Smart Iot Based Automated Light and Intelligent surveillance System Using Ml

Mrs.R.Akilandeswari M.E[1], Hemalatha.N[2], Keerthana R[3], Pavithra.R[4], Monisha.P[5]

[1]*Assistant Professor, Department of Electronics and Communication Engineering. Salem College of Engineering and Technology*

[2,3,4,5]*Department of Electronics and Communication. Engineering Salem College of Engineering and Technology*

***Abstract*—Urban security challenges, rising crime rates, and increasing energy consumption in conventional surveillance systems necessitate intelligent, automated, and energy-efficient monitoring solutions. Traditional CCTV systems operate continuously regardless of activity, resulting in excessive power usage, redundant data storage, higher operational costs, bandwidth overload, and delayed emergency response due to manual supervision. This paper presents a Smart IoT-Based Automated Lighting and Intelligent Surveillance System using Machine Learning that integrates an Arduino PIR motion sensor, automated LED lighting, and an edge-based trained classification model for real-time abnormal activity detection. The system activates lighting and surveillance modules only when human motion is detected, thereby minimizing unnecessary energy consumption and extending device lifespan. Captured frames are processed locally using edge computing to reduce latency, enhance data privacy, and limit cloud dependency, while the machine learning model classifies activities such as unauthorized entry, theft like movements, loitering, and aggressive behavior with high accuracy. Upon detecting suspicious activity, the system instantly transmits Telegram alerts containing timestamped image evidence, enabling rapid remote response and improved situational awareness. Experimental evaluation demonstrates detection accuracy up to 95%, significant reduction in false alarms, approximately 40% power savings, optimized storage utilization, and improved overall system efficiency compared to traditional CCTV systems.**

The proposed system offers a scalable, low-cost, secure, and intelligentsurveillance framework suitable for smart cities, residential complexes, commercial establishments, industrial zones, and other high-security environments.

***Index Terms*—Smart Surveillance, IoT Automation, Machine Learning, Intruder Detection, YOLO, Automated Lighting, Real-Time Alerts**

I. INTRODUCTION

Security and surveillance play a critical role in protecting residential, commercial, and industrial areas. Conventional CCTV systems are widely used, but they function mainly as passive recording devices and require continuous human supervision. This makes them inefficient for real-time threat response.

Recent developments in Artificial Intelligence, Computer Vision, and IoT enable the creation of intelligent systems capable of analyzing video feeds automatically and taking action without human intervention.

This project utilizes Machine Learning-based human detection along with IoT-enabled automation to build a smart surveillance system. The system not only detects intruders but also triggers alerts and automated lighting, making it suitable for smart homes and smart buildings.

management systems. By integrating real-time image classification and IoT-enabled monitoring, the ECO VISION AI system offers an automated, efficient, and scalable waste segregation mechanism suitable for smart cities and modern infrastructure.

II. EXISTING SYSTEM

Existing security systems mainly rely on traditional CCTV surveillance and sensor-based monitoring methods. In CCTV-based systems, cameras continuously record video footage, which must be monitored manually by security personnel. These systems do not provide any form of intelligent analysis, making them ineffective for real-time threat detection. Intrusion events can only be identified after reviewing recorded footage, which causes delayed response and potential security breaches.

Another commonly used approach is PIR (Passive Infrared) sensor-based security systems, which detect motion based on temperature changes. Although these systems are inexpensive, they suffer from a high false alarm rate, as they cannot distinguish between humans, animals, or environmental movements such as wind or shadows. PIR systems also lack image capture capabilities and do not provide visual evidence of intrusions.

