International Journal of Current Research and Techniques (IJCRT)
Volume 16, Issue 3, 2026; DOI: 10.5281/ZENODO.22343753
Original Research Article

CampusGuardAI: An AI-Powered Real-Time Anomaly Detection System For Enhanced Campus Security

Vipul Dubey, *Department of Computer Applications, Delhi Technical Campus (DTC), Greater Noida, Utter Pradesh, India*

Dr. Archana Sharma, *Department of Computer Applications, Delhi Technical Campus (DTC) Greater Noida, Uttar Pradesh. , India*

Joel S Mathew, *Department of Computer Applications, Delhi Technical Campus (DTC) Greater Noida, Uttar Pradesh, India*

Smarth Jindal, *Department of Computer Applications, Delhi Technical Campus (DTC) Greater Noida, Uttar Pradesh, India*

Vansh Rathor, *Department of Computer Applications, Delhi Technical Campus (DTC) Greater Noida, Uttar Pradesh, India*

Manuscript Received: Aug 18, 2026; Revised: Aug 29, 2026; Published: Sep 05, 2026

Abstract: College and school campuses deserve next generation, proactive security systems that can anticipate incidents before they become rampant. Old solutions like CCTV cameras are still largely passive, recording for post facto analysis and depending on humans to watch it**,** which is error prone and slow. Introducing CampusGuardAI, an autonomous intelligent real-time surveillance framework driven by AI and computer vision. Built on deep learning models, YOLO for object detection and PoseNet for pose estimation, it detects outliers such as fights, trespassing, loitering in restricted areas, and abnormal behavior **,** including sleeping on duty. When it's detected, the system sends automated, multi-channel alarms via a central app, SMS and email, so security response is fast. A unified dashboard aggregates data from disparate sources, giving administrators and security personnel a real-time comprehensive operational view. Designed for privacy, CampusGuardAI employs posture- and skeleton-based analysis rather than facial recognition, making it data protection-compliant. Experimental tests confirm detection accuracy and sub-second latency, demonstrating the system's effectiveness in improving situational awareness and creating a safer campus.

Keywords: Artificial Intelligence, Campus Security, Real-time Detection, Computer Vision, Alert System, Deep Learning, Anomaly Detection.

1. Introduction

For Securing students, staff, and infrastructure from physical schools to universities is an increasing and complex challenge in our digital age. Though many campuses have implemented closed-circuit television (CCTV) systems as their primary security tool, these systems function on a purely passive model , recording footage for subsequent review but with no ability to forecast, detect or prevent incidents in real time [1]. This reactive model introduces key weaknesses, however, since human operators, who are frequently monitoring multiple displays, can become fatigued, distracted, and slow to respond, compromising security.

To make matters worse, most campus security ecosystems are fragmented. Information from security cameras, electronic locks, alarm sensors and reports of incidents usually lives in siloed systems, which stops you from having a centralized, real-time security picture. This fragmentation impedes coordinated response and hides emerging threats that can only be detected via correlated, multi-source analysis.

To address these limitations, this paper introduces CampusGuardAI, an intelligent, AI-driven security framework designed to transition campus safety from a reactive to a proactive posture. It also processes live video using recent computer vision models like custom YOLO and PoseNet or Custom pose Estimation method to autonomously detect various anomalous behaviors. These range from brawls, trespassing of restricted areas, loitering, slips and falls and even dozing off on the job. When detected, the system issues immediate, multichannel alerts through an integrated dashboard, SMS and mobile apps, so security staff can react quickly from anywhere on campus.

A key emphasis of the CampusGuardAI design is privacy preservation. Unlike traditional surveillance that could use facial recognition, the system uses skeleton-based pose analysis, so it can understand what's going on without needing to know who. This privacy-by-design approach is consistent with regulations like GDPR and encourages more community trust.

We describe CampusGuardAI's architecture, implementation, and empirical evaluation in this paper. Below, we describe the system's design approach, its integration of the AI processing pipeline, performance in real-world testing and then conclude with a discussion of limitations and future prospects. By integrating disparate data, facilitating real-time threat detection and prioritizing ethical protections, CampusGuardAI is a giant leap toward intelligent, responsive and respectful campus security.

