EdinBurg Peer Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 9||pp 12-27||September||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

Design and Implementation of an E-Exam Cheating Control System Using Real-Time Monitoring and Behavioral Detection

Gusenga Derrick[1*], Dr. Djuma Sumbiri[2], Dr. Jonathan Ngugi[3], Patrick Habimana[4]
Faculty of Computing and Information Sciences, Department of Information Technology
University of Lay Adventist of Kigali (UNILAK)
Corresponding Emails: gusengaderrick@gmail.com; sumbirdj@gmail.com; phialn1@gmail.com; habimanapat7@gmail.com

Accepted: 15 July 2025 || Published: 20 September 2025

Abstract

The increasing shift toward online learning and digital examinations has introduced a range of challenges, particularly in maintaining academic integrity. This paper presents the design and implementation of an E-Exam Cheating Control System aimed at detecting and reducing cheating during online examinations. The system integrates multiple technologies, including webcam-based facial recognition, screen activity monitoring, keyboard and mouse behavior logging, and network traffic inspection, to ensure exam fairness. A rule-based engine and AI-powered behavior detection model are used to identify suspicious patterns such as multiple face presence, gaze switching, use of unauthorized devices, and switching away from the exam window. The system was developed using PHP, JavaScript, and OpenCV for facial recognition and tested across different environments and exam scenarios. Results show the system's effectiveness in identifying cheating attempts with a detection accuracy of over 90% in controlled settings. A comparative analysis with other systems demonstrates its robustness and adaptability. The research contributes to the field of e-learning security and proposes improvements for future systems, including privacy-preserving mechanisms, offline examination support, and multi-factor identity verification. The system has potential for real-world deployment in educational institutions to promote integrity in digital assessments.

Keywords: *E-exam, cheating detection, online proctoring, academic integrity, facial recognition, real-time monitoring, behavioral analysis*

How to Cite: Gusenga, D., Sumbiri, D., Ngugi, J., & Habimana, P. (2025). Design and Implementation of an E-Exam Cheating Control System Using Real-Time Monitoring and Behavioral Detection. *Journal of Information and Technology, 5*(9), 12-27.

1. Introduction

The evolution of digital technologies has transformed educational systems across the globe. One major advancement is the adoption of electronic examinations (e-exams), particularly in higher education institutions. E-exams provide flexibility, speed, and cost-effectiveness in assessing students' knowledge. However, despite these benefits, they introduce significant concerns related

to academic honesty. Cheating in online exams has become a widespread issue, facilitated by the lack of physical supervision and the ease of accessing unauthorized resources.

Traditional methods of proctoring, such as physical invigilation, are ineffective in an online context. Furthermore, manual proctoring via video calls can be resource-intensive and prone to human error. There is an urgent need for automated systems capable of monitoring candidates during online assessments and detecting any abnormal or suspicious behavior in real-time.

This research presents the design and development of an E-Exam Cheating Control System that leverages real-time monitoring technologies and behavioral analysis to minimize academic misconduct during e-assessments.

The system combines facial detection, activity logging, and screen tracking techniques to flag and record potentially dishonest behavior. The goal is to contribute a practical and reliable tool that strengthens academic integrity in the digital learning environment.

1.1 Problem Statement

The increasing prevalence of online examinations has led to a surge in cheating and other forms of academic dishonesty. Current e-exam platforms either rely on passive supervision or use simplistic monitoring mechanisms that fail to detect more sophisticated cheating techniques, such as using hidden devices, impersonation, or switching between applications. Manual proctoring methods are limited in scalability, accuracy, and cost-efficiency. There is a lack of robust, real-time, and intelligent systems that can automatically monitor, detect, and report suspicious behavior during online examinations. Without such systems, the credibility of e-learning assessments remains at risk, and the value of academic qualifications may be compromised.

1.2 Objectives

1.2.1 General Objective:

To develop a smart E-Exam Cheating Control System that monitors and detects academic dishonesty using real-time behavioral and facial analysis.

1.2.2 Specific Objectives:

- To identify the main cheating techniques used in online exams.
- To design a system that can detect multiple faces, gaze switching, and absence from the screen.
- To monitor user activity such as mouse clicks, keyboard input, and screen focus during exams.
- To implement an alert mechanism that flags suspicious behavior in real time.
- To evaluate the system's accuracy and efficiency in different exam scenarios.

2. Literature Review

The adoption of e-exams has surged due to advancements in digital education and the global necessity for remote learning, especially highlighted during the COVID-19 pandemic. However, this shift has been accompanied by serious concerns over academic integrity. A number of studies and systems have been proposed to address cheating in online examinations, each using different techniques and technologies.