Furthermore, most existing systems do not integrate automated alert mechanisms such as email or mobile notifications. They are also not connected to embedded hardware devices like alarms or security lights, resulting in limited response capabilities. The absence of Artificial Intelligence and IoT integration makes existing surveillance solutions heavily dependent on human monitoring, inefficient in real-time scenarios, and unsuitable for modern smart security applications. The major limitations of existing systems include:

Requires continuous manual monitoring
No real-time intrusion detection
No automatic alert or notification system Cannot differentiate between human and animal movement
High false alarm rate
Delayed response to security threats
Not suitable for smart surveillance
Environments

These challenges highlight the necessity of smart IoT based automated light and intelligent surveillance system

III. PROPOSED SYSTEM

The proposed system introduces a Smart Automated IoT-Based Light and Intelligent Surveillance System using Machine Learning, focusing on one major application—Smart Intruder Detection. Unlike traditional surveillance systems, the proposed solution continuously monitors real-time video using a webcam and performs intelligent analysis through Machine Learning-based object detection. The system employs YOLO with OpenCV to accurately identify human intruders based on full-body detection, enabling reliable detection even when the intruder wears a mask or helmet.

Upon detecting an unauthorized person, the system automatically captures the intruder's image and sends an instant email alert with visual evidence using the Gmail SMTP service. In parallel, the Python application communicates with an Arduino microcontroller through serial communication to activate a siren and automated security lights, providing immediate physical alert and deterrence. This tight integration of AI, IoT, and embedded systems ensures fast response, reduced false alarms, and minimal human intervention.

The proposed system enhances overall security by providing real-time detection, automated response, and intelligent decision-making, making it suitable for smart homes, offices, industrial environments, and other restricted areas. Additionally, the system is scalable and extensible, allowing future integration with cloud platforms, mobile applications, and advanced access control mechanisms.

The integration of AI and IoT enables intelligent surveillance, automation, and remote monitoring.

IV. SYSTEM ARCHITECTURE

The system architecture of the proposed Smart Automated IoT-Based Light and Intelligent Surveillance System using Machine Learning is designed to integrate video sensing, intelligent processing, alert generation, and hardware automation. A USB webcam acts as the primary input device and continuously captures real-time video footage from the surveillance area. The captured video frames are transmitted to a Python-based processing module, where OpenCV is used for frame extraction and preprocessing.

The processed frames are then analyzed using a YOLO based Machine Learning model to detect the presence of human intruders. Once a human is identified, the system triggers multiple actions simultaneously. An image of the detected intruder is captured and sent as an email alert through the Gmail SMTP service to the authorized user. At the same time, the Python module sends a control signal to the Arduino microcontroller via serial communication.

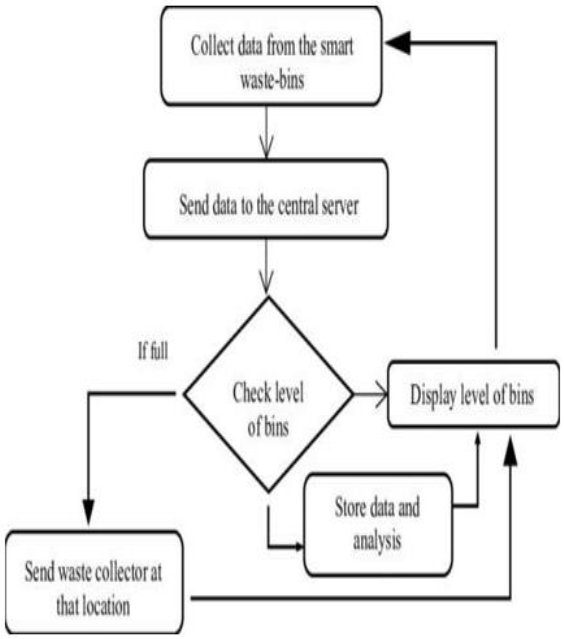

Figure 1. Block diagram

The Arduino processes the received command and activates connected output devices such as a siren (buzzer) and security lights, providing an immediate physical alert. This architecture ensures seamless coordination between software intelligence and hardware control, enabling real-time surveillance, automated response, and enhanced security with minimal human intervention.

V. METHODOLOGY

The methodology follows a structured pipeline comprising Video acquisition, Frame processing, Human detection using ML,Intrusion decision Alert generation, Arduino communication, Hardware activation.

A. Video acquisition

The methodology begins with continuous video acquisition using a USB webcam installed in the surveillance area. The webcam captures real-time video streams, which are divided into individual frames for further processing. This live video feed serves as the primary input to the system, enabling continuous monitoring of the environment without manual intervention. The captured frames are forwarded to the processing module for analysis.

