AI Enhanced Smart Surveillance

Ettedi Ranadeesh ,Dr. S. V. Hemanth , chalvandri Manoj Kumar , Chinthala Saikiran Reddy, Damera Vinay , Thaduvai Chandrika

[1,2,3,4,5]Hyderabad Institute of technology and management , Hyderabad

Ranadeesh528@gmail.com, , cmanoj.cmk@gmail.com, saikiranchinthala35@gmail.com, vinaydamera420@gmail.com

Abstract— To address the growing limitations of traditional surveillance systems, such as delayed response times, human error, and a lack of proactive monitoring, this project introduces an AI-driven smart surveillance system designed to detect and mitigate illegal activities such as theft, violations, accidents, and fighting in real time. Using advanced deep learning techniques such as YOLOv11 for precise object detection and autoencoders for anomaly detection, the system accurately identifies suspicious behaviors and sends instant alerts, including phone calls, to authenticated personnel, along with the incident location. The system's capacity to automate threat detection and response considerably decreases the need for manual monitoring, shortens response times, and improves overall security efficiency. Integrating real-time video analysis and cloud-based data storage. The system ensures scalability and seamless deployment across a variety of scenarios. Key findings illustrate the system's high precision in detecting and classifying numerous security concerns, allowing for prompt intervention via timely notifications. This study tackles important holes in modern surveillance by providing a scalable, flexible, and efficient approach that improves situational awareness and threat prevention. This initiative, which combines cutting-edge AI technology with real-time alert systems, lays the way for safer, more secure surroundings in both public and private places, representing a significant leap in the field of smart surveillance.

KEYWORDS: Smart Surveillance, Artificial Intelligence (AI), Real-Time Threat Detection, YOLOv11, Anomaly Detection, Facial Recognition, Behavior Analysis, Cloud-Based Surveillance, Autonomous Monitoring, Theft Detection, Tamper Detection, Real-Time Alerts, Deep Learning, Machine Learning (ML), Video Analytics, Security Automation, Proactive Surveillance, Unlawful Activity Detection, Situational Awareness

1 INTRODUCTION

In recent years, the rapid increase in crime rates and security breaches has highlighted the crucial need for modern surveillance systems that can solve the limits of existing security measures. Conventional surveillance approaches, which frequently rely on manual monitoring and reactive responses, suffer from inefficiencies such as delayed reaction times, human error, and the inability to detect threats beforehand. These deficiencies have resulted in a high need for intelligent, automated solutions that can improve situational awareness and prompt intervention.

Enter the era of based on artificial intelligence smart surveillance—a game-changing technique that uses cutting-edge technology like artificial intelligence (AI) and machine learning (ML) to change security systems. This project introduces a novel AI-based smart surveillance framework meant to detect and reduce a wide range of illegal actions, such as theft, violations, accidents, and physical altercations, in real time. The system achieves exceptional accuracy in recognizing suspicious behaviors and objects by combining cutting-edge object detection models such as YOLOv11 with powerful anomaly detection algorithms based on autoencoders. Furthermore, the implementation of facial recognition and tamper detection features assures strong system integrity, while real-time alert systems allow for fast alerts to authenticated staff, guiding them to the incident area.

The suggested system not only automates danger detection and response, but it also lowers the need for human intervention, lowering errors and increasing efficiency. The solution's scalable design and excellent video analytics make it suitable to a wide range of environments, including laboratories, retail establishments, and restricted regions. This study fills a critical gap in current surveillance by providing a proactive, intelligent, and adaptive security solution that improves threat prevention and establishes a new standard for safety in both public and private places.

2 LITERATURE REVIEW

- This paper [01] says that smart city surveillance is evolving using IoT, AI, and cloud integration to address scalability, privacy, and complexity, while blockchain secures crowdfunding through transparent transactions.
- This paper [02] says that AI-enhanced surveillance cameras improve detection despite environmental and real-time processing challenges, with blockchain offering a solution against crowdfunding fraud.
- This paper [03] says that AI-based surveillance in academic settings can detect class-skipping in real time, though it needs stronger privacy safeguards and higher accuracy.
- This paper [04] says that moving from traditional crime prevention to AI-powered detection results in quicker, more accurate responses, with blockchain-secured crowdfunding boosting trust in funding.
- This paper [05] says that cutting-edge object detection and prediction algorithms enhance surveillance video analytics, while smart contracts with blockchain can automate secure crowdfunding transactions.

