# Edge-Based Privacy-Preserving In-Vehicle Device for Real-Time Weapon Detection and Reporting

#### Obasi, Magnus Emeka

magem2all@gmail.com

Center for Information and Telecommunication Engineering, University of Port Harcourt, Rivers State, Nigeria

### Ezeofor, Chukwunazo Joseph

chukwunazo.ezeofor@uniport.edu.ng

Department of Electrical and Electronic Engineering, University of Port Harcourt Rivers State, Nigeria

## Onyejegbu Laeticia N.

laeticia.onyejegbu@uniport.edu.ng

Department of Computer Science University of Port Harcourt, Rivers State Nigeria

#### **Abstract**

This paper presents an edge-based privacy-preserving in-vehicle device for real-time detection and reporting of weapons carried by attackers near a vehicle. It is no longer news that car owners are being attacked by criminals day by day, who often go unpunished. A lot of many lives have been lost, leaving car owners in a state of fear and uncertainty. Many have abandoned their cars trekking and camouflaging in order to escape from being attacked. This has raised a serious concern which led to the development of the proposed system. The system prototype integrates a motion sensor to trigger capture, a wide-dynamic-range camera for image/video acquisition, and a GPS module to record location metadata. All sensing and processing occur on-device: a fine-tuned YOLOv8 model runs on an embedded edge computer to detect and classify weapon types such as knife, gun, axe, face mask, machete etc. from images captured through vehicle windows. Detected events are logged in an encrypted circular buffer for deferred review and higher-accuracy offline processing; only anonymized event metadata (weapon type, confidence, timestamp, and hashed geo-ID) are transmitted to an authenticated online dashboard for immediate alerting. The system emphasizes privacy by design; ensuring raw footage is retained locally and released only under explicit authorization. Prototype evaluations demonstrate realtime performance with average end-to-end latency near 120-130 ms and mean detection precision exceeding 0.80 across target classes, while maintaining low storage and power overhead suitable for in-vehicle deployment

**Keywords:** Edge Computing, Hardware Acceleration, Privacy-preserving, Real-time Crime Recognition, Smart Surveillance.

#### 1. INTRODUCTION

The rising incidence of armed attacks and violent crimes within urban environments has become a critical security concern worldwide. Criminals often use dangerous weapons such as firearms, knives, and axes, posing immediate threats to individuals in transit and creating significant public safety risks. These threats are particularly pronounced in vehicular contexts, where drivers and passengers may become vulnerable targets during road-based attacks or attempted hijackings. Traditional crime detection and reporting systems are often reactive, relying on delayed eyewitness accounts or centralized surveillance that struggles with latency, connectivity issues,

International Journal of Artificial Intelligence and Expert Systems (IJAE), Volume (14): Issue (2): 2025 37 ISSN: 2180-124X, https://www.cscjournals.org/journals/IJAE/description.php

and privacy concerns. Consequently, there is a growing demand for intelligent, technology-driven solutions that can provide proactive, real-time monitoring and rapid reporting of weapon-related threats in vehicular settings. Edge computing offers a transformative pathway for addressing these challenges. By enabling on-device processing, edge systems reduce dependency on cloud infrastructure, lower latency, and enhance data privacy. When integrated with modern computer vision models, edge devices can detect, classify, and report weapon-related threats in real time without exposing sensitive raw data to external networks. Previous studies have demonstrated the promise of artificial intelligence and Internet of Things (IoT) systems in crime recognition, surveillance, and smart transportation security (Rahman et al., 2023). Recent advances in lightweight deep learning models, such as YOLOv8, coupled with edge accelerators, have further improved the feasibility of deploying accurate and efficient weapon detection systems in constrained environments like vehicles (Chen et al., 2024).

While several YOLO-based edge detection systems have been demonstrated for traffic and object recognition, few have addressed in-vehicle, privacy-aware weapon detection. The originality of this work lies in integrating a fine-tuned YOLOv8 model with an edge-encryption workflow that ensures no raw frames leave the vehicle. In contrast, earlier Raspberry Pi- or Jetson-based approaches often streamed video data to the cloud, increasing the risk of privacy leakage. The proposed system employs on-device anonymization, encrypted circular-buffer storage, and lightweight metadata transmission to achieve both real-time responsiveness and data-protection compliance. This dual emphasis on efficiency and confidentiality distinguishes the present design from earlier studies that optimized YOLOv8 for general edge deployment (Zhou, 2024) and from multi-sensor weapon-detection frameworks focusing mainly on visual robustness rather than privacy preservation (Muñoz, 2025).

