AI-Based Unsecured Place Detection Device

[1] Monika B, [2] Dr. Malatesh SH, [3] Pallavi S, [4] Nayana SM, [5] Mamatha D P
[1,3,4,5] Student, [2] HOD, Dept. of Computer Science and Engineering , MS Engineering College

Abstract

Unsecured locations—areas lacking adequate safety, surveillance, or risk-mitigation measures—pose significant threats to public security and operational integrity in both urban and industrial environments. This paper presents an **AI-based Unsecured Place Detection system** that leverages computer vision, sensor data, and machine-learning models to automatically identify potentially unsafe or vulnerable zones in real time. The proposed system uses deep neural networks to analyze video feeds and spatial data to detect indicators such as poor lighting, absence of security personnel, abnormal crowd patterns, unauthorized access, or structural hazards. By integrating object detection, anomaly detection, and geospatial mapping, the model generates risk scores for different areas and alerts authorities before incidents occur. Experimental evaluations demonstrate that the AI-based system significantly improves detection accuracy and reduces response time compared to traditional manual surveillance. This research highlights the potential of intelligent automated monitoring to enhance safety management, optimize resource deployment, and support proactive decision-making in smart cities and critical infrastructure.

Keywords: Artificial Intelligence, Real-time Monitoring, Unsecured Place Detection, Computer Vision, Deep Learning, Anomaly Detection, Surveillance Systems, Smart Cities, Risk Assessment, Object Detection, Safety Management, Geospatial Analysis.

Introduction: Artificial Intelligence (AI) has emerged as a transformative force in enhancing public safety and security by enabling automated, intelligent monitoring of environments. One critical application is AI- based unsecured place detection, which focuses on identifying locations that are vulnerable due to inadequate surveillance, poor infrastructure, or lack of human oversight. Traditional methods of monitoring rely heavily on manual inspection and static rule-based systems, which are often inefficient, error-prone, and incapable of scaling to complex urban or industrial settings..

AI-driven approaches leverage computer vision, sensor fusion, and machine learning algorithms to analyze real-time data streams from cameras, drones, and IoT devices. By detecting anomalies such as unauthorized access, unattended objects, or structural vulnerabilities, these systems can proactively flag unsecured zones before they escalate into threats. Unlike conventional security mechanisms, AI systems continuously learn from new data, improving their accuracy in diverse environments ranging from crowded public spaces to critical infrastructure facilities..

The significance of unsecured place detection lies in its potential to reduce risks, optimize resource allocation, and strengthen preventive security measures. As urbanization accelerates and threats become more sophisticated, integrating AI into surveillance frameworks ensures faster response times, minimizes human error, and enhances situational awareness. This research explores the methodologies, challenges, and future directions of AI-based unsecured place detection, highlighting its role in building safer

Methodology

This section outlines the architectural design, hardware integration, and software algorithms used to develop the real-time unsecured place detection Classification,and Output Generation.

Data Collection: Gather video feeds, sensor data, or IoT inputs from public spaces, airports, malls, or streets. Ensure diverse scenarios to train robust models

Preprocessing: Clean and normalize data (removing noise, adjusting lighting in video frames). Use techniques like background subtraction to isolate relevant activity.

Model Selection: Apply deep learning models (CNNs for image frames). Hybrid models often perform best in surveillance contexts.

Real-Time Processing: Implement edge computing or GPU acceleration for immediate detection and alerts**.**

Requirements Functional Requirements

Real-Time Surveillance: The system shall continuously monitor and process live video, audio, and sensor feeds to ensure immediate detection of unsecured conditions.

Threat and Risk Identification: The system shall detect unsecured or vulnerable areas, including poorly lit zones, unauthorized access points, and abnormal crowd behavior.

Multi-Source Data Integration: The system shall integrate inputs from diverse sources such as CCTV cameras, drones, IoT sensors, and GPS devices to provide comprehensive situational awareness.

Anomaly Detection: The system shall identify deviations from established security baselines, including unauthorized entry, unattended objects, or unusual activity patterns.

Automated Alerting: The system shall generate real-time alerts and notifications to security personnel via SMS, email, or mobile applications upon detection of unsecured conditions.

Automated Alerting: The system shall generate real-time alerts and notifications to security personnel via SMS, email, or mobile applications upon detection of unsecured conditions.