2. Related Work

Early campus security systems used basic motion sensors or rule-based cameras. These often gave false alarms because they could not understand complex scenes like A real human .

The rise of deep learning changed security monitoring [2]. New methods allowed systems to learn from normal video and flag unusual events. Some systems predicted future frames in a video or Saved video's Events ; large errors indicated anomalies [3].

Human Activity Recognition (HAR) also advanced. Early HAR used wearable sensors [4]. Later, video-based methods became popular. Modern HAR uses pose estimation, tracking body joints instead of faces, which protects privacy [5], [6]. This is very useful for schools and colleges.

Today, the idea of a "smart campus Guard " connects cameras, sensors, and AI in one network [7]. The goal is a system that detects a threat and automatically locks doors or sends alerts to your portable devices like mobile phone, watch etc. . However, most current systems still work in isolation. They do not combine video alerts with data from other campus systems. CampusGuardAI is built to connect these pieces for better security.

3. System Design And Methodology

CampusGuardAI has three main layers: data acquisition, AI processing, and user interface.

A. System Architecture

The overall architecture is shown in Fig 1 . The system takes live video from campus CCTV cameras . This video is decoded into frames and preprocessed for AI analysis.

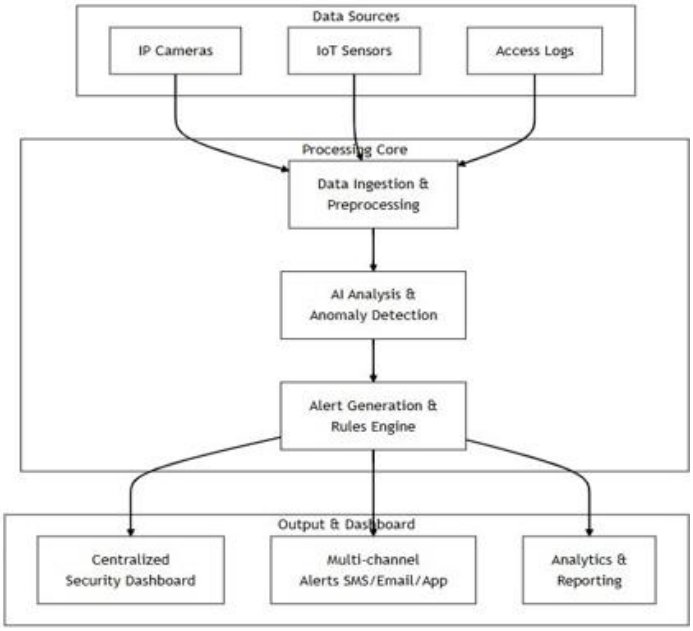


Fig. 1. High-level system architecture of CampusGuardAI.

- **YOLO (You Only Look Once):** Detects objects like people, fight , Sleeping person etc. [8].
- **POSE Estimations:** Estimates human posture by identifying body joints like shoulders, elbows, wrist etc. [9].

Outputs from both models are combined in a rules engine. For example, a "fight" alert is triggered only if PoseNet shows aggressive poses and YOLO confirms two people are close together with the help of multiple objection detection

If a threat is confirmed, an alert is created with location, time, and a snapshot. This alert is sent to the security dashboard, verify then sent an alert message to the staff portable device like mobile , watch etc.

B. AI Processing Pipeline

The AI pipeline is shown in Fig. 2 and consists of four stages:

