International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 01 | Jan - 2026 SJIF Rating: 8.586 ISSN: 2582-3930

AI Based Threat Detection System

Harsh, Vedant, Moiz, Rohit, Guide By:- Mrs. Hiral Patel
Electronics and Computer Science, St. John College of Engineering & Management

ABSTRACT
The increasing incidence of robbery, physical violence, and weapon misuse in public and private environments highlights the limitations of conventional CCTV-based surveillance systems that rely heavily on human monitoring. This paper presents the design and implementation of an AI-powered IoT-based intelligent surveillance system capable of real-time threat detection. The proposed system integrates low-cost ESP32-CAM and NodeMCU modules for image acquisition with a lightweight Convolutional Neural Network (CNN) optimized using TensorFlow Lite for efficient edge inference. The system detects suspicious activities such as robbery, physical fighting, and weapon presence, and sends real-time alerts through an Android application using Firebase services. The proposed solution is cost-effective, scalable, and suitable for deployment in banks, educational institutions, offices, and public areas.

INTRODUCTION
Rapid urbanization and the increasing density of people in public and private spaces have led to a noticeable rise in security related incidents such as robbery, physical assault, and weapon misuse. Locations including banks, educational institutions, office premises, commercial complexes, and public areas are particularly vulnerable. While Closed-Circuit Television (CCTV) systems are widely deployed to address these concerns, traditional surveillance solutions primarily function as passive recording tools. They rely heavily on human operators to continuously monitor live video feeds or review footage after an incident has already occurred. This dependence on manual vigilance makes conventional systems prone to fatigue, delayed responses, and missed critical events, thereby limiting their effectiveness in real-time threat prevention. Recent advances in Artificial Intelligence (AI), computer vision, and Internet of Things (IoT) technologies have opened new possibilities for transforming passive surveillance into proactive and intelligent security systems. By embedding intelligence into Page 1 of 3 cameras and edge devices, it is now feasible to automatically analyze visual data, detect abnormal or suspicious activities, and generate alerts without continuous human supervision. In particular, Convolutional Neural Networks (CNNs) have demonstrated strong performance in recognizing complex visual patterns such as human actions, violent behavior, and the presence of weapons. This project introduces an AI-powered, edge-assisted surveillance system that integrates low-cost IoT camera modules such as ESP32-CAM and NodeMCU with a lightweight CNN model deployed using TensorFlow Lite (TFLite). The system is designed to perform real-time or near- real-time inference on captured image frames to identify suspicious activities including fighting, robbery, and weapon carrying. An Android-based application serves as the primary user interface, providing live system status, alert notifications, and incident details to authorized users. To ensure secure, scalable, and real-time data handling, Firebase Authentication is used for role-based access control, while Firebase Realtime Database enables instant synchronization of detection results, alerts, and device health information across multiple users and locations. The proposed architecture emphasizes affordability, scalability, and ease of deployment, allowing institutions to start with a minimal setup and expand seamlessly as requirements grow.

PROBLEM STATEMENT
The rapid advancement of cyber threats has revealed major shortcomings in conventional security approaches, including signature-based intrusion detection and rule-driven defense systems, which are often ineffective against novel, complex, and zero-day attacks in real time. Recent research shows that Artificial Intelligence (AI) and Machine Learning (ML) methods can substantially enhance detection accuracy and enable more adaptive responses; however, their real-world adoption remains challenging. Key issues include managing high-dimensional and highly imbalanced security datasets, poor model interpretability, vulnerability to adversarial attacks, limited ability to generalize across heterogeneous environments, and difficulties integrating with legacy systems. In addition, the current body of literature lacks a standardized evaluation framework and offers insufficient analysis of the trade-offs between detection effectiveness and operational feasibility. These gaps impede progress toward developing scalable, robust, and explainable

AI-driven cybersecurity solutions. This review paper therefore seeks to systematically examine recent AI-based threat detection techniques, assess their advantages and shortcomings, and highlight open research challenges to inform future developments in intelligent and resilient cybersecurity systems.

