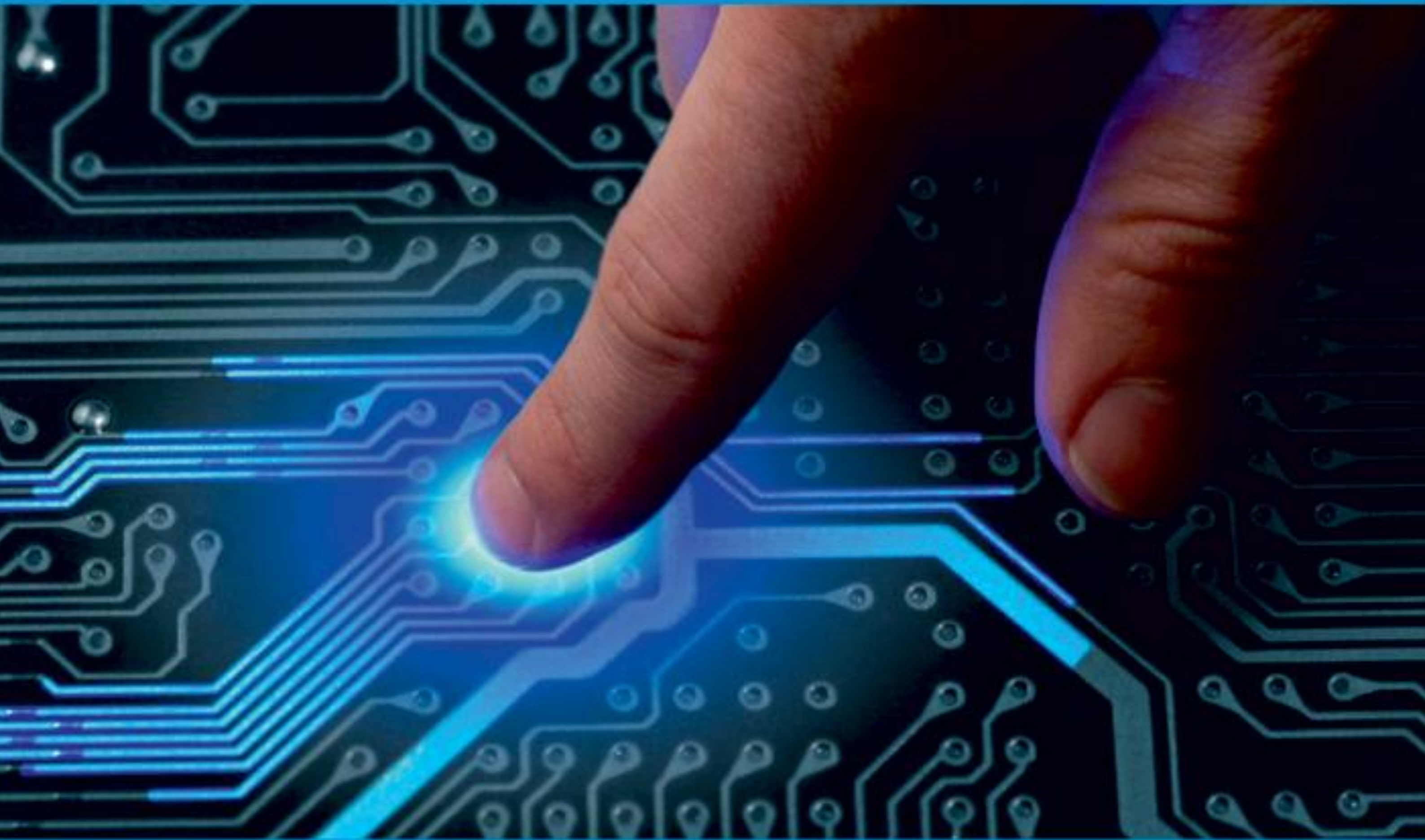
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205336 |

AI-CAMX: Automated Surveillance Camera System

Mr. Kaustubh Shinde[1], Aman Kumar[2], Yash Baad[3], Jignesh Borse[4], Gaurav Pawar[5]