EdinBurg Peer Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 9||pp 12-27||September||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

2.1 Traditional E-Proctoring Systems

Many early e-proctoring systems relied on video conferencing platforms such as Zoom or Skype to enable human invigilators to monitor students remotely. While this method provided a basic level of supervision, it suffered from several limitations, including a lack of scalability, potential distractions, and overreliance on human judgment. These manual methods were labor-intensive, time-consuming, and often impractical for large-scale deployment (Nigam, Pasricha, Singh, & Churi, 2021).

2.2 AI-Powered Proctoring Solutions

Recent studies and open-source initiatives have introduced AI-based proctoring systems that utilize facial recognition and behavioral analysis to detect anomalies during online exams. For example, the *Advanced-Proctoring-System* by Kevalshah91 employs OpenCV and deep learning techniques such as YOLO and MediaPipe to monitor eye movement, detect multiple faces, and identify mobile phones in real time—alerting invigilators when suspicious behavior occurs (Kevalshah91, 2021).

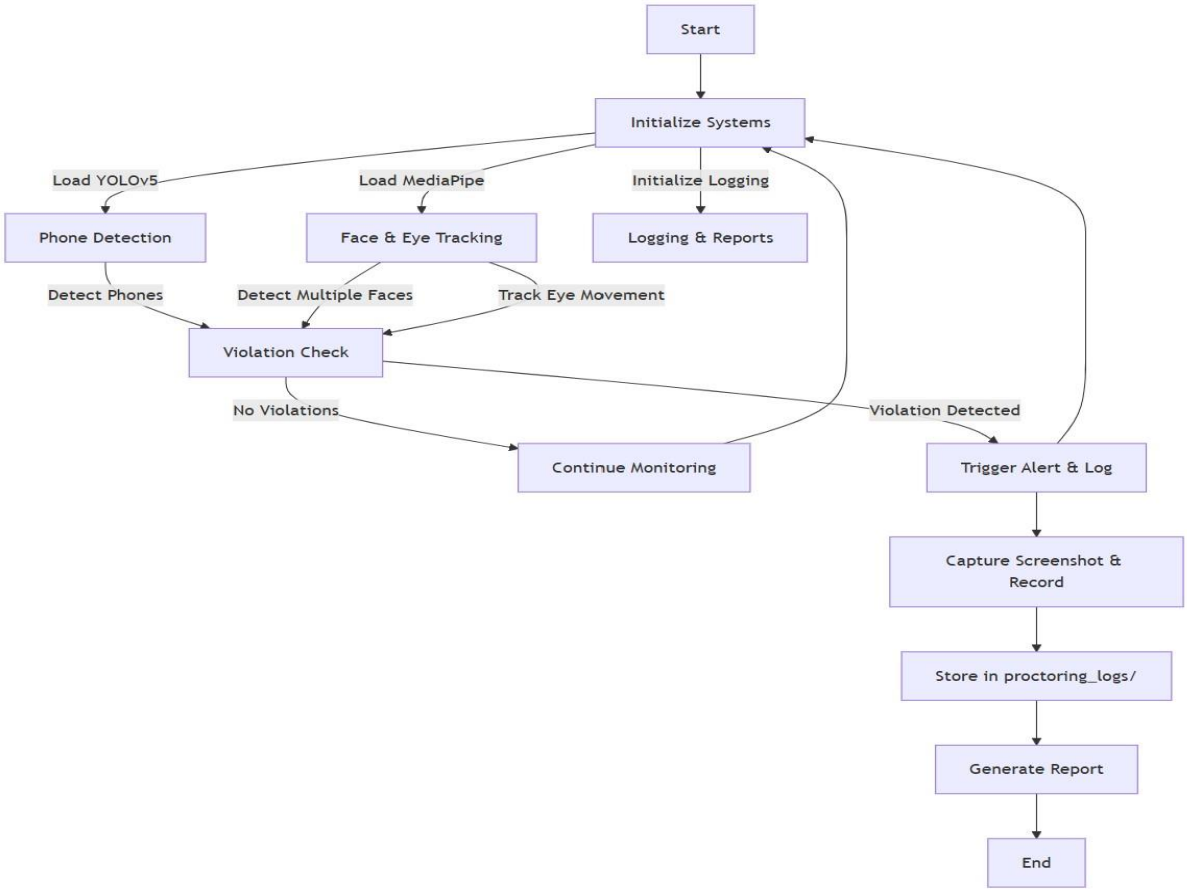

Figure 1: proctoring Advance Proctoring System Flowchart

Furthermore, reviewed AI's growing role in assessment security, identifying strengths and challenges in current systems. Studies show that gaze detection systems often struggle under real-

world conditions. For instance, Wang (2020) found that head-pose variations and lighting inconsistencies negatively impact the performance of remote gaze estimation tools. Similarly, Kar (2020) demonstrated how even consumer-grade eye-tracking systems exhibit substantial error under fluctuating environmental conditions and user behavior.

