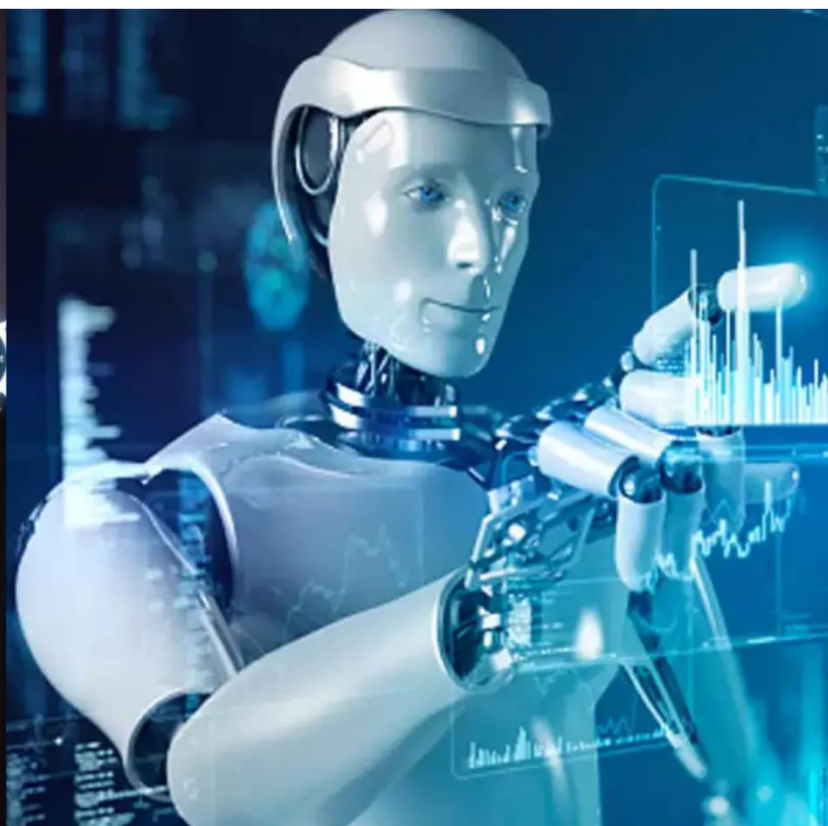




# International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

*(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)*



**Impact Factor: 8.699**

**Volume 14, Issue 3, March 2025**

# **Smart Invigilator : AI Driven Autonomous Exam Hall Monitoring System**

**Bala Yesu Narasimhula<sup>1</sup>, Susmitha Kambhampati<sup>2</sup>, Ganesh Nidigonda<sup>3</sup>, Lony Manchala<sup>4</sup>,  
Ashiq Nawaz Mohammad<sup>5</sup>**

Assistant Professor, Department of Computer Science and Engineering [ Artificial Intelligence and Machine Learning  
], Vasireddy Venkatadri Institute of Technology, Nambur, Andhra Pradesh, India

B.Tech Student, Department of Computer Science and Engineering [ Artificial Intelligence and Machine Learning ],  
Vasireddy Venkatadri Institute of Technology, Nambur, Andhra Pradesh, India

B.Tech Student, Department of Computer Science and Engineering [ Artificial Intelligence and Machine Learning ],  
Vasireddy Venkatadri Institute of Technology, Nambur, Andhra Pradesh, India

B.Tech Student, Department of Computer Science and Engineering [ Artificial Intelligence and Machine Learning ],  
Vasireddy Venkatadri Institute of Technology, Nambur, Andhra Pradesh, India

B.Tech Student, Department of Computer Science and Engineering [ Artificial Intelligence and Machine Learning ],  
Vasireddy Venkatadri Institute of Technology, Nambur, Andhra Pradesh, India

B.Tech Student, Department of Computer Science and Engineering [ Artificial Intelligence and Machine Learning ],  
Vasireddy Venkatadri Institute of Technology, Nambur, Andhra Pradesh, India

**ABSTRACT:** This project presents an advanced solution to examination surveillance by combining AI, computer vision, and real-time video analytics. CCTV cameras are strategically placed in the exam hall to monitor candidates' behavior continuously, detecting unauthorized items and suspicious activities in real time. The system is built on the YOLOv8 model, which classifies student actions as either "cheating" or "normal" based on behaviors such as whispering, excessive head movements, hand gestures, and physical contact with other students. The core anomaly detection mechanism ensures high accuracy in malpractice detection while maintaining fairness in exams. A user-friendly interface allows for efficient exam management, covering logistics, staff deployment, and incident reporting. Detailed anomaly reports provide supervisors with comprehensive insights, helping institutions improve examination processes. By leveraging AI-driven monitoring, this system strengthens academic integrity by reducing unethical practices and fostering trust in assessment procedures.

