"DEEP LEARNING AND EMBEDDED BASED ANOMALY DETECTION AND ALERT SYSTEM IN VIDEOS FOR THE PUBLIC SECURITY AND SURVEILLANCE"

Prof.Farzana Parveen B.A, Mr.Sai Kiran.P, Miss.Srushti.P.S, Miss.Srusti.S.R, Miss.Syeda BiBi Ayesha.

[1] *Prof.Farzana Parveen B.A Assistant professor, E&CE, SJM Institute of Technology Chitradurga, Karnataka, India*
[2] *Mr.Sai Kiran.P student, E&CE, SJM Institute of Technology Chitradurga, Karnataka, India*
[3] *Miss.Srushti.P.S student, E&CE, SJM Institute of Technology Chitradurga, Karnataka, India*
[4] *Miss.Srusti.S.R student, E&CE, SJM Institute of Technology Chitradurga, Karnataka, India*
[5] *Miss.Syeda BiBi Ayesha student, E&CE, SJM Institute of Technology Chitradurga, Karnataka, India*

ABSTRACT

This project aims to design a smart surveillance system that automatically detects unusual or suspicious activities in video streams using deep learning models combined with embedded hardware for real-time alerting. The system processes video data to identify anomalies—such as theft, unauthorized access, or abnormal behaviors—by classifying each frame with a trained neural network, and instantly notifies authorities or stakeholders when such events occur, thereby improving public safety and reducing reliance on manual monitoring.

Keyword: - *Deep learning, Anomaly detection, Video surveillance, Real-time detection, Embedded systems, Automated alerting.*

1. INTRODUCTION

Surveillance video analytics have evolved with the integration of deep learning and embedded systems to automatically detect and respond to abnormal activities. The increasing incidents of crime, accidents, and security breaches in public spaces have driven the need for intelligent solutions that can process massive volumes of video data in real-time, surpassing the limitations of traditional manual monitoring systems.These architectures enable automated detection and instant alert generation, thereby improving the responsiveness and reliability of security operations in diverse and unpredictable environments.

Modern public security demands systems that not only capture video footage but also intelligently analyze it for anomalies such as trespassing, violence, theft, or unattended objects. Embedded platforms paired with deep learning models enhance deployment flexibility by supporting on-site processing with low latency, essential for time-sensitive alerting. These systems optimize resource use by filtering out normal activities, thereby minimizing false alarms and focusing human attention on critical incidents.

The integration of anomaly detection in video surveillance harnesses advances in computer vision, pattern recognition, and edge computing. It addresses challenges like variable lighting, occlusions, and crowded environments by learning complex temporal and spatial patterns beyond traditional rule-based methods. Consequently, such systems are pivotal for smart cities, transportation hubs, commercial zones, and critical infrastructure protection, enabling proactive, continuous public safety management.

1.1 Components

1. ATMEGA328 Microcontroller
2. GSM Modem
3. UART Converter
4. 5Megapixel Camera
5. Quad Core CPU
6. LCD Display(16 x 2)
7. Buzzer
8. Ram

1.2 Methodology

The methodology of a deep learning and embedded-based anomaly detection and alert system for public security and surveillance in videos typically involves a fusion of advanced video analytics and hardware-driven alert mechanisms. The process starts with capturing video streams from surveillance cameras positioned in public areas. These video frames are then fed into a deep learning model, which is trained to understand normal behavioral patterns and identify deviations or abnormalities indicative of suspicious activities or security threats.

Depending on the chosen approach, the deep learning model can be trained in a supervised, semi-supervised, or unsupervised fashion. In practice, semi-supervised techniques are common, where models are trained only on normal events, and anomalies are detected as significant departures from these learned regularities. The model extracts both spatial and temporal features from consecutive frames using architectures like convolutional neural networks (CNNs), convolutional autoencoders, long short-term memory networks (LSTMs), or hybrid models. Once a potential anomaly is detected, the model outputs a signal that is passed to an embedded hardware unit such as the ATMEGA328p microcontroller.