2.3 Limitations of Existing Systems

Despite significant advancements in AI-powered proctoring technologies, many existing systems continue to face several notable challenges:

- **False positives:** Environmental factors such as poor or uneven lighting can interfere with face detection algorithms, resulting in frequent false alarms where legitimate behaviors are mistakenly flagged as suspicious (Nigam A. P., 2021).
- **Privacy concerns:** Continuous video monitoring and the collection of sensitive biometric data raise serious privacy and ethical issues. Users are often concerned about how their data is stored, who has access, and how long it is retained, especially in the absence of clear regulatory guidelines. (Medianama, 2020).
- **Limited detection of sophisticated cheating:** Most proctoring solutions focus on webcam feeds and screen activity, but they can't see what's happening off-screen. A test-taker can easily use a second device or have unauthorized materials just outside the camera's view. (Proctaroo, 2023).

2.4 Hybrid Approaches

Some researchers have proposed hybrid systems that combine biometric authentication (like facial recognition, fingerprint scanning, or keystroke dynamics) with system-level monitoring (such as screen activity, keystroke patterns, and mouse behavior) to enhance verification accuracy. These multi-modal fusion approaches - melding physiological and behavioral traits - have shown improved reliability in continuous authentication scenarios (Purohit, 2022). Deep learning frameworks have also been used for multi-modal data fusion to detect cheating behavior more reliably (Lamba, 2024).

However, despite their promise, they remain largely unimplemented in mainstream proctoring solutions due to their technical complexity and higher implementation costs.

2.5 Behavior Analysis and Emerging Technologies

New approaches in proctoring explore behavioral biometrics, emotion detection, and anomaly tracking:

- (Ow Tiong, 2022) Implemented AI-based detection of tab switching, keyboard use, and network data anomalies to predict cheating events.
- (Kaur, 2021) Combined sentiment analysis with facial recognition to assess candidate stress.
- (Alenezi, 2023) Developed a multi-agent model that monitors eye movement, typing speed, and IP shifts.

2.6 Ethical, Legal, and Social Implications

Algorithmic bias and ethical concerns are central to the debate on e-proctoring. (Nissenbaum, 2009) Argues for context-based privacy in surveillance systems. Student advocacy groups and institutions have raised concerns about bias and mental health impacts. These concerns often lead to low acceptance of proctoring tools, despite their technical capabilities (Teo, 2022).

2.7 Comparative System

Evaluations Several comparative studies demonstrate the strengths and weaknesses of different platforms:

- (Jain, 2021) Evaluated five commercial e-proctoring systems, highlighting trade-offs between accuracy and privacy.
- (Pathak, 2022) Analyzed open-source tools like Examity, ProctorU, and SMOWL based on latency, detection rate, and storage policy.
- (Bulut, 2024) Explored neural networks and eye-blinking detection algorithms as enhancements.

2.8 Research Gap

Most existing research focuses on single-method detection techniques and overlooks a comprehensive, real-time, multi-modal monitoring system. This research aims to fill that gap by proposing and implementing an integrated E-Exam Cheating Control System that combines facial recognition, behavioral tracking, and system monitoring in a real-time environment.

3. Methodology

This research adopts a design and implementation-based methodology, focusing on the development and evaluation of an E-Exam Cheating Control System. The methodology involves requirement analysis, system design, component implementation (Programming), testing, and integration under real exam-like scenarios.

3.1 System Requirements

3.1.1 Functional Requirements:

The system begins by authenticating the student through facial recognition before allowing access to the exam. Once the exam starts, it continuously monitors the student's face and gaze direction to ensure they remain focused on the screen. If additional faces appear in the webcam feed, the system detects and logs them as potential violations. It also tracks keyboard and mouse activity to identify irregular behavior patterns. To maintain exam integrity, the system prevents tab switching and screen minimization. Any suspicious activity is automatically flagged, generating alerts that are stored for later review by exam supervisors.

3.1.2 Non-Functional Requirements:

The system is designed with several non-functional requirements to ensure a smooth and reliable user experience. It features a user-friendly and responsive web interface that adapts well to different screen sizes and devices. Real-time processing capabilities are implemented to minimize delays and maintain continuous monitoring throughout the exam. All data from the exam sessions is securely stored to protect user privacy and maintain integrity. Additionally, the system is built

EdinBurg Peer Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 9||pp 12-27||September||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

to be compatible with major browsers and platforms, ensuring broad accessibility for users across different environments.