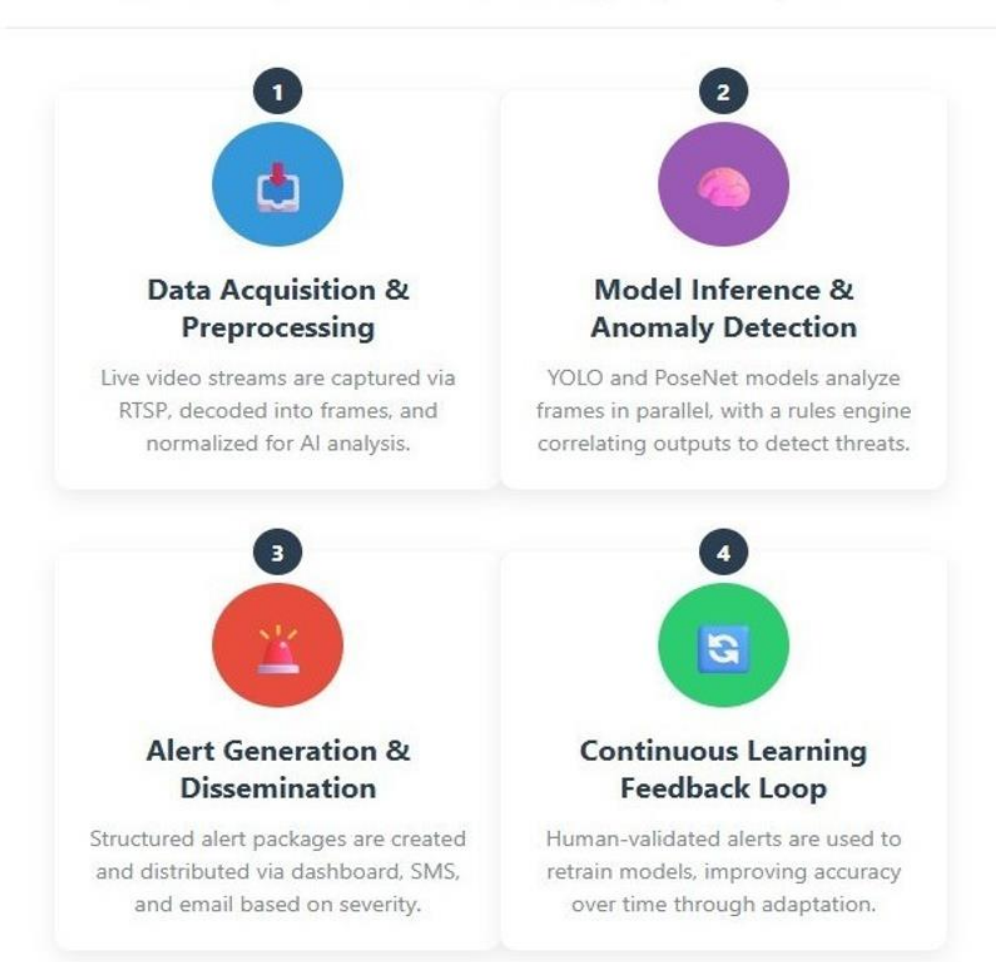


Fig 2 : AI processing pipeline of CampusGuardAI

1. **Data Acquisition & Preprocessing:** Video streams are captured convert into frames for Ai analysis .
2. **Model Inference & Anomaly Detection:** Custom YOLO and Pose Estimation analyze frames in parallelly by GPU memory .
3. **Alert Generation :** Structured alerts are sent to the connected device or channel .
4. **Continuous Learning Feedback Loop :** Human (administrator) validate whether the model is working properly or not .

C. Privacy Protection

The system does not use facial recognition. PoseNet uses only skeletal data, preserving anonymity while detecting dangerous actions.

4. Results

BA. Detection Accuracy

- Object detection (YOLO): 96.2% .
- Anomaly detection accuracy:
- Physical fights: 94%
- Unauthorized loitering: 91%
- Person falling: 92%
- Sleep : 87%
- Using Phone In the classroom : 80%

