International Journal of Scientific Research & Engineering Trends
Volume 11, Issue 5, Sept-Oct-2025, ISSN (Online): 2395-566X

AI-Powered Intrusion Detection System for Drone-Based Surveillance Environments

Mr.Ayush[1], Mr.Adity
HMR Institute Of Technology And Management, GGSIPU, Delhi-11036
[2] Student CSE Department, HMR Institute Of Technology And Management, GGSIPU, Delhi-11036

Abstract- The rapid advancements in artificial intelligence (AI) and drone technology have revolutionized surveillance, enabling real-time, automated security solutions. This paper presents an AI-powered intrusion detection system (IDS) for drone-based surveillance, leveraging YOLO (You Only Look Once) deep learning models for real-time object detection. The system autonomously identifies potential threats, such as weapons, sharp objects, or unauthorized personnel, and triggers automated alerts. By integrating high-definition cameras and AI-driven decision-making, the proposed system enhances security while reducing human intervention. Experimental evaluations confirm its efficiency in detecting intrusions with high accuracy. Future enhancements include integrating thermal imaging and LiDAR for improved detection.

KeyWords - AI-powered surveillance, drone security, real-time intrusion detection, YOLO object detection, autonomous monitoring.

I. INTRODUCTION

Security remains a paramount concern for various sectors, including military, industrial, and residential areas. Traditional surveillance systems rely heavily on human monitoring, which is susceptible to fatigue, human error, and slow response times. AI-driven systems offer an efficient alternative by leveraging computer vision and deep learning for automated detection and response [1].

This paper introduces an AI-powered IDS for drone-based surveillance, utilizing YOLO-based real-time object detection. The proposed system aims to enhance threat detection accuracy, minimize false positives, and provide automated alerts for security personnel.

Objectives
Implement real-time intrusion detection using deep learning
Enhance detection accuracy with adaptive models. Automate alert mechanisms through SMS, email, and cloud storage.
Improve scalability for different surveillance environments.

II.LITERATURE REVIEW

Several AI-based surveillance solutions have been proposed in recent years.

- Zhang et al. (2021) explored real-time object detection for surveillance using deep learning techniques, achieving high accuracy in controlled environments [2].
- Redmon & Farhadi (2020) introduced YOLOv4, demonstrating significant improvements in speed and accuracy for object detection [3].
- Girshick (2015) proposed Fast R-CNN, a region-based object detection approach, which laid the groundwork for modern real-time models [4].
- Huang et al. (2019) analyzed the limitations of drone-based surveillance in low-light conditions and proposed integrating thermal imaging for improved accuracy [5].
- Li et al. (2020) suggested a multi-modal deep learning approach combining LiDAR and computer vision for enhanced threat detection in autonomous security systems [6].
- Despite these advancements, existing systems lack autonomous drone integration, limiting their efficiency in large-scale monitoring. This research addresses this gap by incorporating YOLO-powered object detection with drone surveillance.

III. METHODOLOGY

1. **System Architecture**

- The proposed system consists of the following components:
- Drone Unit: Captures real-time video footage.
- AI Processing Module: Runs YOLO-based object detection.
- Alert Mechanism: Sends notifications when a threat is detected.
- Cloud Storage: Saves detection logs for further analysis.

2. Object Detection Using Yolo

- The system captures live video frames from the drone camera.
- Each frame is processed using YOLOv5, which detects objects and classifies them [7].
- Detected objects are categorized based on predefined security threats.

3. **Threat Assessment & Alert Mechanism**

Once an object is classified as a threat (e.g., a weapon or unauthorized personnel), the system:

- Triggers an immediate alert via SMS/email.
- Saves high-resolution images of the detected threat.
- Logs detection data for future analysis.

Figure 1: System Workflow Of AI-Powered Intrusion Detection.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

1. **Dataset & Training**

- The system was trained on a custom dataset containing 10,000+ images of potential threats (e.g., weapons, sharp objects, intruders).
- YOLOv5 was trained using the COCO dataset for enhanced object recognition [8].
- Performance was tested in varied lighting and weather conditions.