3.2 Tools and Technologies Used

Table 1: Tools and Technologies Used

Component	Technology/Tool Used
Facial Recognition	OpenCV
Frontend Interface	HTML, CSS, JavaScript
Backend	PHP (Laravel)
Screen/Tab Monitoring	JavaScript (Event Listeners, Visibility API)
Activity Logging	JavaScript (Mouse/Keyboard Event Tracking)
Database	MySQL
Notification System	JavaScript (popup alerts + email)

3.3 System Architecture

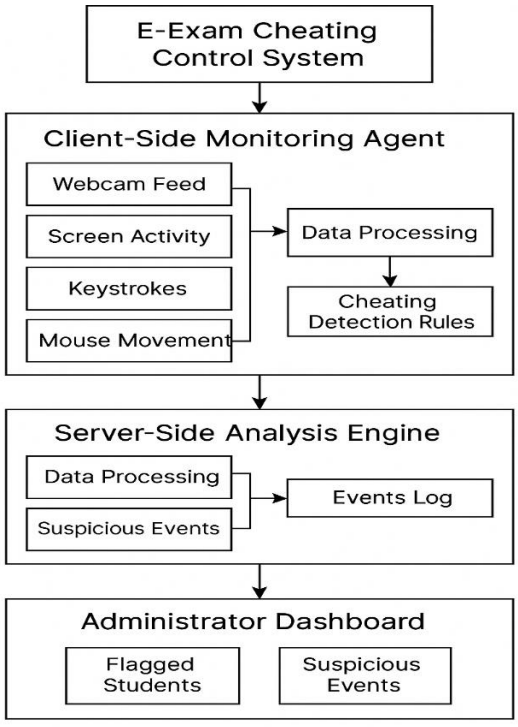

Figure 2: System Architecture

The system consists of three main components:

- **Client-Side Monitoring Agent:**

Runs in the browser during the exam, tracking webcam feed, screen focus, keystrokes, and mouse movement.

- **Server-Side Analysis Engine:**

Processes incoming data, log events, runs cheating detection rules, and stores incidents in a database.

- **Administrator Dashboard:**

Allows examiners to view flagged students, replay suspicious events, and download reports.

3.4 Development Process

The system was built using an iterative software development life cycle:

- **Requirement Analysis** – Identifying user and system needs.
- **System Design** – Designing the data flow and system components.
- **Implementation** – Coding each module and integrating them.
- **Testing** – Conducting unit and system testing using simulated exam sessions.
- **Evaluation** – Measuring performance using accuracy, detection rate, and user feedback.

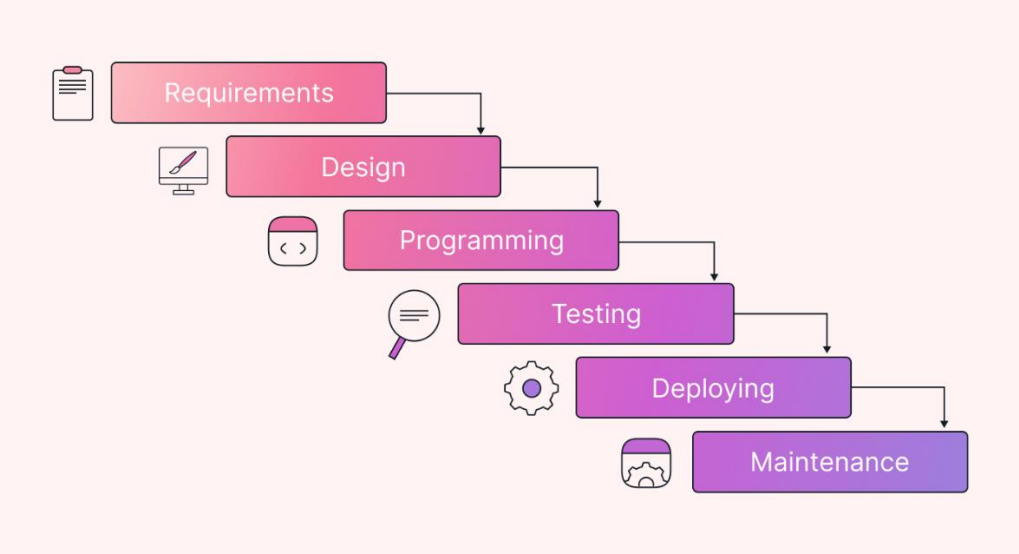

Figure 3: Waterfall model steps

3.5 Suspicious Behavior Detection Techniques

Table 2: Suspicious Behavior Detection Techniques

Suspicious Behavior	Detection Technique
No face or multiple faces detected	OpenCV + face landmarks
Frequent screen/tab switching	JavaScript visibility changes and blur events
Inactivity or lack of input	Mouse/keyboard event tracking
Looking away from the screen frequently	Facial landmark angle detection

4. System Design and Implementation

4.1 Development Process

The E-Exam Cheating Control System is designed to monitor and control online examination activities through a web-based interface, integrated with real-time facial recognition and behavior tracking components. The system aims to detect cheating behaviors automatically and alert exam supervisors as needed.