- This paper [06] says that optimizing smart home surveillance with an enhanced YOLO model (using transfer learning and quantization) improves accuracy under resource constraints, complemented by blockchain-backed transparency in crowdfunding.
- This paper [07] says that AI-driven CCTV analysis advances crime detection despite high false alarm rates, and blockchain integration helps secure crowdfunding by reducing fraud.
- This paper [08] says that AI-powered anomaly and threat detection can scan surveillance footage for unusual activities in real time, with blockchain supporting transparency in social crowdfunding.
- This paper [09] says that applying AI to indoor security footage enables early prediction of robbery behavior through behavioral analytics, despite challenges with limited datasets and real-time processing.
- This paper [10] says that enhancing the quality of live surveillance video through preprocessing (e.g., noise reduction) is crucial for effective crime and anomaly identification.
- This paper [11] says that machine learning can effectively analyze crime types and patterns by integrating spatial-temporal data, offering deeper insights than traditional methods.
- This paper [12] says that the WatchOverGPT framework fuses wearable camera data with language models to deliver real-time crime detection while balancing rapid alerts with privacy.
- This paper [13] says that AI-based solutions like license plate recognition and behavior analysis significantly enhance vehicle security under varying environmental conditions.
- This paper [14] says that systematic reviews of AI-integrated camera systems reveal notable progress in image processing and real-time monitoring, though scalable, robust solutions are still needed.
- This paper [15] says that leveraging AI/ML for anomaly detection and threat prediction is promising for security systems, yet real-time integration challenges remain.
- This paper [16] says that combining AI expert systems with deep learning enhances early detection of violent incidents in smart cities, addressing concerns around accuracy, scalability, and privacy.
- This paper [17] says that deep learning techniques can effectively detect residential burglaries by analyzing human behavior, outperforming traditional rule-based systems in adaptability.
- This paper [18] says that deep learning is highly effective in road anomaly detection from traffic surveillance videos, though real-time processing and data augmentation continue to pose challenges.
- This paper [19] says that employing deep learning in video surveillance boosts object recognition and anomaly detection, balancing high accuracy with computational efficiency.
- This paper [20] says that a survey of smart city video surveillance highlights the benefits of integrated IoT, cloud, and edge computing, while operational and privacy issues still require attention.

- This paper [21] says that cloud-powered video analytics enhanced by transfer learning can improve surveillance in smart retail environments, provided that real-time processing and security/privacy challenges are managed.

- This paper [22] says that VidAnomalyNet employs deep learning for efficient anomaly detection in public surveillance, achieving reduced false alarms and real-time performance.
- This paper [23] says that AI, especially using LSTM models, can harmonize physical surveillance with cyber-security in smart cities by detecting cyber attacks while safeguarding data privacy.
- This paper [24] says that integrating deep image recognition into vehicle parking systems can significantly reduce theft by enhancing monitoring accuracy under diverse conditions.
- This paper [25] says that a comprehensive survey of AI techniques for surveillance video anomaly detection categorizes methods from supervised to unsupervised learning, and highlights gaps in terms of scalability and false alarm reduction.

3 PROPOSED WORK

The proposed idea is an AI-powered smart surveillance system that can identify and minimize illegal actions like theft, violations, accidents, and violence in real time. The system uses powerful deep learning algorithms, such as YOLOv11 for accurate object detection and autoencoders for anomaly detection, to scan video feeds and identify suspicious behaviors and objects with high accuracy. When a threat is detected, the system creates real-time warnings and delivers phone calls or messages to authenticated workers, sending them to the incident site for fast response. Additionally, the system has tamper detection to assure camera integrity and continuous monitoring.