The embedded microcontroller acts as the bridge between the AI-powered detection system and real-world alert mechanisms. Upon receiving an anomaly alert, the microcontroller orchestrates actions like displaying detection results on LCD screens, activating buzzers for audible alerts, and using a GSM module to send SMS notifications to security personnel or authorities. The logic is designed to guarantee immediate, location-specific response, ensuring prompt notification and intervention when abnormal activities are observed. This methodology combines the flexibility and accuracy of AI-based anomaly detection with the robustness and reliability of embedded alerting systems, making it highly effective for public security and intelligent surveillance applications. The deep learning stage commonly employs training on large datasets of mostly normal behaviors (semi-supervised learning), enabling the model to establish strong representations of normality. During inference, deviations from these learned patterns are scored as anomalies, with thresholds set dynamically to reduce false alarms. The extracted anomaly signals are transmitted to the embedded microcontroller using serial communication protocols like UART.

The ATMEGA328p microcontroller acts as a low-power, real-time controller that receives anomaly detection alerts. Upon receiving an anomaly signal, it activates output modules such as an LCD to display status, a buzzer to generate audible warnings, and a GSM module to send SMS notifications to remote security personnel, thereby providing both local and remote alert mechanisms.

Power management ensures the continuous and reliable operation of all hardware components, critical for uninterrupted surveillance. Overall, the methodology integrates powerful deep learning video analytics with robust embedded system design to achieve automated, flexible, and scalable anomaly detection and alerting suitable for enhancing public safety and security in real-world environments.

2. BLOCK DAIGRAM

This block diagram represents a theoretical design of an embedded anomaly detection and alert system, which is commonly used in surveillance and public safety applications. The system integrates a deep learning video processing model with a microcontroller, providing both intelligent analysis and immediate alert responses

In operation, live or recorded video feeds are input to a deep learning model capable of recognizing abnormal activities or patterns. These models often use convolutional neural networks or related architectures to process each frame and identify relevant anomalies. When an anomaly is detected, the model communicates its decision to the system's ATMEGA328p microcontroller via a UART (Universal Asynchronous Receiver/Transmitter) converter, which ensures reliable serial data transfer between high-level computing and low-level hardware control. Once the microcontroller receives an alert signal, it acts as the system's central controller, orchestrating real-time responses by activating multiple output modules. For example, it may display the detected event's details or system status on an LCD screen for visualization and local monitoring. Simultaneously, it triggers a buzzer to provide an immediate audible warning in the monitored area, helping to draw attention to possible security incidents.

