International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2463-2467
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0329

AI Powered Surveillance System for Threat and Anomaly Detection Using CNN and Realgan

Mrs. P. Mahalakshmi [1], Aslam Ashik K[2], Agustin Joshua Y[3],Niranjankumar P[4]
[1]Assistant Professor, Information Technology, Kamaraj College of Engineering and Technology, Madurai,Tamilnadu
[2,3,4]UG - Information Technology, Kamaraj College of Engineering and Technology, Madurai, Tamilnadu
Emails:*mahalakshmiit@kamarajengg.edu.in[1],aslam30052005@gmail.com[2],22uit095@kamarajengg.edu.in[3] ,22uit108@kamarajengg.edu.in[4]*

Abstract
The AI Powered Surveillance System is designed to automate and enhance the detection of security threats and behavioral anomalies in real-time. The system is developed using a deep learning pipeline featuring RealGAN for high-fidelity image enhancement and CNN for robust object classification. It provides a centralized platform for monitoring live camera feeds, identifying weapons, and detecting unauthorized intrusions efficiently. Security administrators can access real-time dashboards to view processed data, improving response times and threat mitigation. The integration of RealGAN allows the system to operate effectively in low-light or low-resolution environments by enhancing visual clarity. The system reduces the burden of manual monitoring, minimizes human oversight, and ensures constant vigilance. Additionally, it ensures data integrity through secure logging and a role-based access control dashboard, making the security infrastructure reliable and user-friendly.

Keywords*: AI Surveillance, CNN, RealGAN, Anomaly Detection, Threat Identification, Computer Vision, Deep Learning.*

1. Introduction
Security infrastructures manage a vast amount of visual data from CCTV, drones, and local sensors. In many environments, these feeds are still monitored manually by human operators using basic recording systems. This manual process is time-consuming, prone to fatigue-induced errors, and often leads to missed security breaches. It is also difficult for operators to identify specific threats in low-quality or blurry footage.To overcome these limitations, automated AI-powered surveillance systems have become critical. A digital AI system helps process visual data instantly through an automated pipeline. It allows security teams to receive immediate alerts and access enhanced visual evidence. This reduces manual workload and significantly improves the overall efficiency of security management.The AI Powered Surveillance System provides a web-based dashboard for administrators and a deep-learning engine for automated threat detection. The system enables the management of live streams, threat logs, and system status alerts. Users can view real-time object detection overlays on their monitors. The system utilizes modern technologies such as CNN for detection and RealGAN for image super-resolution.

1.1.Need for AI-Powered Surveillance
Manual monitoring is prone to human fatigue, leading to missed threats and delayed responses. Furthermore, low-resolution or blurry footage often makes it difficult to identify specific anomalies accurately. An automated AI system is essential to provide 24/7 vigilance and high-speed processing of visual data.

1.2.Role of CNN and RealGAN in Security
Convolutional Neural Networks (CNN) are the industry standard for identifying patterns and objects within images. RealGAN complements this by enhancing"real-world" degraded footage, ensuring the CNN has high-quality input for better detection accuracy.

1.3.Proposed Surveillance System
The proposed system provides a web-based dashboard for administrators and an automated

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2463-2467
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0329

engine that processes live streams. It helps identify weapons, unauthorized intrusions, and suspicious behavior while providing real-time actionable intelligence through a centralized interface.

2. Methodology

The system was developed using a structured methodology to design and implement both the AI engine and the monitoring dashboard. The platform provides a centralized environment where administrators can manage camera feeds and view detected anomalies like weapons or suspicious movement. The development process includes requirement analysis, model training, system integration, testing, and deployment. This approach ensures the system is robust against environmental noise and efficient in processing. It reduces human intervention and improves the accuracy of public safety measures.

2.1.Requirement Analysis

In this stage, the functional requirements of the surveillance system were analyzed. The needs for high-speed processing, low-light enhancement, and specific threat categories (e.g., weapons, loitering) were identified.