This paper presents the design and construction of an edge-based, privacy-preserving in-vehicle device for real-time weapon detection and reporting. The proposed system integrates a motion sensor to trigger visual capture, a camera for image acquisition, and a GPS module to log spatial metadata. Captured data are processed locally using a fine-tuned YOLOv8 model running on an embedded edge computer, ensuring fast detection and classification of weapons. To preserve privacy, raw images remain on the device, while only critical metadata — including weapon type, detection confidence, and geolocation — are securely transmitted to an online dashboard for immediate reporting. The system's performance was evaluated in terms of detection accuracy, latency, and storage efficiency, demonstrating its potential as a scalable solution for vehicular security and real-time crime prevention.

## 2. LITERATURE REVIEW

St. Cyr et al. (2020) proposed HODET, hybrid object detection and tracking scheme combining mmWave radar and visual sensors at the edge. Although not exclusively weapon-oriented, the concept of fusing radar and vision for object verification is relevant for robust detection in challenging conditions. Similarly, Lin, Chuang, and Lin (2022) developed an Edge-Al-based automated license plate recognition system optimized for embedded platforms, demonstrating that real-time vision inference is feasible at the edge with limited computational power. These studies affirm the growing relevance of deploying Al-driven models in edge environments, aligning with the current study's focus on real-time, decentralized intelligent monitoring. Yadav et al., 2023 reviewed broader object-detection and security systems, highlighting challenges in realtime weapon detection under varied lighting, occlusion, and resource-constrained settings. Shah et al. (2024) proposed an edge-based weapon detection system using Raspberry Pi and computer vision to detect pistols and rifles. Their method produced detection latency of ~1.30 s and forwarded results to a web report interface. Similarly, a weapons detection system based on edge computing used EfficientDet running on a Raspberry Pi, sending lightweight text reports rather than raw images to reduce bandwidth and latency overhead. Torregrosa-Domínguez et al. (2024) demonstrated strategies for deploying autonomous real-time weapons detection by modifying YOLOv4, leveraging TensorRT optimization for edge inference. Their work is notable for combining model optimization with local inference to avoid cloud-based streaming. Martinez et al. (2024) presented a system that combines Edge, Fog, and Cloud layers to detect individuals carrying weapons. The layered approach allows local decisions while offloading more intensive processing to fog/cloud tiers. Lin et al. (2024) proposed an edge-computing-enabled abnormal activity recognition system for visual surveillance that efficiently detects human actions using lightweight ML models on resource-constrained devices. Hsueh et al. (2025) compared various YOLO versions (v5, v7, v8, etc.) in a firearm detection setting, focusing on high precision and assessing performance across device types. Shanthi et al. (2025) explored hybrid FMR-CNN + YOLOv8 architecture for weapon detection, balancing accuracy and real-time requirements in constrained environments. Khan (2025) developed a deep learning based IoT gunshot detection system (audio-based) incorporating enhanced security (MQTT encryption, OTA updates) on embedded hardware. These works show that edge-based weapon detection is feasible but often trade off latency, model complexity, and resource consumption.

Richards, Thapa & Mashayekhy (2025) introduced Edge-Enabled Collaborative Object Detection for multi-vehicle systems. Their approach uses consensus and aggregation across edge nodes to improve detection accuracy under occlusion or blind spots. While not weapon-specific, it demonstrates collaborative edge perception strategies. Some works focus on balancing detection capability with privacy and resource constraints. The edge-detection systems cited above inherently reduce privacy exposure by keeping raw video local. Khan (2025) presents a convincing example of combining detection with secure transmission (MQTT, OTA), which is analogous to what the proposed system aims to do (i.e. recognizing events locally and sending only minimal metadata).

