International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

SMART SURVEILLANCE:AI-POWERED INCIDENT DETECTION

[1] Dr.R.Siva Subramanian,[2] Velpula Manoj,[3] Vadla Vyshnavi,[4] Sudhagani Nikitha, [5] Tadivaka Venkatamba

[1] Associate Professor, Department of Computer Science & Engineering (Artificial Intelligence & Machine Learning), Malla Reddy University, Kompally, Hyderabad.
[1] Email : sivar2000@gmail.com
[2,3,4,5] Students, Department of Computer Science & Engineering (Artificial Intelligence & Machine Learning),

Malla Reddy University, Kompally, Hyderabad. [2] velpulamanoj52262@gmail.com,[3]

vyshnavivadla2022@gmail.com, [4] nikithasudhagani12@gmail.com,[5] venkatambasrinivas@gmail.com

Abstract:

Smart surveillance systems powered by Artificial Intelligence (AI) are transforming traditional security monitoring by enabling automated and intelligent incident detection. Conventional surveillance systems rely heavily on human operators to continuously monitor video feeds, which can lead to delayed responses, fatigue-related errors, and missed incidents. AI-driven surveillance addresses these limitations by using advanced technologies such as computer vision, deep learning, and real-time data analytics to automatically detect suspicious activities and security threats.This system analyzes live video streams from surveillance cameras and identifies unusual patterns or predefined incidents such as unauthorized access, violence, accidents, abandoned objects, or intrusion into restricted areas. Machine learning models are trained on large datasets to recognize normal and abnormal behaviors, allowing the system to trigger alerts when anomalies occur. By integrating object detection, facial recognition, motion tracking, and behavior analysis, AI-powered surveillance significantly improves the accuracy and speed of incident detection.The proposed smart surveillance framework also supports real-time notifications and automated reporting, enabling security personnel to respond quickly to potential threats. Additionally, cloud integration and edge computing can enhance scalability and reduce processing delays, making the system suitable for large environments such as airports, public spaces, campuses, and smart cities.Overall, AI-powered incident detection enhances security, reduces human workload, and improves operational efficiency. As AI technologies continue to advance, smart surveillance systems will play a critical role in proactive threat detection and public safety management. This approach not only strengthens monitoring capabilities but also contributes to creating safer and smarter environments through intelligent automation and data-driven decision-making.

Keywords: Smart Surveillance, Artificial Intelligence, Incident Detection, Computer Vision, Deep

Learning, Real-Time Monitoring, Object Detection, Facial Recognition, Anomaly Detection, Security Systems

I.INTRODUCTION

In recent years, the demand for effective security and monitoring systems has increased significantly due to rapid urbanization, population growth, and rising safety concerns in public and private spaces. Traditional surveillance systems rely mainly on human operators to monitor multiple video feeds continuously. However, manual monitoring is often inefficient, time-consuming, and prone to human errors such as fatigue, distraction, and delayed response to critical incidents. As a result, many important events may go unnoticed or be detected too late.To overcome these limitations, Artificial Intelligence (AI) has been integrated into modern surveillance systems to create smart surveillance solutions capable of automatically detecting incidents. AI-powered surveillance uses advanced technologies such as computer vision, machine learning, and deep learning algorithms to analyze video streams in real time. These technologies enable the system to recognize patterns, detect unusual behavior, and identify potential threats without constant human supervision.Smart surveillance systems can detect a variety of incidents including unauthorized access, suspicious movements, abandoned objects, accidents, and violent activities. By automatically analyzing visual data from surveillance cameras, the system can quickly generate alerts and notify security personnel, allowing faster response and improved decision-making. This not only enhances the efficiency of monitoring systems but also reduces the workload on human operators.

Furthermore, with the integration of edge computing and cloud-based platforms, AI-powered surveillance systems can process large volumes of video data efficiently and provide scalable solutions for various environments such as airports, shopping malls, campuses, and smart cities. Therefore, smart surveillance with AI-powered incident detection is emerging as a powerful tool for improving security, safety, and situational awareness in modern society.