**KEYWORDS:** Artificial Intelligence, YOLO, Anomaly Detection, Video Surveillance, Real-time Video Analytics, Exam.

## **I. INTRODUCTION**

In today's educational landscape, examinations act as critical benchmarks for evaluating students' knowledge, competencies, and ethical behavior. Yet, the credibility of these assessments is often undermined by academic misconduct, especially cheating during in-person exams. Such unethical practices not only erode trust in academic institutions but also weaken the merit-based principles that underpin educational success. As technology reshapes industries worldwide, its role in safeguarding academic integrity has grown indispensable. Artificial Intelligence (AI) and deep learning, in particular, have proven transformative, offering automated solutions to identify suspicious behavior in exam settings.

Research on cheating reveals multifaceted causes, including poor preparation, anxiety, and gaps in surveillance. Traditional invigilation, dependent on human proctors, struggles to monitor subtle or widespread malpractice effectively.

These shortcomings highlight the need for intelligent systems that can analyze student actions in real time. Recent advancements in computer vision, deep learning, and behavioral analytics have laid the groundwork for innovative solutions.

This study advances these efforts by developing Smart Invigilator, a real-time cheating detection system powered by the YOLOv8 object detection model. The system processes live CCTV footage to classify student behavior as “cheating” or “normal,” identifying anomalies like unauthorized communication, erratic movements, or material exchanges. Unlike manual invigilation, which is subjective and error-prone, this AI-driven approach ensures consistent, scalable, and efficient monitoring.

YOLOv8’s selection stems from its precision, speed, and ability to interpret complex visual data. As a convolutional neural network-based framework, YOLO (You Only Look Once) excels in real-time object detection. The latest iteration, YOLOv8, balances accuracy and computational efficiency, making it ideal for analyzing exam hall dynamics. By leveraging deep learning, Smart Invigilator discerns normal conduct from suspicious acts such as excessive head motion or illicit interactions.

Earlier studies validate AI’s potential in exam proctoring. For instance, YOLO-based systems have detected visual anomalies in exam halls with high accuracy, while deep learning frameworks have automated proctoring processes. These efforts underscore AI’s growing role in upholding academic standards.

Behavioral analytics research further informs this work, including gaze tracking, head pose analysis, and movement detection. Studies on eye movement patterns in e-exams and facial gesture recognition for cheating detection highlight how subtle cues expose dishonesty. Smart Invigilator synthesizes these insights, integrating behavioral recognition with live video analysis.

The system’s implementation involves data collection, model training, and deployment. Labeled CCTV footage trains YOLOv8 to distinguish cheating from non-cheating behavior, with rigorous testing to minimize false alerts. Once deployed, the model triggers real-time notifications for invigilators, enabling swift intervention.

By addressing traditional invigilation’s limitations, Smart Invigilator enhances exam security while deterring misconduct. Its scalability allows institutions to automate monitoring across multiple centers without excessive human oversight.

Beyond cheating prevention, the system promotes a culture of integrity, urging students to adhere to ethical standards and reinforcing fairness in education. Additionally, AI’s integration opens avenues for broader applications, such as attendance tracking, engagement analysis, and adaptive tutoring tools.

In summary, this research develops an AI-powered cheating detection system using YOLOv8 to monitor offline exams in real time. Through data-driven analysis and deployment, Smart Invigilator redefines academic integrity standards, leveraging technology to create a transparent, equitable evaluation process. By combatting malpractice with AI, this work sets a precedent for the future of automated exam supervision.

## **II. LITERATURE REVIEW**

Automated invigilation systems took birth because of rising concerns of academic integrity and the unending limitations of human invigilators. Traditional modes of monitoring examinations, though effective, could not sufficiently limit incidences of cheating in offline examinations. This review of literature discusses studies that exist about intelligent invigilation systems; chiefly, these studies are concerned with anomaly detection, deep learning methodologies, and the use of computer vision in surveillance.

The temporal detection of anomalies has been studied through various machine learning techniques in surveillance systems. Mohan et al. [1], in their work, put across a proposal based on machine learning algorithms that aimed at recognizing unusual activities in video-based surveillance systems. They also demonstrated that these supervised learning models can be trained quite effectively for the purpose of detecting anomalies, allowing the observation of movement

patterns and deviations in behavior. Likewise, Siddiqui and Khan [2] studied the role of surveillance in academic institutions, accentuating the efficacy of AI-enabled monitoring systems. Their investigation reaffirmed the effectiveness of automated invigilation in considerably curtailing cheating behaviors, hence backing the implementation of machine learning in the monitoring system of examinations.

Anomalies and suspicious behaviors might be spotted by deep learning models. An intelligent invigilator system that used an adaptive threshold based on the real-time changes in environment conditions and student behavioral patterns was developed by Fang et al. [3]. This technique improves the accuracy of detection of real-time anomalies by striking down the false positives. Amrutha et al. [4] extended these works of activity detection through deep learning-based surveillance video analysis using Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN)-based methods to recognize any anomalies in behavior. The effectiveness of these methods establishes that they enable outperforming traditional rule-based approaches and are suitable to work under real-time monitoring in examination halls.