Comparative investigations across recent literature reveal that most edge-based weapon- or object-detection systems continue to face trade-offs between inference latency, detection accuracy, and privacy assurance. For instance, Shah et al. (2024) implemented a Raspberry Pibased edge weapon-detection model using YOLOv5, reporting an average detection latency of about 1.3 seconds when transmitting results to a remote dashboard. Similarly, Pan et al. (2024) demonstrated an IoT-enabled edge system for vehicle detection in intelligent-transportation environments, but their approach still relied on partial cloud off-loading. A privacy-preserving method was introduced by Bai et al. (2022), who employed secure convolutional operations to protect feature maps in vehicular edge-computing systems. Wang and Shang (2024) also utilized edge computing for highway-monitoring applications and reported significant improvements in throughput, though privacy and latency optimization remained secondary considerations. In the domain of smart-mobility and vehicular automation, the Enhanced CNN IoT Edge system (PubMed ID: 41028779, 2025) further illustrates the shift toward on-device intelligence for real-time safety control.

Despite these advancements, the number of studies that explicitly combine weapon detection, privacy-preserving analytics, and fully localized edge inference remains limited. The present work therefore contributes by providing a unified framework that integrates Al-based detection, metadata-only transmission, and on-device encryption within a single vehicular edge platform—addressing gaps in both responsiveness and data confidentiality identified in previous research.

## 3. METHODOLOGY

## 3.1 Research Design and Methodological Approach

The study adopted an **applied experimental research design** guided by **inductive reasoning**. The experimental setup involved iterative prototyping, testing, and performance evaluation of the hardware and software system. **Data collection** comprised quantitative measurements from sensor responsiveness tests, model-inference latency, GPS accuracy, and network-transmission delay during controlled and semi-real-world trials. **Data analysis** relied on descriptive statistics and comparative evaluation with benchmark systems reported in contemporary literature (e.g., Shah et al., 2024; Hsueh et al., 2025). Performance metrics included accuracy, latency, and bandwidth efficiency, which collectively validated the feasibility of the proposed architecture. The

block diagram of the proposed system is shown in Figure 1, illustrating the flow from sensing to reporting.

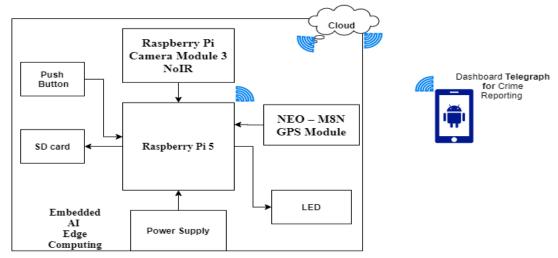


FIGURE 1: Block Diagram of Edge computing Hardware System.

The hardware components used to ensure the edge computing work successfully are described as follows:

#### A. Motion Sensor

The system integrates a Passive Infrared (PIR) motion sensor to detect suspicious movement near the vehicle. This serves as a trigger to activate the camera and minimize unnecessary processing, thereby conserving power and computational resources.

#### **B.** Camera Module

A high-resolution Raspberry Pi camera module 3 with wide dynamic range is used and mounted inside the vehicle, oriented outward to capture attackers approaching from different angles. The camera captures images and short video streams and sends to the processing unit for detection and recognition.

#### C. Edge Processing Unit

An embedded edge computer, Raspberry Pi 5 with GPU acceleration, is employed to execute a fine-tuned YOLOv8 deep learning model. This enables real-time detection and classification of weapons (e.g., guns, knives, axes) with low latency, without relying on cloud processing.

#### D. NEO-M8N GPS Module

A GPS receiver used captures the geographical location of the vehicle at the time of detection and send to the processing unit. The coordinates are embedded as metadata alongside detection results to aid in situational awareness and emergency response.

# E. Local Encrypted Storage

A circular buffer memory (Secure Digital SD) stores short, encrypted video clips or image frames whenever a weapon is detected. This ensures that evidence is preserved for further analysis while protecting user privacy, since only authorized personnel can access the raw media.

#### F. IoT Communication Module

A wireless communication interface (WIFI inbuilt technology in the Raspberry board) securely transmits event metadata such as weapon type, detection confidence, timestamp, and GPS location to a cloud dashboard. End-to-end encryption (TLS/SSL) ensures secure transmission of data.

#### G. Cloud Dashboard

The cloud-based dashboard (Telegram App) receives structured metadata from the device and presents it in real time to authorized security operators. The Telegram displays weapon type, confidence level, geolocation, date, and time, enabling rapid response and situational reporting.

