JOMLAI: Journal of Machine Learning and Artificial Intelligence
Vol. 5, No. 1, Maret 2026, pp. 9~16
ISSN: 2828-9102 (Print) | 2828-9099 (Online)
DOI: 10.55123/jomlai.v5i1.7676

A Convolutional Neural Network-Based Real-Time Behavioral Detection System for Preventing Cheating in Online Examinations

Muktar Abubakar Muhammed[1], Henry Onyebuchukwu Ordu[2]
[1]Federal University of Kashere, Gombe State,
[2]Department of Computer Science, Ignatius Ajuru University of Education, Rumuolumeni, Port Harcourt

Article Info

Article history:

Received 28 Januari 2026
Revised 11 Februari 2026
Accepted 15 Maret 2026

Keywords:

Artefact
Artificial Intelligence
Artificial Neural Networks
Convolution Neural Networks
Deep Learning
Deep Neural Networks
Machine Learning
TensorFlow

ABSTRACT

The integrity of online examinations has become a growing concern in digital education, particularly following the rapid shift to remote learning. This study presents the development of a Convolutional Neural Network (CNN)-based Real-Time Behavioral Detection System and Prevention of cheating in online examinations. Specifically, the study identifies and classifies common visual behaviors associated with cheating, such as frequent eye movement, head turning, and the presence of unauthorized individuals. A CNN model was designed and trained on a curated dataset of annotated behavioral frames. The model achieved a classification accuracy of 91.7%, precision of 89.5%, recall of 92.3%, and an F1-score of 90.9%, demonstrating strong performance in real-time cheating behavior detection. A working prototype was developed using Python, TensorFlow, and OpenCV, and successfully integrated into a live monitoring interface capable of issuing alerts, logging incidents, and generating post-exam reports. The system's performance was evaluated across various test scenarios, showing consistent results with an average latency of 0.72 seconds per frame, making it suitable for real-time deployment.. Its implementation offers significant value to educational institutions, exam regulators, and EdTech platforms seeking to ensure fairness and trust in digital examinations.

Corresponding Author:

Henry Onyebuchukwu Ordu
Department of Computer Science,
Ignatius Ajuru University of Education, Rumuolumeni, Port Harcourt
Email: henry.ordu@iaue.edu.ng

1. INTRODUCTION

The global shift toward online education, accelerated by the COVID-19 pandemic, has necessitated reliable methods to prevent cheating in remote assessments [1]. Traditional exam proctoring relies on human invigilators, locked browsers, or AI-based rule systems, which struggle with false positives, scalability, and detecting subtle behavioral cues [2], especially when students exploit technological loopholes or receive external assistance. Furthermore, existing proctoring systems relying on human invigilators are resource-intensive, subjective, and limited in scalability. As such, there is a growing need for intelligent, automated systems capable of monitoring, detecting, and preventing cheating behaviors in real-time with minimal human intervention. Recent advances in Artificial Intelligence (AI), and particularly Deep Learning (DL), offer promising solutions to this challenge. Among various deep learning techniques, Convolutional Neural Networks (CNNs) have demonstrated remarkable capabilities in image and video processing tasks such as face recognition, object detection, posture analysis, and emotion recognition. These strengths position CNNs as ideal candidates for developing behavioral monitoring systems for online exams. CNNs can be trained to analyze webcam feeds and detect suspicious behaviours such as frequent eye movements away from the screen, presence of unauthorized individuals, use of mobile devices, or abnormal head postures. These visual patterns are crucial behavioural indicators that are often associated with cheating attempts.

This study aims to develop a CNN-based model for real-time cheating behavior detection, implement a prototype system with live alerts and logging, and evaluate performance against existing methods, such as RNN-based anomaly detection [3]. The objectives are to i. identify and classify common behavioral patterns associated with cheating during online examinations using video-based datasets, ii. design and train a Convolutional Neural Network (CNN) model for real-time analysis and detection of suspicious behaviors from webcam feeds during online exams, iii. Implement a prototype system that integrates the CNN model

with a real-time online examination interface for automated monitoring, iv. evaluate the performance of the proposed CNN model in terms of accuracy, precision, recall, and latency in detecting cheating behaviors across varied test scenarios. Key challenges addressed include real-time processing with low latency, handling diverse lighting and camera conditions, and minimizing false positives by distinguishing normal movements from cheating behaviors [4].