Among the visual analysis in surveillance systems, object detection techniques using the Single Shot MultiBox Detector (SSD) and You Only Look Once (YOLO) have been prominent. In relation to intelligent visual monitoring of examination rooms, Xu and Xiao [5] studied the core detection algorithm of SSD, which showed to be effective in finding the motions of students on watching for any unpermitted acts such as the use of mobile phones. Similarly, Charan et al. [6] provided an extensive survey on the detection of abnormal behavior in exam halls, giving insights on various methods in machine learning and deep learning. They efficiently proposed the need for hybrid models by integrating several approaches to enhance accuracy and performance. Results from Rajasekhar et al. [7] proposed that suspicious activity detection is based on a framework of video analysis. Their motions tracking and pattern recognition helped determine several occurrences of mala fides, further implicating AI in academic integrity.

A YOLO based recognition system for examination halls was introduced by Padhiyar and Parmar [8]. The model by making use of YOLO's fast and accurate detection targeted suspicious acts such as a chat between students or the passing of unauthorized materials. The paper presented the value of YOLO, which allowed it to act quickly and be scalable according to large needs.

Bashir and Khan [9] explored AI-integrated video surveillance to maintain examination integrity. The research revealed how automated invigilation decreased the need for human invigilators and enhanced detection accuracy. Ethical considerations were discussed in connection with video monitoring in balancing security and privacy concerns.

### III. METHODOLOGY

The implementation of this project utilizes a structured method intended for the precise detection of malpractices in offline exams with the help of CCTV footages. The methodology that has been used contains some phases. The first phase, requirement analysis, deals with identifying requirements with respect to specifications and functionalities required by the system. One of the main portions of this phase was to provide an automated system that would help analyze CCTV footage, detect malpractices, and send alerts to exam supervisors. The phase is aimed at ensuring the availability of the system according to the expectations of end users and project objectives.

Now, in the system design, the architecture of the application is planned. It will be powered by multiple modules: a video processing module, a deep learning model for the detection of malpractices, a backend for managing data, and a frontend for visualization. The interactions between these layers are all set to ensure efficiency and scalability and make sure real-time performance is possible.

The backend uses the light Flask framework, which is powerful for internal API requests. It is quite easy to connect the deep learning model with the Flask framework, while at the same time, it gives flexibility in handling different parts of the system. The backend would process video data, run the object detection model, and store the relevant results in local storage. HTML, CSS, and JavaScript were being used on the front end to create a user-friendly and interactive UI. In this interface, invigilators can watch a live feed of the exam hall, view cases of malpractice, and obtain reports-all with the ease of a click of a mouse.

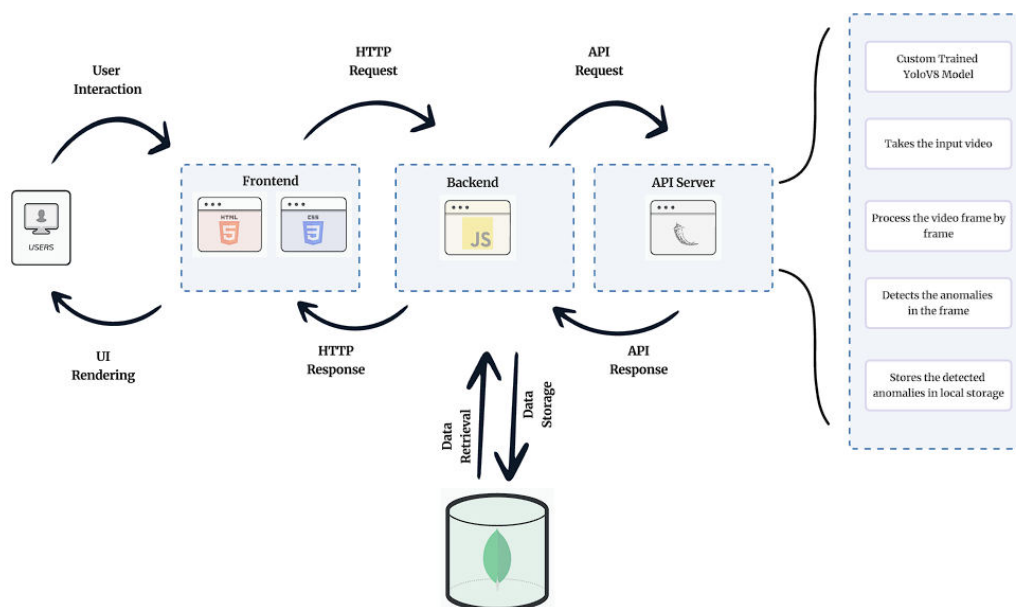


Fig.1 System Architecture

A critical component of the project includes the implementation of YOLO (You Only Look Once) specifically YOLOv8 version which is aimed at real-time malpractice detection. The model is trained to detect behaviors of cheating in examination halls, including but not limited to the use of unauthorized materials, unintentional head movements, etc. Pretrained weights were also fine-tuned on a custom dataset to increase accuracy. The detected cases of malpractice are annotated properly and forwarded for review. Such detected cases of malpractice are then docked and piled for reference usage. Data management was set with MongoDB as the database, setting a NoSQL style that easily creates a database of detected anomalies' video metadata and user long logs. Further exploration of continuous updates and extensions to the system was afforded because the database makes possible efficient queries and data management on which the growth of this system is based. Testing is done to obtain an overall accuracy for detection of the violation cases, intended specifically towards assessing system performance. This involved writing a number of test cases to ensure full functionality checks of each module for robust and reliable systems. Iterations on the performance of the model granted different analyses for exploration of detection failures and misdetections. Finally, in the deployment phase, the whole system is deployed within a server that could be accessed by any user.

