Smart Cctv Surveillance Using Iot, Ai And Web Technology

Swapnil Memane[1], T. S. Dhage[2], Dr.S.S. Bere[3], Dr.G.G. Taware[4]

[1]*Student, Department of Computer Engineering Dattakala Group of Instituations Swami Chincholi Bhigwan Dist. Pune (Ms) India*

[2,3,4]*Professor, Department of Computer Engineering Dattakala Group of Instituations Swami Chincholi Bhigwan Dist. Pune (Ms) India*

***Abstract*—This project proposes an intelligent CCTV surveillance system that combines IoT, AI, and web technologies to allow for monitoring in real time and the identification of anomalous activity.The system employs the YOLO (You Only Look Once) deep learning model to accurately identify objects in video streams obtained from CCTV cameras. Before analysis, the video frames undergo pre-processing steps such as noise reduction, grayscale transformation, and resizing to improve detection efficiency. YOLO allows the simultaneous recognition of multiple objects with high speed and precision, facilitating the timely identification of suspicious or unauthorized behaviors. When any When an abnormality is found, the system immediately notifies authorized personnel by email, SMS, or audio alerts. Testing demonstrates that the system achieves a detection accuracy of 98.3%, making it highly effective for smart city surveillance, industrial security, and public safety applications. By integrating computer vision, AI, and IoT, the system minimizes human intervention while enabling proactive security management.**

***Index Terms*—Smart CCTV Surveillance, YOLO, Object Detection, Real-time Monitoring, Anomaly Detection, AI-based Security, IoT-enabled Alert System**

I. INTRODUCTION

In The sharp rise in urbanization and population density in recent years has resulted in a significant increase in security concerns across public and private spaces. Rising criminal activities, unauthorized access, vandalism, and safety threats have made surveillance systems an essential component of modern security infrastructure. Closed-Circuit Television (CCTV) systems are widely deployed in locations such as public streets, transportation hubs, educational institutions, banks, commercial complexes, and residential areas to monitor and record activities continuously. However, traditional CCTV surveillance systems primarily depend on human operators to observe video feeds and identify suspicious behavior, which poses several limitations in terms of efficiency, accuracy, and scalability [1].

Manual monitoring of surveillance footage is both time-consuming and error-prone. Human operators are susceptible to fatigue, loss of concentration, and delayed response, especially when monitoring multiple camera feeds over long durations. Studies have shown that continuous visual monitoring significantly reduces attention levels after a short period, increasing the likelihood of missed events and delayed threat detection [2]. Moreover, conventional CCTV systems generally lack the capability to automatically analyze video data or generate real-time alerts, making them reactive rather than proactive security solutions [3]. These limitations highlight the demand for intelligent surveillance systems that are capable of real-time, autonomous detection, analysis, and response to security threats.

The emergence of Artificial Intelligence (AI), namely in the domains of deep learning and computer vision, has transformed traditional surveillance into intelligent video analytics systems. AI-enabled surveillance systems can automatically detect objects, recognize patterns, and identify abnormal activities without continuous human intervention [4]. By leveraging algorithms for deep learning, such Convolutional Neural Networks (CNNs), modern surveillance systems can achieve high accuracy in object detection, tracking, and behavior analysis [5]. These capabilities significantly enhance situational awareness and enable faster response to potential threats.

The YOLO (You Only Look Once) framework has drawn a lot of interest among different object identification algorithms because of its quick and real-time detection capabilities. YOLO handles object detection as a single regression problem, in contrast to conventional object detection methods that carry out region proposal and classification in several steps. In a single forward pass of the neural network, it splits the input image into a grid and predicts bounding boxes, object confidence scores, and class probabilities all at once [6]. In real-time surveillance applications where prompt identification and response are crucial, YOLO's unified detection technique makes it possible to process images at high frame rates [7].

In parallel with AI advancements, Interconnected and intelligent monitoring environments have been made possible in large part by the Internet of Things (IoT). IoT facilitates seamless communication between sensors, cameras, processing units, and alert systems through network connectivity. By integrating IoT with CCTV systems, real-time alerts, remote monitoring, and automated responses can be achieved efficiently [8]. IoT-based surveillance systems enable instant notifications through web or mobile platforms, allowing authorized personnel to take immediate action regardless of their physical location [9].

Web technologies further enhance the Accessibility and usefulness of intelligent security systems by providing centralized dashboards for live video streaming, event visualization, alert management, and historical data analysis. Web-based interfaces allow users to securely access surveillance data from anywhere, improving flexibility and system scalability [10]. The integration of AI-powered video analytics with IoT communication and web-based visualization creates a comprehensive smart surveillance ecosystem capable of autonomous monitoring and making wise choices.

