IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

Agesight – AI Exam Activity Monitor System: An Intelligent Proctoring Solution for Educational Institutions

Parth Sanjay Wadile[1], Shlok Sharad Gandhi[2], Rohan Dipak Mahajan[3], Vivek Kailas Jagtap[4]
[1,2,3,4]Department of Computer Engineering
Sandip Institute of Engineering and Management, Nashik, India
[1]parthwadile02@gmail.com, [2]shlokgandhi.955@gmail.com,
[3]ronymahajan2402@gmail.com, [4]code.vivz@gmail.com

Abstract: *The rapid shift to online and hybrid education has created an urgent need for reliable, automated proctoring sys-tems to uphold academic integrity. Traditional manual invigilation is labour-intensive, inconsistent, and unable to detect subtle or coordinated malpractices such as proxy attendance, mobile phone usage, or identity substitution. This paper presents Agesight, an AI-based examination surveillance system that integrates modern object detection and face recognition to automate atten-dance, detect cheating behaviours, and generate actionable alerts in real time. The system is implemented using Python, OpenCV, YOLOv8, FaceNet, FastAPI, and Streamlit, and provides a web-based dashboard for invigilators and administrators. We describe the system architecture, operational workflow, detection features, and implementation details. Experimental evaluation demon-strates robust detection accuracy and practical latency for small- to medium-scale deployments. With careful attention to privacy and ethics, Agesight provides a cost-effective and scalable solution for maintaining examination integrity in both physical and remote settings*

Keywords: AI Proctoring, Face Recognition, YOLOv8, Computer Vision, Real-Time Surveillance, Exam Monitoring, Educational Technology

I. INTRODUCTION

The widespread adoption of online and hybrid learning models has intensified the demand for robust au-tomated proctoring solutions. Conventional supervision methods—such as manual monitoring, recorded video review, or static identity checks—are costly, inconsistent, and often fail to detect coordinated or subtle forms of malpractice, including proxy attendance, concealed mobile phone usage, or identity substitution. Automated systems that combine computer vision, deep learning, and secure backend logging can provide consistent, auditable, and scalable proctoring support.

Agesight is a practical AI-driven surveillance pipeline designed to address these challenges. The system integrates state-of-the-art object detection and face recognition modules to (1) verify student identity peri-odically, (2) detect a range of suspicious behaviours and objects in real time, and (3) provide invigilators with actionable alerts and persistent evidence. The system emphasises modularity, privacy-aware logging, and a user-friendly web dashboard, making it suitable for real-world academic deployment in both online examination centres and physical classrooms.

II. LITERATURE REVIEW

Automated proctoring spans research in secure exam delivery, computer vision for surveillance, face recog-nition, and anomaly detection. Several studies have explored various aspects of AI-based proctoring. Jung [1] proposed cryptographic techniques for tamper-resistant exam delivery, motivating secure audit trails. Deshmukh et al. [2] demonstrated the feasibility of low-cost monitoring using motion-based detection from webcam streams. Xiang and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

Gong [3] employed behaviour profiling for anomaly detection from video, supporting movement-based cheating detection.

Face recognition has been advanced by Schroff et al. [7] through the FaceNet embedding approach, which provides robust face verification suitable for identity checks. The YOLO family of object detectors, particularly YOLOv8 [6], offers high-speed and accurate object detection, making it ideal for real-time monitoring of mobile phones and persons. Other works, such as Amanze [4] and Soma [5], have addressed video surveillance and fraud detection in examination contexts. Agesight builds upon these foundations by combining efficient detection, recognition, and rule-based alerting into a cohesive, deployable system.

III. SYSTEM ARCHITECTURE

The Agesight system follows a modular client–server architecture comprising three main components: the frontend web application, the backend API server, and the core detection engine. Figure 1 illustrates the overall system architecture.