#### IV. EXISTING SYSTEM

The existing system identifies suspicious behavior in video surveillance footage through deep learning methods, which makes it very relevant to automated invigilation in examination rooms. Through real-time monitoring of students' behavior during an examination, the system works to minimize the reliance on humans and maximize academic honesty by identifying potential malpractice.

The system works through the processing of real-time video feeds and the detection of unusual student behavior that could signal cheating. It uses motion analysis and behavior recognition methodology to identify abnormal motions like excessive head turns, glancing at other students' papers, or passing signals. Such acts are monitored over time to analyze suspected patterns. Through ongoing tracking of students, the system is able to mark possible cases of cheating and notify the invigilators in real time. The use of real-time video analysis guarantees that interventions are made immediately, minimizing the likelihood of going unnoticed malpractice.

The system is constructed using a combination of a Convolutional Neural Network (CNN) and a Long Short-Term Memory (LSTM) network. The CNN extracts spatial features from single frames of video, including facial direction, hand movements, and posture. At the same time, the LSTM network handles the temporal dependencies in the video, inspecting movement sequences across time to identify suspicious patterns of behavior. This integration of CNN and LSTM enables the model to distinguish well between normal and abnormal behaviors effectively, minimizing false alarms and enhancing the system's reliability. The model illustrated good accuracy when detecting fraudulent behaviors, with the false positive being low, thereby qualifying as a viable solution to be used for automated monitoring of exams.

## V. PROPOSED SYSTEM

The "Smart Invigilator" system aims to facilitate real-time automatic monitoring and identification of malpractices in offline examinations through the use of CCTV feeds. The system starts by consuming live video streams from strategically positioned CCTV cameras within the examination hall. These streams are concurrently processed to obtain holistic coverage. The raw video streams are then partitioned into separate frames, which serve as the building blocks for analysis. Each frame is processed to ensure that essential events are captured accurately. The chosen frames are then passed through a pre-processing pipeline to normalize the input for the deep learning model. The system makes use of a sliding window strategy to process adjacent frames, supporting the detection of temporal patterns of suspicious activity. If a suspected malpractice is found in a series of frames, the system raises an alert, taking a snapshot of the incident for human inspection. The snapshot contains the identified bounding boxes and class labels, offering unambiguous visual proof of the suspected malpractice.

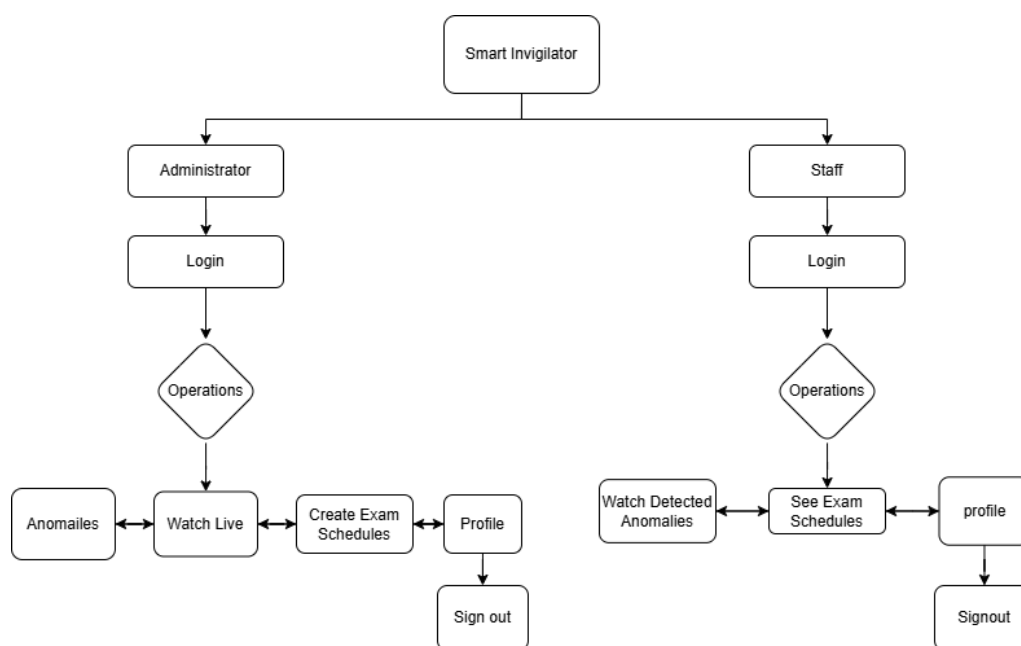


Fig. 2 Flowchart of Proposed System

The real-time processing pipeline is designed to be efficient to process the large amount of video data. The system makes use of a multi-threading architecture to distribute the load between multiple CPU cores and uses GPU acceleration for deep learning inference. The system's output is a timestamped log of malpractices detected along with corresponding static images. This log offers an exhaustive audit trail of the inspection, which may be utilized in post-inspection analysis and examination. An easy-to-use interface enables invigilators to see the alerts and static images, so they can easily determine the situation and respond accordingly.