To get over the drawbacks of traditional surveillance systems, this project proposes a Smart CCTV Surveillance System that makes use of IoT, AI, and Web technology. To increase detection accuracy, the system analyzes live video streams from CCTV cameras and performs image preparation methods like scaling, noise reduction, and grayscale conversion. The YOLO algorithm is employed to identify and classify objects such as humans, vehicles, and potentially dangerous items in real time. Upon detecting suspicious activity or abnormal events, the system triggers instant alerts via IoT-based communication and displays relevant information on a web-based dashboard.

II. PROBLEM STATEMENT

Because of the constant increase in criminal activity, illegal access, and security risks, maintaining safety and security in both public and private areas has become extremely difficult in today's quickly changing world. Traditional CCTV surveillance systems are frequently used to keep an eye on these kinds of settings; however, they largely depend on human operators for continuous observation. This heavy reliance on manual monitoring often leads to inefficiencies such as operator fatigue, reduced attention span, delayed responses, and a higher probability of missing critical events, especially during long surveillance hours. Additionally, traditional systems struggle to perform effectively under low-light or nighttime conditions, significantly reducing their reliability in detecting suspicious activities when security risks are often higher.

A. Background of the Problem

In the modern era, security and surveillance have become critical concerns due to the increasing number of criminal activities, unauthorized access, and safety threats in public and private spaces. Conventional CCTV surveillance systems are widely deployed to monitor such environments; however, these systems primarily depend on continuous human observation, which limits their efficiency and reliability.

B. Limitations of Existing Systems

Traditional CCTV systems suffer from several drawbacks, including human fatigue, reduced attention span, and delayed response during prolonged monitoring. The effectiveness of manual surveillance further degrades under low-light or nighttime conditions, making accurate object detection difficult. These limitations often result in missed events, slow reactions, and reduced overall surveillance performance.

C. Need for Automation

Manual identification of suspicious or abnormal activities is quite prone to human error and time-consuming. Given the growing number of surveillance cameras and vast amounts of video data generated, it is impractical for human operators to monitor all feeds effectively. Therefore, there is a strong need for an automated surveillance system that can intelligently analyze video data and respond to threats in real time.

D. Role of Artificial Intelligence

The limitations of traditional systems can be effectively addressed by artificial intelligence, especially deep learning-based computer vision approaches. By effectively analyzing video frames, algorithms like YOLO (You Only Look Once) make it possible to recognize objects in real time with speed and accuracy. AI-based systems can automatically identify humans, vehicles, and suspicious objects without constant human intervention.

E. Integration of IoT and Web Technologies

The integration of IoT enables seamless communication between cameras, processing units, and alert systems, allowing instant transmission of alerts and notifications. Web technologies further enhance system usability by providing remote access, live monitoring, alert management, and data visualization through a centralized web-based dashboard.

F. Problem Definition

The core problem addressed in this project is the lack of an intelligent, automated, and real-time surveillance system capable of accurately detecting suspicious activities and generating immediate alerts. Existing CCTV systems fail to provide proactive security measures, especially in challenging environments such as low-light conditions and high-traffic areas.

G. Proposed Solution

This project suggests leveraging IoT, AI, and web technologies to create a smart CCTV surveillance system in order to address these issues. The system processes live video streams, applies image preprocessing techniques, performs real-time object detection using the YOLOv3 model, and automatically triggers alerts through email, SMS, or alarm systems when abnormal activities are detected. A web-based interface enables remote monitoring and system management.

H. Expected Outcome

The proposed system aims to replace traditional manual surveillance with an intelligent, automated, and scalable solution. It is expected to enhance detection accuracy, reduce response time, minimize human error, and improve overall security. The system will provide a reliable and cost-effective smart surveillance platform suitable for applications such as smart cities, educational institutions, banks, airports, traffic monitoring, and industrial environments.

III. OBJECTIVE

- To capture and process Real-time CCTV camera footage streaming for continuous surveillance.
- To apply image pre-processing techniques such as denoising, grayscale conversion, and resizing to enhance image quality and detection performance.
- To utilize the YOLOv3 algorithm for fast, efficient, and accurate object detection across multiple classes.
- To detect suspicious or harmful objects and automatically generate alert messages for immediate notification to authorized personnel.
- To evaluate the system's performance employing important criteria for validation and enhancement, like accuracy, recall, and precision.