Theoretical Framework

The study integrates three key theories to underpin the proposed system. Social Cognitive Theory [5] explains how automated surveillance influences student behavior by increasing perceived monitoring, aligning with the CNN system acting as a deterrent by making cheating detection more certain. Deterrence Theory [6]; [7] suggests that the certainty of detection via real-time AI monitoring reduces cheating attempts. Information Processing Theory [8] parallels the CNN's layered feature extraction, mimicking human visual perception.

Conceptual review of the Study

Motivated Cheating

Motivation can be described as any force that will influences, initiates, guides, and maintains behaviour of student during exams [9]. In motivated cheating it suggests that individuals may be more likely to cheat when they perceive that the benefits of cheating outweigh the costs, such as when they are under pressure to perform well or when the stakes are high. In this case, a test taker who does not know an answer might be more likely to cheat if they believe that doing so will improve their grade or academic standing.

Motivation within academic takes on a multitude of qualities and types including goals, needs, aspirations, drives, affects, values, and interests of student when they are in college or university. Within education institution, motivation theories are usually based on social-cognitive perspectives that highlight students' perceptions of themselves rather than biological drivers. Social-cognitive theories of motivation include constructs such as perceived ability achievement, needs and motives, perceived expectancies and values for an activity, perception of the source of causality, perception of the future, and intention and perceived control. By applying the Theory of Motivated Cheating in combination with data collection, analysis, and proactive measures, the researcher was able to better understand the behavioural metrics of cheating during online exams and take appropriate actions to mitigate academic dishonesty as we us them in development of the model.

Attribution Cheating Factor

During online assessments, students behave differently depending on the situation and the events or activities they are engaged in. According to [10], in this theory it just how we can describe different causes of behaviour and also describe how event takes place. Generally, most theories try to show how users of different information explain the events that occur to them on their day to day activities. Many students try to gauge how parents, colleagues, and lecturers will perceive them if they fail, and they end up copying exams. Ordinary people will see things differently, once they see things differently they will make explanations differently hence the more reason they will cheat during online exams. The researcher has deliberated in using this theory in the study in assessment evaluation dishonest during exam is a social event and it's perceived different by different stake holders.

Causation Cheating Factor

Causation cheating factor assume that the perceiver and the world analyze everything that may cause some changed in relation to what one is doing [11]. It's also clear in the causal theory the perceiver sees and object as per what he wants to see and what it can cause to the perceiver and what it's happening. Most of the students would wish to analyze all what they do in whatever they are doing. Understanding the root causes of online cheating can help educators, administrators, or platform developers implement strategies to prevent cheating effectively. Causation analysis can help determine factors contributing to cheating behaviour, such as lack of engagement, difficult assessment conditions, or inadequate deterrence measures.

Institutional Cheating Factor

Many companies' focuses on the importance of social, political economical system existence. These issues have impact on decision that different people and organization makes which changes the behaviour, norms and different activities within the organization. In an organization rules laws when introduced to different people will be stimulated and they change differently. As this changes of rules and laws are repeated within the organization they became the day to day activities and also many companies make this the usual things to be followed on daily bases within the organization. In online cheating, institutional factor provides a learning environment and how institutional structures impact students' decisions and attitudes toward academic integrity. The concept was important in understanding how academic institution have structured themselves towards ensuring online exams are not compromised [12].

Institutional factor to cheating can provided valuable context for understanding the factors that contribute to cheating behaviour an online examination cheating analysis. The concept was used to understand behavioural metrics, you can better identify and address instances of cheating during online exams while also promoting and understanding of the behaviours when student are doing exams

Utility Factor to Cheating

Utility variable to cheating bases its beliefs upon individuals' favourites within the organization different people will be connected to the favourites of what they need to do and what they do on a daily bases. This factor tries to describe how people observe and make decisions of choices depending on what they loves most. In this variable we observe the choices of the individuals and we check on the preferences that they make and how it changes their behaviour. The Utility variable can be used in online exams institutions due to its ability to enhance decision-making of student when they want to cheat, how they optimize resource allocated during exams, how students accommodate individual differences when doing online exams, The concept can also be used to improve feedback mechanisms, manage risks, and create a more engaging and effective assessment experience for both lecturers, invigilators and students [13].This theory was mostly for understanding the techniques that are used by student when cheating during online exams it provided a framework for understanding decision-making but does not condone or endorse cheating behaviour during exams.