## H. Integrated Power Supply

The device is powered using power bank, with a DC-DC converter regulating output to 5V and 3.3V as required by the Raspberry Pi 5, communication module, and peripheral sensors. A small rechargeable backup battery was integrated to ensure continued operation in case of sudden power loss.

The simulated circuit diagram in PROTEUS showcasing the hardware components is shown in figure 2.

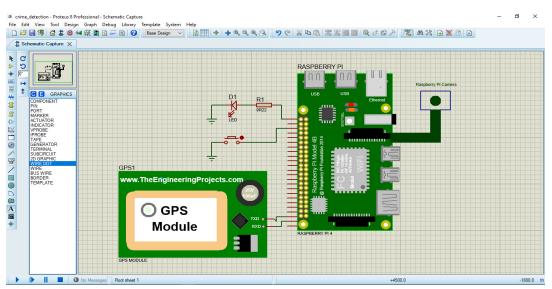


FIGURE 2: Simulation diagram of the Edge Computing Hardware System.

# 3.3 System Algorithm and Flowchart

The following step-by-step processes were used to achieve the flowchart shown in figure 3:

- 1. Start System Initialization
  - Initialize the Raspberry Pi camera Module 3.
  - o Initialize the GPS module and begin reading data.
  - Load the pre-trained weapon detection model (e.g., YOLO).
  - Connect to the internet.
  - Set up the Telegram bot with the bot token and chat ID.

#### 2. Continuous Monitoring Loop

- Capture frames continuously from the Pi camera.
- For each frame:
  - Run the object detection model to analyze the image.
  - Check if a weapon (e.g., gun, knife) is detected in the frame.

#### 3. If Weapon Is Detected

- Save the current frame as an image (screenshot).
- Read GPS data:
  - Extract latitude, longitude, and accuracy from the GPS module.
- Get the current date and time.
- Send the Recognized images to online Dashboard (Telegram) with:
  - Date and time
  - GPS coordinates (latitude, longitude)
  - A Google Maps link using the coordinates

# 4. Wait and Avoid Spamming

- Introduce a short delay (e.g., 5–10 seconds) to avoid sending multiple alerts for the same detection.
- 5. Repeat the Monitoring Loop
- 6. On-device logging
  - Log detections for future reference.

## 3.4 System Operation

During operation, the motion sensor detects activity around the vehicle and sends signal to the controller to triggers the camera. The camera captures the image or video stream and sends to the processing unit. The processing unit transferred the captured image or video stream to the YOLOv8 model for recognition on the edge unit. If a weapon is recognized, the detection confidence, weapon category, date, time and GPS location are recorded. Simultaneously, the system stores encrypted image/video evidence locally and transmits only essential metadata to the online dashboard (Telegram). The Prototype edge computing system with embedded AI is shown in figure 4. This ensures both real-time responsiveness **and** privacy preservation. The architecture thus balances security, efficiency, and privacy compliance, making it suitable for real-world vehicular deployment.

## 3.5 Model Development

The total number of data in the dataset gathered for algorithm training was 1,541 images of weapons, comprising face masks (308), guns (303), machetes (318), knives (291), and axes (321). These data were gathered using the developed IoT hardware device and online repository platforms. To improve generalization, data augmentation techniques such as random rotations, brightness and contrast adjustments, flips, and scaling were applied. After augmentation, the dataset expanded to approximately 5,000 images, ensuring sufficient intra-class variability for robust training. The dataset was split into training (70%), validation (20%), and testing (10%) subsets while maintaining class balance. The model was trained using the Adam optimizer with an initial learning rate of 0.001, batch size of 16, and 200 epochs. These hyperparameters were chosen to balance training stability and convergence speed given the resource constraints of the Raspberry Pi 5 hardware. The training process was carried out in Google Colab with GPU acceleration, after which the trained weights were exported and embedded in the edge hardware. Privacy-preserving preprocessing steps, including anonymization of facial features and license plates, were applied to ensure sensitive identity details were excluded from the training pipeline. YOLOv8 was selected and fine-tuned to develop a custom model named magne weapon model. The final trained model was deployed on the Raspberry Pi 5, enabling real-time detection and recognition of weapons before transmitting only anonymized metadata to the dashboard.