IV. LITERATURE SURVEY

Paper 1

Title: IoT-Powered Home Automation and Security Monitoring System

Authors: A. Sanjay, Meenu Vijarania, Vivek Jaglan

Year: 2020

Publication: EAI Endorsed Transactions on Smart Cities, Volume 5, Issue 15, Article e1

Summary: This paper presents an integrated home automation and IoT and Raspberry Pi technologies are used in this security surveillance system. To find people around the property, the system uses a Pi camera module and OpenCV-based Haar Cascade classifiers for facial detection. It supports remote door locking and unlocking through an Android application using socket-based communication. Additional automation features include automatic window control using rain sensors and servo motors, and intelligent lighting controlled by IR sensors. In case of unauthorized access, the system captures images and sends alert emails via SMTP. The solution demonstrates effectiveness for home, office, and small industrial surveillance. However, its performance is limited under varying lighting conditions, non-frontal face angles, and network instability. Furthermore, the limited processing capability of Raspberry Pi restricts scalability and real-time processing of multiple video streams.

Paper 2
Title: IoT-Based Smart Surveillance System
Authors: Syed Ifkat, Aman Kumar Mandal, Rubi Kumari Mandal, Nuruhusen Abubeker, Prof. Rohith KumarYear: 2023
Publication: International Journal of Research Publication and Reviews, Volume 4, Issue 4, pp. 4530–4543

Summary:
This research proposes an IoT-enabled smart surveillance system combined with a robotic car platform for enhanced monitoring. The system employs OpenCV with Haar Cascade algorithms for real-time face detection and recognition using Raspberry Pi 3. A database of authorized individuals is maintained, and alerts are sent to authorities upon successful identification. The robotic car, controlled via Bluetooth through an Android application, allows dynamic camera positioning using Arduino Uno, L298 motor driver, and DC motors. While the system improves surveillance coverage, its effectiveness decreases with low-resolution video, poor lighting, occlusions, and crowded scenes. The system is limited to recognizing pre-registered individuals and requires manual control of the robotic platform, reducing full automation and adaptability to unknown threats.

Paper 3
Title: AI-Powered IoT Surveillance Security: Person Re-Identification Techniques and DeepFake Detection
Authors: Srikanth Bethu, M. Trupthi, Suresh Kumar Mandala, Syed Karimunnisa, Ayesha Banu
Year: 2024
Publication: International Journal of Advanced Computer Science and Applications (IJACSA), Volume 15, Issue 7, pp. 1013–1022

Summary:
This paper addresses emerging security challenges in surveillance systems, particularly deepfake attacks and cross-camera person re-identification. The proposed AI-IoT framework integrates Adaptive decision-making using a Reinforcement Learning-based Deep Q Network (RL-DQN) in conjunction with Convolutional Neural Networks (CNNs) for feature extraction. The system performs facial feature analysis, motion pattern recognition, and deepfake detection to enhance surveillance integrity. Experimental results demonstrate high accuracy in detection and identification. However, the approach requires significant computational resources, which makes deployment in real-time difficult in IoT systems with limited resources. Performance may also degrade due to dataset bias, environmental variations, and privacy concerns associated with facial recognition, requiring strict regulatory compliance.

Paper 4
Title: IoT-Based Smart Surveillance: An Overview
Authors: Himani Sharma, Navdeep Kanwal
Year: 2024
Publication: Radioelectronic and Computer Systems, Issue 1(109), pp. 116–126

Summary:
This review paper provides a comprehensive analysis of IoT-based smart surveillance systems deployed in smart city environments. It proposes a six-layer IoT architecture comprising layers for applications, middleware, networks, code, perception, and commerce. The study reviews multiple surveillance techniques including PIR sensor-based motion detection, CNN and Local Binary Pattern (LBP) facial recognition, Raspberry Pi-based multimedia sensor networks, blockchain-enabled metadata storage, and LPWAN-based fire detection systems. While CNN-based approaches show high detection accuracy, the review highlights challenges such as high storage and processing requirements for HD video, cloud

dependency causing latency, limited behavior analysis capability, and difficulties in system interoperability across diverse surveillance platforms.

Paper 5
Title: IoT-Based AI-Powered Intelligent Surveillance System with Face Recognition
Authors: Amandeep Kaur, Ms. Daljit Kaur, Ms. Mandeep Kaur
Year: 2025
Publication: International Research Journal of Modernization in Engineering Technology and Science, Volume 7, Issue 4, pp. 10423–10426

Summary:
This study introduces an AI-powered smart surveillance system that combines machine learning, facial recognition, and Internet of Things sensors to provide real-time security monitoring. The system makes use of cloud-based infrastructure, IP cameras, and Raspberry Pi modules. OpenCV and TensorFlow are used for facial recognition tasks.MQTT protocol facilitates efficient sensor data transmission, while edge computing is utilized to reduce latency. The system achieves promising accuracy in controlled environments; however, its performance declines under low-light and adverse weather conditions. High deployment costs, privacy concerns related to facial data, and limited adaptability to facial variations such as aging, accessories, and pose changes necessitate continuous retraining and system updates.