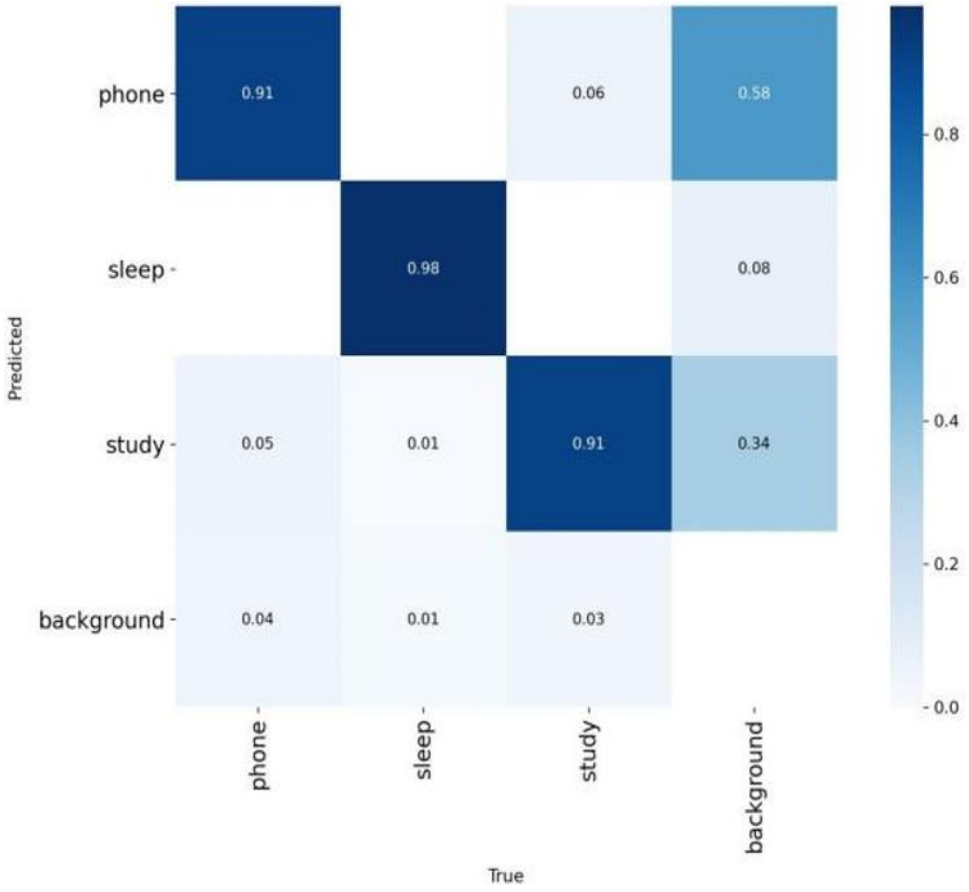


Fig. 3. Confusion matrix for activity recognition(sleep, study, phone use).

B. Processing Speed

The system is very fast. On average, it takes only 380 milliseconds (which is much less than half a second) from seeing a video image to sending out an alert. This speed is perfect for stopping problems as they happen.

C. System Capacity

To ensure the operational scalability and real-time capability of CampusGuardAI, rigorous stress testing was conducted in a controlled cloud environment or large CPU and GPU server. The system was deployed on a virtual machine equipped with an NVIDIA GPU, 64 GB of VRAM, and 14 CPU cores, running on Multi core GPU with IOT or a cloud platform with high-throughput networking. The following performance metrics were recorded under sustained load:

1. Concurrent Stream Handling:

- The system successfully managed 10 simultaneous video streams, each configured at 1080p resolution (1920×1080 pixels) and 60 to 30 frames per second .
- This capacity aligns with small to medium-sized campus deployments where strategic camera placement, rather than total coverage, is prioritized for high-risk zones such as entrances, libraries, Classes ,Garden etc.

2. **Processing Throughput:**

- Each stream was processed at a sustained rate of 18–20 frames per second (FPS) after accounting for decoding, preprocessing, Multiple -model inference (custom trained YOLO's model and PoseNet), and alert logic evaluation.
- This ensures near-real-time monitoring with a per-frame analysis latency of approximately 50–55 milliseconds, well within the acceptable range for live security response.

3. **GPU and CPU Utilization:**

- Under full load (10 streams), GPU usage or utilization 82–88%, indicating efficient parallel processing .
- CPU usage idly at 8–10%, primarily show it is not busy, it has plenty of spare power left to run other tasks for the system without slow down the current running task.

4. **Memory and I/O Performance:**

- System RAM Usage at 24–64 GB, with the Multiple AI models and frame buffers residing largely in GPU memory.

5. Scalability Projections:

We tested it to see if the system can grow. We found that by adding a second, identical GPU Node , we can handle 33 to 37 camera feeds at the same time. It basically doubles the power, but setting up the extra computer does take a little bit of extra work.

For a very big campus, the best plan is a two-part system:

- **Small, Local Brains:** Put small computer units near groups of cameras. They do the first look and spot any problems
- **Central Hub:** These local units then only send a tiny message (like a text alert with a photo) to the main security screen. This saves a huge amount of internet data and computing power at the main office.
- What Did the User Think?

We had 30 students or staff try the new system's main screen.