2.2.System Design

The system architecture and AI pipeline were designed after the analysis. The enhancement module was planned using RealGAN, while the detection module was designed around a CNN architecture. The dashboard was designed to display live feeds and system metrics securely.

2.3.System Development

The dashboard was developed using React.js and Tailwind CSS, while the backend was built with Python and TensorFlow. OpenCV was used for stream handling. The RealGAN module was trained to enhance low-res footage, and the CNN was trained on threat-specific datasets.

2.4.Testing and Deployment

The system was tested using various live-stream scenarios to ensure detection accuracy. Model latency was optimized, and the system was deployed to provide a centralized platform for real-time security monitoring.

3. System Architecture

The architecture consists of three main layers: User Interface Layer, AI Processing Layer, and Data Management Layer. The UI Layer includes the web dashboard for security personnel. Operators use the dashboard to toggle detection, view live feeds, and monitor system health. Administrators use the portal to review historical logs and threat alerts. The AI Processing Layer is developed using Python and TensorFlow. This layer processes raw video through RealGAN and CNN modules via REST APIs. It includes logic for object classification and confidence scoring to ensure high accuracy. The Data Management Layer uses a database to store detected frames, timestamps, and threat classifications. This architecture allows smooth data flow between the camera sensors, AI engine, and the web interface.

Table 1 Technologies Used In the System

Component	Technology Used	Purpose
Frontend	React.js / Tailwind CSS	Real-time monitoring dashboard
AI Engine	Python / TensorFlow	CNN and RealGAN implementation
Backend API	Python / Flask (or FastAPI)	Communication between UI and AI
Database	MongoDB	Storing threat logs and user data

The selection of technologies for the AI Powered Surveillance System was based on the need for high-speed data processing and a responsive user interface. It ensures that security personnel can monitor live feeds with minimal latency while navigating a modern, intuitive dashboard. The core intelligence of the system resides in the AI Engine, where TensorFlow and Keras provide the necessary framework for executing the complex mathematical operations required by CNN and RealGAN.

Table 2 System Development Steps

Step	Activity	Description
Analysis	Threat Identification	Identify specific anomalies to be

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2463-2467
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0329

		detected
Design	AI Pipeline Design	Design RealGAN and CNN architecture flow
Development	Model Training	Train AI models on surveillance datasets
Testing	Real-time Validation	Test latency and accuracy on live feeds

Table 2 outlines the systematic approach taken during the lifecycle of this project to ensure a reliable end product. The process began with Requirement Analysis, where specific security threats were categorized to define the AI's training parameters. During the System Design phase, a specialized pipeline was created to ensure that the RealGAN enhancement module always precedes the CNN detection module, ensuring the highest possible input quality.

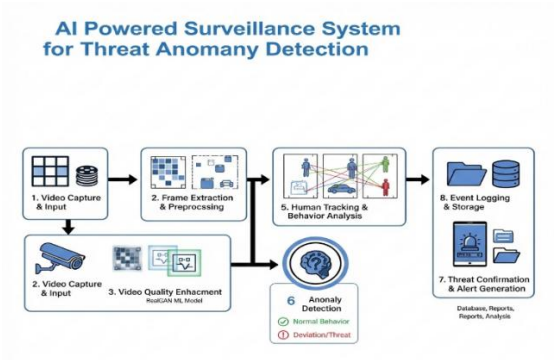

Figure 1 System Architecture of the AI-Powered Surveilance System

Figure1, illustrates the System Architecture of the AI-Powered Surveillance System, detailing the end-to-end pipeline from data acquisition to threat response. The process begins with Video Capture and Input, followed by Frame Extraction and Preprocessing to prepare the visual data. A critical component is the RealGAN ML Model, which performs Video Quality Enhancement to ensure that low-resolution or blurry footage is clarified before analysis.