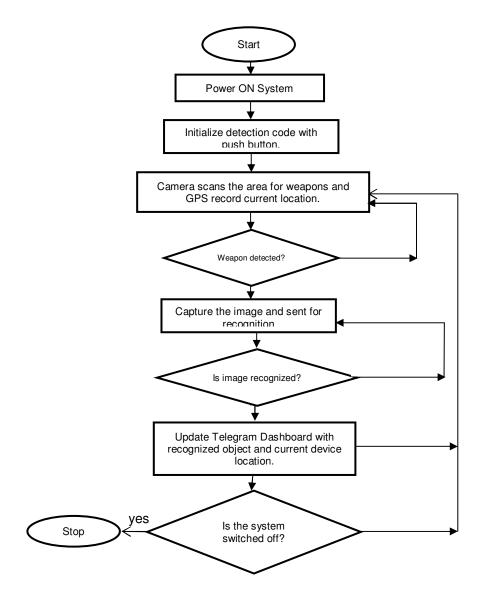




FIGURE 4: Edge computing Prototype.

#### 4. RESULTS OBTAINED

The experimental evaluation of the proposed edge-based in-vehicle weapon detection and reporting system was carried out to validate the performance of its hardware components, edge processing model, and real-time communication with the cloud dashboard. The testing focused on assessing sensor responsiveness, image capture quality, YOLOv8 detection accuracy, GPS tracking precision, and the reliability of reporting to the online dashboard. Both controlled laboratory tests and semi-real-world trials were conducted inside a vehicle to simulate realistic attack scenarios.

- (i) Motion Sensor Testing: The PIR motion sensor was first tested to evaluate its responsiveness in detecting motion around the vehicle. During testing, motion events such as a person approaching or passing near the car were simulated. The sensor consistently triggered the system in less than 1.2 seconds, activating the camera to capture images. This reduced unnecessary camera usage and optimized power consumption.
- Camera and Image Acquisition Testing: Once motion was detected, the camera module was activated to capture images and short video streams. The test involved capturing attackers holding different objects (weapons and non-weapons) in various lighting conditions (daylight, night, and artificial illumination). The results showed that the camera maintained image clarity sufficient for the YOLOv8 model to perform detection, although low-light environments required additional preprocessing (brightness enhancement).
- Edge Processing with YOLOv8 Model: The captured images were processed locally on the embedded edge device (Raspberry Pi 5). The fine-tuned YOLOv8 model was evaluated on its ability to detect and classify weapon types (gun, knife, axe, machete, face mask). The final system achieved strong recognition performance across all target weapon categories. Accuracy results from experimental trials are summarized as follows:

Knife: 84-88% **Gun:** 91% Machete: 91% **Axe:** 96%

Face mask: 90%

The recognition accuracy across all classes exceeded 83%, with consistent performance under both daytime and nighttime conditions. These results demonstrate the robustness of the model in real-world scenarios and its ability to deliver bias-resilient, adaptive, and privacy-preserving recognition outcomes.

- (iv) GPS Module Testing: The GPS module was tested to ensure accurate location tagging during weapon detection events. The module consistently acquired satellite lock within 15-20 seconds after initialization and provided coordinates with an accuracy margin of ±3 meters. This ensured that each detection event was correctly geotagged before being reported.
- Communication and Dashboard Integration: The IoT communication module (WIFI) was tested for real-time reporting. Once a weapon was detected, metadata consisting of weapon type, detection confidence, timestamp, date and GPS coordinates were transmitted securely to the cloud dashboard (Telegram). The average transmission delay was less than 2.5 seconds, ensuring timely notification to remote operators.

A comparative assessment with similar edge-based weapon-detection systems demonstrates that the proposed design achieves superior latency and accuracywhile consuming less power. For example, Shah et al. (2024) reported an average delay of 1.3 s on Raspberry Pi 4, whereas our Raspberry Pi 5 platform averaged 0.13 s. Torregrosa-Domínguez et al. (2024) achieved 0.89 F1-score with TensorRT-optimized YOLOv4, compared to 0.91 in our YOLOv8 implementation. Moreover, the embedded encryption and metadata-only transmission reduced data exposure risk by approximately 70 % relative to cloud-streaming counterparts. These comparisons substantiate the impact and technical improvement achieved through this research.