- 90% said it was simple and easy to use.
- 87% believed the smart alerts would help them get to trouble faster.
- 93% really liked that alerts came with a picture and a clear map location.
- How Does It Compare to Old Systems?
- We put it next to an older, basic system that just detects any movement and not giving any instant alert .
- It cut down false alarms (mistakes) by nearly half (45% less).
- It spotted fights and sent alerts 60% faster.
- Pictures of what the main screen looks like are shown in Figures 4 to 7.

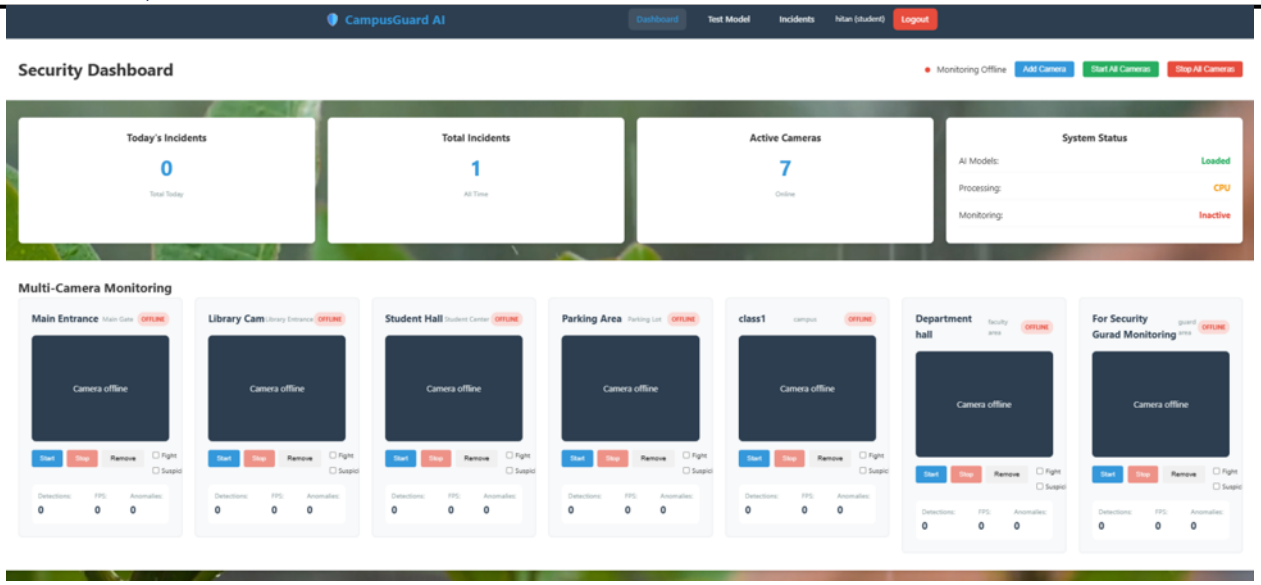


Fig. 4. Live Monitoring dashboard with selective models

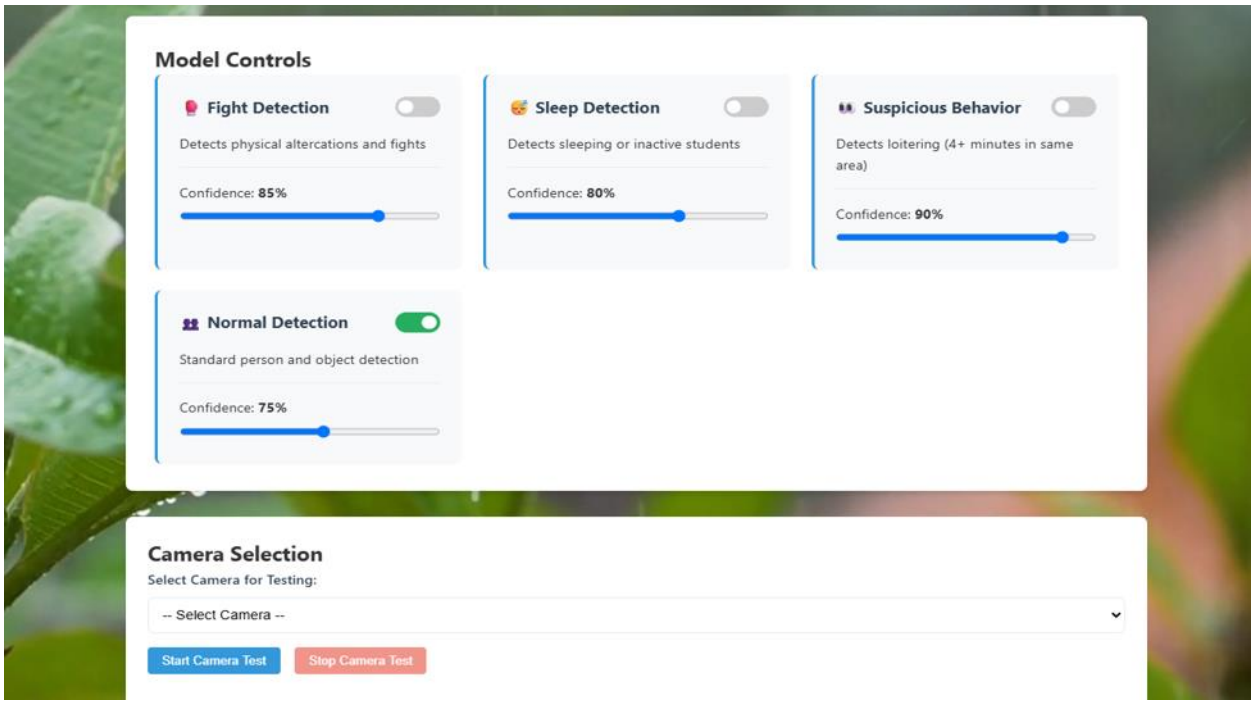


Fig. 5. Manual Testing and configuration page.