LITERATURE SURVEY

Surveillance systems increasingly rely on deep learning rather than pure human monitoring to identify threats like violence and weapons. In late 2021, Bhatti, Khan, Aslam, and Fiaz published "Weapon Detection in Real-Time CCTV Videos using Deep Learning" in IEEE Access. They built a CNN-based detector capable of identifying weapons like handguns in live CCTV streams, and highlighted persistent challenges such as false positives under varying lighting and low resolution, underscoring the need for optimized models for real environments.

Moving into 2023, the field saw a notable push toward fast and efficient violence detection. Huszar,

METHODOLOGY

Also in 2024, Ukey, Patil, Chavan, and Sawant presented "Enhancing Public Safety: Real-Time Weapon Detection through Deep Learning using YOLOv9" at the 2024 IEEE International Conference on Innovations in High Speed Communication and Signal Processing (IHCSP). This conference paper showcased how a modern YOLOv9 object detector can be trained for real-time weapon detection in surveillance footage, significantly improving performance metrics (e.g., precision and processing speed) compared to earlier object detection models. In 2025, the work by B. D. Jadhav with Rohan Kanegaonkar, Atharva Pathrikar, and Kshitija Inamdar on "Real-Time Violence Detection and Alert System" (published in the Journal of Information Systems Engineering and Management) shifts focus from weapons to detecting violent human actions. Their system combines motion analysis, CNN and RNN models, and pose estimation to classify aggressive behaviors even in crowded scenes, triggering real-time alerts with contextual information.

Adhikarla, Negyesi, and Krasznay published "Toward Fast and Accurate Violence Detection for Automated Video Surveillance Applications" in IEEE Access. Their work emphasizes the dual need for speed and accuracy: detection systems must process video in real time while minimizing misclassifications, especially when deployed across multiple cameras in busy environments. They evaluated architectures that balanced computation cost with reliable violence recognition.

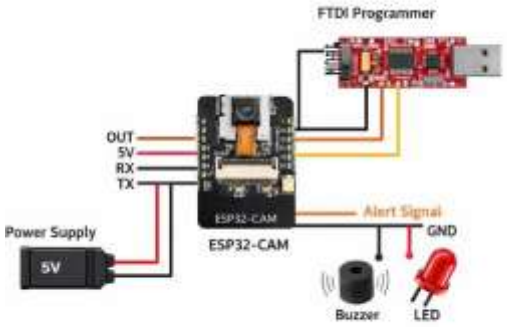
The proposed system consists of an ESP32-CAM module for image acquisition, a Node MCU controller for communication, a CNN model deployed using TensorFlow Lite for threat detection, Firebase services for data synchronization, and an Android application for user alerts. The system captures image frames, processes them using the CNN model, and sends alerts to authorized users upon detection of suspicious activity.

Requirements Analysis and Related Work Review

AI-driven threat detection systems are expected to satisfy several critical criteria, including strong detection accuracy, minimal false-positive rates, real-time analysis capabilities, scalability, and the ability to adapt to continuously evolving attack behaviors [1]. Recent research also highlights that practical deployment depends heavily on factors such as model interpretability, resistance to adversarial exploitation, and the protection of sensitive data and user privacy [2].Existing studies indicate that conventional machine learning methods, including Support Vector Machines (SVM), Random Forests, and k-Nearest Neighbors (k- NN), are effective at identifying known attack patterns but depend largely on labeled data and handcrafted feature extraction [3]. To overcome these constraints, more recent work has shifted toward deep learning architectures such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, which enable automatic feature learning and enhance the detection of complex and zero-day threats [4]. Despite these advances, challenges related to class imbalance, significant computational overhead, and

weak generalization across heterogeneous deployment environments continue to persist [5].

CIRCUIT DIAGRAM



Simple ESP32-CAM AI Threat Detection System

Project Explanation Using Circuit Diagram (Rephrased)

The circuit diagram illustrates a basic AI-driven threat detection system built around the ESP32-CAM module. In this design, the ESP32-CAM functions as the main unit responsible for image capture, processing, and system control.

ESP32-CAM Module

The ESP32-CAM serves as the central component of the system, combining a microcontroller, integrated Wi-Fi capability, and an OV2640 camera. It continuously acquires images or video frames and wirelessly transmits them to a cloud platform or a local processing unit, where AI algorithms perform threat detection and analysis.