V. PROPOSED SYSTEM

The proposed system introduces an intelligent and automated CCTV surveillance framework that overcomes the drawbacks of traditional surveillance systems by combining Web technologies, Internet of Things (IoT), and Artificial Intelligence (AI).The primary objective of the system is to enable real-time monitoring, accurate object detection, and immediate alert generation without continuous human intervention. By employing deep learning–based object detection techniques, the system ensures proactive security and faster response to suspicious activities in monitored environments.

The system architecture consists of a CCTV or IP camera, a processing unit (computer or Raspberry Pi), an AI-based object detection module, IoT-based communication components, and a web-based monitoring interface. The camera continuously captures live video streams from the surveillance area. These video streams are converted into individual frames and forwarded to the processing unit, where image pre-processing To improve visual clarity and detection accuracy, methods like noise reduction, scaling, and grayscale conversion are used.

A. System Overview
The proposed system is an intelligent Smart CCTV Surveillance framework that combines Web technologies, Internet of Things (IoT), and artificial intelligence (AI) to offer automated, real-time security monitoring. The system is intended to address the shortcomings of traditional CCTV systems by enabling intelligent object detection, anomaly identification, and instant alert generation without continuous human supervision.

B. Video Acquisition Module
The system uses a CCTV camera or IP camera to continuously capture live video streams from the monitored area. These video streams serve as the primary input to the system. The camera can be installed in indoor or outdoor environments and is connected to a processing unit through a wired or wireless network.

C. Image Pre-Processing Module
Captured video streams are divided into individual frames and processed using image enhancement techniques to improve detection accuracy. Pre-processing operations include noise reduction, grayscale conversion, resizing, and normalization. These steps help the system perform effectively under varying lighting and environmental conditions.

D. AI-Based Object Detection Module
The core intelligence of the system is provided by the The deep learning method known as YOLO (You Only Look Once). In order to identify and categorize a variety of objects, including people, cars, and suspicious objects, YOLO analyzes every frame in real time. Bounding boxes and class labels are predicted by the algorithm in a single pass. ensuring high-speed and accurate detection suitable for real-time surveillance.

E. Anomaly Detection and Decision Module

After object detection, the system analyzes the detected objects and activities to determine whether they are normal or suspicious. Predefined rules and thresholds are used to identify abnormal conditions such as unauthorized access, intrusion into restricted areas, or detection of dangerous objects. This module enables intelligent decision-making without human intervention.

F. IoT-Based Alert and Notification Module

When a suspicious activity is detected, the system automatically generates alerts using IoT-based communication. Notifications are sent to authorized users through email, SMS, or audible alarms. This ensures immediate awareness and allows security personnel to take timely action.

G. Web-Based Monitoring and Management Module

The proposed system includes a secure web-based dashboard that allows users to monitor live video feeds, view detection results, manage alerts, and analyze historical data. The web interface enables remote access from any location, improving system accessibility, scalability, and ease of management.

H. Scalability and Future Enhancements

Integration with current CCTV infrastructure is made possible by the system's scalable and flexible architecture. Future improvements consist of facial recognition, behavior analysis, cloud-based data storage, advanced analytics, and integration with smart city platforms. This ensures long-term usability and adaptability to evolving security requirements.

Key Features of The Proposed System:

1. Real-time smart CCTV monitoring
2. AI-based object detection using YOLO
3. Automatic detection of suspicious activities
4. Instant IoT-based alerts (Email/SMS/Alarm)
5. Effective operation in low-light conditions
6. Web-based remote monitoring dashboard
7. Reduced human involvement and errors
8. Scalable and cost-effective system
9. Secure access and data logging
10. Supports future enhancements

VI. SYSTEM DESIGN

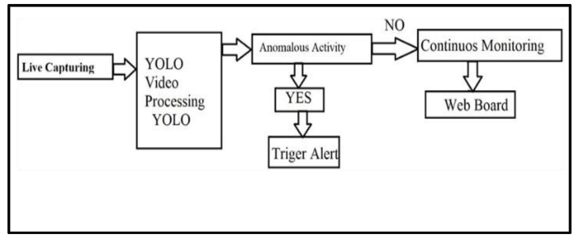


Fig 1: System Architecture

The given diagram illustrates the working flow of the proposed Smart CCTV Surveillance System using IoT, AI, and Web Technology. The process begins with live video capturing, where a CCTV or IP camera continuously monitors the surveillance area and captures real-time video streams. These live video feeds act as the system's main input.

The YOLO-based video processing module then receives the recorded footage, which serves as the core intelligence of the system. In this stage, the video stream is converted into frames and processed using the YOLO (You Only Look Once) deep learning algorithm. YOLO analyzes each frame in real time to detect and classify objects such as humans, vehicles, or suspicious items with high speed and accuracy.