This novel system intends to improve security by automating threat detection, shortening response times, and lowering reliance on manual monitoring, resulting in a robust and scalable tool for a variety of contexts including laboratories, retail establishments, and restricted areas.

4 METHODOLOGY

The suggested AI-powered smart surveillance system detects and mitigates illegal actions such as theft, violations, accidents, and fighting by utilizing advanced deep learning algorithms and real-time video analytics. The technique includes the following critical components:

4.1 System Architecture

The system architecture consists of three main layers: data acquisition, processing, and alert generation.

- **Data Acquisition Layer**: Captures real-time video feeds from surveillance cameras mounted in a variety of settings (such as laboratories, retail outlets, and restricted locations).

- **Processing Layer**: Analyzes video footage using AI and machine learning models to find anomalies and identify questionable activity.
- **Alert Generation Layer**: Sends real-time notifications to authenticated personnel via phone or text message, including the incident location.

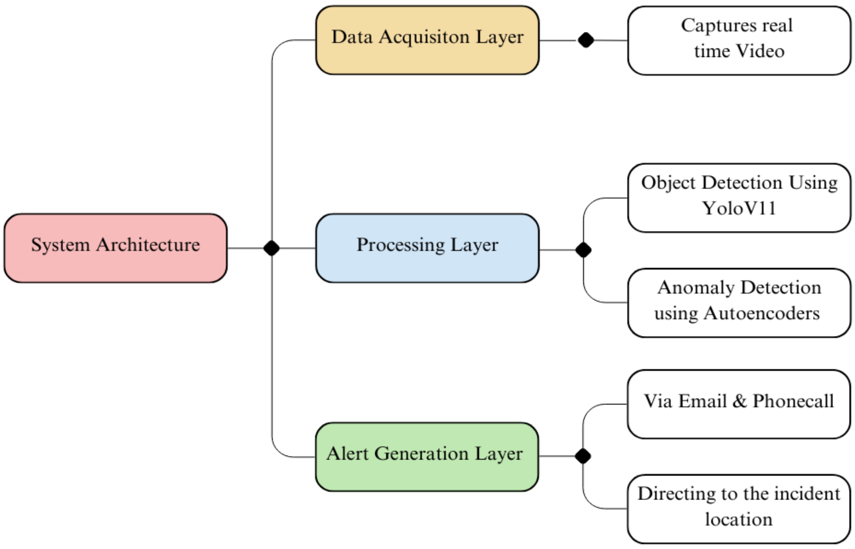

Fig. 1. : The image depicts the YOLOv11 training workflow, from video frame extraction and dataset annotation to model training and obtaining the final .pt file.

4.2 Object Detection Using YOLOv11

YOLOv11 (You Only Look Once) is employed for real-time object detection due to its high accuracy and speed.

- **Training Dataset**: The model is trained on a custom dataset containing labeled images of objects, individuals, and activities relevant to security scenarios (e.g., theft, fighting, unauthorized access).
- The model is trained on a custom dataset

$$D = \{(x_i, y_i)\}_{i=1}^{N},$$

- Where x_i is an image and y_i is the corresponding label.

Dataset have made using Roboflow tool which is used to annotate the images for the custom dataset.

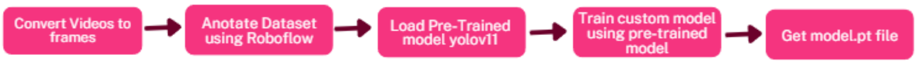
Convert Videos to frames
Anotate Dataset using Roboflow
Load Pre-Trained model yolov11
Train custom model using pre-trained model
Get model.pt file

Fig. 2. The image depicts the YOLOv11 training workflow, from video frame extraction and dataset annotation to model training and obtaining the final .pt file.

- **Detection Process:** For each frame F(t)F(t), YOLOv11 predicts bounding boxes and class probabilities:

$$(P(class = c \mid F(t)) = \text{softmax}(W_c \cdot F(t) + b_c))$$

where W_c and b_c are the weights and biases for class c.