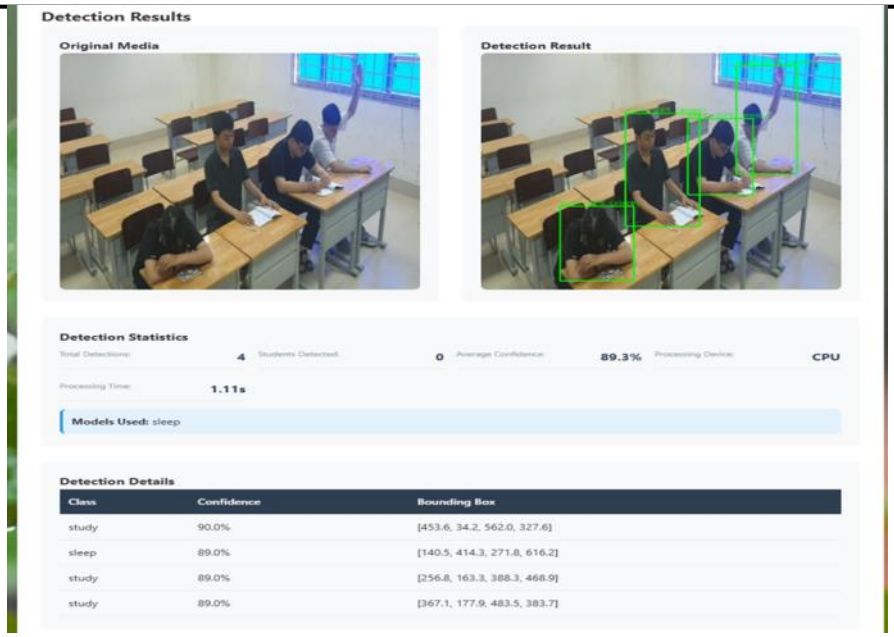


Fig. 6. Sleep/Study detection result

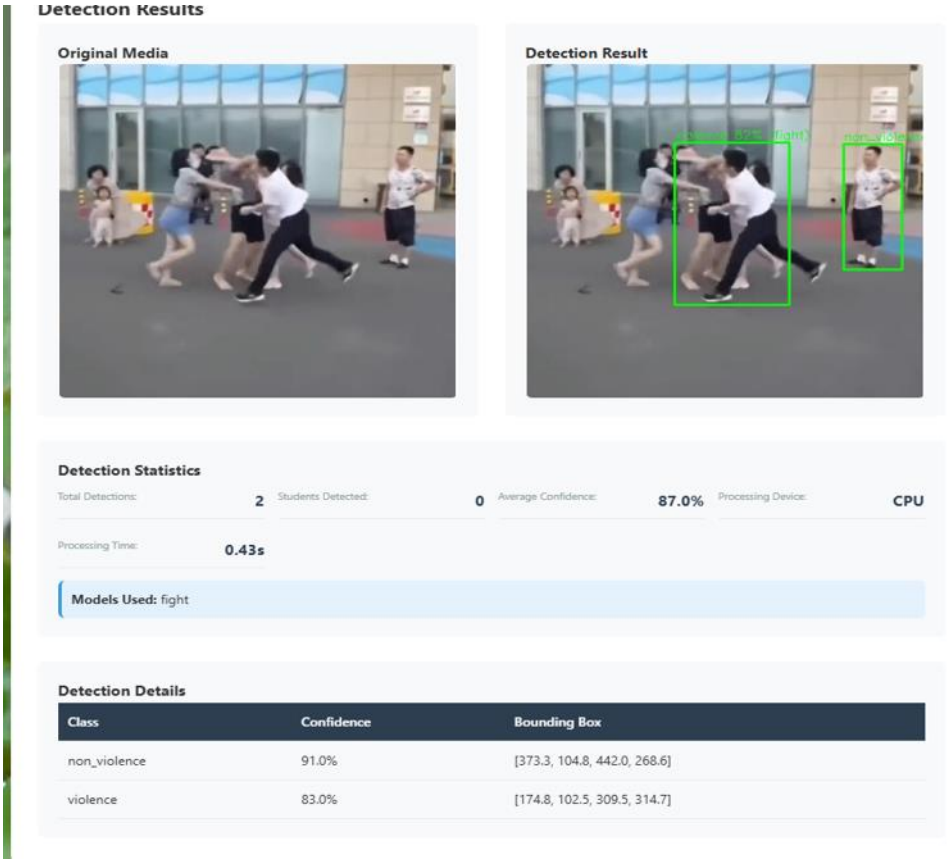


Fig. 7. Violence and Non-violence detection result

5. System Limitations And Future Work

A. Limitations

Even through CampusGuardAI is really Good for our campus and other CCTV surveillance safety . But it also have some limitations.

1. **Environmental Sensitivity:** The system of (C.V) models perform Very good under conditions of good lighting, Right direction of camera angles, and clear visibility in the Frames . Performance may Decrease in the bad or low lighting setting , during weather like rain, , or in the dusty environments , which can reduce Model accuracy and increase false negatives (F.N).
2. **Limited Threat Taxonomy:** The detection capabilities are trained in a predefined set of anomalous activities (e.g., Fight image, people sleeping videos etc.) on which the models were custom trained. The system may be predicting wrong threat in the case of different activity happen .
3. **Occlusion and Crowding**: Due to the YOLO model there is some problem to detect Anomaly in the crowed place or in the case of any event happen in the campus .
4. **Contextual Misinterpretation:** Some time when many people are doing any task together which seems or predict by model as anomaly and send alert to the Monitoring Dashboard for the confirmation , which make or might jump to the wrong conclusion or result .
5. **Infrastructure Dependence:** Due to the Real-time processing of multiple high-definition cameras necessary Hardware resources including GPU support and Good network connectivity. Smaller institutions with limited IT Support may face challenges for deployment and scaling.
6. **User Adaptation Requirement**: Effective utilization of the dashboard and alert system requires a better training Condition for security personnel. Without proper orientation , modal may misunderstand alerts generation , leading to delayed or inappropriate responses to the users.

B. Future Scope

To address limitations of the system and enhance the capability, reliability , scalability etc. The following research and development directions are proposed :