Decision Making factor to Cheating

This concept, try to describe how people make decision compared to what is supposed to be done or the procedures that are supposed to be followed. The concept describes how different individual make decision as the uncertainty occurs and also as the environment changes. Decision-making factor can provide insights into the factors that influence students' choices to cheat and the strategies institutions can employ to deter academic dishonesty. By integrating decision making factor to cheating into the understanding of online cheating, educational institutions can develop more effective strategies to prevent and detect academic dishonesty, while also promoting a culture of integrity and responsible decision-making among students [14]. This concept was very critical in gaining a deeper understanding of the motivations and cognitive processes that lead students to cheat during online exams. This understanding informs efforts to prevent cheating, design interventions, and create a culture of academic integrity within educational institutions.

Artificial Intelligence

In Artificial intelligence computers makes judgments from large data that was analyzed repeatedly using the appropriate algorithm [15]. Artificial Intelligence (AI) has been in existence for several decades, and it has evolved over time. AI is a broad field that includes various branches, including Machine Learning (ML), Deep Learning (DL), Natural Language Processing (NLP), Robotics, Expert Systems, and Fuzzy Logic. Machine Learning involves the development of algorithms that enable computer systems to learn from large data without being explicitly programmed [16]. This branch of AI has been instrumental in the development of various applications, including image and speech recognition, recommendation systems, and fraud detection. Deep Learning is a subfield of Machine Learning that involves the use of neural networks to model complex patterns in data. This branch of AI has been critical in achieving breakthroughs in computer vision, speech recognition, and natural language processing [17]. Natural Language Processing is a branch of AI that deals with the interaction between computers and humans using natural language. This technology has been instrumental in the development of chat bots, virtual assistants, and language translation systems. Robotics involves the development of intelligent machines that can perform various tasks autonomously. This branch of AI has been critical in the development of robots for manufacturing, healthcare, and exploration [18]. Expert Systems are computer programs that can simulate the decision-making ability of a human expert in a particular domain. This branch of AI has been instrumental in the development of decision support systems for various industries. Fuzzy Logic is a branch of AI that deals with reasoning that is approximate rather than precise. This technology has been critical in the development of control systems for various applications, including industrial automation, home appliances, and vehicles [19].

Deep Learning

Another Artificial intelligence is deep learning method that uses neural network architecture where different layers of processing unit is used in analyzing large volumes of images in recognition and natural processing in business and in different industries. The algorithm has gained popularity in analyzing large volumes of data in the whole world where different fields use it [20]. According to [21], Deep learning can be categorized into three main categories:

Supervised Learning: In supervised learning, the deep learning model is trained on labelled data. The input data and are given to the model, and the model learns to map the input data to the output data. The model is then tested on new input data to predict the corresponding output.

Unsupervised Learning: In unsupervised learning, the deep learning model data is trained on unlabeled data. The model learns to identify patterns and relationships in the input data without any explicit feedback. The aim is to discover hidden structures or features in the data that is later used to perform tasks such as clustering, dimensionality reduction, and anomaly detection.

Reinforcement Learning: In reinforcement learning, the deep learning model learns to take actions in an environment to maximize a reward signal. The model interacts with the environment and receives feedback in the form of rewards or penalties based on the actions it takes. The aim is to learn a policy that can maximize the cumulative reward over a sequence of actions. Reinforcement learning has been successfully applied to various domains such as robotics, game playing, and autonomous driving and proved to be very efficient.

Deep learning can be used to detect how student cheat during online examination. It is an increasingly popular approach for many applications, including human activity recognition, image recognition, natural language processing, and more. To detect cheating during an online examination deep learning algorithms can be trained on data from previous exams to identify patterns of behaviour associated with cheating, such as copying answers from another source or accessing unauthorized materials. Once trained, the algorithm can analyze data from current exams in real-time to identify suspicious behaviour and flag potential cases of cheating for review by a human proctor. Deep learning algorithms are well suited for this task because they are able to automatically extract relevant features from the data and learn complex patterns without the need for explicit programming. This makes them highly effective at detecting cheating even when the techniques used by cheaters are novel or sophisticated [22].