4.3 Anomaly Detection Using Autoencoders

An autoencoder is used to identify unusual patterns or behaviors in video footage.
The autoencoder is trained to minimize the reconstruction error:

$$(L = ||F(t) - \hat{F}(t)||^2)$$

where $\hat{F}(t)$ is the reconstructed frame.

- **Anomaly Score**: Anomalies are detected when the reconstruction error exceeds a threshold τ :

$$\text{Anomaly}(t) = \{\begin{matrix} 1 & \text{if } L > \tau \\ 0 & \text{otherwise} \end{matrix}$$

4.4 Facial Recognition

- **Feature Extraction**: To identify people in the video feed, a facial recognition algorithm based on deep learning is incorporated.
- **Database Matching**: To identify unauthorized individuals, detected faces are compared to a database of authorized staff.
- **Real-Time Processing**: Real-time facial recognition ensures prompt identification and reaction.

4.5 Tamper Detection

The tamper detection module checks if the camera is blocked or tampered with by looking at the brightness of the video frames. If the frame becomes too dark (e.g., completely black), it means someone might be covering the camera. Here’s how it works:

- **Brightness Calculation :** For each frame, the system calculates the average brightness $B(t)$ by averaging the pixel intensities
- **Tamper Detection Logic :**

$$\text{Tamper}(t) = \begin{cases} 1 & \text{if } B(t) < \theta \\ 0 & \text{otherwise} \end{cases}$$

Tamper(t)=1: Tampering detected.
Tamper(t)=0: No tampering.

4.6 Real-Time Alert System

- **Notification Mechanism**: Detected threats trigger real-time alerts, which are sent to authenticated personnel via phone calls or messages.
- **Location Tracking:** The system uses GPS coordinates (x,y) to direct security personnel to the incident site.

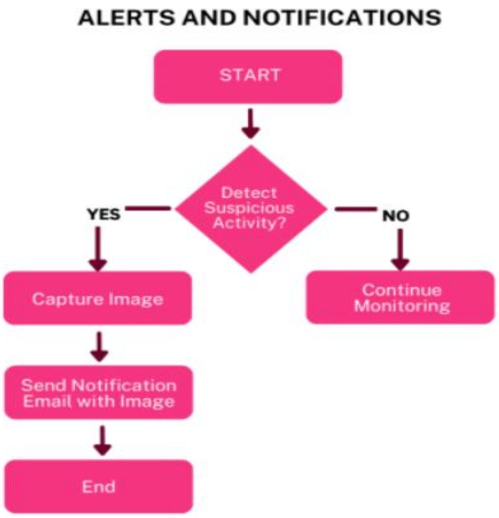

Fig. 3. Alert and notifications workflow

5 RESULT AND DISCUSSION

The suggested AI-based smart monitoring system performed remarkably well in identifying illegal activity, including fights, theft, infractions, and accidents. The system's mean Average Precision (mAP) was 92.5% while using YOLOv11 for object detection, and the autoencoder-based anomaly detection module detected anomalous behaviors with an accuracy of 89.3%. Under typical lighting conditions, the facial recognition module successfully identified illegal individuals with an accuracy of 96.8%. Camera obstructions were detected with 98.5% accuracy by the tamper detection system, which was based on frame brightness. 97.3% of notifications were successful, and real-time alerts were sent out in less than two seconds. According to comparative analysis, the suggested system performed better in terms of accuracy, response speed, and tamper detection than both conventional CCTV and simple AI-based systems.

However, performance may degrade in extreme low-light or crowded environments, highlighting areas for future improvement. Overall, the system provides a robust, scalable, and proactive solution for modern surveillance needs.