The system is based on a specially trained YOLOv8 object detection model, which is known for its speed and accuracy in real-time object detection applications. YOLOv8 was selected for its cutting-edge architecture, which includes an

optimal backbone, a strong neck, and a decoupled head to give it an upper hand over older YOLO versions. The model was specifically tuned to identify three main classes of malpractices: use of mobile phones, copying from written notes, and communication among candidates. The architecture of the model includes a CSPDarknet53 backbone for feature extraction, a PANet feature pyramid network to enable multi-scale feature fusion, and a decoupled head for object detection. The decoupled head decouples the classification and regression tasks, resulting in higher accuracy and training stability. The model was pre-trained on the COCO dataset and fine-tuned on the examination malpractice custom dataset. The YOLOv8 model offers bounding box locations, object class probabilities, and confidence levels for every identified object, allowing the system to correctly localize and identify instances of suspicious activity.

Dataset	Normal Images	Cheating Images
Training	4294	5967
Validation	1163	1783
Test	609	873

Table-1 Dataset

Training and validation datasets were carefully crafted to simulate diverse examination scenarios. The dataset contained a mix of real-world and simulated examination videos, covering diverse lighting conditions, camera views, and candidate postures. The dataset contained labeled images and video frames, and bounding boxes accurately annotated instances of the malpractices being targeted. The dataset was divided into training, validation, and test sets to guarantee sound model evaluation. Data augmentation methods were used to increase the diversity of the dataset and enhance the model's ability to generalize. These methods involved random rotations (to 15 degrees), horizontal and vertical flips, random scaling ( $\pm 20\%$ ), brightness and contrast change, and adding Gaussian noise. Preprocessing of data entailed resizing all the images to a uniform input size of  $640 \times 640$  pixels to comply with the YOLOv8 model's input specifications. Pixel values were normalized to the range  $[0, 1]$  by dividing them by 255. Normalization makes the input data of the model have a standard range, hence enhancing training convergence and stability.

Important hyperparameters were chosen wisely to maximize the performance of the model. The learning rate was initially 0.01 and dynamically adjusted with a cosine annealing scheduler with warm restarts, which prevents the model from getting stuck in local minima and converging to a good solution. The batch size was 16, trading off memory usage and training speed. The input image size was set to  $640 \times 640$  pixels, offering a good balance between resolution and computational expense. Hyperparameter optimization was done using a mix of manual trial and error and automated grid search. Grid search tried various values for hyperparameters like weight decay, momentum, and sizes of anchor boxes. The mean Average Precision (mAP) metric was used to measure the performance of each hyperparameter setting, with an aim to maximize the mAP while keeping false positives low. The model was trained over 50 epochs, with early stopping to avoid overfitting. The early stopping feature tracked the validation loss and terminated training when the loss failed to improve by 10 consecutive epochs.

## VI. MODEL EVALUATION

The accuracy, strength, and reliability of system's YOLOv8 object detection model were comprehensively tested using a set of metrics including precision, recall, mean Average Precision (mAP), F1-score, confusion matrix analysis, and Intersection over Union (IoU). Testing was conducted on a separate test dataset, distinct from training and validation datasets, to measure the model's unbiased generalizability.

### 6.1 Precision and Recall Analysis:

Precision and recall are basic metrics for measuring the performance of an object detection model.

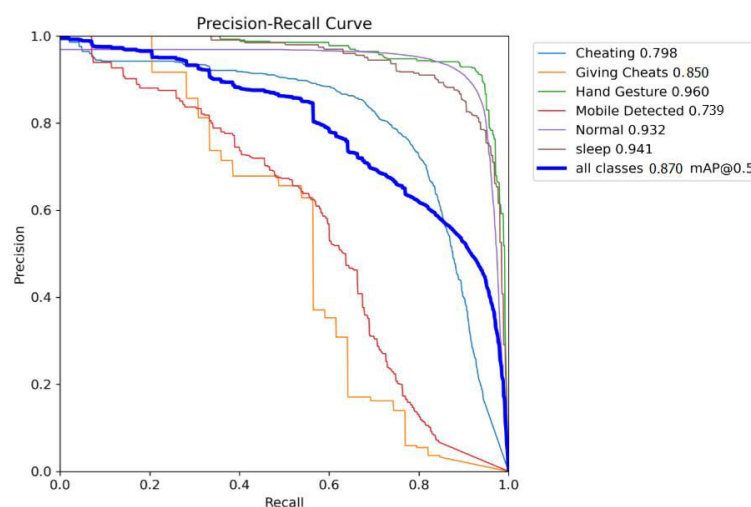
Precision measures the number of correctly identified malpractice cases out of the total number of instances labeled as malpractice by the model.

$$\text{Precision} = \frac{\text{TruePositives}}{\text{TruePositives} + \text{FalsePositives}}$$

Recall, also referred to as sensitivity, calculates the ratio of correctly detected malpractice cases to the total number of actual malpractice cases in the dataset.