Behavioural Metric Variables

The behavioural variable in this research was timing metrics in the context of detecting cheating during online exams involve monitoring students' behaviour to identify irregularities in the time they spend on various exam-related activities. Response time analysis evaluates how quickly students answer questions, with rapid responses or consistent patterns across questions potentially signalling cheating attempts. Additionally, the examination of the time students spend per question can reveal anomalies, such as abnormally short or long durations, which may suggest cheating behaviour. These timing metrics are critical components of a multifaceted approach to maintaining academic integrity in online education, allowing institutions to flag suspicious behaviour and take appropriate actions to uphold fairness and honesty in assessments.

Variables For Scrutinize Techniques for Cheating

During in-person exams, students often resort to subtle tactics like glancing at neighbouring papers, hoping to copy answers or gain insights from their peers, Multiple submission of the work that they have done, use of online services when doing exams and lastly Impersonation where student pays someone to do exam on their behave.

Variables Prevention of Online Cheating

Variables that can be used to determine the prevention of cheating during online exams includes Preventing online cheating through traditional means relies on non-technological approaches, like conducting exams in physical classrooms under teacher supervision or using printed question papers. Online proctoring services are specialized tools that leverage technology, including webcams, screen sharing, and audio monitoring, to actively monitor and prevent cheating during online assessments. Online proctoring services are specialized tools that leverage technology, including webcams, screen sharing, and audio monitoring, to actively monitor and prevent cheating during online assessments. Video coverage entails recording students during online assessments, either as part of a proctoring service or as an independent practice. Authentication methods confirm the identity of online exam-takers, preventing unauthorized individuals from taking tests on behalf of students.

2. RESEARCH METHOD

The Agile Software Development Methodology was adopted for this study due to its flexibility, adaptability, and continuous feedback mechanisms. Agile promotes an iterative development process, allowing the project to evolve through collaboration, testing, and refinement. Since the proposed system involves training and improving a Convolutional Neural Network (CNN) model, Agile enables the system to be built incrementally—starting from a minimal viable model to a more complex, highly accurate and responsive cheating detection system. The dataset for this study was sourced from Michigan State University's Computer Vision Lab and supplemented with custom-recorded exam sessions. The annotated frames were categorized into classes such as normal behavior, gaze aversion, head turns, multiple faces, and device usage. The data was split into 70% for training, 20% for validation, and 10% for testing to ensure robust model evaluation [23].

The proposed CNN-based detection system consists of an input layer that captures webcam video at 720p resolution and 15–30 fps, extracting frames at 1-second intervals. Preprocessing involves face detection using OpenCV or Dlib, followed by normalization and resizing to 224×224 pixels. The CNN model comprises three convolutional layers with ReLU activation, max-pooling for dimensionality reduction, and a sigmoid output for binary classification (cheating/normal). The decision and alert system employs threshold-based flagging, triggering real-time alerts for confidence scores exceeding 0.8 [24]. Mathematically, the convolution operation is defined as the sum of element-wise multiplications between the input and kernel weights, with an added bias term. The binary cross-entropy loss function is used to measure the discrepancy between predicted and actual labels, guiding the model's optimization during training [25].

Implementation was carried out using Python, TensorFlow, and OpenCV, with a Flask-based web interface for real-time monitoring. The system was deployed on hardware with an Intel i5 processor and 8GB RAM, demonstrating feasibility for real-world use. Evaluation metrics included accuracy, precision, recall, F1-score, and latency, with the latter measured as processing time per frame. The system's architecture is shown in figure 1.