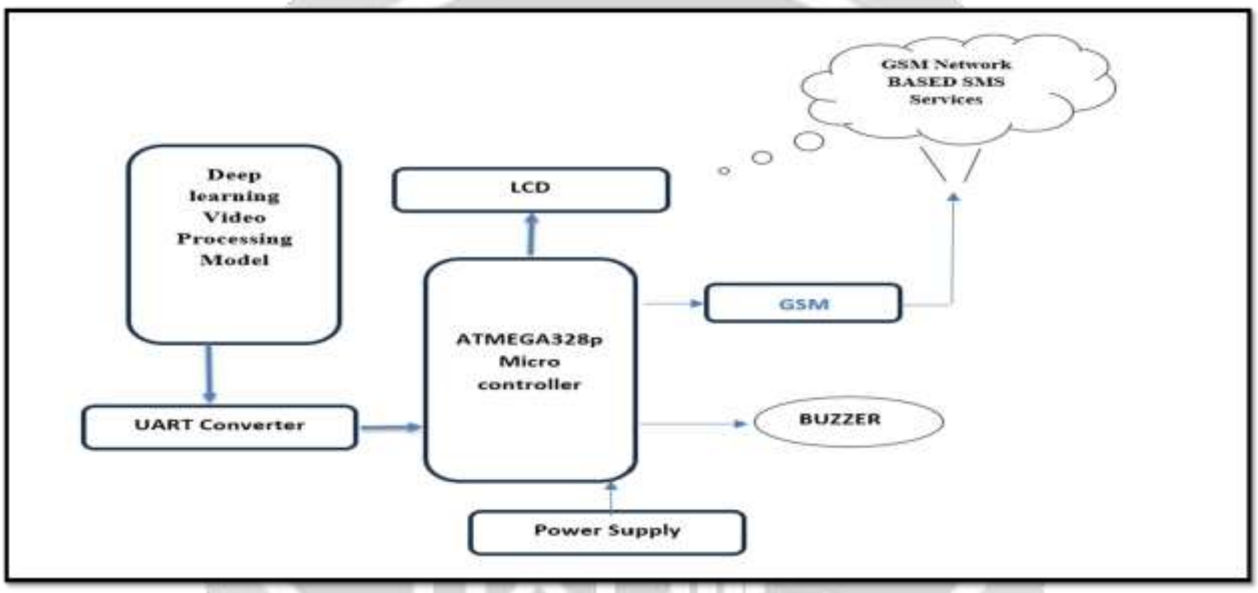

Fig -1: Block diagram of anomaly detection

Additionally, the system incorporates a GSM module that connects to cellular networks, enabling the transmission of SMS-based notifications. This feature is crucial for remote alerting, as it allows instant communication with external stakeholders or security personnel when an anomaly is observed. All subsystems, including the microcontroller, LCD, GSM, and buzzer, are powered by a regulated supply to maintain reliable and seamless operation.

The synergy between deep learning video analytics and embedded hardware control enables automated surveillance systems to transition from passive monitoring to intelligent, active intervention. Such designs exemplify modern trends in building resource-efficient, scalable, and highly responsive public security solutions using microcontrollers and AI models

The output from this model is communicated to the microcontroller via the UART interface. UART serves as a reliable means of facilitating the connection between high-computation devices (like PCs handling video processing) and resource-constrained embedded units such as the ATMEGA328p. The microcontroller is programmed to interpret the received anomaly signal and coordinate the system's response according to pre-defined logic.

When an anomaly is detected, the microcontroller instantly activates connected devices to ensure immediate awareness and response. For instance, the LCD display is engaged to provide a simple visual summary of the detected event. At the same time, the system's buzzer produces an audible alarm, which is critical in alerting personnel on site. The integration of the GSM module marks the system's capability for remote notification. The microcontroller relays a signal to the GSM component, which proceeds to send an SMS alert to specified contacts or authorities via cellular networks. This dual approach of local alerting and remote communication enhances the overall security and responsiveness of the surveillance system.