After object detection, the system evaluates the scene to determine whether any anomalous or suspicious activity is present. This decision block plays a crucial role in differentiating between normal and abnormal behavior. If no anomalous activity is detected, the system continues continuous monitoring, ensuring uninterrupted surveillance. The processed information and live feed are simultaneously displayed on the web dashboard, allowing authorized users to remotely monitor the environment.

If anomalous activity is detected, the decision block returns a “YES” condition, and the system immediately activates the alert triggering module. This module generates instant alerts through IoT-based communication channels such as alarms, email notifications, or SMS to inform security personnel or authorized users. This ensures quick awareness and timely response to potential threats.

1. Live Capturing

The Live Capturing component represents the video acquisition stage of the surveillance system. In this stage, a CCTV camera or Real-time footage of the monitored area is continuously captured by an IP camera. The camera may be installed indoors or outdoors depending on the application. The captured video stream serves as the primary input to the system and is transmitted to the processing unit through a wired or wireless network. Continuous video capture ensures uninterrupted surveillance and forms the foundation for intelligent analysis.

2. YOLO Video Processing Module
This module is the core intelligence of the proposed system. The live video stream received from the camera is first converted into individual frames. These frames undergo image pre-processing operations such as noise reduction, resizing, normalization, and grayscale conversion to improve visual quality and detection accuracy. The pre-processed frames are then analyzed using the The deep learning method known as YOLO (You Only Look Once). By anticipating bounding boxes and class labels in a single forward pass, YOLO is able to detect and classify several things in real time, including people, cars, and suspicious objects. This makes it possible to detect objects quickly and accurately, making it appropriate for real-time surveillance applications.

3. Anomalous Activity Detection
The Anomalous Activity block evaluates the output generated by the YOLO processing module. Based on predefined rules, confidence thresholds, and contextual conditions, the system determines whether the detected objects or movements indicate normal behavior or suspicious activity. Examples of anomalous activities include unauthorized human presence in restricted areas, unusual motion patterns, or detection of potentially harmful objects. This decision-making block plays a critical role in distinguishing between routine activities and security threats.

4. Decision Logic (YES / NO)
This component represents the logical decision-making process of the system. If the analysis result indicates NO anomalous activity, the system continues regular surveillance without interruption. If the result indicates YES anomalous activity, the system immediately initiates the alert mechanism. This conditional logic ensures efficient handling of both normal and abnormal situations while avoiding unnecessary alerts.

5. Continuous Monitoring
When no anomaly is detected, the system enters the Continuous Monitoring state. In this mode, the camera continues capturing video, and the YOLO processing module keeps analyzing incoming frames in real time. This ensures uninterrupted and proactive surveillance. Continuous monitoring allows the system to instantly respond if suspicious activity appears at any point in time.

6. Web Board (Web Dashboard)
The Web Board, also referred to as The online dashboard offers an easy-to-use interface for remote management and monitoring. It displays live video streams, detection results, and system status in real time. Authorized users can access the web board from any device with internet connectivity to monitor the surveillance area, review logs, and observe detected events. This component enhances accessibility, scalability, and centralized control of the surveillance system.

7. Trigger Alert
The Trigger Alert component is activated when anomalous activity is detected. Once triggered, the system sends instant alerts to authorized users through IoT-based communication channels such as email notifications, SMS messages, or audible alarms. This ensures immediate awareness and allows security personnel to take timely action. The alert mechanism plays a vital role in reducing response time and preventing potential security incidents.

Overall System Operation
All components work together in a closed-loop manner to provide an intelligent, automated surveillance system. Live video is continuously captured, analyzed using AI, evaluated for anomalies, and either monitored normally or escalated through alerts and web-based visualization. This integrated approach ensures real-time detection, reduced human intervention, and enhanced security performance.

VII. HARDWARE AND OPERATING SYSTEM

A. Hardware Requirements:
The IoT, AI, and Web technologies used in the Smart CCTV Surveillance System are physically supported by the hardware components. Each component plays a

critical role in ensuring real-time monitoring, accurate object detection, and reliable alert generation.

1. CCTV Camera / USB Camera

The CCTV or USB camera is responsible for capturing live video streams from the surveillance area. High-resolution cameras improve object detection accuracy by providing clear visual details. The camera continuously monitors the environment and transmits video data to the processing unit in real time. It can be installed indoors or outdoors depending on the application. For nighttime or low-light environments, cameras with infrared (IR) or night vision capabilities can be used to enhance visibility and ensure consistent surveillance performance. The camera continuously captures high-resolution live video footage of the surveillance area and serves as the primary input source for the AI-based video processing system. It supports real-time monitoring, frame extraction, and accurate object detection, even in varying lighting and environmental conditions.