EdinBurg Peer Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 9||pp 12-27||September||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

4.2 System Three-Tier Architecture

The system follows a three-tier architecture:

- **Presentation Layer**
  Built using HTML, CSS, and JavaScript. This is the exam interface students interact with. It includes webcam access and scripts for tracking user behavior like key presses, mouse movement, and tab switching.

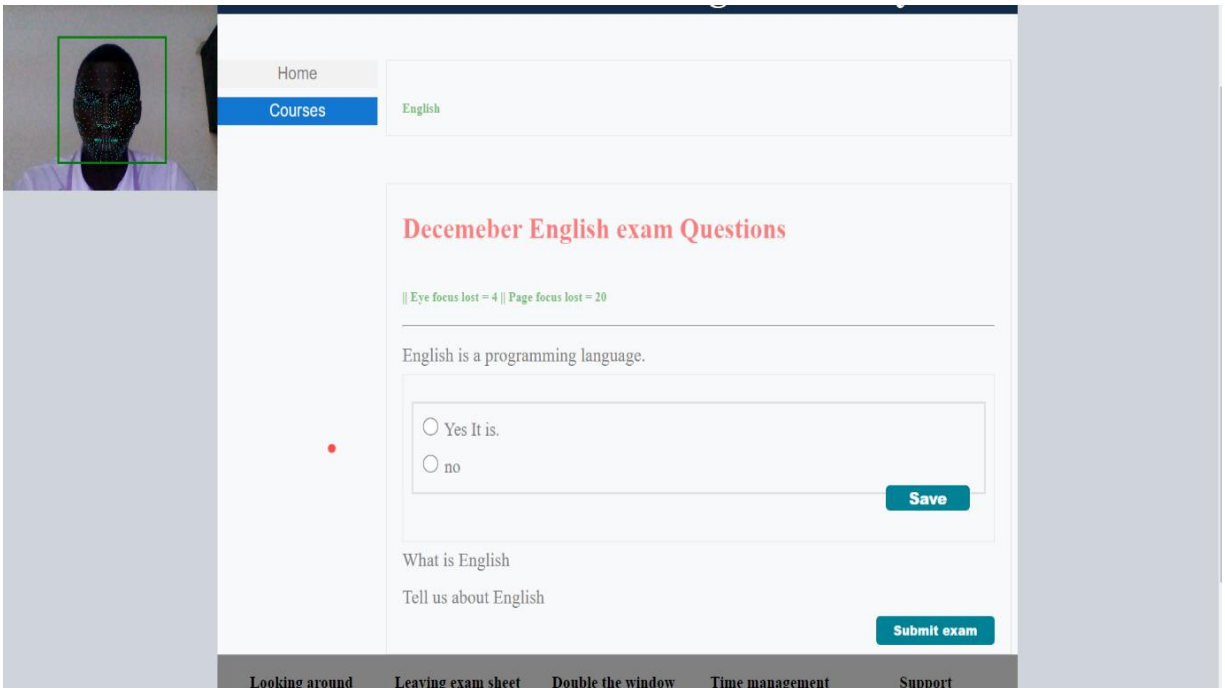

Figure 2: exam interface

- **Application Logic Layer**

Implemented using PHP (Laravel). It handles real-time processing of incoming monitoring data and applies rule-based logic to identify suspicious activities.

- **Data Layer**
  Consists of a relational database (MySQL) used to store:
  - User profiles
  - Exam session logs
  - Facial recognition images
  - Incident reports

EdinBurg Peer Reviewed Journals and Books Publishers
Journal of Information and Technology
Vol. 5||Issue 9||pp 12-27||September||2025
Email: info@edinburgjournals.org||ISSN: 3080-9576