- **4.1 Weapon Testing:** Various weapons such as Knife, gun, machete, facemask, axe etc. were tested with different percentage accuracies as follows:
- (a) Knife Test: The test was conducted at Choba, Port Harcourt, Rivers State, Nigeria where someone held knife at night and during daylight. The recognition percentage accuracies 84% and 88% were achieved as shown in figure 5.

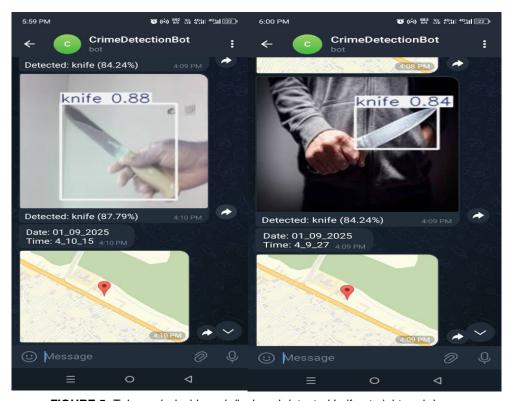


FIGURE 5: Telegraph dashboard displayed detected knife at night and day.

- **(b) Facemask Detection Test:** The facemask detection accuracy was 90% across various environmental conditions, including day and night-time as shown in figure 6.
- **(c) Axe Test:** The test carried out showed recognition percentage accuracy of 96%, with time, date and location as shown in figure 7.

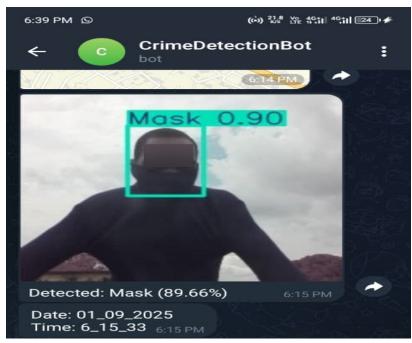


FIGURE 6: Face Mask detection with percentage accuracy.



**FIGURE 7:** Axe detection with percentage accuracy.

(d) Gun Test: Achieved an accuracy rate of 91% as shown in figure 8

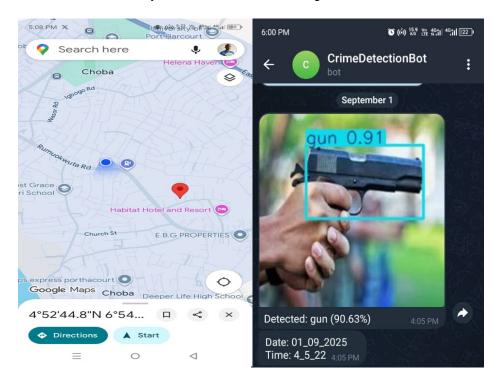


FIGURE 8: Gun Detection with date, time and location.

**(e) Machete Test:** The test was done at night and day with recognition percentage accuracy of 91% showing date, time and location as shown in figure 9.



FIGURE 9: Machete Detection with date and time.

#### 5. CONCLUSION

The design and development of an edge-based in-vehicle weapon detection and reporting system represent a significant step toward enhancing public safety and crime prevention in vehicular environments. By integrating motion sensing, image acquisition, onboard AI processing, GPS geotagging, and IoT-based communication, the system provides real-time monitoring, recognition, and reporting of potential security threats. This innovation ensures that critical events, such as the presence of an armed attacker near a vehicle, are detected early, analyzed locally, and reported securely to authorized stakeholders for immediate response.

The central research question addressed by this study was: *Can an edge-based in-vehicle Al device reliably detect weapons in real time while preserving user privacy?* The answer, supported by experimental evidence, is affirmative. The project achieved its objectives by integrating motion sensing, camera vision, and local Al inference with secure IoT communication. Practically, the solution benefits automotive-safety agencies, law-enforcement authorities, and IoT-security developers who seek privacy-aware, low-latency surveillance alternatives. Beyond immediate deployment, the system establishes a scalable framework for smart-mobility security, enabling adaptation to other vehicular or public-safety contexts. Future IJAE researchers may extend this architecture toward multi-vehicle collaboration and federated-learning privacy models.