II.LITERATURE SURVEY

The field of smart surveillance has evolved rapidly with the advancement of Artificial Intelligence (AI), computer vision, and deep learning techniques. Earlier surveillance systems were primarily designed for video recording and manual observation. These systems depended heavily on human operators, making them less efficient in detecting incidents in real time. Researchers identified the limitations of traditional surveillance, such as delayed response, reduced accuracy, and high dependence on continuous human attention.With the growth of machine learning, intelligent surveillance systems began incorporating automated motion detection, background subtraction, and object tracking techniques. These methods improved the

ability of surveillance systems to identify moving objects and detect simple abnormal events. However, such conventional image processing techniques often struggled in complex environments with poor lighting, occlusion, or crowded scenes.Recent literature highlights the significant role of deep learning models, especially Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and You Only Look Once (YOLO) algorithms, in enhancing surveillance performance. CNN-based models are widely used for image classification and object detection, while YOLO and SSD frameworks enable fast and accurate real-time detection of people, vehicles, weapons, and suspicious objects. Similarly, Long Short-Term Memory (LSTM) networks and RNNs are applied for behavior analysis and activity recognition in video sequences.Many researchers have also focused on anomaly detection in surveillance videos. These systems learn normal behavioral patterns and identify deviations that may indicate incidents such as theft, intrusion, violence, or accidents. Facial recognition and person re-identification have further strengthened surveillance by allowing identification and tracking of individuals across multiple cameras.Overall, the literature shows that AI-powered surveillance systems are more accurate, responsive, and scalable than conventional methods. Current research continues to improve detection accuracy, reduce false alarms, and address challenges related to privacy, data security, and real-time processing.

III.EXISTING SYSTEM

The existing surveillance systems mainly rely on traditional Closed-Circuit Television (CCTV) cameras for monitoring activities in various environments such as public places, offices, shopping malls, and transportation hubs. These systems primarily function by continuously recording video footage and displaying it on monitoring screens. Security personnel are responsible for observing the video feeds and identifying any suspicious activities or incidents.However, traditional surveillance systems have several limitations. One of the major drawbacks is the heavy dependence on human operators to monitor multiple screens for long periods of time. Continuous monitoring can lead to fatigue, reduced attention, and human errors, which may result in missing important events or delayed detection of incidents. Additionally, manual surveillance requires a large workforce to monitor numerous cameras, making it costly and inefficient.Another limitation of existing systems is that they usually detect incidents only after they have occurred. Most CCTV systems are mainly used for reviewing recorded footage during investigations rather than preventing incidents in real time. These systems lack the capability to automatically analyze video content or detect unusual behavior.Furthermore, traditional surveillance systems do not have advanced analytical capabilities such as object recognition, facial recognition, or behavior analysis. As a

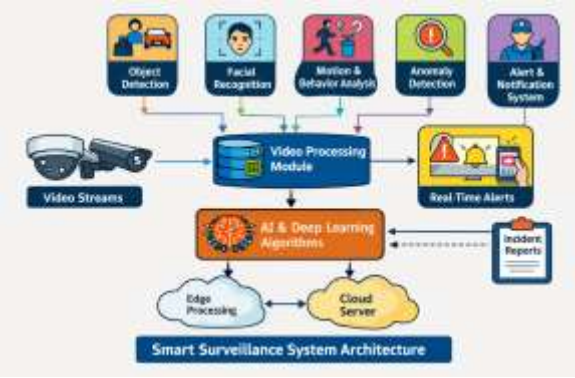
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
IJARST
ISSN: 2457-0362

result, identifying suspects, tracking movements, or detecting suspicious activities becomes a difficult and time-consuming task.Due to these limitations, existing surveillance systems are not fully effective in ensuring proactive security and real-time incident detection. This has led to the need for intelligent surveillance solutions that can automatically analyze video data and detect incidents using advanced technologies like Artificial Intelligence and computer vision.