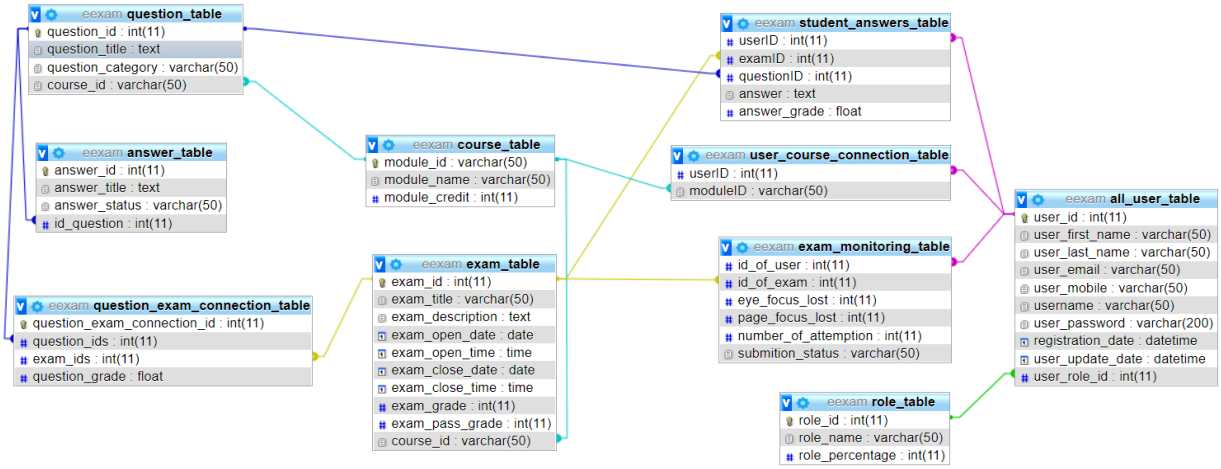

Figure 3: MSQL relational database

4.3 System Components and Modules

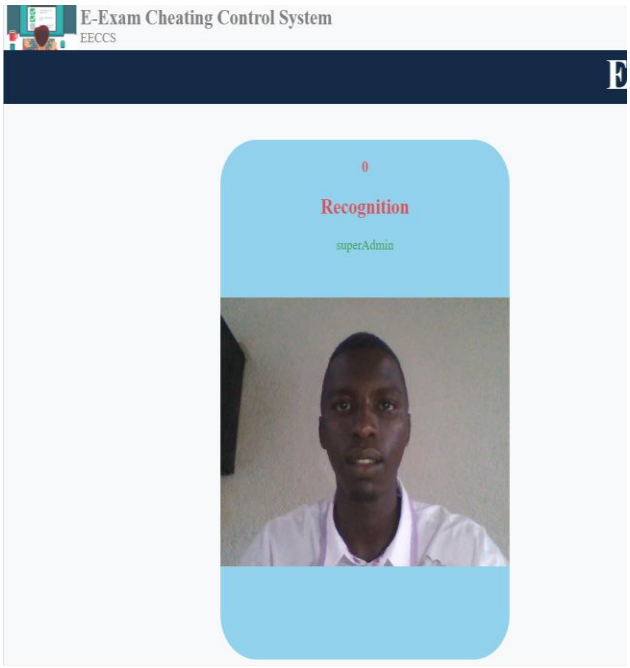

Figure 4: Facial Recognition

4.3.1 User Authentication and Exam Initialization

- Students log in securely using credentials.
- A facial recognition scan is performed to validate the identity.
- If the student is verified, the exam starts.

4.3.2 Facial Recognition Module

Uses OpenCV and face recognition libraries.

Checks for:

- Face presence
- Multiple faces
- Head orientation (gaze tracking)

4.3.3 Screen Activity Monitor

- JavaScript APIs (document.hidden, blur, focus) detect if the student switches tabs or minimizes the screen.
- Events are logged in real-time.

4.3.4 Input Behavior Logger

Captures:

- Mouse movements
- Click frequency
- Keyboard activity (without recording typed content)

Sudden inactivity or robotic patterns are flagged.

4.3.5 Cheating Detection Engine

A rule-based decision engine analyzes data patterns.

Triggers alerts if:

- The student looks away for too long.
- Another face is detected.
- The browser tab is changed frequently.

4.3.6 Admin Panel

- Displays a summary of each student's session.
- Visual alerts for flagged behavior.
- Allows video replay or log download of suspicious sessions.

4.4 Implementation Technologies

Table 3: Implementation Technologies

Component	Technology
Frontend	HTML5, CSS3, JavaScript
Backend	PHP (Laravel)
Face Detection	OpenCV, Face Recognition libraries
Activity Tracking	JavaScript Event Listeners
Database	MySQL
Authentication	Session-Based Auth
Communication	AJAX for real-time data transfer

4.5 Testing and Validation

The system was tested under various controlled scenarios:

- Single user under normal conditions (expected behavior).
- A second person entering the camera frame (cheating scenario).
- The student switching tabs frequently.
- Minimal mouse/keyboard activity (possible impersonation).

Each scenario was logged and analyzed to validate system accuracy.

5. System Evaluation

5.1 Experimental Setup

To evaluate the performance of the E-Exam Cheating Control System, a test environment was set up involving 10 volunteer participants simulating different examination scenarios. Each participant was asked to complete an online quiz under varying levels of supervision and behavior (normal, suspicious, and cheating). The test sessions were monitored using the implemented system.

The following scenarios were tested:

- **Normal behavior:** One face, eyes mostly on screen, no tab switching.
- **Minor violations:** Looking away frequently, short screen switches.
- **Major violations:** Presence of a second person, multiple tab switches, and long inactivity.