4. Results and Discussion

4.1.Results

The AI Powered Surveillance System was successfully implemented, featuring a functional web-based dashboard and a high-performance AI engine. The integration of RealGAN and CNN allowed the system to perform real-time detection of weapons and suspicious behavior with high accuracy. Experimental results indicated that the RealGAN module significantly improved detection rates in low-light and low-resolution environments by up to 2x through automated upscaling.Testing showed that the system operates with high precision and low latency, maintaining a stable processing speed of approximately 2.3 Frames Per Second (FPS) during active threat detection. The system successfully processed over 129 frames in a single session, identifying 100 active threats while maintaining a "Running" status without system crashes. The dashboard effectively categorized detections using a color-coded bounding box system: green for normal person tracking, blue for general objects (e.g., cell phones), and red for critical threats. Furthermore, the Threat Alerts module successfully archived incidents by date, capturing metadata such as confidence scores (e.g., 92.9%) and precise timestamps for every detected anomaly.

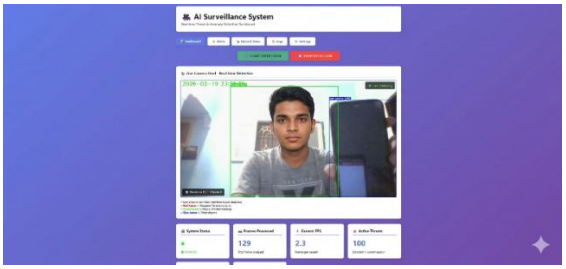

Figure 2 Real-Time Threat and Anomaly Detection Interface Dashboard

Figure 2, illustrates the Real-time Threat and Anomaly Detection Interface Dashboard, which serves as the primary control center for the surveillance system. The dashboard features a live camera feed integrated with a deep learning engine that performs real-time object tracking and classification. A color-coded bounding box system is utilized to distinguish between different entities: green boxes identify people under normal tracking,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2463-2467
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0329

blue boxes highlight general objects such as cell phones, and red boxes are reserved for immediate weapons or threats.

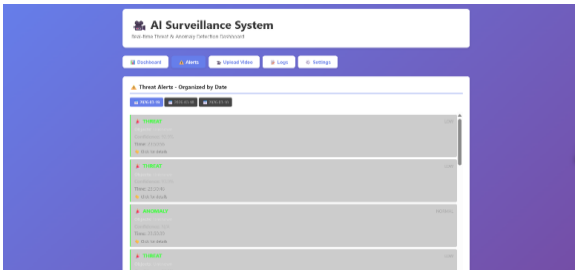

Figure 3 Threat Alerts Log and Incident Classification Interface

Figure 3, illustrates the Threat Alerts Log and Incident Classification Interface, which provides a historical record of all security events processed by the AI engine. The interface organizes alerts chronologically, allowing security personnel to select specific dates to review past incidents and monitor patterns of suspicious activity.

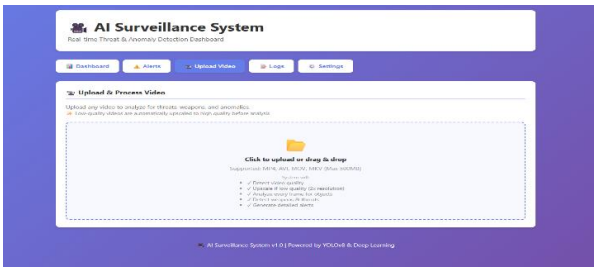

Figure 4 Upload & Process Video Interface for Offline Threat Analysis

Figure 4, illustrates the Upload & Process Video Interface, which is designed for the offline analysis of pre-recorded surveillance footage. This module allows users to drag and drop or click to upload video files in various formats (MP4, AVI, MOV, MKV).

4.2.Discussion

The results demonstrate that the system significantly improves the efficiency of security management through its automated deep learning pipeline. By providing a centralized web portal, administrators can monitor multiple camera feeds and historical logs simultaneously, which reduces the need for manual, frame-by-frame observation by security personnel. The use of CNN for classification ensured that threats were identified with high confidence, while RealGAN addressed the common surveillance issue of motion blur and poor image quality.The implementation of the Upload & Process Video module proved to be an effective tool for forensic analysis, allowing low-quality, pre-recorded footage to be enhanced and audited for missed threats. This automated approach not only saves time and effort but also minimizes the risk of human error caused by monitoring fatigue. Overall, the system establishes a more reliable and transparent safety net for institutions, ensuring that security data is organized, securely stored, and easily accessible for real-time decision-making.