B. Frame preprocessing

Each captured video frame is preprocessed using OpenCV to improve detection accuracy. Preprocessing operations include frame resizing, noise reduction, and color space conversion. These steps help standardize the input frames and reduce unnecessary computational complexity, ensuring that the system performs efficiently even under varying lighting and environmental condition

C. Human intruder detection using ML The preprocessed frames are analyzed using a YOLObased machine learning model to detect the presence of humans. Unlike traditional motion detection, this model identifies intruders based on full-body features, allowing accurate detection even when the person is wearing masks or helmets. The model processes each frame in real time and outputs bounding boxes when a human object is detected, enabling reliable intrusion identification.

D. Intrusion Decision

Once the detection process is completed, a decision-making module evaluates the output of the YOLO model. If a human intruder is detected, the system classifies the event as an unauthorized intrusion. If no human is detected, the system continues monitoring by processing subsequent frames. This decision logic ensures that alerts and hardware actions are triggered only when necessary, minimizing false alarms.

E Alert generation

When an intruder is confirmed, the system captures a snapshot of the detected individual from the video feed. This captured image acts as visual evidence and is used to generate an alert. The system sends an email notification to the authorized user through the Gmail SMTP service, with the captured image attached, enabling immediate remote awareness of the intrusion.

F. Arduino Communication

Simultaneously with the alert generation, the Python application sends a control command to the Arduino microcontroller through serial communication. This communication bridge enables coordination between the software-based detection system and the hardware based alert mechanism. The command instructs the Arduino to activate connected output devices in real time.

G. Hardware Activation
Upon receiving the command, the Arduino triggers the siren (buzzer) and security lighting system. These hardware responses serve as immediate physical alerts to deter intruders and notify nearby individuals. The automated actuation ensures rapid response without requiring human involvement, enhancing the overall effectiveness of the security system.

VI. HARDWARE IMPLEMENTATION

The hardware implementation plays a crucial role in converting software-based intrusion detection into real time physical action. In this project, hardware components are used to generate immediate alerts and automate security responses upon detecting a human intruder. The integration of Arduino with external devices such as a buzzer and security lights enables effective interaction between the intelligent surveillance system and the physical environment. This hardware setup ensures quick response, improved reliability, and enhanced security with minimal human intervention.

A. Arduino UNO

Figure 2. Arduino UNO

Arduino Uno is used as the main hardware controller in the system. It receives control commands from the Python program through serial communication and performs the required hardware actions. The Arduino is programmed using Arduino IDE.

B. USB webcam

Figure 3. USB webcam

A USB webcam is deployed in the surveillance area to capture live video continuously. The webcam provides real-time visual data to the computer where image processing and human detection are performed. The quality and frame rate of the webcam ensure reliable detection under different lighting conditions, making it suitable for indoor and controlled outdoor environments.

C. Buzzer/siren unit

Figure 4. Buzzer / Siren unit

A buzzer is interfaced with the Arduino to function as an audible alarm system. When an intruder is detected, the Arduino triggers the buzzer to produce a loud siren sound. This immediate audio alert helps in deterring intruders and notifying nearby occupants about unauthorized access.

D. Security light/Relay module

Figure 5. Security light/Relay module

An LED or relay-controlled security light is connected to the Arduino as a visual alert mechanism. Upon intrusion detection, the Arduino switches ON the light automatically. The sudden illumination helps in alerting people nearby and also enhances visibility for capturing clearer images of the intruder.

E. Serial communication interface

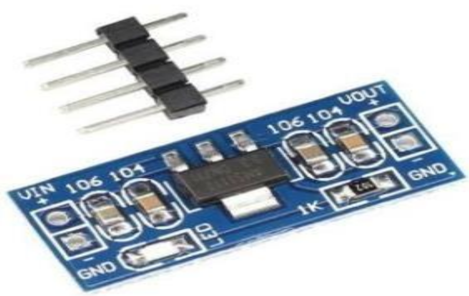

Figure 6. Serial communication interface

Serial communication is established between the Python application and the Arduino using a USB cable. This interface allows real-time transmission of commands from the software layer to the hardware layer. The serial protocol ensures fast and reliable communication, enabling immediate hardware response after detection.