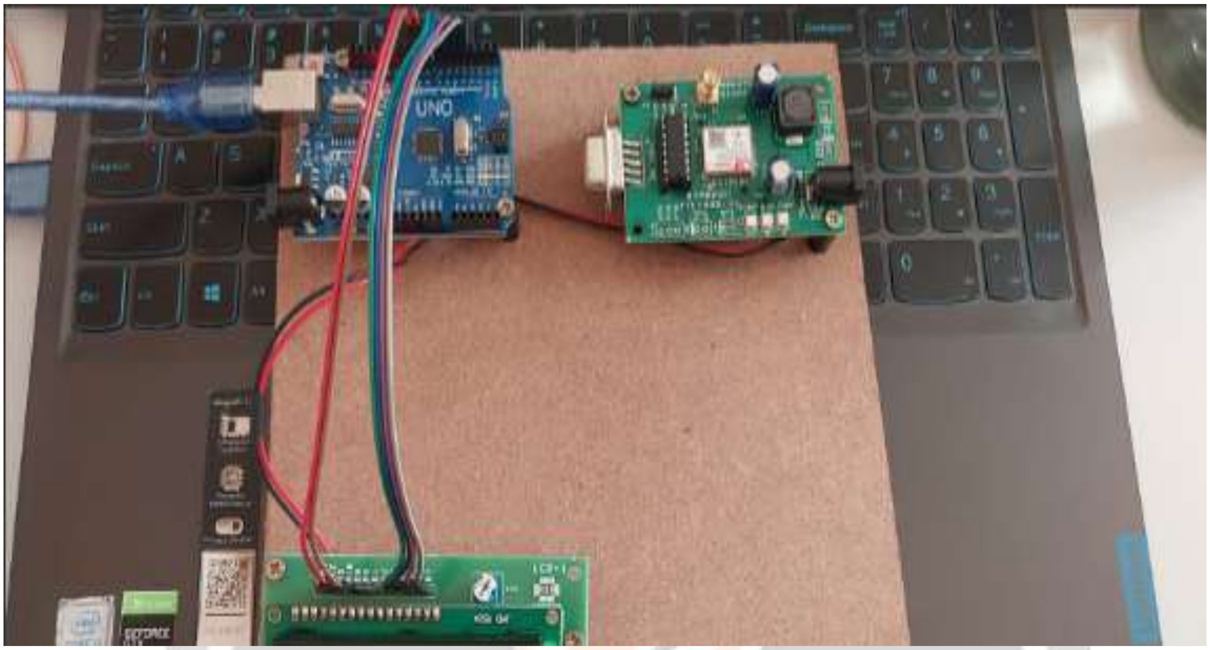

Fig -2: Making anomaly detection connection using hardware components.

The power supply ensures the stable operation of all hardware components, making the system suitable for deployment in diverse environments. Such a setup demonstrates how embedded systems can utilize state-of-the-art deep learning algorithms to automatically detect unusual events in real time and rapidly propagate alerts across multiple channels—a significant advance over traditional surveillance solutions.
An embedded System for normality Detection and Alert in Public Security and Surveillances Videos is a research direction focused on enhancing the safety of public space through automation, real-time intervention, and advanced analytics. This project aims to monitor live video stream or recordings, distinguish between normal and abnormal human behaviors, and generate timely alert for rapid response by security personnel or authorities.
By leveraging advancement in embedded systems and deep learning, this research holds the potential to make public surveillance both intelligent and proactive addressing critical challenges in modern security.

2.1 Objective

The objective of the "Deep Learning and Embedded Based Anomaly Detection and Alert System in Videos for Public Security and Surveillance" is to develop an intelligent system that can automatically analyze video surveillance footage in real-time to detect unusual or abnormal activities that could indicate security threats or suspicious behavior. This system uses deep learning models, usually convolutional neural networks, to learn normal patterns from extensive video datasets and to distinguish anomalies that deviate from these patterns. When an anomaly is detected, the system generates alerts to notify security personnel promptly, enabling quick and efficient responses to potential security incidents. Incorporating embedded systems ensures the solution is lightweight and can operate on edge devices for real-time processing without requiring heavy computational resources or continuous human monitoring.

Key objectives include:

- Automatic and real-time detection of abnormal activities in public surveillance videos.
- Reducing the reliance on continuous human observation, which is labor-intensive and prone to error.

- Enhancing public safety by providing early warnings and rapid alerts for suspicious behaviors such as theft, unauthorized access, and other crimes.
- Integrating with existing surveillance infrastructure to improve situational awareness.
- Minimizing false alarms through sophisticated spatial-temporal feature extraction and anomaly scoring.
- Making surveillance systems scalable and adaptable across different environments like schools, malls, offices, and public spaces.

This approach combines deep learning's pattern recognition capabilities with embedded system efficiency to create a proactive security tool that improves operational security, crime prevention, and overall public safety in surveillance context

2.2 Importance and Motivation

The importance and motivation behind developing a "Deep Learning and Embedded Based Anomaly Detection and Alert System in Videos for Public Security and Surveillance" revolve around addressing the limitations of traditional surveillance and enhancing public safety through automation and intelligence.

Importance:

- Traditional video surveillance relies heavily on manual monitoring, which is labor-intensive, error-prone, and inefficient since abnormal events are rare and easily missed.
- Deep learning enables real-time, automatic analysis of video feeds to detect unusual or suspicious behavior patterns, such as unauthorized access, aggressive actions, or loitering, improving the accuracy and response times of security systems.
- Embedded systems allow the solution to operate efficiently on edge devices, facilitating faster alerts and reducing dependence on centralized, high-cost computational resources.
- These systems significantly reduce false alarms by precisely distinguishing between normal and abnormal activities, lowering the workload on security personnel and ensuring focus on genuine threats.
- The integration of advanced anomaly detection enhances safety in diverse public environments like schools, malls, transportation hubs, and public events, where quick threat identification can prevent crimes and ensure timely interventions.