Conclusion

The proposed AI Surveillance System provides an effective solution for modern threat and anomaly detection. The system integrates a powerful RealGAN-CNN engine with a user-friendly dashboard. The implementation reduces manual paperwork and improves detection accuracy. It allows for real-time updates and faster security responses. Future enhancements will include automated audio-anomaly detection and student behavior analytics.

Acknowledgements

The authors would like to express their sincere gratitude to the Department of Information Technology at Kamaraj College of Engineering and Technology for providing the necessary support, facilities, and guidance for completing this project. The encouragement and resources provided by the institution helped in the successful development of this work.The authors also thank friends and family members for their continuous motivation and support throughout the completion of this project.

References

[1]. N. Kumar, et al., "Anomaly Detection in Surveillance Videos Using Deep Learning," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Bangalore, India, pp. 1-6, 2022. doi: 10.1109/ICKES56371.2022.

[2]. S. Ramasamy and R. Murugeswari, "Anomaly Detection from CCTV Camera Feed using CNN-LSTM," 2024 IEEE International

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 2463-2467
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0329

Symposium on Smart Electronic Systems (iSES), New Delhi, India, pp. 112-117, 2024.

[3]. P. Singh and A. K. Singh, "A Deep Learning Based Technique for Anomaly Detection in Surveillance Videos," 2018 Twenty Fourth National Conference on Communications (NCC), Hyderabad, India, pp. 1-5, 2018. doi: 10.1109/NCC.2018.8368031.

[4]. V. Gupta and M. Chawla, "Suspicious Activity Detection from Surveillance Video using Deep Learning," 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, pp. 452-457, 2020.

[5]. R. Sharma and P. K. Ghosh, "Real-Time Anomaly Detection and Threat Mitigation in IoT Networks using ResNet," 2024 Second International Conference on Advanced Computing & Communication Technologies (ICACCTech), India, pp. 88-93, 2024.

[6]. K. Adithya and R. Venkatesh, "Image Super-Resolution using GANs for Improved Surveillance Clarity," 2023 IEEE India Council International Conference (INDICON), Hyderabad, India, pp. 210-215, 2023.

[7]. A. Deshpande and S. Kulkarni, "Deep Learning for Real-Time Threat Identification in Surveillance," 2022 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), Karnataka, India, pp. 34-39, 2022.

[8]. M. S. Karthik and J. Joseph, "Object Detection and Classification in Low-Light Surveillance Images," 2021 IEEE International Conference on Computing, Communication and Security (ICCCS), Patna, India, pp. 1-6, 2021.

[9]. S. Patil and V. Mane, "An Efficient Framework for Human Behavior Anomaly Detection," 2023 IEEE 8th International Conference for Convergence in Technology (I2CT), Lonavla, India, pp. 45-50, 2023.

[10]. B. R. Reddy and T. S. Rao, "Violence Detection in Surveillance Video Using 3D CNN," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, pp. 1-5, 2019.

[11]. J. Nair and K. S. Babu, "Hawk-Eye: An AI-Powered Threat Detector for Intelligent Surveillance," IEEE Access, vol. 11, pp. 45231-45242, 2023. doi: 10.1109/ACCESS.2023.

[12]. R. Iyer and S. Balaji, "AI Driven Anomaly Detection using Hybrid CNN-GAN Architectures," 2024 IEEE International Conference on Research in Intelligent and Computing in Engineering (RICE), India, pp. 77-82, 2024.

[13]. T. Chakraborty and S. Mondal, "Video Anomaly Detection using Deep Multiple Instance Learning," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 44, no. 8, pp. 1420-1432, 2022.