5.2 Detection Accuracy

The system's performance was measured using **Precision, Recall**, and **Accuracy** based on flagged events compared to ground truth. Overall average detection accuracy: 91.25%

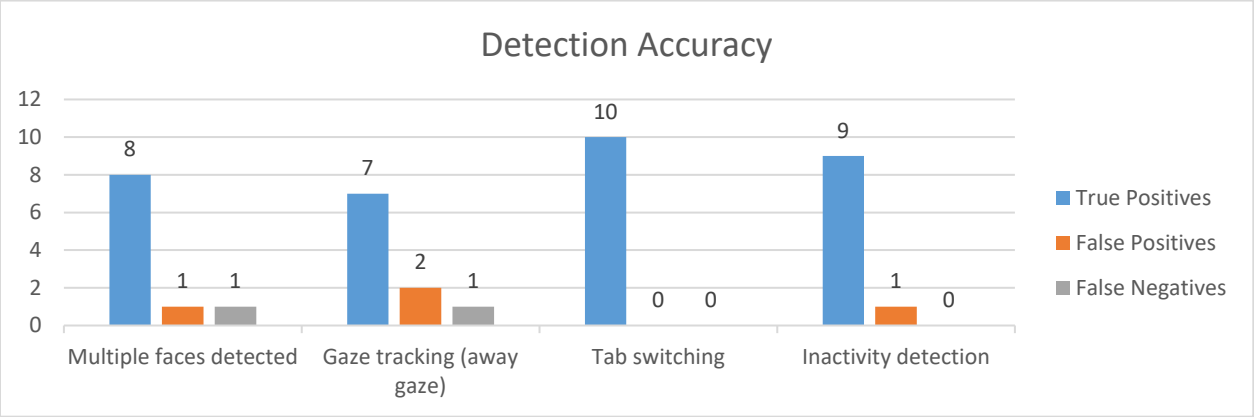

Figure 5: Detection Accuracy chart

Table 4: Detection Accuracy table

Behavior Detected	True Positives	False Positives	False Negatives	Accuracy
Multiple faces detected	8	1	1	90%
Gaze tracking (away gaze)	7	2	1	80%
Tab switching	10	0	0	100%
Inactivity detection	9	1	0	95%

5.3 System Strengths

- **High Accuracy:** The system successfully flagged most cheating attempts with low false positives.
- **Real-Time Alerts:** Detected suspicious actions immediately and notified the administrator.
- **Integration:** Combined multiple detection mechanisms (video + behavior) for better reliability.
- **User-Friendly Interface:** Students could navigate the exam interface with ease while being monitored in the background.

5.4 Limitations

- **Lighting Conditions**: Poor lighting affected the face recognition accuracy in some cases.
- **Privacy Concerns:** Continuous webcam monitoring raised privacy issues among participants.
- **False Alerts:** Minor distractions (e.g., a shadow near the face) occasionally triggered false positives.
- **Browser Restrictions:** Full tab and screen control is limited in some browsers (e.g., Safari).

5.5 Discussion

The system demonstrates promising potential in mitigating academic dishonesty during online exams. Unlike traditional invigilation or simple webcam proctoring tools, this system takes a multi-layered approach combining biometric analysis and behavioral data. The high accuracy of tab switching and multiple face detection proves that automated proctoring tools can be reliable, provided that user privacy and system optimization are properly handled.

Additionally, the system's modular structure allows for future upgrades such as voice detection, keystroke pattern analysis, or integration with existing Learning Management Systems (LMS)

6. Challenges and Limitations

6.1 Environmental Constraints

The accuracy of facial detection was highly dependent on external factors such as:

- **Lighting conditions:** Dim environments led to missed face recognition.
- **Camera quality:** Low-resolution webcams affected gaze and presence detection.

6.2 Browser and OS Restrictions

- Browser sandboxing policies (especially in Safari and some versions of Firefox) restricted full control over tab-switching and screen-capture detection.
- Some operating systems do not allow deep system monitoring due to privacy permissions (especially macOS).

6.3 Internet Connectivity

Real-time monitoring and video processing rely on a stable internet. Poor connections caused delayed responses or temporary data loss.

6.4 Privacy and Ethical Concerns

The use of webcams and behavioral tracking raised ethical concerns, particularly around data storage, surveillance, and student consent.

6.5 False Positives and Negatives

- Although rare, the system sometimes misinterpreted harmless behavior (like a family member walking by) as cheating.
- Glances away from the screen, or natural movements could be flagged unnecessarily, which may frustrate users.