Motivation:

- Increasing public security challenges and growing surveillance data volumes demand intelligent systems capable of filtering and identifying real threats automatically.
- The need to optimize security operations by reducing costs related to human monitoring and enhancing operational efficiency through automation.
- Desire to leverage advances in AI and deep learning to transform video monitoring from passive observation to proactive security, enabling early warnings and rapid alerts.
- Addressing privacy and scalability issues by employing embedded, on-device processing rather than sending video data to cloud servers for analysis.
- Supporting security personnel with actionable insights and alerting mechanisms that improve situational awareness and decision-making.

In essence, this system is motivated by the goal to create smarter, faster, and more reliable security surveillance that combines deep learning’s pattern recognition with embedded system efficiency to enhance public safety and operational effectiveness while reducing costs and human error.

3. WORKING

The working of a deep learning and embedded-based anomaly detection and alert system in videos for public security and surveillance begins with continuous video feed acquisition from cameras installed in public areas. The video stream is processed frame by frame by a deep learning model, which is designed to detect patterns and behaviors that differ from the learned norm of normal activities. This detection is achieved through feature extraction and classification layers in the model, which analyze spatial and temporal data to identify suspicious or irregular events.

The deep learning model outputs its anomaly detection results to a UART converter, which translates the data into signals understandable by the embedded microcontroller ATMEGA328p. This microcontroller serves as the decision-making hub, interpreting the anomaly alerts sent from the AI model. Upon confirmation, the microcontroller triggers multiple modules to respond appropriately: it activates an LCD to present the detected event or system status for monitoring purposes; it drives a buzzer to generate an immediate local audible alert; and it controls a GSM module to transmit SMS alerts through the cellular network, ensuring remote notification to relevant security personnel or authorities. Power supply units ensure all components receive stable power for uninterrupted operation. This integration between deep learning's computational intelligence and embedded hardware's real-time control allows the system to operate autonomously and respond swiftly to potential threats, significantly enhancing public security surveillance capabilities by enabling real-time anomaly detection and multi-level alert dissemination.