Assistant Professor, Department of Computer Engineering, Sinhgad Institute of Technology and Science, Pune, India[1]

Student, Department of Computer Engineering, Sinhgad Institute of Technology and Science, Pune, India[2-5]

ABSTRACT: The AI-CAMX Automated Surveillance System is an innovative project designed to enhance security through advanced surveillance technologies. Utilizing OpenCV and TensorFlow, this system leverages artificial intelligence and computer vision to perform real-time image and video analysis for accurate anomaly detection. The primary objectives of the project include the development of a user-friendly interface, implementation of sophisticated AI algorithms, and ensuring reliable performance through rigorous testing.

This project addresses the growing need for automated and intelligent surveillance solutions capable of differentiating between routine activities and potential security threats. The AI-CAMX system automatically detects anomalies and triggers alerts, allowing for prompt responses from security personnel. Key features include real-time monitoring, scalability, and integration with existing security infrastructures.

The successful implementation and evaluation of the AI-CAMX system demonstrate its potential to revolutionize surveillance practices, offering significant improvements in efficiency and effectiveness. This abstract summarizes the project's aims, methodologies, and key achievements, highlighting its contribution to the field of automated surveillance systems and its readiness for future advancements.

KEYWORDS: Surveillance System, Administrative efficiency, User-Friendly Interface, Automated Anomaly Detection, Artificial Intelligence, Machine Learning.

I. INTRODUCTION

In an era marked by technological advancements, safety, and security have taken center stage, necessitating innovative solutions for real-time threat detection and response. This project introduces an Automated Surveillance System utilizing the power of OpenCV and TensorFlow to address these concerns comprehensively. By harnessing computer vision, artificial intelligence, and deep learning technologies, this system offers the capability to autonomously identify and report accidents and incidents of violence, ensuring swift and informed responses from concerned authorities.

The integration of OpenCV and TensorFlow enables the system to analyze live surveillance footage with remarkable precision. It can detect patterns and anomalies in real-time, differentiating between routine activities and potentially harmful situations. This groundbreaking technology empowers organizations, institutions, and communities to enhance their security measures while minimizing response times.

This report will delve into the technical intricacies, design considerations, and performance evaluations of the Automated Surveillance System. It aims to provide a comprehensive understanding of how OpenCV and TensorFlow are employed to create a sophisticated surveillance solution that can significantly improve incident detection, response efficiency, and overall safety.

II. RELATED WORK

This paper [1], addresses the crucial role of human surveillance in ensuring safety, particularly in environments like schools, hospitals, airports, and malls. It highlights the limitations of current monocular camera-based surveillance systems in providing three-dimensional depth information for person detection and tracking due to their fixed field of view. As safety concerns escalate, automated video surveillance systems have garnered significant attention. Detecting and classifying objects for subsequent tracking has become a standard feature, albeit challenged by factors such as lighting variations, pose changes, occlusion, and motion blur. Night vision detection, despite its challenges, remains vital for combating crime and ensuring public safety. Another significant challenge is the detection of abandoned objects in public areas, for which the paper proposes a method utilizing background reduction and morphological filtering in real-time settings. The ultimate objective is to promptly identify abandoned suspicious objects and notify the appropriate authorities.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205336 |

This paper [2], examines recent advancements in automated surveillance systems, driven by IoT and machine learning, which have significantly enhanced security and operational efficiency across various domains. Research highlights their application in smart cities, using intelligent algorithms for traffic management and public safety. Technologies like Vehicle License Plate Recognition (VLPR) employ sophisticated image processing and neural network techniques to improve accuracy. However, these advancements also raise ethical and privacy concerns, emphasizing the need for robust regulatory frameworks. Case studies in law enforcement, retail, and transportation illustrate the practical benefits, despite challenges in data security and system interoperability. Ultimately, responsible implementation and continuous research are crucial to maximizing the potential of these systems.