IV.PROPOSED SYSTEM

The proposed system introduces a **Smart Surveillance system powered by Artificial Intelligence (AI)** to automatically detect incidents and improve security monitoring. Unlike traditional surveillance systems that rely heavily on manual observation, the proposed system uses advanced technologies such as **computer vision, deep learning, and real-time video analysis** to identify suspicious activities and potential threats automatically.In this system, surveillance cameras continuously capture video footage from different locations. The captured video streams are processed using AI-based algorithms that analyze each frame in real time. Deep learning models such as **Convolutional Neural Networks (CNN)** and object detection algorithms are used to identify objects, human activities, and abnormal behaviors. The system is trained using large datasets to recognize patterns of normal activities and detect anomalies or unusual events.When the system detects incidents such as **unauthorized entry, suspicious movement, abandoned objects, accidents, or violent behavior**, it immediately generates alerts and notifications. These alerts can be sent to security personnel through a monitoring dashboard, mobile devices, or alarm systems. This enables faster response and helps prevent potential threats.The proposed system can also integrate additional features such as **facial recognition, motion detection, object tracking, and behavior analysis** to enhance monitoring capabilities. Cloud computing or edge processing can be used to handle large amounts of video data efficiently and reduce processing delays.Overall, the proposed AI-powered smart surveillance system improves **accuracy, efficiency, and real-time incident detection**. It reduces the dependency on human monitoring, minimizes errors, and provides a proactive approach to security management in environments such as **smart cities, airports, campuses, and public spaces**.

V.SYSTEM ARCHITECTURE



The system architecture of the **Smart Surveillance: AI-Powered Incident Detection** model consists of several interconnected modules

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

that work together to monitor, analyze, and detect incidents in real time.The process begins with **video streams** collected from surveillance cameras installed in different locations. These cameras continuously capture live footage and send it to the **Video Processing Module**. This module acts as the core component of the system, where the incoming video frames are processed and prepared for intelligent analysis.The processed video data is then forwarded to various AI-based detection modules. The **Object Detection** module identifies important objects such as people, vehicles, bags, or suspicious items. The **Facial Recognition** module is used to identify and verify individuals by comparing detected faces with stored databases. The **Motion and Behavior Analysis** module examines movements and activities in the video to recognize suspicious or unusual behavior. The **Anomaly Detection** module further analyzes patterns and detects abnormal events that differ from normal activities, such as intrusion, violence, or abandoned objects.At the center of the architecture, **AI and Deep Learning Algorithms** play a major role in enabling accurate detection and decision-making. These algorithms are trained on large datasets to improve the system's ability to recognize incidents. To ensure efficient processing, the system can use both **Edge Processing** and **Cloud Server** support. Edge processing handles immediate local analysis, while the cloud provides storage, scalability, and advanced computation.When an incident is detected, the system activates the **Real-Time Alerts** and **Alert & Notification System**, which instantly informs security personnel. Finally, the system generates **Incident Reports** for documentation, review, and future analysis.