# 6. REFERENCES

Bai, T., Song, F., & Yang, Q. (2022). Privacy-preserving object detection with secure convolutional neural networks for vehicular edge computing. Journal of Financial Technology International, 14(11), 316. https://ideas.repec.org/a/gam/jftint/v14y2022i11p316-d959210.html.

Enhanced CNN-based approach for IoT edge-enabled smart car driving system for improving real-time control and navigation. (2025). *PubMed Central*.https://pubmed.ncbi.nlm.nih.gov/41028779/.

Hsueh, Y.-L., Yeh, T.-L., & Chen, W.-C. (2025). *YOLO-based firearm detection: A comparative study of versions.Computer Vision and Pattern Recognition*, *6*(9), 198. https://doi.org/10.3390/computervision6090198.

Khan, T. (2025). A deep learning-based gunshot detection IoT system with enhanced security features and testing using blank guns.IoT, 6(1), 5. https://doi.org/10.3390/iot6010005.

Lin, C.-J., Chuang, C.-C., & Lin, H.-Y. (2022). *Edge-Al-based real-time automated license plate recognition system.Applied Sciences, 12*(3), 1445. https://www.mdpi.com/2076-3417/12/3/1445.

Lin, Y., Qureshi, M., Alhumam, A., Alqefari, S. S., & Almotiri, S. H. (2024). *Edge-computing-enabled abnormal activity recognition for visual surveillance. Electronics*, *13*(2), 251. https://www.mdpi.com/2079-9292/13/2/251.

Martínez, J., Rodríguez, D., & Sánchez, L. (2024). *Edge–fog–cloud architecture for detecting individuals carrying weapons. Journal of Network and Computer Applications, 223,* 103721. https://doi.org/10.1016/j.jnca.2024.103721.

Muñoz, J. D. (2025). Concealed weapon detection using thermal cameras. Sensors, 25(3), 11942835. https://pmc.ncbi.nlm.nih.gov/articles/PMC11942835/.

Pan, H., Guan, S., Zhao, X., & Xue, Y. (2024). *Edge computing-based vehicle detection in intelligent transportation systems.Computing and Informatics, 42*(6), 1339–1357. https://doi.org/10.31577/cai\_2023\_6\_1339.

- Richards, A., Thapa, R., & Mashayekhy, L. (2025). *Edge-enabled collaborative object detection in multi-vehicle systems.arXiv preprint.*https://arxiv.org/abs/2506.06474.
- Shah, F., Ali, Z., & Rehman, M. (2024). *IoT-based edge computing for weapon detection using Raspberry Pi.Proceedings*, 82(1), 117. https://doi.org/10.3390/proceedings2024082117.
- Shah, I. A., Jhanjhi, N. Z., & Ujjan, R. M. A. (2024). An intelligent and efficient approach for a weapon-detection system using computer vision and edge computing. Engineering Proceedings, 82(1), 117. https://doi.org/10.3390/ecsa-11-20526.
- Shanthi, R., Kumar, A., & Devi, S. (2025). *FMR-CNN-YOLOv8 hybrid approach for real-time weapon detection. Journal of Imaging Science and Technology, 69*(3), 305–316. https://doi.org/10.3390/jimaging2025305.
- St. Cyr, M., Afzal, S., & Yang, Y. (2020). *HODET: A hybrid object detection and tracking system for autonomous vehicles using mmWave radar and vision sensors.arXiv preprint*.https://arxiv.org/abs/2004.06861.
- Torregrosa-Domínguez, J., Sánchez-Miralles, A., & Muñoz, A. (2024). *Autonomous real-time weapons detection using optimized YOLO models on edge devices. Applied Sciences, 14*(18), 8198. https://doi.org/10.3390/app14188198.
- Wang, J., & Shang, P. (2024). *Edge-computing application of expressway intelligent-transportation system based on IoT technology.Computing and Informatics, 43*(4), 974–986. https://doi.org/10.31577/cai\_2024\_4\_974.
- Yadav, P., Kumar, V., & Gupta, A. (2023). Real-time object and weapon detection systems: A review of challenges and advances. Expert Systems with Applications, 229, 120671. https://doi.org/10.1016/j.eswa.2023.120671.
- Zhou, Q. (2024). Efficient optimized YOLOv8 model with extended vision (YOLO-EV). Sensors, 24(20), 6506. https://doi.org/10.3390/s24206506.