This paper [3], presents a novel approach to real-time crowd anomaly detection, leveraging spatiotemporal texture (STT) models for identifying abnormal behaviors in video surveillance. Existing methodologies in crowd behavior analysis predominantly utilize top-down approaches, focusing on individual entity tracking and aggregation, which prove ineffective in real-world scenarios due to occlusions and density fluctuations. Bottom-up approaches, which model crowd anomalies based on group-level characteristics, have shown greater promise. Early studies, such as those by Ali et al. with the finite time Lyapunov exponent field, integrate dynamic crowd information like density and movement direction into optical flow fields for anomaly detection. The STT model proposed in this research enhances these methods by incorporating both global and local features of crowd dynamics, thus providing a robust framework for detecting localized abnormalities that might indicate hazardous situations. This work builds on foundational techniques in optical flow and wavelet transformation, demonstrating significant improvements in detection sensitivity and real-time processing, which are crucial for effective surveillance and timely response in public safety applications.

This paper [4], presents Hawk-Eye, an innovative AI-powered threat detection system for smart surveillance cameras, aimed at enhancing public security by identifying potential threats in real-time. Leveraging recent advances in AI and IoT, Hawk-Eye transforms traditional surveillance systems from passive monitors to active security agents capable of detecting on-body weapons, masked faces, suspicious objects, and unusual traffic patterns. The system operates both on centralized cloud servers and locally at the network edge, utilizing edge computing to reduce communication overhead and enable rapid security responses. The cloud component employs a Mask R-CNN model to generate high-quality segmentation masks for detected objects, providing classification confidence and processing times. On the edge, Hawk-Eye uses a Raspberry Pi 3, Intel Neural Compute Stick 2, and Logitech C920 webcam to run a CNN model that processes image streams in real time, displaying results through a user-friendly interface. A motion detection module captures images upon detecting movement, ensuring continuous monitoring. Experimental evaluations demonstrate Hawk-Eye's robust performance, achieving an average prediction accuracy of 94% on the tested dataset, thus proving its effectiveness for real-time threat detection in various public settings.

This paper [5], situates its proposed approach within the broader context of visual surveillance. It begins by discussing the integration of video technology with sensors, as advocated by Cucchiara (2005), which inspires the exploration of CCTV and infrared fusion. The study also aligns with the common processing framework outlined by Hu et al. (2004) for surveillance systems. Furthermore, it contrasts with the real-time system described by Haritaoglu et al. (2000), which focuses on gray-scale or thermal video analysis, unlike the proposed approach that leverages multiple spectral bands for improved object detection and tracking. This literature review underscores the novelty of integrating various spectral modalities to enhance detection and tracking robustness.

III. PROPOSED WORK

A. Problem Statement

The problem this project addresses is the development of an AI-CAMX Auto-mated Surveillance System that effectively integrates AI and computer vision technologies to provide advanced surveillance capabilities. This system should be capable of real-time image and video analysis, anomaly detection, and automated alerts, making it suitable for various applications across industries.

B. Objective

The project is aimed to design a website with the basic versions of the following features:

1. To design and develop the AI-CAMX Automated Surveillance System, incorporating state-of-the-art AI and computer vision technologies.
2. To create a user-friendly interface for configuring surveillance parameters and receiving real-time alerts.
3. To implement advanced anomaly detection algorithms to identify potential security threats or operational issues.
4. To evaluate the system's performance through rigorous testing and fine-tuning, ensuring accuracy and reliability.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205336 |

5. To document and present the results and findings in a comprehensive project report.

C. Diagrams

Use Case Diagram: Figure 4.5 depicts the use case diagram which shows the interaction between the actors and the system.

The actor in the use case diagram is Surveillance System, Police, Ambulance, Fire Department.