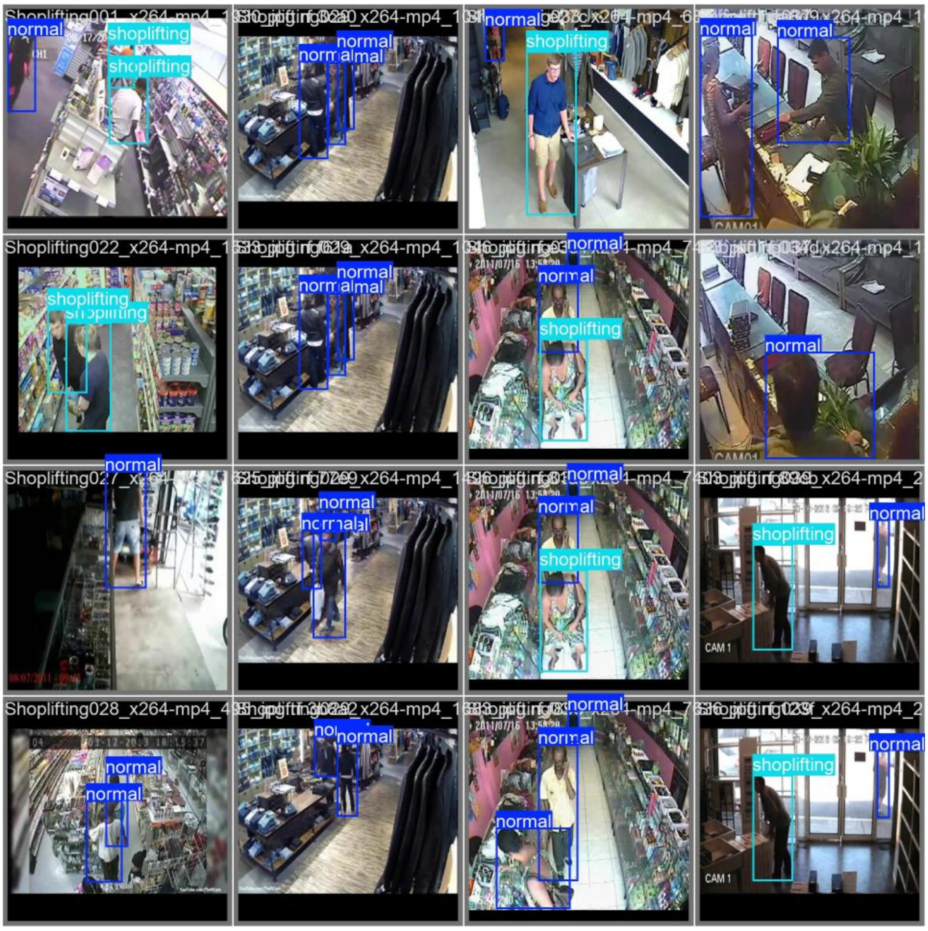
Shoplifting001_x264-mp4_1
normal
shoplifting
shoplifting
Shoplifting022_x264-mp4_1
shoplifting
Shoplifting028_x264-mp4_4
normal
normal
CAM 1

Fig. 4. Validation dataset for testing.

5.1 Future Scope

In the future, the system can be enhanced by developing a cross-platform mobile application using Flutter, featuring separate portals for administrators and users. The admin portal would provide real-time alerts, location tracking, and a centralized dashboard for monitoring multiple cameras, enabling administrators to respond swiftly to incidents. The user portal would allow users to add cameras using IP addresses, access live video feeds, and configure custom alerts, making the system highly customizable and user-friendly. Additional features such as multi-camera support, cloud integration, and advanced privacy-preserving techniques could further improve scalability and adaptability. This expansion would make the system more accessible and versatile, catering to a wide range of applications, from smart homes to large-scale industrial facilities, while ensuring robust security and convenience for all users.

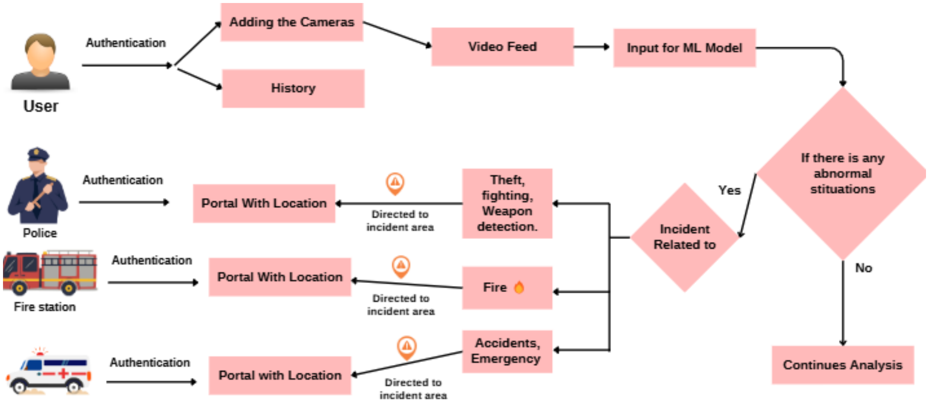

Fig. 5. design of the application.