Power Supply

A stable and regulated 5V power source is supplied to the ESP32-CAM through its 5V and GND pins. This ensures reliable operation of the module, enabling uninterrupted image acquisition and monitoring.

FTDI Programmer

An FTDI programmer is utilized to upload firmware to the ESP32-CAM. During programming, the TX and RX pins of the FTDI module are connected to the corresponding RX and TX pins of the ESP32-CAM, allowing serial communication for code transfer and debugging.

Camera Operation

The built-in camera captures images either periodically or based on instructions defined in the firmware. These captured frames act as input for AI-based threat detection tasks, such as recognizing unauthorized individuals or suspicious activity.

Alert Devices (LED / Buzzer)

Optional output devices, including an LED or a buzzer, are connected to the GPIO pins of the ESP32-CAM. When the AI model identifies a potential threat, the microcontroller triggers these components to provide immediate visual or audible notifications.

Working Principle

1. The ESP32-CAM is powered on and connects to a Wi-Fi network.
2. The camera captures images continuously or at predefined intervals.
3. The captured data is transmitted to a cloud server or local system.
4. AI algorithms analyze the images to detect potential threats.
5. Upon threat detection, alerts are generated through the LED, buzzer, or a web-based dashboard.

This setup demonstrates a simple yet effective architecture for implementing AI-enabled threat detection using embedded hardware.

ADVANTAGE

1. Cost-Effective Security Solution Review studies highlight that IoT-based AI surveillance systems using low-cost hardware such as ESP32 significantly reduce deployment cost compared to traditional CCTV systems [1].
2. Real-Time Threat Detection AI-enabled camera systems provide real-time monitoring and faster response to security

threats by continuously analyzing visual data [1], [2].

3. Wireless and Remote Monitoring Built-in Wi-Fi support enables remote access and cloud connectivity, allowing users to monitor security events from anywhere [2].

4. Reduced Hardware Complexity Integration of microcontroller, camera, and communication module into a single board minimizes external hardware requirements, as emphasized in recent IoT security reviews [1].

5. Scalability and Flexibility Review papers report that AI-IoT architectures can be easily scaled by adding multiple camera nodes and integrating cloud dashboards [2].

6. Support for Intelligent Decision-Making AI-based image analysis improves threat identification accuracy and reduces false alarms compared to motion-based systems [1], [2].

DISADVANTAGES

1. **Limited Edge Processing Capability** Review literature indicates that low-cost IoT platforms such as the ESP32 possess constrained processing and memory resources, which restrict their ability to run computationally intensive deep learning models directly at the edge [1].

2. **Reliance on Cloud-Based Processing** Many AI-enabled surveillance solutions depend on cloud servers for image analysis, which can lead to increased latency and a strong reliance on continuous and stable internet connectivity [1], [2].

3. **Image Quality Constraints** The ESP32-CAM is equipped with a low- resolution camera module that may struggle in low-light conditions or outdoor environments, potentially degrading threat detection performance [2].

4. **Security and Privacy Risks** Wireless transmission of image data introduces privacy and security concerns, particularly if proper encryption, authentication, and access control mechanisms are not adequately implemented [1].

5. **Edge-Level Scalability Challenges** While cloud infrastructure can scale efficiently, deploying and maintaining a large number of camera nodes with limited on-device intelligence can increase system complexity and operational overhead [2].

6. **Increased False Positives in Vision-Only Systems** Review studies highlight that camera-based threat detection systems lacking additional sensor inputs may generate higher false alarm rates due to environmental factors such as lighting variations or background movement [1], [2].

APPLICATIONS

The system can be deployed in banks, educational institutions, offices, shopping malls, and public spaces to enhance security and reduce response time.

They demonstrated scalability across multiple camera feeds with high accuracy, directly addressing real surveillance constraints. Although not all work is IEEE-indexed, the arXiv paper “Real-Time Weapon Detection Using YOLOv8 for Enhanced Safety” by Ayush Thakur, Akshat Shrivastav, Rohan Sharma, Triyank Kumar, and Kabir Puri (2024) represents a state-of-the-art deep learning approach that achieves a strong balance between detection accuracy and real-time inference speed. Their evaluation across metrics such as precision, recall, F1-score, and mean Average Precision (mAP) showed robust performance on weapon classes, reinforcing the utility of YOLO architectures for practical surveillance deployments.