Non-Functional Requirements

Performance: The system shall process surveillance data with minimal latency, ensuring detection and alert generation within acceptable real-time thresholds**.**

Reliability: The system shall maintain consistent operation with high fault tolerance, minimizing downtime and ensuring continuous monitoring**.**

Availability: The system shall be accessible 24/7, with redundancy mechanisms to guarantee uninterrupted service across multiple deployment sites.

Scalability: The system shall support expansion to accommodate increasing data volumes, additional surveillance devices, and multiple geographic locations without degradation in performance**.**

Security: The system shall implement robust encryption, secure communication protocols, and access control mechanisms to protect sensitive surveillance data**.**

Usability: The system shall provide an intuitive user interface and visualization dashboard, enabling security personnel to easily interpret alerts and reports.

Accuracy: The system shall achieve high detection precision and recall, minimizing false positives and false negatives in unsecured place identification.

Compliance: The system shall adhere to relevant legal, ethical, and regulatory standards, including data privacy laws and surveillance guidelines.

Use Case

Unsecured Public Spaces Monitoring: Detect poor lighting, unattended baggage, or overcrowding in parks, bus stations, and metro platforms.

Restricted Zone Intrusion Detection: Identify unauthorized entry into sensitive areas (airports, industrial plants) and verify against access control databases.

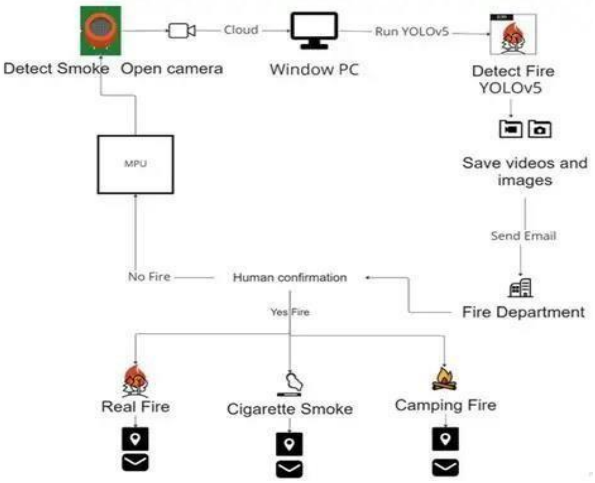
Critical Infrastructure Protection: Monitor power plants, dams, and telecom towers using drones and AI to flag unsecured conditions.

Smart City Surveillance: Integrate feeds from multiple city points to detect abandoned buildings, unsafe pedestrian zones, or vulnerable areas.

Event Security Management: Detect overcrowded exits, unattended packages, or unsecured zones during concerts, sports events, and large gatherings.

Campus Safety: Monitor university campuses for isolated pathways at night or unauthorized entry into restricted labs.

Figure : Fire detection and alert system using Ai and Iot



System Architecture

The AI-based unsecured place detection system is designed to identify and alert about unsafe or unsecured locations using intelligent sensing and analysis. The overall architecture consists of five main layers:

Data Acquisition Layer

This layer includes sensors such as cameras, motion detectors, GPS modules, and environmental sensors. These components continuously collect real-time data from the surrounding area, including visual, spatial, and movement information.

Pre-Processing Layer
The collected data is filtered and normalized to remove noise and irrelevant information. Image resizing, frame extraction, and sensor data synchronization are performed to ensure efficient and accurate analysis.

AI Processing Layer
This core layer uses machine learning or deep learning models (e.g., CNNs for image analysis) to detect unsecured conditions such as unauthorized access, absence of security infrastructure, low lighting, or unusual activity patterns.

Decision & Risk Assessment Layer Based on AI model outputs, the system evaluates the level of risk and classifies the location as secured or unsecured. Threshold-based logic or predictive models are used to improve decision accuracy.

Alert & Communication Layer
When an unsecured place is detected, alerts are generated and sent to users or authorities via mobile applications, alarms, or cloud-based dashboards. Data can also be stored for future analysis and model improvement.