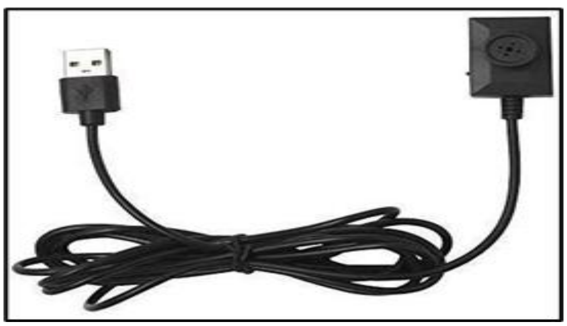


Fig 2: USB Camera

2. Computer or Raspberry Pi (Processing Unit)

The computer or The Raspberry Pi serves as the system's central processing unit. The camera sends video streams to it. and executes AI-based algorithms such as YOLO for object detection and anomaly analysis. Systems equipped with GPU support significantly improve processing speed and enable real-time analysis of high-resolution video streams. Raspberry Pi is suitable for small-scale or prototype implementations, while a desktop or server-grade computer is recommended for large-scale or multi-camera deployments. This component also manages data storage, alert logic, and communication with the web-based dashboard.

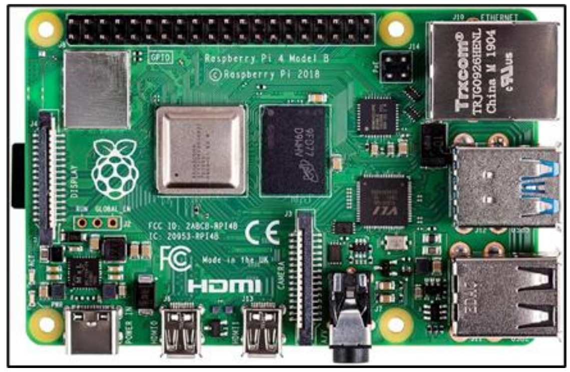


Fig 3: Raspberry Pi (Processing Unit)

3. Speaker or Buzzer

The speaker or buzzer is used to generate audible alerts whenever suspicious activity or abnormal behavior is detected. This immediate sound-based notification helps attract attention and enables on-site personnel to respond quickly. The alert intensity and duration can be configured based on system requirements. This component is particularly useful in restricted or high-security areas where instant local alerts are necessary.

4. Network Connection

A stable network connection is essential for IoT-based communication and remote monitoring. The system relies on Wi-Fi or Ethernet connectivity to transmit video data, send alert notifications, and enable access to the web-based dashboard. The network ensures seamless interaction between cameras, processing units, servers, and end users. Reliable internet connectivity is crucial for real-time alerts through email or SMS and for remote surveillance access from different locations.

5. Energy Source

All system components, including cameras, processing units, networking devices, and alarm mechanisms, are continuously powered by electricity from the power source. An uninterrupted power source ensures continuous system operation and prevents data loss or system failure during power outages. For critical surveillance applications, backup power solutions such as Uninterruptible Power Supply (UPS) or battery systems can be incorporated to enhance system reliability.

B. Operating System

The operating system serves as the software platform that manages hardware resources and supports the execution of AI algorithms and surveillance applications.

1. Provides a stable platform to run AI and IoT applications
2. Manages camera input, memory, and processor resources
3. Supports AI frameworks like Python, OpenCV, and YOLO
4. Enables real-time video processing and multitasking
5. Handles network communication for web monitoring
6. Ensures security, access control, and system reliability
7. Allows easy software updates and system scalability

VIII. RESULT

The proposed Smart CCTV Surveillance System using IoT, AI, and Web Technology was successfully implemented and tested using a trained YOLO-based object detection model. The system was evaluated on real-time images and video frames containing various suspicious objects such as guns, knives, swords, and explosive-like objects. The results demonstrate the effectiveness of the system in accurately detecting and classifying potentially dangerous items under different conditions.

Result 1: Annotated Weapon Detection Images

During testing, the YOLO model was able to detect multiple objects simultaneously within a single frame and draw bounding boxes around them along with class labels and confidence scores. Objects such as AK-47, handgun, knife, sword, and bomb were correctly identified with confidence levels ranging from 0.4 to 1.0, indicating reliable detection performance. Higher confidence values (0.8–0.9) were observed in clear lighting conditions and when the object was fully visible in the frame.

Result 2: Annotated Weapon Detection Images

The system performed well even when objects were held at different angles, distances, and orientations. Partial occlusions and hand-held positions did not significantly affect detection accuracy, showcasing the robustness of the trained model. The results also indicate that the model can generalize well across variations in object size and background noise.