FUTURE SCOPE

The AI-powered firearm detection system has a lot of room for improvement and could be used in many more areas related to smart surveillance and security. One important area to focus on is making the system more accurate by training the AI with a bigger and more varied set of data, including different types of guns, various angles, and different environmental conditions. Also, improving the system's ability to tell the difference between real guns and replicas can help cut down on false alarms and make the whole

system more dependable. Another big improvement could be combining this technology with facial recognition. By linking firearm detection with identity checks, security teams can better spot potential threats and keep track of people who are acting suspiciously. This would be especially helpful in places like airports and government buildings.

Conclusion

Recent survey studies conclude that Artificial Intelligence has substantially improved the performance of threat detection systems by enabling automated data analysis, adaptive behavior, and real-time decision-making when compared with traditional security solutions [1]. The integration of AI-based surveillance with IoT devices, such as camera- equipped edge nodes, offers cost-efficient and scalable security architectures that are well suited for smart and connected environments [2]. By leveraging machine learning and deep learning techniques, these systems achieve higher detection accuracy for both known and previously unseen threats.

Nevertheless, the reviewed literature also identifies several persistent challenges, including the limited computational resources of edge devices, reliance on cloud-based processing, concerns related to data privacy, and insufficient model interpretability [1], [2]. Despite these issues, ongoing advancements in lightweight AI models, edge–cloud collaborative frameworks, and secure communication mechanisms demonstrate significant potential to mitigate existing limitations. Overall, the findings from recent reviews suggest that AI-driven threat detection systems represent a promising and viable direction for future cybersecurity and intelligent surveillance applications, provided that challenges related to robustness, scalability, and privacy are effectively addressed.

REFERENCES

1. **[1]** A. Kumar et al., *"A Review on AI-Based Intelligent Surveillance Systems,"* **IEEE Access**, 2022.
2. **[2]** S. Patel et al., *"IoT and Deep Learning Approaches for Smart Security Systems: A Survey,"* **Elsevier Computer Networks**, 2023.
3. Z. K. Maseer, R. Yusof, B. Al-Bander, A. Saif, and Q. K. Kadhim, "Meta-Analysis and Systematic Review for Anomaly Network Intrusion Detection Systems: Detection Methods, Dataset, Validation Methodology, and Challenges," *arXiv Preprint*, 2023. arXiv
4. S. B. Molina, P. Nespoli, and F. G. Mármol, "Tackling Cyberattacks through AI-based Reactive Systems: A Holistic Review and Future Vision," *arXiv Preprint*, 2023. arXiv
5. R. Pal, A. C. Chakraborty, A. Bhar, and M. Ghosh, "AI-Based Cybersecurity Solutions in Threat Detection and Incident Response," *Int. J. Eng. Comput. Sci.*, vol. 12, no. 11, 2023. ijecs.in
6. Y. Reddy K. and G. ShankarLingam, "Artificial Intelligence in Intrusion Detection Systems: Trends, Frameworks, and Future Directions for Cybersecurity," *Int. J. Intell. Syst. Appl. Eng.*, 2024. ijisae.org
7. T. Sowmya and M. A. E. A., "A Comprehensive Review of AI-Based Intrusion Detection System," *Measurement: Sensors*, 2023. ResearchGate
8. V. Karanam, "Is There a Trojan!: Literat ure survey and critical evaluation of ML based modern intrusion detection systems in IoT environments," *arXiv Preprint*, 2023. arXiv
9. V. Sivagaminathan, M. Sharma, and S. K. Henge, "Intrusion Detection Systems for Wireless Sensor Networks Using Computational Intelligence Techniques," *Cybersecurity*, 2023. SpringerLink
10. "Unveiling machine learning strategies and considerations in intrusion detection systems: A comprehensive survey," *Frontiers in Computer Science*, 2024.