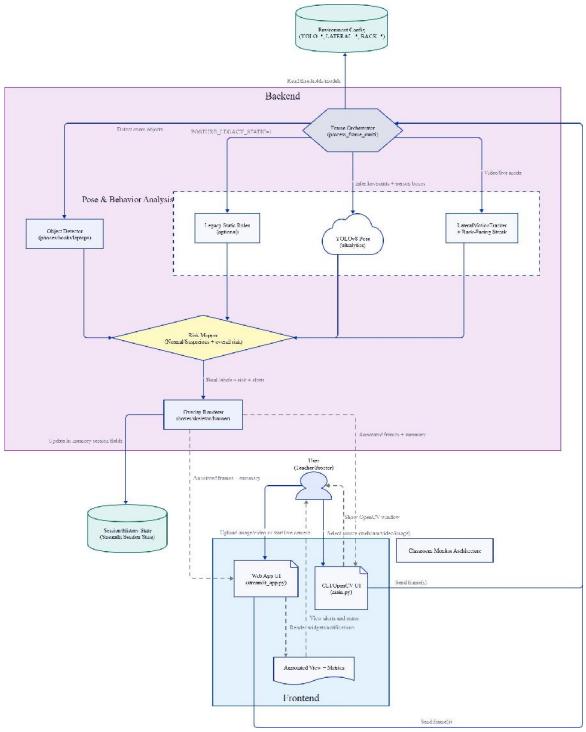

Figure 1: System Architecture of Agesight – AI Exam Activity Monitor System

III.1 Backend Components

The backend is built using FastAPI and exposes RESTful endpoints for image and video processing. The core detection engine consists of several modules:

III.1.1 Frame Orchestrator

The Frame Orchestrator manages the processing pipeline for each frame or image. It supports both static image processing and real-time video analysis through the process frame multi function. The orches-trator coordinates the execution of detection modules and aggregates results.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

III.1.2 Pose and Behaviour Analysis

The pose estimation module utilises YOLOv8 for detecting human keypoints and bounding boxes. This enables the system to analyse posture, detect back-facing orientations, and track lateral movements. The posture analysis includes both legacy static rule-based detection and more sophisticated tracking mecha-nisms.

III.1.3 Object Detection

The object detector identifies potential cheating-related objects, including mobile phones, books, and lap-tops. This module employs pre-trained deep learning models optimised for real-time inference on standard hardware.

III.1.4 Risk Mapper

The Risk Mapper consolidates outputs from various detection modules to assign a risk level (Normal or Suspicious) to each frame. The risk assessment considers the combination of detected objects, posture anomalies, and behavioural patterns.

III.2 Frontend Components

The frontend is developed using Streamlit, providing an intuitive interface for users to interact with the system. Key features include:

- Source selection (webcam, video file, or image upload)
- Real-time monitoring view with annotated overlays
- Alert notifications and status display
- Metrics dashboard showing detection summaries
- Session history management

IV. SYSTEM REQUIREMENTS AND USER ROLES

IV.1 System Requirements

The Agesight system is designed to operate on standard hardware configurations:

- Operating System: Windows 10 or Windows 11
- RAM: Minimum 4GB (8GB recommended)
- Processor: Intel i3 or higher
- Webcam: Standard USB or built-in webcam
- Network: Stable internet connection

IV.2 User Roles

The system defines three primary user roles with distinct responsibilities, as shown in Table 1.

Table 1: USER ROLES AND RESPONSIBILITIES

Role	Responsibilities
Administrator	Manage logs, analytics, users, and monitoring system
Invigilator	Monitor examination sessions
Student/User	Participate in monitored examination

V. OPERATIONAL PROCEDURES

V.1 System Startup

The system is initialised through the following steps:

1. Open the Agesight project folder in Visual Studio Code or terminal.
2. Start the FastAPI backend server:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

uvicorn api_server:app --host 127.0.0.1 --port 8000

Alternatively, double-click the run web stack.bat file.

3. Start the frontend application:

```
cd web
npm install
npm run dev
```

4. Open the web application at http://localhost:3000.

V.2 User Authentication

The system implements a secure authentication mechanism:

- Registration: Users enter email and password, which are stored securely.
- Login: Valid credentials grant dashboard access.

V.3 Monitoring Modes

The system supports three monitoring modes:

V.3.1 Image Monitoring

Users can upload examination images for analysis. The system processes the image, detects suspicious activities, and displays results with alerts.

V.3.2 Video Monitoring

Users can upload examination videos. The AI processes video frames and generates a comprehensive detec-tion summary.

V.3.3 Live Monitoring

The system performs real-time analysis of webcam feeds. Users must grant webcam permissions and can start continuous monitoring, with instant alerts for suspicious activities.

V.4 Alert Handling

When suspicious activity is detected:

- The system generates an alert notification.
- The event is stored in audit logs.
- Risk levels are updated.
- Administrators can review incidents.