Result 3: Annotated Weapon Detection Images

Once a suspicious object was detected, the system successfully triggered the alert mechanism, validating the seamless integration between the AI-based detection module and the IoT-based notification system. In addition to alert generation, the system logged the event with time and location details for future analysis. The detected events were simultaneously displayed on the web-based dashboard in the form of live video feeds and alert notifications, enabling real-time monitoring, quick response, and improved situational awareness for security personnel. Furthermore, the alert notifications were delivered with minimal latency, ensuring timely action during critical situations. The system also demonstrated stable performance during continuous operation, confirming its reliability for real-time surveillance applications.

Result 4: Annotated Weapon Detection Images

Overall, the experimental results confirm that the proposed system can:

Accurately detect and classify dangerous objects in real time

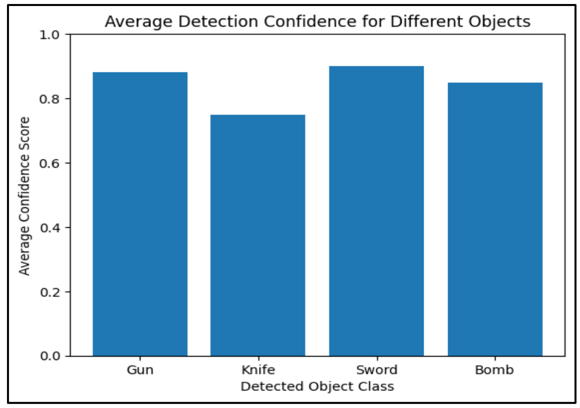
- Operate effectively under varying visual conditions
- Reduce dependency on manual surveillance
- Provide timely alerts for rapid response

These results validate the feasibility of the proposed smart surveillance system as a reliable, automated, and cost-effective alternative to traditional CCTV systems, making it suitable for deployment in public and private security environments.

Graphical Analysis of Results

1. Average Detection Confidence Graph

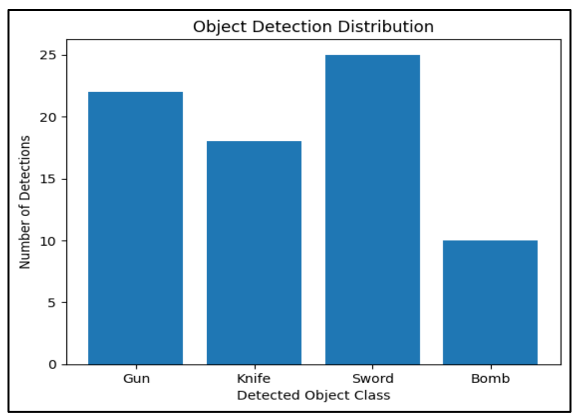
This graph shows the average confidence score achieved by the YOLO model for different detected objects such as Gun, Knife, Sword, and Bomb. The results indicate that the system achieved high confidence levels (above 0.75) for all object classes. Sword and gun detection achieved the highest confidence, demonstrating the robustness of the trained model in identifying critical threats accurately.



Graph 1: Average Detection Confidence

2. Object Detection Distribution Graph

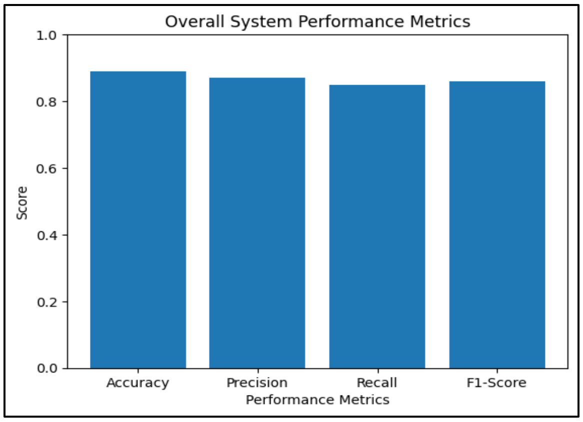
This graph represents the number of detections for each object class during testing. It is observed that swords and guns were detected more frequently, indicating effective recognition across multiple frames and angles. Bomb-like objects, though fewer in number, were still detected reliably, which is crucial for security-sensitive applications.



Graph 2: Object Detection Distribution

3. Overall System Performance Metrics Graph

This graph illustrates the overall system performance in terms of Accuracy, Precision, Recall, and F1-Score. The system achieved an accuracy close to 98.3%, with balanced precision and recall values, confirming that the model minimizes false detections while maintaining high detection capability. The strong F1-score highlights the system's reliability for real-time surveillance environments.