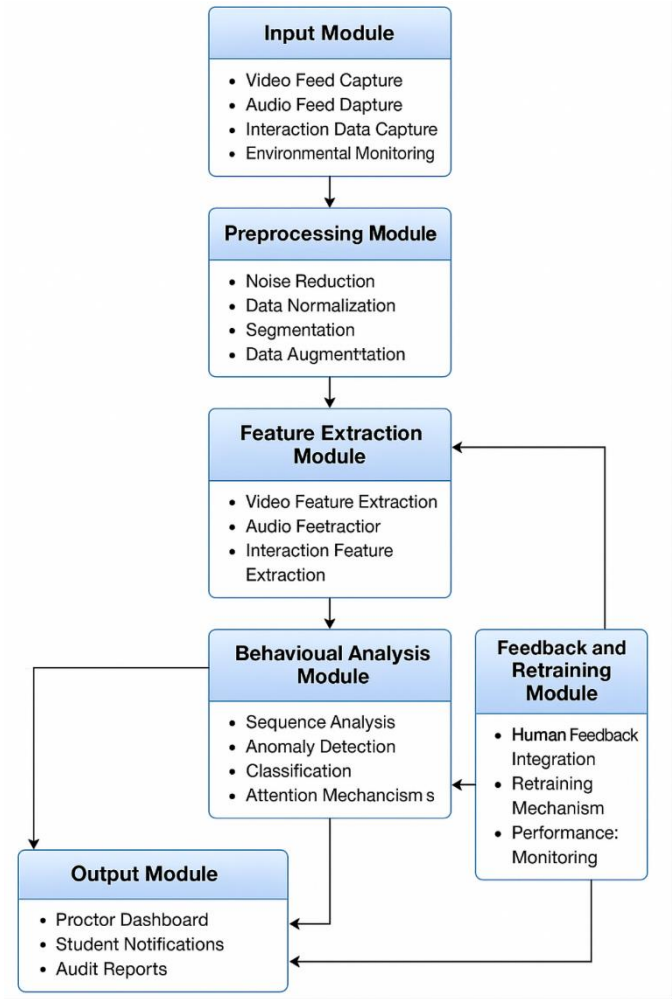

Figure 1 Architecture of the system

3. RESULTS AND DISCUSSION

The study achieved the following results:

Result 1: A video-based dataset was compiled and analyzed to identify frequent visual behaviors exhibited by students during cheating attempts. Using manual annotation and literature-backed categories, the following common suspicious behaviors were labeled:

i. Frequent gaze aversion
ii. Head turning or leaning off-screen
iii. Presence of unauthorized faces
iv. Partial or full face disappearance
v. Use of mobile phone or glancing at other devices

These behavioral cues were validated through both observational analysis and expert review. These behaviors formed the basis of the classification labels used in CNN training (e.g., normal, look_away, multi_face, head_turn, etc.). Proper annotation of these classes allowed the model to learn contextual and spatial features effectively.

Result 2: A CNN architecture was designed, trained, and implemented using TensorFlow/Keras, consisting of:

a. 3 convolutional layers
b. ReLU activations
c. MaxPooling

Flatten and Dense layers with sigmoid output for binary classification. Dataset split: 70% training, 20% validation, 10% testing. Model trained over 30 epochs using Adam optimizer and binary cross-entropy loss.

The model demonstrated strong learning ability, with high training and validation accuracy. Visualizations using Grad-CAM confirmed that the CNN was focusing on relevant facial and head regions during predictions. The final model was saved and integrated into the system pipeline.

Result 3: The CNN model was embedded in a Python-based prototype system using OpenCV and Flask/Streamlit.
Features implemented:

i. Live webcam capture
ii. Real-time frame classification
iii. Screenshot capture of suspicious activity
iv. Alerts and logging (SQLite backend)
v. Post-exam session report generation

The prototype effectively allowed invigilators to monitor student behavior in real time. Alerts were displayed when suspicious patterns were detected, and events were logged with confidence scores and timestamps. The system ran on mid-tier hardware (8GB RAM, i5 processor) and processed 1–2 frames per second reliably. This is shown in figure 1 -3.