VI.IMPLEMENTATION

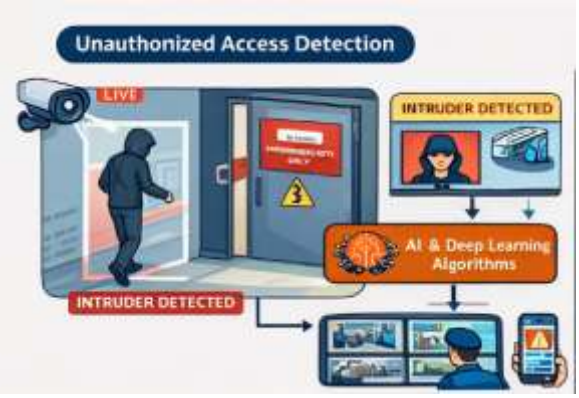


Fig 6.1 Admin Login

Fig 6.2 Manage Users

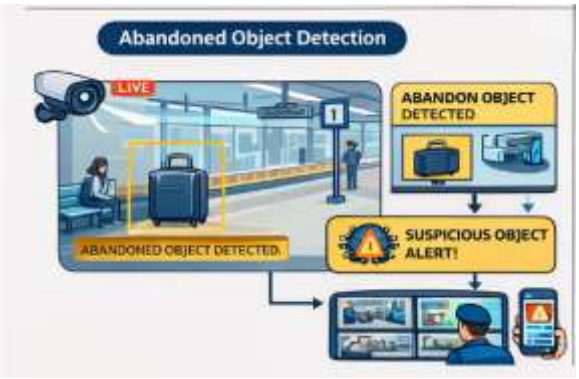


Fig 6.3 Models Train

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

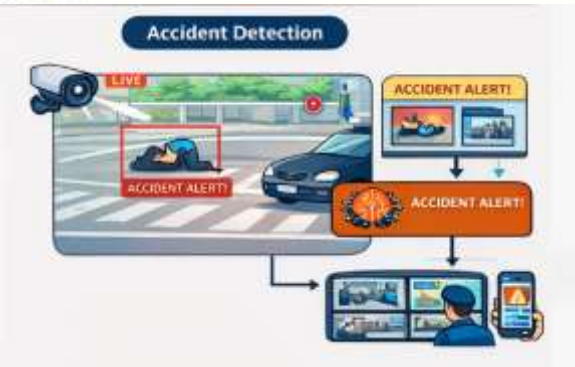


Fig 6.4 Line Chart

VII.CONCLUSION

The **Smart Surveillance: AI-Powered Incident Detection** system provides an advanced and intelligent approach to modern security monitoring. Traditional surveillance systems rely heavily on manual observation, which can lead to human errors, delayed responses, and inefficient monitoring of large areas. By integrating **Artificial Intelligence, computer vision, and deep learning technologies**, the proposed system overcomes these limitations and enables automated, accurate, and real-time incident detection.The system continuously analyzes video streams from surveillance cameras and identifies suspicious activities, abnormal behavior, or potential threats. Features such as **object detection, facial recognition, motion tracking, and anomaly detection** help improve the accuracy and reliability of the monitoring process. Real-time alerts and notifications ensure that security personnel can respond quickly to incidents, thereby improving safety and preventing potential risks.In addition, the integration of **edge computing and cloud technology** allows efficient processing and storage of large volumes of video data, making the system scalable and suitable for various environments such as **smart cities, airports, campuses, offices, and public spaces**.Overall, the proposed smart surveillance system enhances security management by reducing human workload, increasing monitoring efficiency, and enabling proactive threat detection. As AI technologies continue to evolve, such intelligent surveillance solutions will play a significant role in building **safer, smarter, and more secure environments** for society

VIII.FUTURE SCOPE

The **Smart Surveillance: AI-Powered Incident Detection** system has significant potential for further development as Artificial Intelligence and computer vision technologies continue to advance. Future improvements can focus on enhancing detection accuracy, expanding system capabilities, and integrating additional smart technologies to make surveillance systems more efficient and intelligent.One possible advancement is the integration of **advanced deep learning models** that can better understand complex human behaviors and detect more sophisticated threats such as crowd violence, suspicious gatherings, or unusual movement patterns. Improved **behavior analysis algorithms** can help predict incidents before they occur, enabling a more proactive security system.

Another important area of future development is the integration of **Internet of Things (IoT)**

devices with surveillance systems. Smart sensors, drones, and connected cameras can work together with AI models to provide more comprehensive monitoring of large areas such as smart cities, airports, railway stations, and industrial zones.The system can also be enhanced with **improved facial recognition and biometric authentication**, which can help in identifying individuals more accurately and maintaining secure access control in restricted areas. Additionally, integrating **cloud computing and edge AI** will further improve real-time processing, scalability, and data storage capabilities.Future research may also focus on **privacy protection and data security**, ensuring that surveillance systems comply with ethical and legal standards while protecting user data.Overall, the future scope of AI-powered surveillance systems lies in creating **fully automated, intelligent, and predictive security solutions** that can enhance safety, improve response times, and support the development of smarter and more secure environments.