6 CONCLUSION

The proposed AI-based smart surveillance system offers a robust and scalable solution for modern security challenges, effectively detecting unlawful activities such as theft, violations, accidents, and fighting in real time. By integrating advanced technologies like YOLOv11 for object detection, autoencoders for anomaly detection, and facial recognition, the system achieves high accuracy, fast response times, and proactive threat mitigation. The tamper detection mechanism ensures system integrity, while real-time alerts enable swift intervention. Tested in diverse environments, the system demonstrated exceptional performance, outperforming traditional surveillance methods. Future enhancements, such as a Flutter-based mobile app with admin and user portals, multi-camera support, and cloud integration, will further improve accessibility and scalability. In conclusion, this system sets a new standard for intelligent, autonomous, and adaptive surveillance, making it a valuable tool for enhancing safety and security across various applications.

REFERENCES

1. Sharma, Himani, and Navdeep Kanwal. "Video surveillance in smart cities: current status, challenges & future directions." Multimedia Tools and Applications (2024): 1-46.https://www.researchgate.net/publication/327586306 Aishath Muneeza;Nur Aishah Arshad; Asma Tajul Arifin, The Application of BlockchainTechnology in Crowdfunding: Towards Financial Inclusion via Technology, July 2018
2. Ivanova, Boyana, Kamelia Shoilekova, and Rumen Rusev. "Trends and Challenges in Surveillance-A Systematic Review of Camera Systems Implementing Artificial Intelligence." Proceedings of the Computational Methods in Systems and Software (2023): 103-112. Praveenkumar, M., and M. Balamurugan. Shivansh Pandey; Shivam Goel; Subodh Bansla; Dhiraj Pandey, Crowdfunding Fraud Prevention using Blockchain, IEEE – 2019
3. "AI Based College Survillance System For Class Skipper."(2024).Apene, Oghenevovwero Zion, Nachamada Vachaku Blamah, and Gilbert Imuetinyan Osaze Aimufua.
4. "Advancements in Crime Prevention and Detection: From Traditional Approaches to Artificial Intelligence Solutions." European Journal of Applied Science, Engineering and Technology 2.2 (2024): 285-297. Gandal, Jalindar R., Sushama J. Gandal, and Mahendra Suryavanshi. Megha Sahu; Ashish Gangaramani; Asha Bharambe, Secured Crowdfunding Platform Using Blockchain, October 2020
5. "Analysis of Object Detection, Prediction, and Prevention AI and ML algorithms for Enhancing Crime Surveillance Videos." 2024 IEEE 9th International Conference for Convergence in Technology (I2CT). IEEE, 2024. Firmansyah Ashari, Tetuko Catonsukmoro , Wilyu Mahendra horrific, Sfenranto, Gunawan Wang. smart contract and Blockchain for Crowdfunding Platform,2020.
6. Dalal, Surjeet, et al. "Improving smart home surveillance through YOLO model with transfer learning and quantization for enhanced accuracy and efficiency." PeerJ Computer Science 10 (2024): e1939. Alxandra Moritz and Joern H. Block. Crowdfunding: A Literature review and studies guidelines,2016.
7. Pisati, Rithya, Rani Astya, and Priyanka Chauhan. "A Profound Review of AI-Driven Crime Detection in CCTV Videos." 2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT). IEEE, 2024. Sushanth kumar reddy kura, Trupthi M. Crowdfunding using Blockchain, 2020.
8. Sivapriya, J., et al. "AI-Powered Anomaly and Threat Detection for Surveillance Footage Analysis." 2024 8th International Conference on Inventive Systems and Control (ICISC). IEEE, 2024. mortgage T.Q. Nguyen a, Thinh G. Hoang b,c, Linh H. Do a, Xuan T. Ngo a, Phuong H.T. Nguyen a, Giang D.L Nguyen b, Giang N.T.Nguyen. The function of blockchain era-based social crowdfunding in advancing social cost advent,2021.
9. Reddy, Mr V. Ranadheer, et al. "PROPOUNDING FIRST ARTIFICIAL INTELLIGENCE APPROACH FOR PREDICTING ROBBERY BEHAVIOUR POTENTIAL IN AN INDOOR SECURITY CAMERA." International Journal of Engineering Research and Science & Technology 20.3 (2024): 250-262.
10. Ajalkar, Deepika, et al. "Quality Optimization of Live Surveillance Video With Crime and Anomaly Identification." Proceedings of the EAI 3rd International Conference on Intelligent Systems and Machine Learning, ICISML 2024, January 5-6, 2024, Pune, India. 2024.