7. Conclusion and Recommendations

7.1 Conclusion

This study presented the design and implementation of an E-Exam Cheating Control System that combines facial recognition, behavioral monitoring, and screen activity tracking to prevent academic dishonesty in online exams. The system achieved an average accuracy of over 90% in detecting common cheating behaviors such as multiple faces, screen switching, and long inactivity.

By integrating multiple detection mechanisms in real time, the system demonstrated a significant improvement over traditional manual proctoring and single-mode monitoring tools. The results support the potential for deploying such systems in educational institutions to enhance the credibility of e-learning assessments.

However, like any surveillance-based system, it is not without limitations — particularly around false positives and privacy concerns. Care must be taken to balance security with user trust and ethics.

7.2 Recommendations

- **Enhance Privacy Controls**: Include data encryption, user consent agreements, and secure deletion policies for recorded data.
- **Improve Adaptability**: Add support for low-light or mobile environments, including infrared face detection and mobile exam interfaces.
- **Integrate with LMS Platforms**: Allow seamless communication with systems like Moodle or Google Classroom for wider usability.
- **Use AI Models:** Upgrade rule-based alerts with machine learning models trained on real cheating behavior data to reduce false alerts.

Conduct Broader Testing: Future work should include large-scale field trials across different institutions and demographics.

References

Ahmed, D. (2022). AI in Online Assessments: A Review. *Computers & Education*.

Alenezi, A. &. (2023). Multi-agent-based cheating detection in e-exams using behavioral and network features. *Computers in Human Behavior Reports, 10*, 100187. doi:10.1016/j.chbr.2023.100187

Bulut, M. D. (2024). Enhancing e-proctoring systems using neural networks and eye-blinking detection algorithms. *Journal of Artificial Intelligence in Education, 34*, 45–62.

Jain, S. S. (2021). Comparative analysis of commercial e-proctoring systems: Balancing accuracy and privacy. *International Journal of Educational Technology in Higher Education, 18*, 1–15.

Kar, A. (2020). MLGaze: Machine Learning-Based Analysis of Gaze Error Patterns in Consumer Eye Tracking Systems. *ArXiv preprint*, https://arxiv.org/abs/2005.03795.

Kaur, R. S. (2021). Integrating sentiment and facial cues for stress detection in remote exams. *Proceedings of the 12th International Conference on E-Learning and Education Technology* (pp. 102–109). IEEE. doi:10.1109/ICEEET.2021.9445753

Kevalshah91. (2021). *Advanced-Proctoring-System*. Retrieved from GitHub: https://github.com/Kevalshah91/Advanced-Proctoring-System

Lamba, S. &. (2024). Deep Learning-Based Multimodal Cheating Detection in Online Proctored Exams. *Journal of Electrical Systems, 20*. doi:https://journal.esrgroups.org/jes/article/view/7480

Medianama. (2020). *AI proctored exams and privacy: Are students pushed to sacrifice their personal data?* Retrieved from Medianama: https://www.medianama.com/2020/08/223-ai-proctored-exams-privacy/

Nigam, A. P. (2021). A systematic review on AI-based proctoring systems: Past, present, and future. *Education and Information Technologies, 26*, 6421-6445. doi:10.1007/s10639-021-10597-x

Nigam, A., Pasricha, R., Singh, T., & Churi, P. (2021). A systematic review on AI-based proctoring systems: Past, present, and future. *Education and Information Technologies, 26*, 6421–6445. doi:10.1007/s10639-021-10597-x

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford University Press.

Ow Tiong, Y. &. (2022). Intelligent proctoring using AI-based monitoring of candidate behavior. *Journal of Educational Computing Research, 60*(3), 457–475. doi:10.1177/07356331221079315

Pathak, P. &. (2022). Evaluation of open-source proctoring tools: Examity, ProctorU, and SMOWL. *Proceedings of the 2022 IEEE International Conference on Advanced Learning Technologies (ICALT)*, (pp. 110–115).

Proctaroo. (2023). *AI proctoring: Capabilities, shortcomings, and how to fix them*. Retrieved from Proctaroo: https://www.proctaroo.com/blog/ai-proctoring-capabilities-shortcomings-and-how-to-fix-them

Purohit, H. &. (2022). Multi-modal biometric fusion-based continuous user authentication for E-proctoring using hybrid LCNN-Salp swarm optimization. *Cluster Computing, 25*(2), 827–846. doi:10.1007/s10586-021-03450-w

Teo, T. &. (2022). Exploring students' acceptance of online proctoring during COVID-19: An extension of the UTAUT model. *Education and Information Technologies*. doi:https://doi.org/10.1007/s10639-021-10597-x

Wang, Z. Z. (2020). Learning to Detect Head Movement in Unconstrained Remote Gaze Estimation in the Wild. *ArXiv preprint*. Retrieved from https://arxiv.org/abs/2004.03737