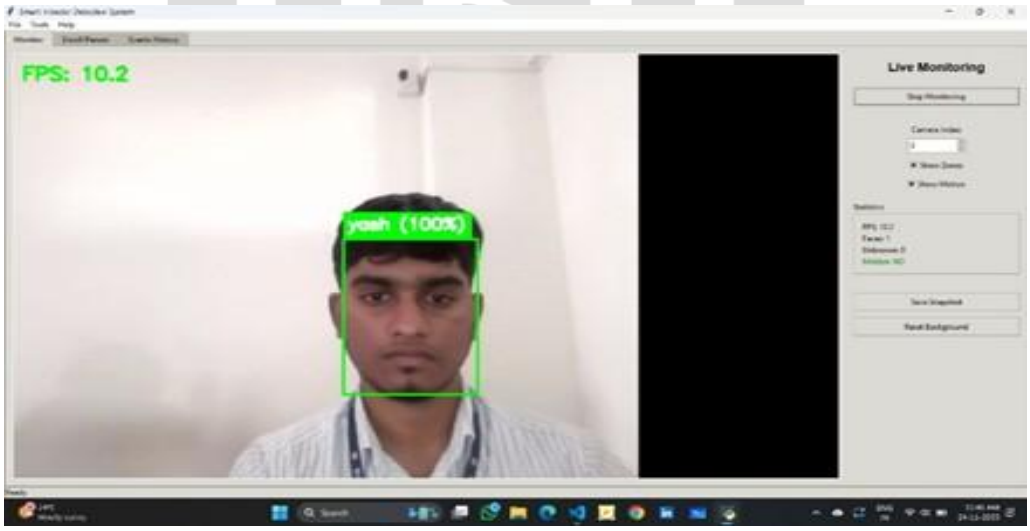

Figure 3: Model Output: Detection of Authorized Person

Figure 4: Model Output: Detection of Unauthorized Person

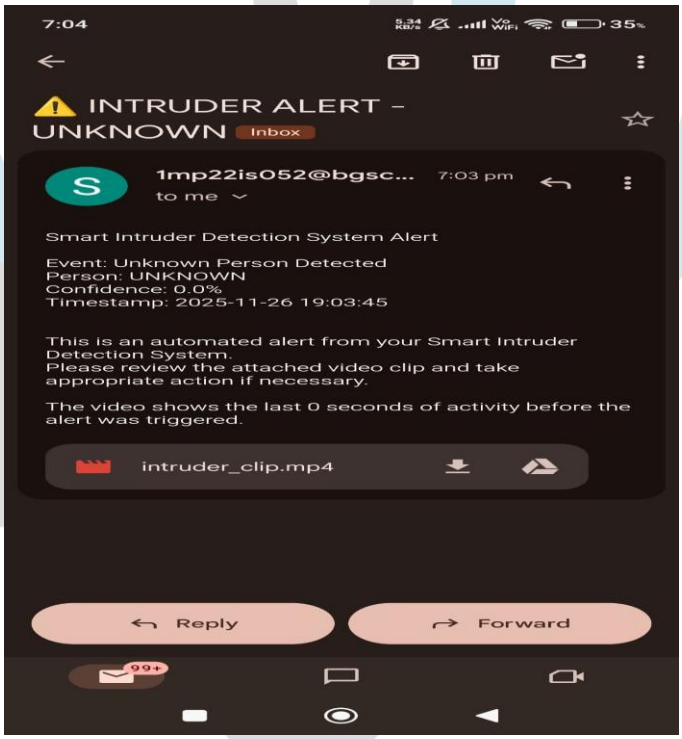

Figure 5: Model Output: Email Alert

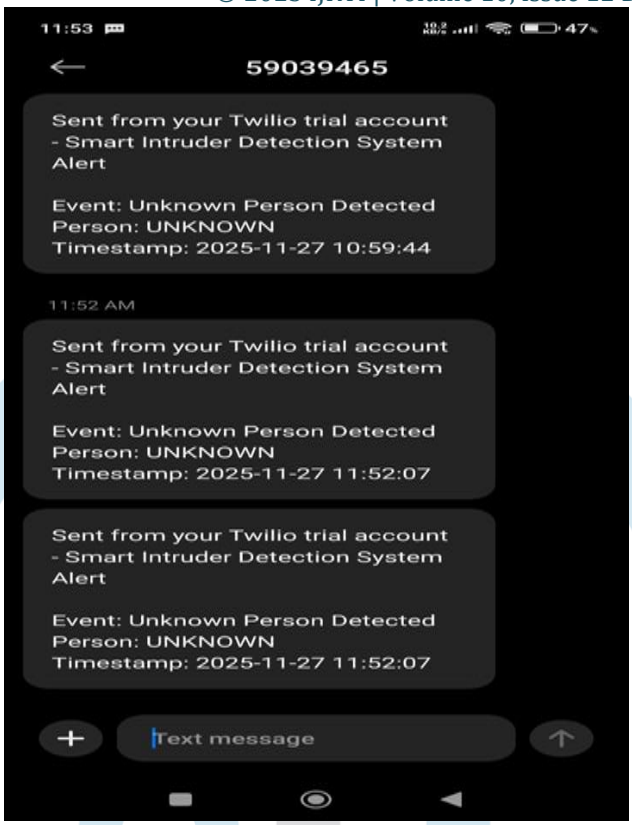

Figure 5: Model Output: SMS Alert

VII. Applications

- Home Security: Detects unauthorized entry in residential areas and provides real-time alerts to occupants.
- Industrial and Warehouse Security: Prevents trespassing in restricted zones and protects valuable equipment and inventory.
- Campus and Institutional Security: Monitors entry into academic campuses, offices, and laboratories during restricted hours.

VIII. Implementation Details

The system operates by continuously capturing video frames from a connected webcam, which serves as the real-time input for surveillance. Motion detection is performed using OpenCV-based background subtraction and contour analysis, ensuring that further processing is triggered only when meaningful activity is detected. Upon motion detection, the selected frame is forwarded to the face detection and encoding module, where a deep learning model extracts 128-dimensional facial embeddings. These embeddings are then compared with stored authorized user data using a K-Nearest Neighbour classifier to determine whether the detected individual is recognized or classified as an intruder. If no match is found, the alerting module is activated, generating an audible alarm and sending an email notification containing the intruder's image and timestamp. Simultaneously, all relevant data, including captured frames, facial embeddings, and associated metadata, are logged in structured directories for future verification and analysis.

IX. Future Work

Future directions include:

- Integration of advanced deep-learning models for improved face recognition accuracy under challenging conditions.