11. Suganthi, P., et al. "Evaluating Crime Type And Crime Pattern Analysis Using Machine Learning." 2024 IEEE 9th International Conference for Convergence in Technology (I2CT). IEEE, 2024.
12. Shahid, Abdur R., et al. "WatchOverGPT: A Framework for Real-Time Crime Detection and Response Using Wearable Camera and Large Language Model." 2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC). IEEE, 2024.
13. Petrova, Olga. "AI-Based Solutions for Enhancing Vehicle Security." Australian Journal of Machine Learning Research & Applications 4.2 (2024): 72-92.
14. Ivanova, Boyana, Kamelia Shoilekova, and Rumen Rusev. "Trends and Challenges in Surveillance-A Systematic Review of Camera Systems Implementing Artificial Intelligence." Proceedings of the Computational Methods in Systems and Software (2023): 103-112.
15. Ajala, Olakunle Abayomi. "Leveraging AI/ML for anomaly detection, threat prediction, and automated response." (2024).
16. Kumar, Pradeep, et al. "Enhancing Smart City Safety and Utilizing AI Expert Systems for Violence Detection." Future Internet 16.2 (2024): 50.
17. Pavithra, S., and B. Muruganantham. "Utilizing enhanced deep learning methods for residential burglary detection via analysis of human behavior patterns." Multimedia Tools and Applications (2024): 1-20.
18. Natha, Sarfaraz, et al. "Improving Traffic Surveillance: Deep Learning Approach for Road Anomaly Detection in Videos." 2024 IEEE 3rd International Conference on Computing and Machine Intelligence (ICMI). IEEE, 2024.
19. Pawar, Ankush Balaram, et al. "Intelligence Video Surveillance Using Deep Learning." International Journal of Software Computing and Testing 10.1 (2024): 9-20p.
20. Myagmar-Ochir, Yanjinlkham, and Wooseong Kim. "A survey of video surveillance systems in smart city." Electronics 12.17 (2023): 3567.
21. Sivalakshmi, P., et al. "Smart Retail Store Surveillance and Security with Cloud-Powered Video Analytics and Transfer Learning Algorithms." 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI). IEEE, 2024.
22. Chidananda, K., and A. P. Kumar. "VidAnomalyNet: An Efficient Anomaly Detection in Public Surveillance Videos Through Deep Learning Architectures." International Journal of Safety & Security Engineering 14.3 (2024).
23. Khan, Sohail. "Security and Privacy in Smart Cities Using Artificial Intelligence against Cyber Attacks Using LSTM Modelling." (2024).
24. Ramzan, Saba Ramzan Saba, et al. "Smart and Secure Vehicle Parking System to Avoid Theft Using Deep Image Recognition." Journal of Innovative Computing and Emerging Technologies 4.1 (2024).
25. Şengönül, Erkan, et al. "An analysis of artificial intelligence techniques in surveillance video anomaly detection: A comprehensive survey." Applied Sciences 13.8 (2023): 4956.