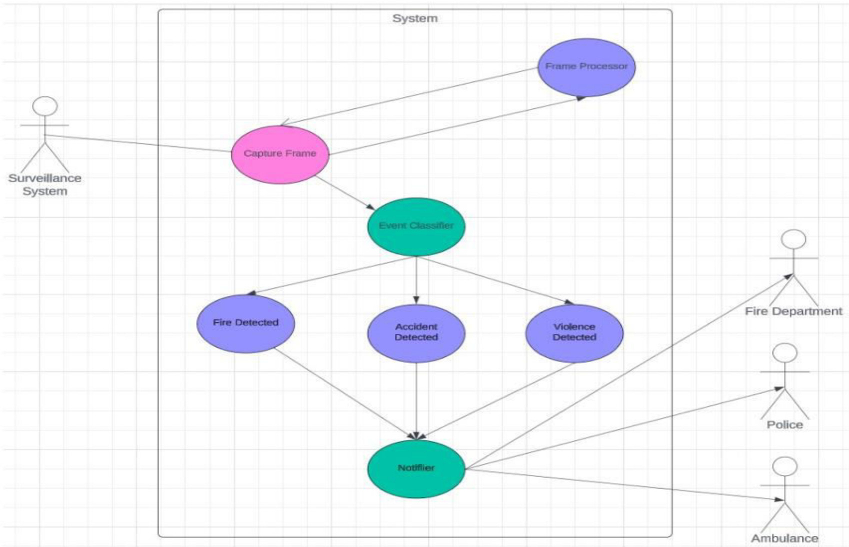


Figure 3.1: UML Use Case Diagram for Automated Surveillance System

Activity Diagram: Figure 4.6 illustrates the flow of control in the system and shows the steps involved in the execution of a use case. User Activity decides the flow of the control. Activities have predefined flow and execute as per the conditions. The process of capture of video footage and detection of abnormalities is shown below.

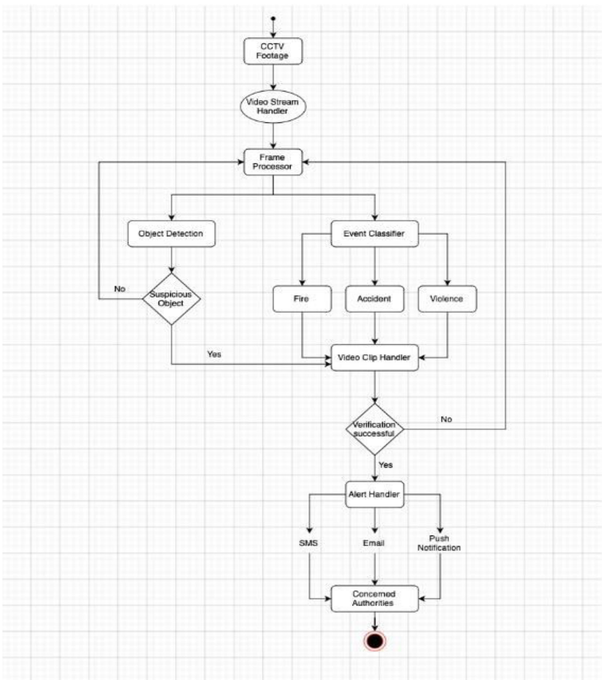


Figure 3.2: UML Activity Diagram for Automated Surveillance System

Sequence Diagram: High-level interaction between active objects in a system is visualized using sequence diagram. In Figure 4.7 the sequential flow of the system and the exchange of messages between the object is shown. Active Objects/Actors in the sequence diagram are CCTV, Video Stream Handler, Object Detector, Event Classifier, Video Clip Handler, and Alert Handler.