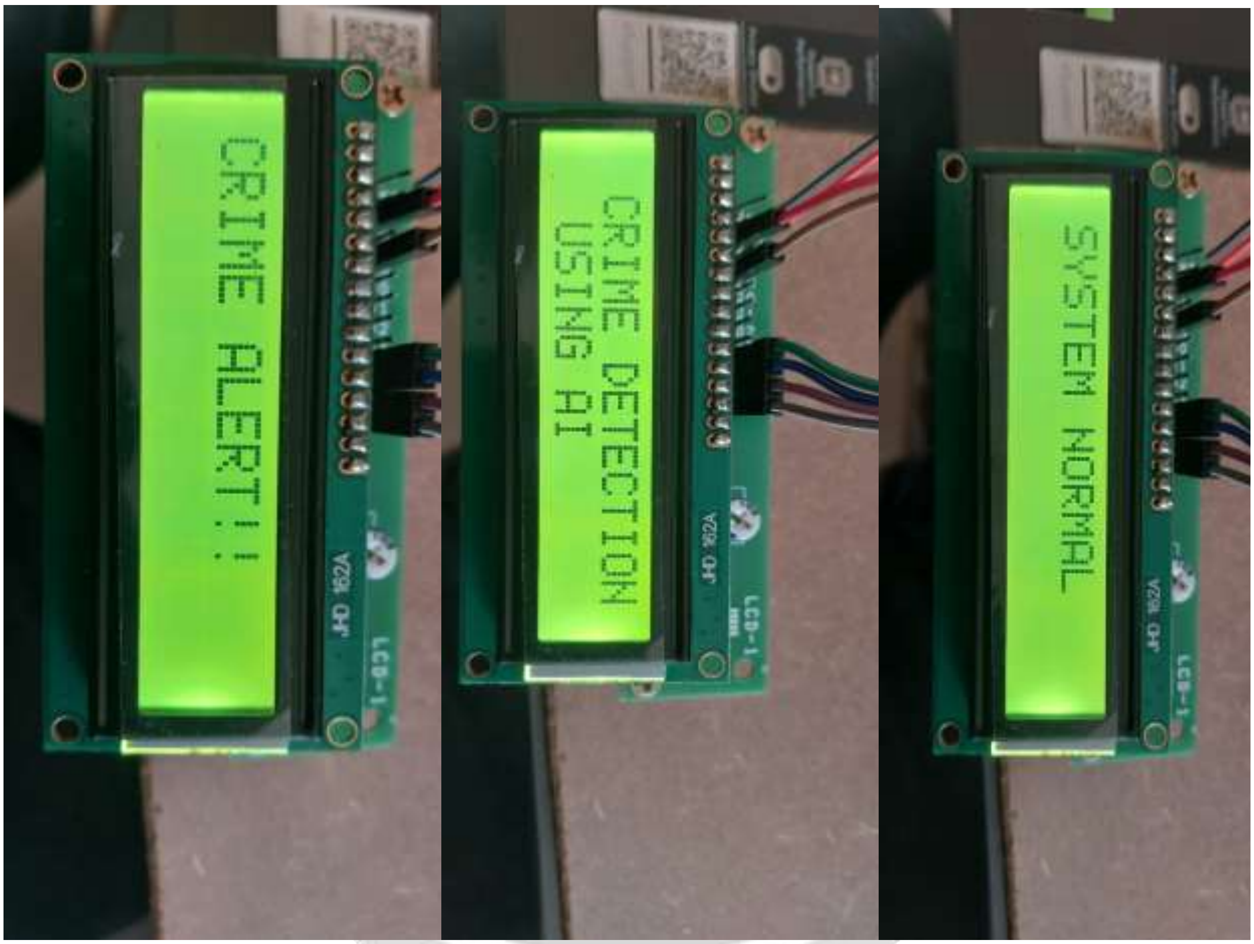

Fig -3: Outputs of anomaly detection

The CNN layers focus on extracting high-level spatial features from individual video frames, such as identifying objects, shapes, and their contexts. Simultaneously, recurrent units manage the temporal aspect by learning patterns across consecutive frames, distinguishing normal sequential behaviors from anomalies. This dual spatial-temporal approach improves accuracy in detecting rare or unusual events that deviate significantly from learned regular patterns.After the deep learning model processes incoming frames and identifies a potential anomaly, it sends alert signals through a UART interface to an embedded microcontroller like the ATMEGA328p. This microcontroller operates as the system's control core, interpreting incoming signals and activating appropriate response components. It drives an LCD module to display event information locally, triggers a buzzer for audible warnings on-site, and commands a GSM module to send SMS alerts to remote monitoring personnel. Power supply units ensure sustainably continuous operation of all modules.The overall workflow combines the adaptive intelligence of deep learning video analysis with the responsiveness and reliability of embedded hardware control. This synergy provides a scalable solution for real-time monitoring and immediate alerts in public security, enabling efficient detection and response to anomalous activities in crowded or complex environments

3.1 Application and Public Impact

Deep learning and embedded-based anomaly detection and alert systems in video surveillance are crucial for enhancing public security. These systems use advanced deep learning models to detect unusual, suspicious, or threatening activities in real-time video feeds, enabling rapid alerting and response to potential threats, crimes, or emergencies.

Applications in Public Security and Surveillance

- These systems are deployed in public spaces such as bus and railway stations, airports, banks, malls, schools, parking lots, and roads to detect anomalies like theft, street crimes, illegal access, vandalism, and accidents.
- They leverage deep learning architectures including convolutional neural networks (CNNs), recurrent neural networks (RNNs), and graph convolutional networks (GCNs) to analyze video frames for anomalous behavior.
- Real-time detection allows for classification of events such as robbery, fighting, arrest, abuse, shootings, and traffic accidents, helping authorities to intervene quickly.
- The technology is useful for not only crime prevention but also emergency response, crowd control, and traffic monitoring.
-

Public Impact

- Automated anomaly detection enhances surveillance efficiency by reducing the need for constant human monitoring of video feeds, allowing security personnel to focus on actionable alerts.
- It improves public safety by enabling faster reaction times to potential threats, potentially preventing criminal or hazardous events from escalating.
- These systems can generate alerts in real-time, enabling proactive rather than reactive security measures.
- Widespread implementations contribute to safer urban environments by continuously monitoring public areas with high accuracy and low false alarm rates.