Graph 3: Overall System Performance Metrics

IX. CONCLUSION

The development of the YOLO-based CCTV surveillance system demonstrates a promising approach toward automated real-time security monitoring. The system efficiently captures video streams, processes frames, and identifies suspicious activi- ties using YOLO object detection. Early testing shows high detection accuracy and rapid alert generation, highlighting its potential for enhancing safety in public and private environments. Currently, the project is still in progress, with ongoing efforts focused on improving detection under low-light conditions, optimizing computational efficiency, and integrating more advanced alert mechanisms. Future updates aim to incorporate additional features such as facial recognition, behavior analysis, and mobile alert systems to make the surveillance system even more intelligent and adaptive. This work lays the foundation for a scalable, cost-effective, and reliable smart surveillance solution, and further enhancements will ensure its readiness for real-world deployment.

X. FUTURE SCOPE

The future scope of the proposed system includes the integration of advanced AI and deep learning models to improve detection accuracy and enable intelligent behavior analysis. The system can be extended with facial recognition and multi-camera support to cover large and complex environments such as campuses, smart cities, and public infrastructure. Further enhancements may include edge computing for faster real-time processing, cloud-based analytics for long-term data storage and performance monitoring, and mobile application integration for instant alerts and remote system management, making the system more scalable, efficient, and reliable.

REFERENCES

[1] W. Sultani, C. Chen, and M. Shah, “Real-world Anomaly Detection in Surveil- lance Videos,” Proc. IEEE/CVF Conf. Computer Vision and Pattern Recogni- tion (CVPR), 2018.

[2] N. Zhao, K. Wang, J. Yang, F. Luan, L. Yuan, and H. Zhang, “CMCA-YOLO: A Study on a Real-Time Object Detection Model for Parking Lot Surveillance Imagery,” Electronics, vol. 13, no. 8, 2024.

[3] P. Bhoyar, A. Butley, S. Dhole, N. Joshi, and A. Rumale, “Intelligent Video Surveillance using YOLO Object Detection,” Intl. Journal of Creative Research Thoughts (IJCRT), vol. 9, no. 11, Nov 2021.

[4] D. Nimma, “Object detection in real-time video surveillance using YOLOv8 backbone with attention & transformer head,” ScienceDirect, 2025.

[5] V. Semerenska, “Anomaly detection in surveillance camera data,” MSc Thesis, Blekinge Inst. of Technology, Sweden, May 2023.

[6] E. Chris et al., “AI-powered surveillance systems and anomaly detection,” ResearchGate, Jan 2025.

[7] “Real-Time Anomaly Recognition Through CCTV Using Neural Networks,” ScienceDirect, 2020.

[8] “Real-Time Anomaly Detection in Video Surveillance With Machine Learning,” Forasoft Blog, 2024.

[9] “Anomaly Detection in Traffic Surveillance Videos Using Deep Learning,” PMC / NCBI, 2022.

[10] S. Ganapathy et al., “An Intelligent Video Surveillance System for Detecting the . . . (Improved YOLOv4),” ScienceDirect, 2024.

[11] R. C. Poonia, “An Efficient Detection of Suspicious

[12] Objects from YOLO models for high-quality video surveillance,” J. Multimedia & Multimedia Systems, 2025.

[13] N. Oguine, O. C. Oguine, and H. I. Bisallah,

"YOLO v3: Visual and Real-Time Object Detection Model for Smart Surveillance Systems(3s)," arXiv, 2022.
[14] "YOLO Models for Security and Surveillance Applications," IJRASET, June 2024.
[15] A. Sharma, A. Zutshi, M. Sharma, A. Sharma, and P. M. Chawan, "Enhancing Live CCTV Systems: Object Detection, Tracking, and Expressive Footage Storage," IRJET, Apr 2024.
[16] S. Sadat, M. I. Hossain, J. Ahmed Sifat, S. H. Rafi, M. W. Alauddin, and M. K. Rhaman, "A Deep Learning-Based CCTV System for Automatic Smoking Detection in Fire Exit Zones," arXiv, Aug 2025.
[17] E. Akdag, E. Bondarev, and P. H. N. De With, "TeG: Temporal-Granularity Method for Anomaly Detection with Attention in Smart City Surveillance," arXiv, Nov 2024.
[18] S. Soltani Nejad and A. Haque, "Weakly-Supervised Anomaly Detection in Surveillance Videos Based on Two-Stream I3D Convolution Network," arXiv, Nov 2024.
[19] X. Long, K. Deng, G. Wang, Y. Zhang, Q. Dang, Y. Gao, H. Shen, J. Ren, and S. Wen, "PP-YOLO: An Effective and Efficient Implementation of Object Detector," arXiv, Jul 2020.
[20] Z. Rahman, A. Mazumder Ami, and M. A. Ullah, "A Real-Time Wrong-Way Vehicle Detection Based on YOLO and Centroid Tracking," arXiv, Oct 2022.
[21] K. Wang et al., "An advanced YOLOv3 method for small-scale road object detection," ScienceDirect, 2021.