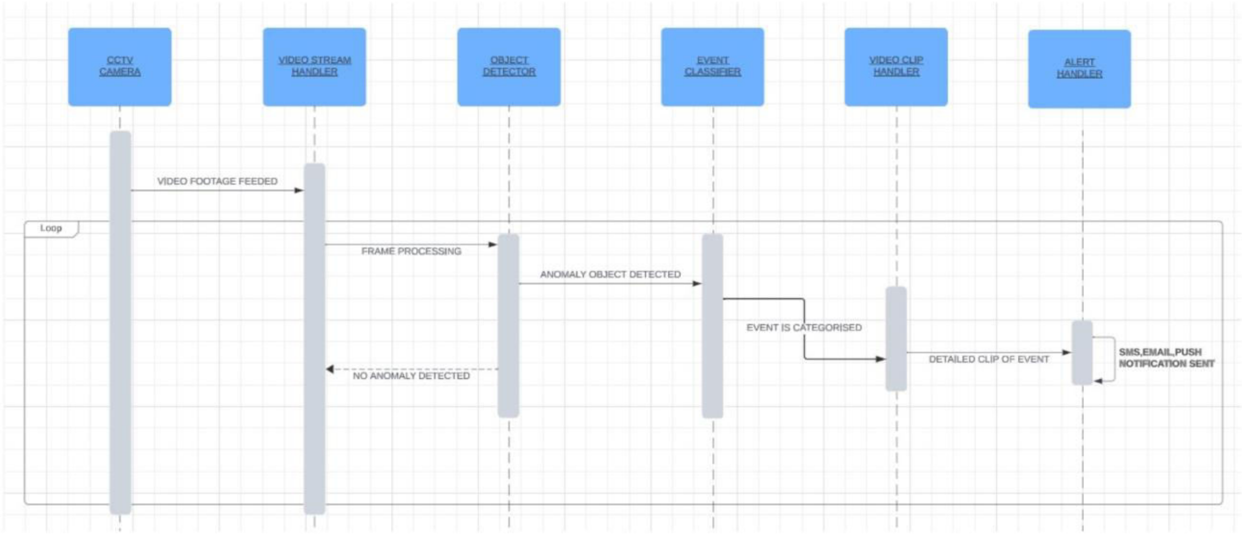


Figure 3.3: UML Sequence Diagram for Automated Surveillance System

IV. RESULTS AND DISCUSSION

The AI-CamX Automated Surveillance System has significantly enhanced security measures by providing a real-time, efficient platform for monitoring and analyzing live video feeds. The system uses OpenCV and TensorFlow to detect accidents, fire, and violent incidents in real time, ensuring prompt and accurate threat identification.

Users benefit from advanced event recognition features, which ensure high precision in identifying events. The anomaly detection capability reliably identifies unusual activities, while automated alerts notify authorities promptly, improving response times.

The system's scalable architecture supports the addition of more cameras and users, and its user-friendly interface allows for easy configuration and monitoring. The robust integration of AI technologies and a well-organized structure have demonstrated a marked improvement in incident detection and response efficiency, providing a robust and scalable surveillance solution.

Figure 4.1. Login Page

AiCamX Login Page: Figure 1 facilitates user login, where users can securely access their accounts by providing their email address and password. This screen is equipped with user authentication features and a sleek interface, ensuring a seamless and secure login experience.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205336 |

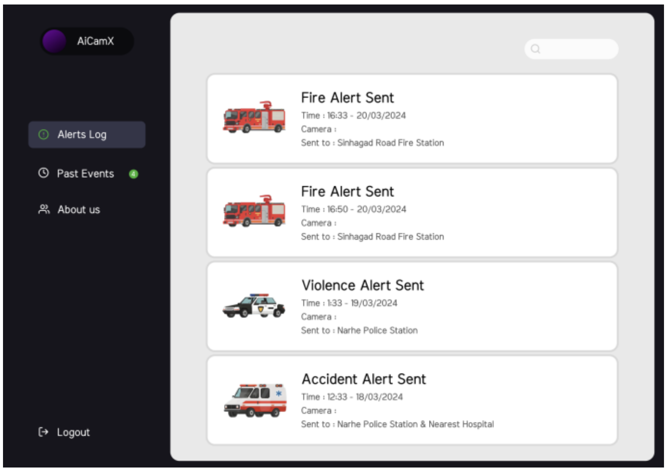


Figure 4.2. Alerts Page

AiCamX Alerts Log: Figure 1 serves as a critical component of the AiCamX security system. It presents a comprehensive record of recent security alerts and provide vital information for security personnel. The log meticulously chronicles each alert, including the date, time, and type (fire, violence, accident). Additionally, it specifies the location of the incident, ensuring prompt dispatch of emergency services. By centralizing alert data, Figure 1 empowers security teams to effectively monitor and respond to security threats, safeguarding lives and property.