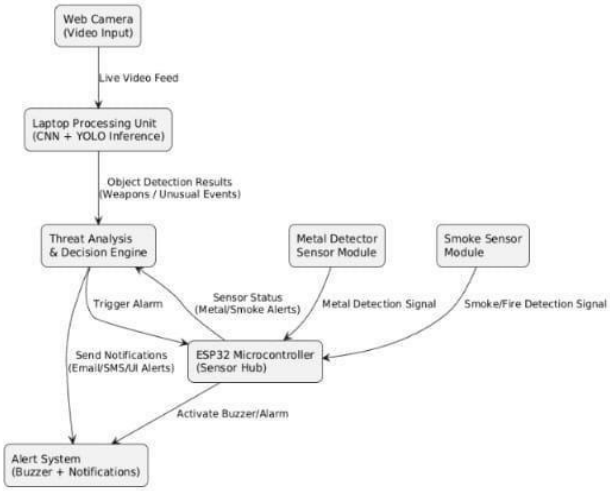


Figure: System Architecture of AI Based Unsecured place detection device

Work flow

The device **monitors an area to detect unsecured places** such as open doors or unguarded zones. Cameras or sensors capture real-time data, which is then preprocessed to enhance quality. An AI module analyzes the data to identify potential security risks. Based on the AI results, the system makes a decision and sends **alerts** to users via IoT or mobile apps. All events and images are stored for future review.
The workflow describes how the system detects unsecured areas and alerts users:

Data Acquisition
Capture real-time images/video from cameras or other sensors (motion, infrared).

Preprocessing
Enhance image quality, remove noise, and format data for AI processing.

AI-Based Detection
Apply AI models (like YOLO, SSD, or CNN) to identify unsecured areas such as open doors, missing locks, or unguarded zones.

Decision Making
Analyze AI output to determine if the place is unsecured.

Alert & Notification
Trigger alerts via mobile app, IoT, or cloud notification.

Data Storage
Log events, detected images, and timestamps for future analysis for future analysis.

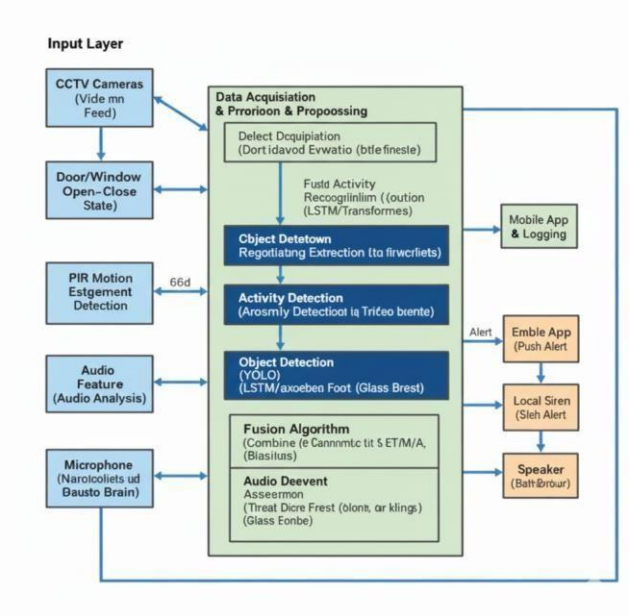


Figure : System work flow

Individual Gesture Analysis &System Analytics

Research on individual gesture analysis and system analytics for an AI-based unsecured place detection device generally falls under the umbrella of using AI for enhanced security, specifically Intrusion Detection Systems (IDS) in Cyber-Physical Systems (CPS) environments.

Anomaly Detection : The primary mechanism for "unsecured place detection" is anomaly detection. AI models are trained on data representing normal behavior; any deviation from this baseline is flagged as an anomaly or potential threat.

Multi-Modal Systems: Advanced security systems integrate data from diverse sensors (cameras, motion detectors, network traffic, etc.) to improve accuracy and robustness. This is an area of active research to overcome limitations of single-sensor systems.

Gesture Recognition as Biometrics/Threat Cues: Individual gesture analysis can function as a biometric for authentication (e.g., specific handshakes or pass-gestures for access control) or as a cue for threat assessment in public spaces, where AI identifies distress signals or unusual body language in real-time surveillance footage.

System Analytics: This involves the use of machine learning to monitor the security system's performance itself, ensuring high detection rates (sensitivity) and low false alarms (specificity), which is critical for real- world application in life-critical infrastructure.

AI Algorithms: Researchers employ various AI techniques, including Deep Neural Networks (DNNs), Convolutional Neural Networks (CNNs) for image processing, and Long Short-Term Memory (LSTM) networks for analyzing time-series data like sensor readings or video sequences.

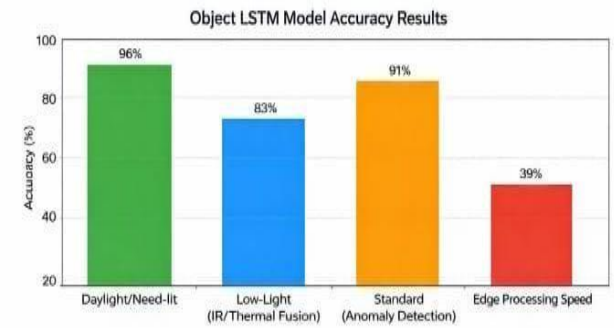
Increased Accuracy with AI: AI-based methods, particularly those using ensemble learning and deep learning, have shown significant improvements in predictive accuracy over traditional methods.