Technical Highlights

- The models extract spatiotemporal and contextual features from videos, combining spatial and temporal data for better anomaly recognition.
- Embedded implementations on platforms like microcontrollers make these systems suitable for continuous, on-site, low-power video analysis.
- Transfer learning and pre-trained deep models accelerate training and improve anomaly recognition despite challenges like occlusions and varying lighting conditions.

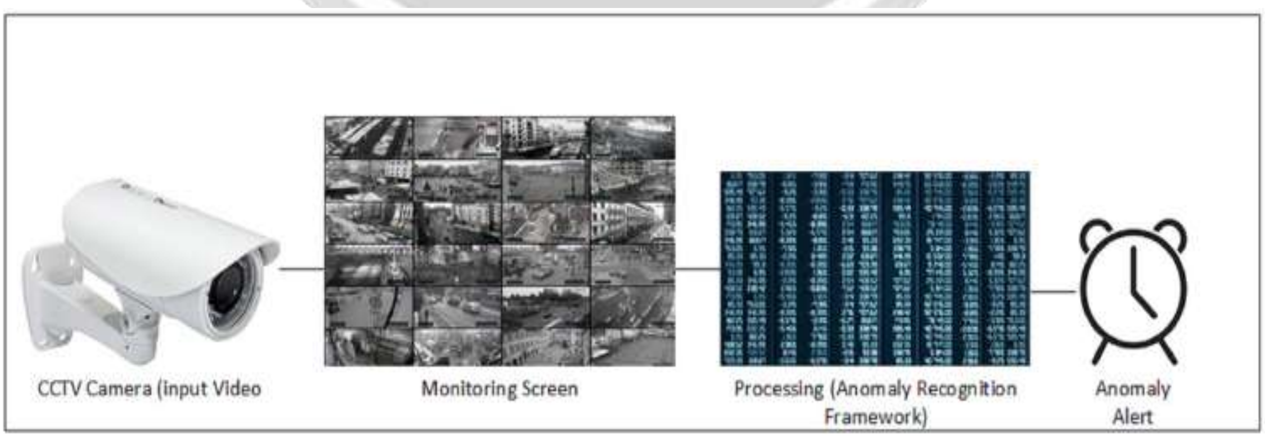

Fig-4: Block Diagram of Deep Learning–Based Video Anomaly Detection and Alert System.

4. CONCLUSION

Deep learning and embedded-based video anomaly detection systems have shown high effectiveness for real-time surveillance, enhancing both the rate and accuracy of abnormal event detection. These systems can promptly alert authorities, enabling preventive action and reducing security incidents, thanks to continuous monitoring and advanced feature extraction capabilities. Overall, integrating deep learning algorithms with embedded platforms provides a proactive, scalable solution for improving public safety through automated and intelligent surveillance..

Deep learning and embedded anomaly recognition platforms are the foundation for future-ready, automated, and ethical security solutions for public environments.

5. REFERENCES

[1] Wang, B., et al. (2022). "Detection Anomaly in Video Based on Deep Support Vector Data Description." This paper proposes a deep learning framework for video anomaly detection and reports improved accuracy over traditional methods using datasets like Avenue and ShanghaiTech.

[2] Berroukham, A., et al. (2023). "Deep learning-based methods for anomaly detection in video surveillance: a review." This review discusses various deep learning techniques, algorithms, comparison metrics, and publicly available datasets relevant to video anomaly detection.

[3] Wu, P., et al. (2024). "Deep Learning for Video Anomaly Detection: A Review." The authors present a comprehensive overview of supervised and unsupervised deep learning models for video anomaly detection and highlight important research directions.

[4] Krishnan, S.R., et al. (2024). "Comprehensive survey on video anomaly detection using deep learning." This survey provides an in-depth study of deep learning techniques used to detect and predict anomalous events in surveillance videos.