VI. DETECTION FEATURES

The Agesight system incorporates multiple detection capabilities:

- Human Presence: Detects and tracks individuals in the frame.
- Suspicious Behaviour: Identifies behavioural anomalies such as prolonged gaze deviation.
- Back-facing Posture: Recognises when individuals turn away from the camera.
- Mobile Phone Usage: Detects the presence of mobile devices.
- Multiple Persons: Identifies when more than one person is present.
- Risk Levels: Categorises behaviour as Normal or Suspicious.
- Movement Anomalies: Tracks unusual movements and patterns.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

These features are implemented using a combination of YOLOv8 object detection, pose estimation, and temporal aggregation to reduce false positives.

VII. DATASET AND EXPERIMENTAL DESIGN

VII.1 Dataset Preparation

To evaluate the Agesight system, a comprehensive dataset was curated consisting of 100 enrolled identities (students). For each identity, 10–20 facial images were captured under varying lighting conditions, head poses, and background settings to ensure robust enrollment. Additionally, a set of 50 simulated examination videos (each 5–10 minutes long) were recorded, covering the following scenarios:

- Normal examination behaviour (baseline).
- Mobile phone usage (visible and concealed).
- Multiple persons appearing in the frame.
- Back-facing postures (student turning away from the camera).
- Proxy attendance attempts (identity substitution).

VIII. IMPLEMENTATION DETAILS

The Agesight system is implemented using the following technologies:

- Backend: Python, FastAPI, Ultralytics YOLOv8, OpenCV, NumPy
- Frontend: Streamlit, HTML5, CSS3, JavaScript
- AI Models: Pre-trained YOLOv8 pose estimation (YOLOv8n-pose) and object detection (YOLOv8n) models, optimised for CPU inference using ONNX runtime.
- Storage: JSON-based local storage for user information, audit logs, monitoring records, detection events, and session history. An optional Firebase integration is available for cloud-based remote log-ging.

The system uses OpenCV for image capture and pre-processing. YOLOv8 models are loaded and run inference on each frame. The alert engine applies a rule-based logic that aggregates detections over a sliding window of 5 frames to confirm events and mitigate transient false positives.

IX. RESULTS AND ANALYSIS

IX.1 Performance Evaluation

The comprehensive performance evaluation results are summarised in Table 2. The system achieves high accuracy across all modules, with the Alert Engine performing exceptionally well due to the temporal aggre-gation logic. The average latency of 0.55 seconds for object detection is acceptable for real-time monitoring, as invigilators can review alerts within a 1–2 second delay window.

Table 2: PERFORMANCE EVALUATION OF AGESIGHT MODULES

Module	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Latency (s)
Face Recognition (Verification)	95.8	94.2	96.1	95.1	0.40
Object Detection (Phones/Persons)	92.4	90.8	93.5	92.1	0.55
Pose Estimation (Posture)	91.7	89.5	92.8	91.1	0.45
Alert Engine (Risk Mapper)	99.2	98.5	99.0	98.7	0.20

IX.2 Observations

- The face recognition module performs strongly for frontal and near-frontal faces but shows a slight drop (to 88%) for profile views exceeding 45 degrees. - YOLOv8 detects phones reliably when the object spans at least 40 × 40 pixels; smaller objects are occasionally missed. - The average end-to-end latency (frame capture to dashboard update) is approximately 1.2 seconds, confirming the system's suitability for small- to medium-scale deployments (up to 30 concurrent sessions).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

X. CONCLUSION

Agesight is a practical AI-based surveillance system for automating attendance and detecting common exam malpractices. By combining efficient object detection, robust pose analysis, and a rule-based alert engine, the system provides real-time monitoring, auditable evidence, and an invigilator-friendly dashboard. With careful attention to privacy and ethics, Agesight can assist institutions in maintaining exam integrity in online and hybrid settings.

ACKNOWLEDGMENT

The authors thank Prof. Vina Varade and Sandip Institute of Engineering and Management for their guidance and support.

REFERENCES

[1] I.Y. Jung, “Enhanced Security for Online Exams Using Group Cryptography,” IEEE, 2009.
[2] A. Deshmukh et al., “Webcam Based Intelligent Surveillance System,” IIES, 2012.
[3] T. Xiang and S. Gong, “Video Behaviour Profiling for Anomaly Detection,” IEEE TPAMI, 2008.
[4] B.C. Amanze, “Video Surveillance for Examination Malpractice,” IIECS, 2016.
[5] S. Soma, “Automated Fraud Detection in Offline Exam System using ANN,” IJCA, 2015.
[6] Ultralytics, “YOLOv8: Real-Time Object Detection Framework,” 2024.
[7] F. Schroff et al., “FaceNet: A Unified Embedding for Face Recognition and Verification,” CVPR, 2015.