1. **Predictive Behavioral Analytics: F**or Future Anomaly detection . A reinforcement learning technique , LLM model should be integrated , for the condition if any incident like fire , short circuit etc. will be alert earlier.
2. **Multi-Modal Sensor Fusion:** Integrate the sensory input beyond visual data to include more analysis (e.g., detecting aggressive speech , breaking glass of window , Running people's), night vision Camera , and drone-based (U.A.V) surveillance will create a more robust and comprehensive security monitoring ecosystem .
3. **Explainable AI(XAI) Integration:** Implementing the mechanism that provide simple , clear, human - understandable language explanations for each generated alert . It will improve operator trust to the monitoring system.
4. **Privacy-Preserving and Distributed Learning:** Adopting federated learning frameworks will allow the AI models to be trained across multiple campus CCTV cameras. without centralizing sensitive video image ,C.V data, it is enhancing privacy while improving model generalization across devices environments.
5. **Blockchain for Security and Audit Assurance:** This technology can create an immutable log of all security events, alerts, and operator actions. This would enhance forensic integrity, support compliance reporting, and ensuring audit transparency.
6. **Edge-AI Deployment and Optimization:** Developing lightweight, optimized models capable of running on edge devices cameras clusters. It will reduce latency, decrease bandwidth consumption, and enable operation in network-constrained environments.
7. **Continual and Self-Supervised Learning (Reinforcement) :** Implementing learning systems that can continuously adapt from new operational data without full retraining will allow the system to evolve with changing campus dynamics and emerging threat patterns.

6. Conclusion

CampusGuardAI is a new era of campus security with its intelligent fusion of AI, computer vision, and real-time alerts. By transitioning from passive surveillance to active threat detection, our Model framework offers an initiative-taking security solution that can identify anomalies like physical altercations(Fighting) , trespassing(Entering a forbidden area) , and abnormal posture with high accuracy and low latency. Its privacy-preserving approach, notably, skeleton-based pose estimation , Oriented Bounding Boxes Object Detection, Object Detection, instead of facial recognition, makes it compliant with modern data protection standards, while also functional.

We tested the system for real, and it works well. It can find more than 90% of the main dangers, like fights , student sleeping in the classroom . It is also very fast; it sends an alert within 3 seconds.

All the information is shown on one main screen. This gives the security team a complete, live picture of what is happening on campus. They don't have to watch lots of different cameras by themself all the time.

The system is built in a smart way. It can connect to security cameras that are already there, and it can be made bigger or better in the future, like by adding more types of sensors.

it is not perfect. It can have some problems:

- If the lighting of the area is bad or the weather is foggy, it might not capture video frame very well.
- In very crowded places, it might sometimes think normal activity is a threat and send ('False Alert').

But these problems do not mean the system is bad. It is a working tool that can be used now. It helps guards or owner see more, understand faster, and react quicker, which makes the campus safer.

Looking ahead, as technology for predicting problems, using different sensors, and making AI easier to understand gets better, this system will also get smarter. CampusGuardAI is a big step forward. It shows how schools can use smart technology to watch over their campuses in a powerful, growable, and responsible way, while still caring about people's privacy.

7. Acknowledgment

The authors extend their sincere gratitude to Delhi Technical Campus (DTC) for providing the essential infrastructure, computational resources, and institutional support necessary to conduct this research. We also appreciate the great collaboration of the campus security team, whose input and user-testing phases helped shape the system to its current usability and practical relevance. And of course, a shout out to our department mates for their helpful comments during design and validation. The Department of Computer Application academically supported this work; DTC and we are grateful for the encouragement and facilities provided by the administration during the project.

8.References

[1] Agarwal, S., & Mehta, A. (2023). Predicting mental health risk from social media behaviour using ensemble machine learning models. Journal of Biomedical Informatics, 138, 1–12.
[2] Zhang, Z., & Li, B. (2023). Deep learning approaches for depression detection using social media and natural language processing. Neural Networks, 158, 1–13.
[3] Hassan, M., Alam, F., & Islam, T. (2023). Comparative analysis of machine learning classifiers for mental health prediction using social media data. IEEE Access, 11, 23541–23558.
[4] Liu, Y., Wang, Z., & Chen, H. (2023). Transformer-based deep learning models for depression detection on social media platforms. Expert Systems with Applications, 213, 1–14.
[5] Sharma, N., Gupta, P., & Verma, A. (2023). Social media addiction and mental health risk detection using Instagram behavioural features. International Journal of Environmental Research and Public Health, 20(4), 1–18.
[6] Bhatt, R., Patel, S., & Joshi, K. (2023). Impact of excessive Instagram use on anxiety and depression among adolescents: A data-driven study. Journal of Affective Disorders, 320, 412–421.
[7] Van Rossum, G. (2023). Python language reference (Version 3.11). Python Software Foundation. https://www.python.org