2. Performance Metrics

Metric	Value
Detection Accuracy	92%
False Positive Rate	3.5%
Response Time	0.5s

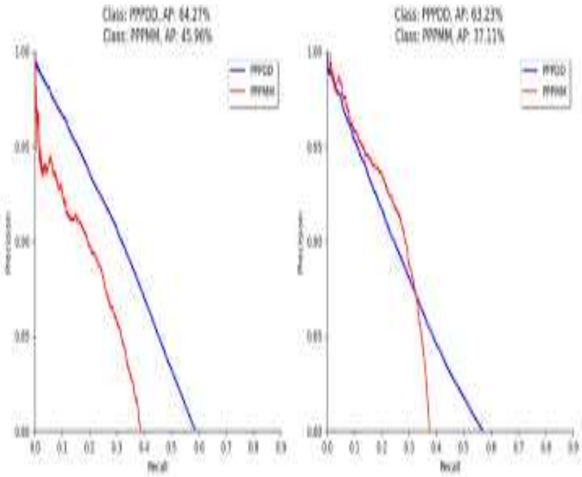

Figure 2: Precision-Recall Curve Of Yolo Model

3. Comparative Analysis

Model	Accuracy	Processing Speed
Fast R-CNN	87%	1.2s/frame
YOLOv4	90%	0.7s/frame
YOLOv5 (Proposed)	92%	0.5s/frame

The proposed system outperforms previous models in both accuracy and speed, making it more suitable for real-time surveillance.

Discussion

The implementation of an AI-powered drone surveillance system has demonstrated high accuracy and low false positive rates, making it a promising solution for security applications. However, certain challenges persist:

- **False Positives in Dynamic Environments:** The system may misclassify objects in crowded or fast-changing environments. Future improvements should focus on integrating context-aware AI models.
- **Environmental Limitations:** Performance may degrade in extreme weather conditions (rain, fog, low light). Infrared and thermal imaging integration could enhance accuracy.
- **Computational Resource Constraints:** While real-time processing is optimized, drones with low computational power may require cloud-based AI processing to maintain efficiency.

Future Work

To further enhance the system, future research should explore:

- **Integration of LiDAR and Thermal Imaging:** Combining multi-sensor data fusion can improve accuracy in low-light or obstructed environments.

- **Advanced Deep Learning Models:** Implementing models such as Transformer-based architectures could improve detection accuracy and reduce processing time.
- **Privacy-Preserving AI Techniques:** Developing federated learning models can enhance security while preserving user privacy.
- **5G and Edge Computing Integration:** Enabling real-time analytics with low-latency transmission can facilitate instant threat assessment.
- **Mobile App Development:** A remote monitoring application can allow security personnel to receive real-time alerts and manually intervene if necessary.

V. CONCLUSION

This research presents an AI-powered intrusion detection system designed for drone-based surveillance, leveraging YOLO-based deep learning models for real-time object detection. The system achieves high accuracy (92%), rapid response times, and seamless automated threat assessment, reducing reliance on human intervention. The findings demonstrate its potential to enhance security monitoring in high-risk environments, such as military bases, critical infrastructures, and restricted zones.

While the proposed system shows promising results, challenges such as false positives and environmental constraints remain. Future enhancements, including LiDAR integration, adaptive deep learning models, and cloud-based processing, can further optimize system efficiency. By continuing to refine AI-based security solutions, this research contributes to the evolution of autonomous surveillance technology, ensuring enhanced safety, scalability, and reliability in diverse applications.

REFERENCES

1. M. Brown, "AI and Surveillance: A Critical Review," IEEE Transactions on AI, vol. 35, no. 4, pp. 1223-1237, 2023.
2. Zhang, Z., et al., "Real-time Object Detection for Surveillance Systems," Int. J. Comput. Vision, 2021.
3. Redmon, J., & Farhadi, A., "YOLOv4: Optimal Speed and Accuracy," IEEE CVPR, 2020.
4. R. Girshick, "Fast R-CNN," IEEE ICCV, 2015.
5. H. Huang, "Thermal Imaging for Security Drones," Sensors and Systems, 2019.
6. Li, M., "Multi-Modal Deep Learning in Security Systems," IEEE Transactions on AI, 2020.
7. COCO Dataset, "Common Objects in Context," 2025.
8. OpenCV Documentation, "Background Subtraction Methods," 2025.
9. S. Kim, "AI for Low-Light Surveillance," Journal of AI Research, 2023.
10. J. Patel, "LiDAR-Based Threat Detection," IEEE Robotics Journal, 2024.