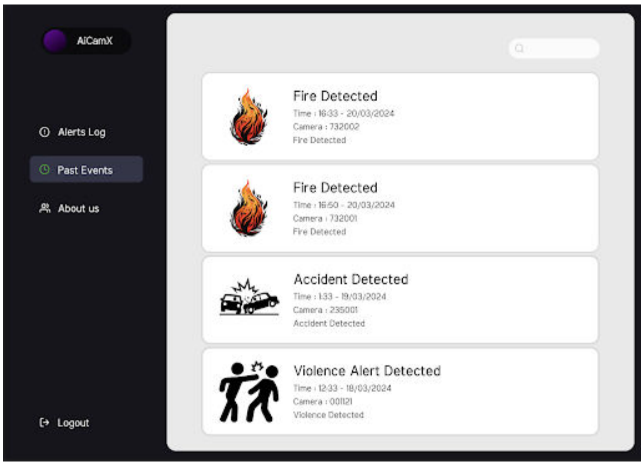


Figure 4.3. Past Events Page

AiCamX Past Events Log: Figure 3 showcases a vital aspect of the AiCamX security system: a detailed log of recent security incidents. This record serves as a central repository for security personnel, providing them with crucial information for investigation and response. Each entry within the log meticulously documents the date, time, and type of alert (fire, violence, accident). Furthermore, it pinpoints the location of the incident, facilitating a swift deployment of emergency services. By consolidating alert data in a centralized location, Figure 1 empowers security teams to efficiently monitor and address security threats, ultimately protecting lives and property."

V. CONCLUSION

The AI-CAMX Automated Surveillance System represents a significant advancement in surveillance technology, integrating state-of-the-art artificial intelligence and computer vision capabilities to enhance security measures across various sectors. The project successfully demonstrates the application of OpenCV and TensorFlow for real-time image and video analysis, enabling accurate anomaly detection and prompt automated alerts. This system not only addresses current security needs but also sets a foundation for future enhancements and scalability.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205336 |

The project was designed with clear objectives, including the development of a user-friendly interface, implementation of advanced anomaly detection algorithms, and rigorous performance evaluations to ensure reliability and accuracy. The system's ability to differentiate between routine activities and potential threats marks a critical improvement in surveillance technology, allowing for swift and informed responses from relevant authorities.

Moreover, the project highlights the importance of continuous learning and adaptability in surveillance systems. By incorporating mechanisms for ongoing optimization and integration with other security technologies, the AI-CAMX system is well-positioned to evolve alongside emerging threats and technological advancements.

In conclusion, the AI-CAMX Automated Surveillance System not only meets its initial objectives but also provides a robust platform for future developments. It exemplifies how modern AI and computer vision technologies can revolutionize surveillance, making environments safer and more secure. This project stands as a testament to the potential of AI-driven solutions in addressing complex security challenges and enhancing operational efficiency.

REFERENCES

[1]. Neha Thotapalli, Raghava Rao Neerukattu, Ravi Kumar Poluru, “A Review On Automated Surveillance System”, 2023 IEEE Engineering Informatics, DOI: 10.1109/IEEECONF58110.2023.10520571

[2]. Ling Hu and Qiang Ni, Senior Member, IEEE, “IoT-Driven Automated Object Detection Algorithm for Urban Surveillance Systems in Smart Cities”, IEEE Internet of Things Journal, DOI 10.1109/JIOT.2017.2705560.

[3]. Jing Wang, Zhijie Xu, “Crowd Anomaly Detection for Automated Video Surveillance”, 6th International Conference on Imaging for Crime Prevention and Detection (ICDP-15), DOI: 10.1049/ic.2015.0102.

[4]. Ahmed Abdelmoamen Ahmed, (Member, IEEE), AND Mathias Echi, “Hawk-Eye: An AI-Powered Threat Detector for Intelligent Surveillance Cameras “, IEEE Internet of Things Journal, DOI: 10.1109/ACCESS.2021.3074319

[5]. C.0 Conaire, N.E.O'Connor, E.Cooke, A.E Smeaton, “MULTISPECTRAL OBJECT SEGMENTATION AND RETRIEVAL IN SURVEILLANCE VIDEO”, Centre for Digital Video Processing, Dublin City University, Ireland, DOI: 10.1109/ICIP.2006.312905