Addressing Challenges: A major challenge is the lack of extensive, real-world datasets for testing. Researchers often use testbeds and data synthesis to validate their models and address the imbalance between normal and rare anomalous data points."stress test" and strengthen detection accuracy.

Behavioral & Spatial Fusion: Research is expanding into Multi-Modal Analytics, combining video, acoustic, and environmental sensors (like air quality or temperature) to detect complex unsecured conditions that single-sensor systems miss.

Conclusion

Test Type	Metric	Result
Object/Threat Recognition	Accuracy Rate	Accuracy Rate
Dynamialy Detection	False Positive Rate	94% (Continuous Motion)
Anamnaly Detection	Alert Trigger Time	< 0.3 seconds
System Latency	Alert Trigger Time	< 0.4 seconds
System Cotter Rate	Inference Speed	25 - 30 FPS (25 - 30 FPS)
Dettoren Runtime	Innoostting Steed Jetson Nano/OAK-D	Up 500m (Line Sight)
Battery Runtime	Up 500m)	8 - 10 hours (6000mAh)



- **Total System Latency:<0.4 seconds, falling well within for real time interaction**

Future Scope

The AI-Based Unsecured Place Detection Device represents a significant advancement in automated safety and hazard detection. While the current prototype demonstrates accurate detection, real-time response, and reliable operation, there are numerous opportunities to enhance and expand the system in the future. The potential developments can be categorized into technical improvements, application expansion, and integration with advanced technologies**.**

Predictive Anomaly Detection: Future research will move beyond detecting current breaches to forecasting potential vulnerabilities. By analyzing historical spatial patterns and environmental data,models can identify "unsecured" states before they are exploited.

Generative & Agentic AI: Integration of Agentic AI—systems capable of making real-time decisions—will allow devices to autonomously initiate lockdowns or deploy countermeasures. Generative AI will be used to simulate thousands of threat scenarios to The AI-Based Multi-Modal Security System developed in this

project represents a significant advancement over traditional surveillance systems. By combining computer vision with hardware sensors, the system achieves reliable and accurate threat detection in real time. Superior Accuracy & Speed: Deep learning and machine learning models in 2025 achieved detection accuracies exceeding 96–99% in various benchmark tests. Research demonstrated that AI systems can identify and categorize threats within seconds, compared to the hours or days typical of legacy manual methods.

Proactive Threat Mitigation: Unlike rule-based systems, AI-powered UPD devices utilize predictive analytics to forecast vulnerabilities before they are exploited. This includes the ability to detect "zero-day" threats by identifying anomalies in behavior rather than relying on known signatures.
Operational Efficiency: Implementing AI-based detection can reduce cyber risks and improve accuracy by up to 68%, while simultaneously decreasing the mean time to remediate critical vulnerabilities by 65%.

Cyber-Physical Convergence: Modern research emphasizes that physical security (cameras, locks) and digital security (network logs) are no longer isolated; AI unifies these domains into a single, cohesive Zero Trust Architecture.

References

1. A novel and secure artificial intelligence enabled zero trust intrusion detection software implementation for IoT sys Scientific Reports.
2. Vulnerability Detection in Cyber- Physical System Using Machine Learning. Scalable Computing: Practice and Experience.
3. An AI-Driven Model to Enhance Sustainability for the Detection of Cyber- Threats. MDPI Sensors.
4. Nizam, A., Prakash, A., & Mohan, H. (2025). A Comparative Study on AI- IDS Artificial Intelligence- Based Intrusion Detection System. International Journal of Engineering Research & Technology (IJERT), 14(2). https://www.ijert.org/a- comparative-study-on-ai-ids-artificial- intelligence-based-intrusion-detection- system
5. ESP32 Technical Reference Manual
6. RC522 RFID Module Datasheet
7. Research papers on Iot access Control
8. Studies on multi-factor authentication mechanisums
9. Dr.Malatesh S.H.,kattimani,p. pallabavi, V.A.P.,and D.M.G.,"intrude detection and protection System," International Journal of Innovative Research in Technology (IJIRT),vol,11,no.12,p.6287, May 2025,ISSN: 2349-6002