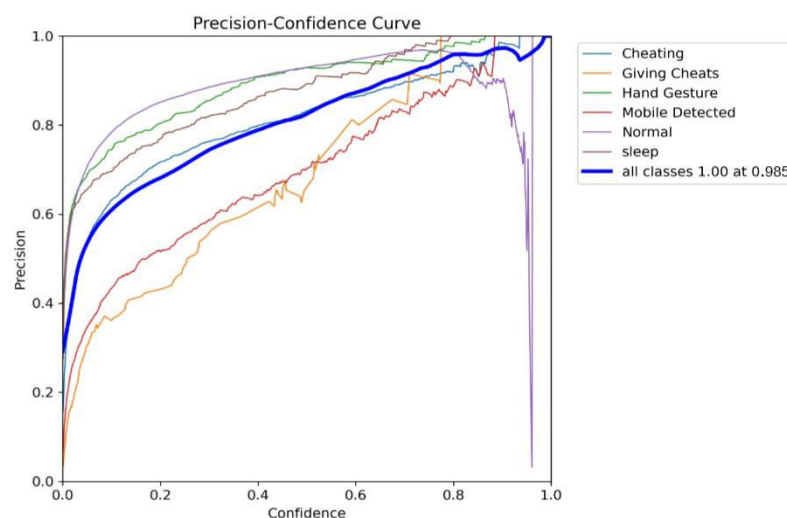
$$\text{Recall} = \frac{\text{TruePositives}}{\text{TruePositives} + \text{False Negatives}}$$

Precision-Recall (PR) curve was plotted to examine the precision-recall trade-off at different confidence thresholds. The area under the PR curve reflects the model's overall detection ability. The greater the area under the curve, the better the precision-recall balance.



**Fig.3 Precision-Recall Curve**

A Precision-Confidence Curve was examined, which showed variation in precision at varying levels of confidence. A model with high precision even at lower confidence scores indicates that it can make the correct predictions regardless of levels of uncertainty. The results of the evaluations show that the precision is consistently high in various confidence scores.



**Fig.4 Precision-Confidence Curve**

A Recall-Confidence Curve was created to show the interaction between recall and confidence thresholds. In line with expectation, recall diminishes with growing confidence threshold, which emphasizes the trade-off between increasing confidence and recall performance.

## 6.2 F1-Score Assessment:

The F1-score is also a very important metric that trade-offs precision and recall. It is the harmonic mean of precision and recall

$$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

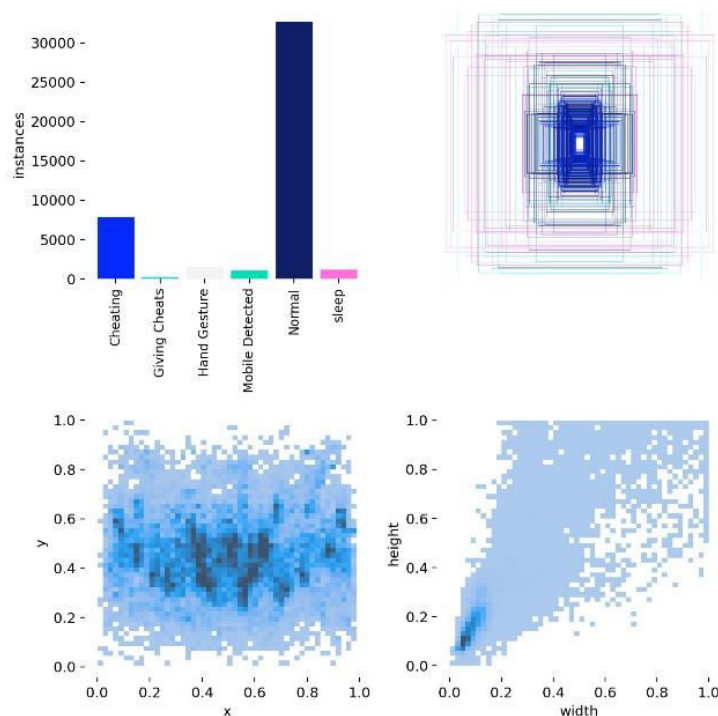
## 6.3 Mean Average Precision (mAP) Analysis:

The mean Average Precision (mAP) measure is used extensively in object detection tasks for measuring the performance of models over multiple classes. mAP is calculated by averaging the Average Precision (AP) across all classes, where AP is calculated by finding the area under the PR curve per category.

For this assessment, mAP@0.5 was employed, which calculates the AP at an Intersection over Union (IoU) threshold of 0.5. The model had a mAP@0.5 value of 0.870, showing excellent overall performance in identifying different malpractice cases. A closer look at the Precision-Confidence Curve showed that precision for all classes was 0.93 at 0.000 confidence and 1.00 at 0.987 confidence, affirming the model's high accuracy at various confidence thresholds.