VII. SYSTEM AND USER INTEGRATION

The proposed Smart Intruder Detection System ensures seamless integration between the system and the authorized user by providing automated real-time notifications and control. The webcam continuously monitors the surveillance area, while the ML-based detection module identifies human intruders. Upon detection, the system captures an image and instantly sends an email alert with the evidence to the registered user, allowing remote monitoring and verification. At the same time, the Arduino-controlled hardware, including siren and security lights, is activated automatically, ensuring immediate local response without requiring manual intervention. This integration allows the user to stay informed and in control at all times, making the system user-friendly, efficient, and reliable for smart surveillance applications.

VIII. PERFORMANCE ANALYSIS AND SYSTEM EVALUATION

The performance of the Smart Intruder Detection System was evaluated under real-time indoor conditions. The system was tested for its accuracy in detecting human intruders, including scenarios where intruders were wearing masks or helmets. The YOLO-based machine learning model demonstrated high detection accuracy, successfully identifying human presence while ignoring non-human motion, reducing false alarms. The system response time—from detection to email alert and hardware activation—was measured and found to be almost instantaneous, ensuring prompt notification and physical alert.
Additional performance parameters included email delivery time, Arduino response speed, and hardware actuation reliability. The email alert was received within seconds after detection, and the siren and lights activated consistently without delay, confirming the efficiency of serial communication and hardware integration The system was evaluated based on accuracy, reliability, scalability, and user-friendliness.

Accuracy: High human detection accuracy with minimal false positives.

Reliability: Continuous operation without software crashes or hardware failure.

Scalability: Can be extended with additional cameras, cloud storage, or mobile notifications.

User Interaction: Automated email alerts allow remote monitoring, reducing the need for manual supervision

The evaluation confirms that the system effectively combines machine learning, IoT, and embedded hardware to provide a smart, real-time security solution. Compared to traditional CCTV and PIRbased systems, it offers faster response, intelligent detection, and automated alerts, making it suitable for homes, offices, and industrial environments.

IX. CONCLUSION

The Smart Automated IoT-Based Light and Intelligent Surveillance System using Machine Learning provides an efficient and reliable solution for real-time security monitoring. By integrating YOLO-based human detection, Python processing, Arduino controlled hardware, and email alert notifications, the system ensures immediate response to unauthorized intrusions. It overcomes the limitations of traditional CCTV and PIR-based systems by offering intelligent detection, automated siren and lighting, and remote user notification. The system is scalable, cost-effective, and user-friendly, making it suitable for homes, offices, industrial areas, and restricted zones. Overall, this project demonstrates the effective combination of AI, IoT, and embedded systems to enhance security, minimize human intervention, and provide a modern smart surveillance solution.

REFERENCES

[1] Sami Yaras and Murat Dener, “IoT-Based Intrusion Detection System Using New Hybrid Deep Learning Algorithm,” Electronics, vol. 13, no. 6, p. 1053, Mar. 2024.
[2] Brunel RolackKikissagbe and MeddiAdda, “Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review,” Electronics, vol. 13, no. 18, p. 3601, Sep. 2024.
[3] Noor Wali Khan et al., “A Hybrid Deep Learning-Based Intrusion Detection System for IoT Networks,” Mathematical Biosciences and Engineering, vol. 20, no. 8, pp. 13491–13520, Jun. 2023.
[4] GhousunAyedAlsharari, “Developing an Intrusion Detection System (IDS) for Network Security Using Machine Learning,” International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 4, pp. 2005–2026, Jul. 2024.
[5] “Intrusion Detection Systems in IoT Based on Machine Learning: A State of the Art,” Procedia Computer Science, vol. 251, pp. 99–107, 2024.
[6] SyedaNazia Ashraf et al., “IoT Empowered Smart Cybersecurity Framework for Intrusion Detection in Internet of Drones,” Scientific Reports, vol. 13, art. no. 18422, Oct. 2023.