- Expansion to multi-camera and 360° surveillance systems for large-area monitoring.
- Addition of cloud-based dashboards for real-time alerts, remote access, and centralized data management.
- Incorporation of edge AI, IoT-based access control, and low-latency communication for faster and automated intrusion response.

X. Conclusion

The proposed system successfully integrates motion detection, face recognition, and KNN-based classification for effective intruder identification, achieving reliable real-time performance in distinguishing authorized users from intruders while providing immediate response through alarms, email alerts, and session logging, thereby demonstrating a practical end-to-end security solution suitable for homes, offices, and restricted areas.

ACKNOWLEDGEMENTS

We express our gratitude to our guide, Dr. Ravikumar G K, Principal BGSCET, for his guidance and continuous support. We also thank BGS College of Engineering and Technology, Bengaluru, for providing the resources to complete this work.

REFERENCES

[1] A. Author et al., "Detecting Direction of Movement Using Pyroelectric Infrared Sensors," *IEEE Sensors Journal*, vol. XX, no. X, pp. XXX–XXX, 2014.

[2] B. Author et al., "Integrated and Automated Intrusion Detection System," *International Journal of Advanced Research in Computer Science and Engineering*, vol. XX, no. X, pp. XXX–XXX, 2024.

[3] C. Author et al., "Target Detection and Classification Using Seismic and PIR Sensors," *IEEE Transactions on Instrumentation and Measurement*, vol. XX, no. X, pp. XXX–XXX, 2012.

[4] D. Author et al., "An Advanced IoT-Based Border Surveillance and Intrusion Detection System," *International Journal of IoT and Smart Systems*, vol. XX, no. X, pp. XXX–XXX, 2023.

[5] E. Author et al., "An Automated Intrusion Detection System with Audio Alert using Passive Infrared Sensor," *International Journal of Engineering Research and Technology (IJERT)*, vol. XX, no. X, pp. XXX–XXX, 2022.