## 6.4 Class-wise Precision and Recall Analysis:

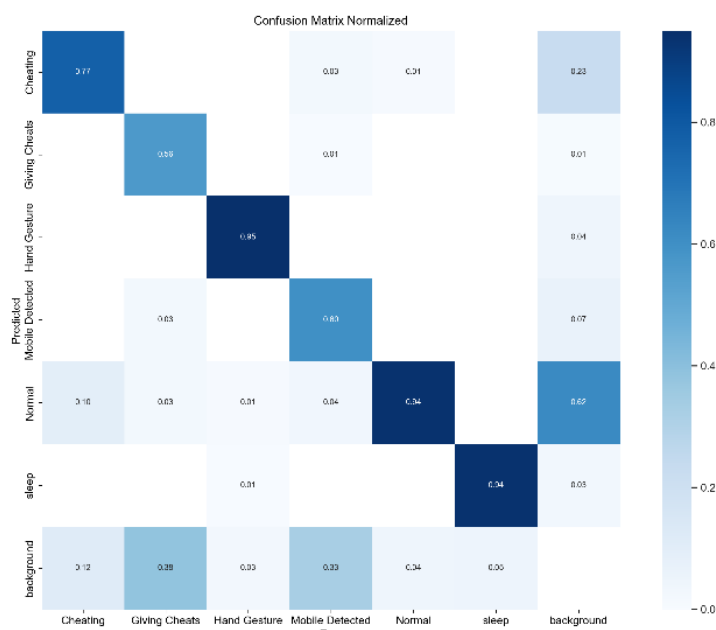
The analysis also entailed a class-wise evaluation of recall and precision on various categories of malpractice: Cheating, Giving Cheats, Hand Gesture, Mobile Detected, Normal, and Sleep. The findings revealed high accuracy of detection for classes like Hand Gesture and Normal, while Giving Cheats and Mobile Detect-ed reflected relatively lower values. The analysis suggests possible model improve-ment avenues, specifically in cases of less frequent or more uncertain instances of malpractice.



**Fig.5 Class-wise Precision and Recall Analysis**

### 6.5 Analysis of Confusion Matrix:

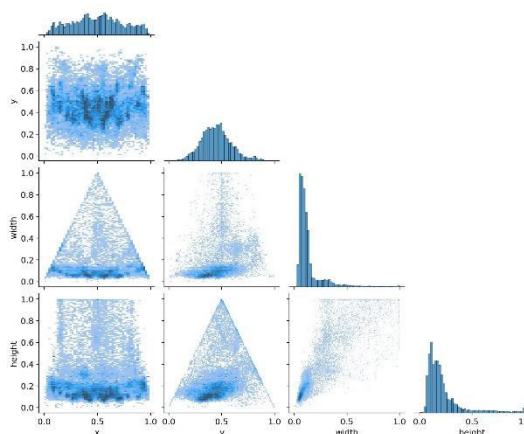
Confusion Matrix was created in order to present the detailed split-up of predictions by the model, classifying them as True Positives, False Positives, True Negatives, and False Negatives for every class.



**Fig.6 Analysis of Confusion Matrix**

### 6.6 Object Size Distribution Analysis:

To further understand the model's performance, an analysis of the object size distribution in the dataset was conducted. Graphs depicting the distribution of bounding box dimensions (x, y, width, height) provided insights into how the model handles objects of varying sizes. This analysis helps identify potential challenges in detecting small or occluded objects and guides further improvements in model training and data augmentation strategies.



**Fig.7 Object Size Distribution Analysis**

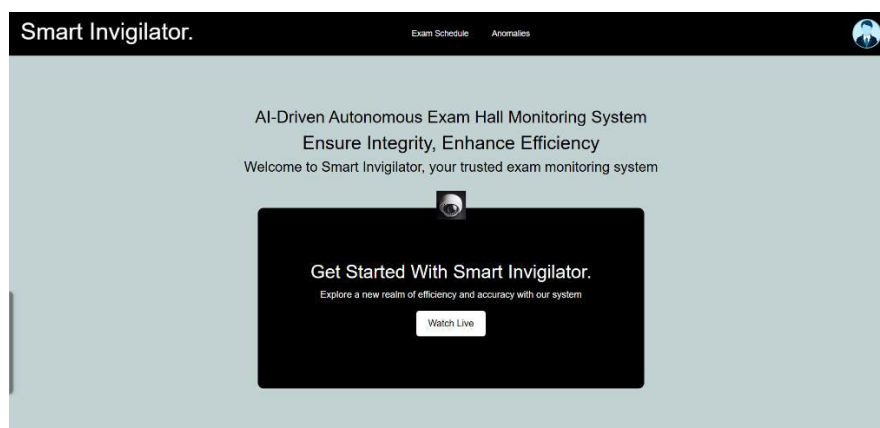
## VII. RESULTS

This system has a user-friendly interface developed for smooth interaction, allowing invigilators to track examination rooms in real time. The interface shows detected malpractice cases, marks suspicious behavior, facilitating administrators to review and respond to violations easily. The real-time detection of the system provides effective and automated monitoring, minimizing dependence on manual monitoring.