IX.REFERENCES

[1] Duong, H. T., et al. (2023). *Deep Learning-Based Anomaly Detection in Video Surveillance: A Review.* Sensors. DOI: https://doi.org/10.3390/s23115024

[2] Nayak, R., et al. (2021). *A comprehensive review on deep learning-based methods for video anomaly detection.* Image and Vision Computing. DOI: https://doi.org/10.1016/j.imavis.2020.104129

[3] Sreenu, G., & Durai, M. S. (2019). *Intelligent video surveillance: A review through deep learning techniques.* Journal of Big Data. DOI: https://doi.org/10.1186/s40537-019-0212-5

[4] Berroukham, A., et al. (2023). *Deep learning-based methods for anomaly detection in video surveillance.* Bulletin of Electrical Engineering and Informatics. DOI: https://doi.org/10.11591/eei.v12i1.3944

[5] Khan, S. W., et al. (2022). *Anomaly Detection in Traffic Surveillance Videos Using Deep Learning.* Sensors. DOI: https://doi.org/10.3390/s22176580

[6] Gandapur, M. Q., et al. (2022). *End-to-end video surveillance-based deep learning model for crime detection.* Image and Vision Computing. DOI: https://doi.org/10.1016/j.imavis.2022.104402

[7] Elmetwally, A., et al. (2024). *Deep learning-based anomaly detection in real-time video surveillance.* Multimedia Tools and Applications. DOI: https://doi.org/10.1007/s11042-024-19116-9

[8] Cui, C., et al. (2024). *A cutting-edge video anomaly detection method using attention mechanisms.* Alexandria Engineering Journal. DOI: https://doi.org/10.1016/j.aej.2024.01.041

[9] Qasim, M., et al. (2023). *Video anomaly detection system using deep convolutional neural networks.* Internet of Things. DOI: https://doi.org/10.1016/j.iot.2023.100783

[10] Dhongde, V. S., & Sharma, C. (2025). *Anomaly Detection in Video Surveillance using Deep Learning Techniques.* DOI: https://doi.org/10.1109/ICOECA66273.2025.00134

[11] Salman, M., et al. (2025). *Enhancing surveillance anomaly detection with keyframe extraction.* DOI:

https://doi.org/10.1016/j.aej.2025.01.018

[12] Jebur, S. A., et al. (2022). *Review on deep learning approaches for anomaly event detection in surveillance videos.* Electronics. DOI: https://doi.org/10.3390/electronics12010029

[13] Patrikar, D. R., & Parate, M. (2022). *Anomaly detection using edge computing in video surveillance.* Sensors. DOI: https://doi.org/10.3390/s22072655

[14] Aberkane, S., et al. (2022). *Deep reinforcement learning-based anomaly detection for surveillance systems.* Informatica. DOI: https://doi.org/10.31449/inf.v46i7.3603

[15] Phapale, A., et al. (2025). *Deep context-aware feature extraction for anomaly detection in surveillance videos.* Engineering, Technology & Applied Science Research. DOI: https://doi.org/10.48084/etasr.9810

[16] Sultani, W., Chen, C., & Shah, M. (2018). *Real-world anomaly detection in surveillance videos.* DOI: https://doi.org/10.1109/CVPR.2018.00735

[17] Chen, J., et al. (2019). *Distributed deep learning model for intelligent video surveillance with edge computing.* DOI: https://doi.org/10.1109/ICDCS.2019.00070

[18] Tiezzi, M., et al. (2019). *Video surveillance of highway traffic events using deep learning architectures.* DOI: https://doi.org/10.1109/ITSC.2019.8917242

[19] Rezaee, K., et al. (2021). *Deep learning-based crowd anomaly detection for surveillance systems.* DOI: https://doi.org/10.1109/TCSS.2021.3050821

[20] Chaquet, J., Carmona, E., & Fernández-Caballero, A. (2013). *A survey of video datasets for human action and anomaly detection.* DOI: https://doi.org/10.1016/j.cviu.2013.01.013