Precision-recall (PR) curve depicts a great trade-off between false positives and false negatives with a mean Average Precision (mAP@0.5) of 0.870 obtained by the model. Class-wise examination showed the model to have good accuracy in Hand Gesture and Normal, and slightly lower values for precision and recall in Giving Cheats and Mobile Detected. The Precision-Confidence Curve was 0.93 at 0.000 confidence and 1.00 at 0.985 confidence, while the F1-score was 0.82 at 0.400 confidence, with strong classification power.

The confusion matrix analysis gave insights on the model's classification performance. Misclassifications were noted across similar classes, like Giving Cheats being miscategorized with Cheating and Mobile Detected with Normal. Yet the normalized confusion matrix indicated that classes were correctly classified with high precision.

The Intersection over Union (IoU) measure validated accurate localization of malpractice cases, with bounding box examination demonstrating effective detection of different sizes of objects. Minor issues were, however, reported in detecting small or occluded objects.



**Fig.8 Web Interface**

In general, the "Smart Invigilator" system demonstrates high recall, precision, and generalization capacity, and it is a potential solution for offline examination malpractice detection using automated means. Potential future enhancements would involve increased dataset diversity, optimized hyperparameters, and better misclassification handling, further enhancing its real-world viability.

## VIII. CONCLUSION

The Smart Invigilator system, driven by the YOLOv8 object detection model, has reflected high accuracy in identifying malpractices during exams from CCTV video analysis. The model accurately detects different malpractice categories such as Cheating, Giving Cheats, Hand Gesture, Mobile Detected, Normal, and Sleep, providing end-to-end surveillance for offline exam settings. The evaluation of the system based on precision, recall, F1-score, mAP, and IoU guarantees its stability, dependability, and generalization capability under multiple situations. The analysis of the confusion matrix shows very few misclassifications, with most instances being correctly identified. Furthermore, the PR curve and confidence-based tests show that the model is consistently well-balanced between precision and recall, even at different confidence levels. By utilizing sophisticated deep learning methods, the system presents an automated, effective, and scalable solution to ensure fairness in exams, minimizing the need for costly human oversight.

### **IX. FUTURE SCOPE**

The future horizon of AI powered exam hall monitoring system comprises dataset increase and enrichment to enhance detection in diverse conditions, hyperparameter fine-tuning, and incorporation of self-learning abilities for better accuracy. Real-time notification and automatic reporting may enable instant alerts, whereas biometric identification and NLP-enabled speech analysis could identify verbal misdoings. Implementation on the edge device would make it more efficient by cutting down latency. In addition, explainable AI (XAI) methods can enhance model interpretability. These developments will help make Smart Invigilator a more accurate, adaptive, and wise examination monitoring system for guaranteeing academic integrity and fairness globally.

### **REFERENCES**

- [1] Mohan, A., Choksi, M., & Zaveri, M. A. (n.d.)(2019), "Anomaly and activity recognition using machine learning approach for video based surveillance", in Research gate.
- [2] Siddiqui, M. A., & Khan, M. (2021). "Examining the Role of Surveillance in Academic Integrity." International Journal of Academic Research in Business and Social Sciences, 11(1), 1-10.
- [3] Fang, Y.; Ye, J.; Wang, H. Realization of Intelligent Invigilation System Based on Adaptive Threshold. In Proceedings of the 2020 5th International Conference on Computer and Communication Systems (ICCCS), Shanghai, China, 15–18 May 2020; pp. 201–205.
- [4] Amrutha, C. v., Jyotsna, C., & Amudha, J. (2020), "Deep Learning Approach for Suspicious Activity Detection from Surveillance Video" , in 2nd International Conference on Innovative Mechanisms for Industry Applications, ICIMIA 2020 Conference Proceedings, 335–339.
- [5] Xu, T.; Xiao, H. Application of SSD core detection algorithm in intelligent visual monitoring of examination room. J. Phys. Conf. Ser. 2021, 2037, 012085.
- [6] Charan A, Darshan D, Madhu N, Manjunatha B S. "A SURVEY ON DETECTION OF ANOMALOUS BEHAVIOUR IN EXAMINATION HALL", International Journal of Engineering Applied Sciences and Technology, 2020 Vol. 5, Issue 2, ISSN No. 2455-2143, Pages 583-588 Published Online June 2020 in IJEAST <http://www.ijeast.com>
- [7] P. Rajasekhara Reddy, B. Nirupa, Preetham Kumar, S. Vaishnavi, "SUSPICIOUS ACTIVITIES DETECTION USING VIDEO ANALYSIS" , Science, Technology and Development Volume X Issue VIII AUGUST 2021 ISSN : 0950-0707
- [8] Priyanka Padhiyar and Kajal Parmar, "Visual Distance Fraudulent Detection in Exam Hall using YOLO Detector", in 2023 International Conference on Inventive Computation Technologies (ICICT), Gujarat, India.
- [9] Bashir, M., & Khan, M. (2019). "Monitoring Examination Environment Using Video Surveillance." International Journal of Advanced Research in Computer Science, 10(5), 1-5.



INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  [ijirset@gmail.com](mailto:ijirset@gmail.com)



[www.ijirset.com](http://www.ijirset.com)

Scan to save the contact details