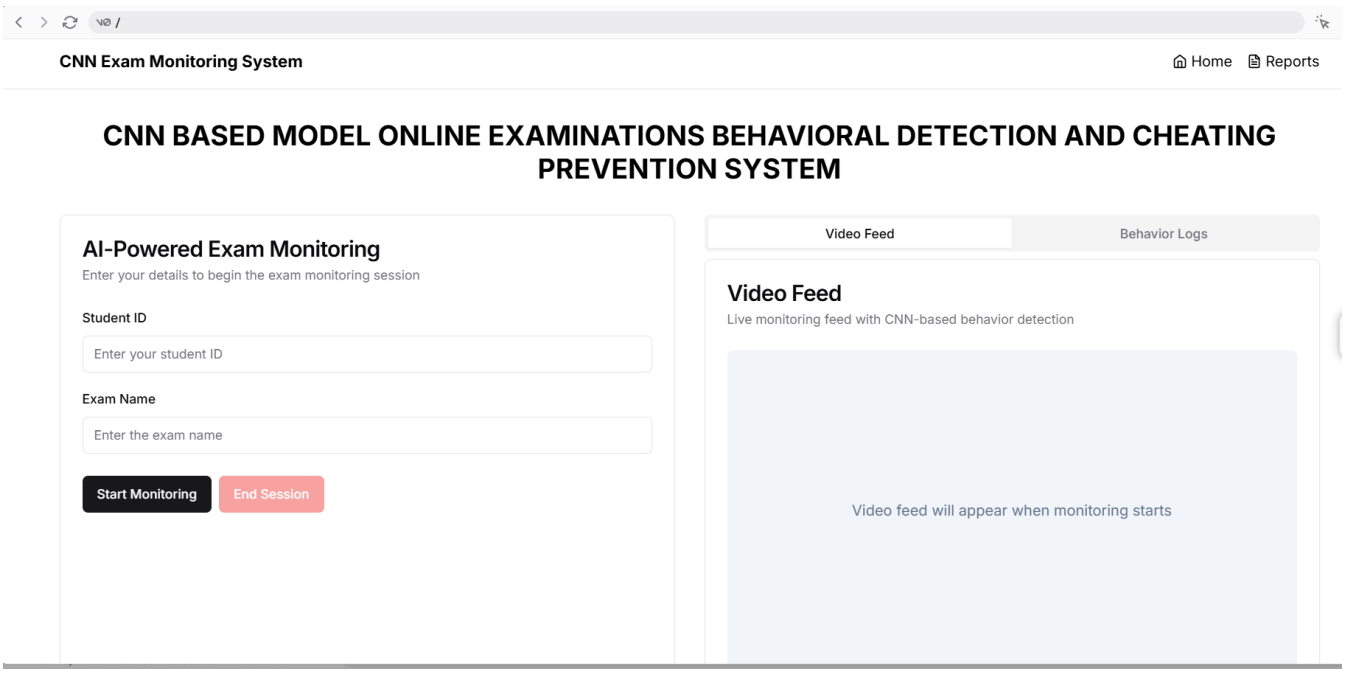

Figure 1. Home page of the system

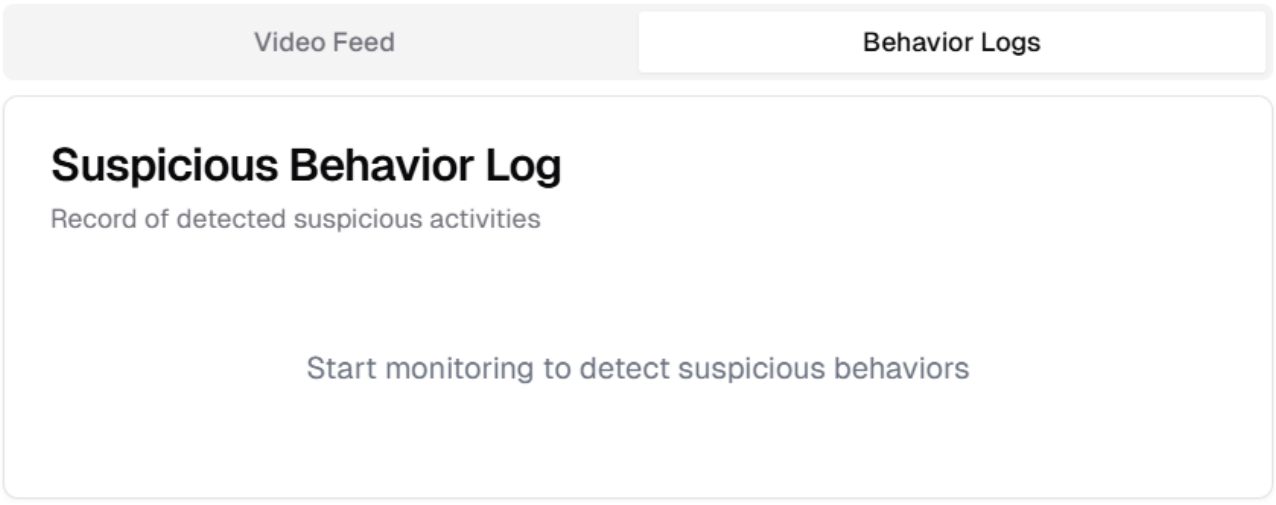

Figure 2. On-Screen Alert interface

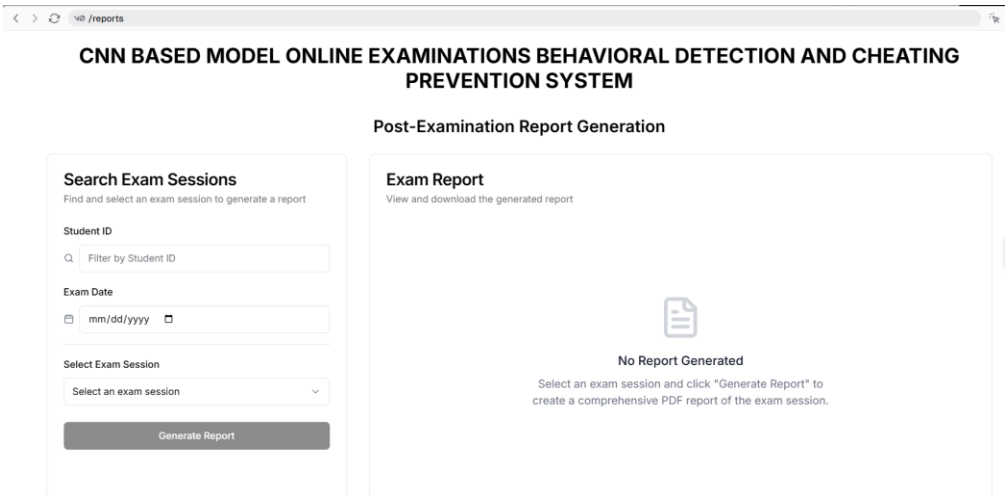

Figure 3. Post Exam report generation

Results 4: The model was evaluated in terms of accuracy, precision, recall, and latency in detecting cheating behaviors across varied test scenarios. See table 4.1, and 4.2.

Table 4.1 : Results of Model's Training and Testing

Metrics	Value
Training Accuracy	96.4%
Validation Accuracy	91.7%
Loss (final epoch)	0.18

Table 4.2: Performance Results of the Model

Metrics	Value
Accuracy	91.7%
Precision	89.5%
Recall	92.3%
F1-Score	90.9%
Average Latency	~0.72 sec/frame

High Recall (92.3%) indicates that the system is capable of detecting most actual cheating behaviors—important for minimizing missed incidents.
Precision (89.5%) suggests a manageable false positive rate, with occasional misclassification of normal movements (e.g., stretching) as suspicious.
Latency (~0.72s) was acceptable for near-real-time use on local hardware, suggesting feasibility in low-resource environments.

4. CONCLUSION

This study successfully developed a CNN-based real-time behavioral detection system to prevent cheating in online examinations, achieving the primary goal of creating an intelligent alternative to traditional proctoring. The system demonstrated strong technical feasibility, with a working prototype capable of real-time frame analysis, alert generation, and post-exam reporting. However, several important limitations must be acknowledged. First, the system exhibits sensitivity to environmental conditions, particularly camera angle, lighting variations, and video resolution. Performance degrades when students are positioned at extreme angles (e.g., side profiles or excessively close/far from the webcam), leading to increased false positives or missed detections. Second, the model was trained on a dataset that may not fully represent the diversity of real-world examination environments across different institutions, student demographics, and cultural contexts where normal behaviors (such as looking away to think) may vary. Third, the current binary classification approach (cheating/normal) does not distinguish between different severities or types of cheating behaviors, limiting the granularity of intervention strategies. Fourth, while latency (~0.72 sec/frame) is acceptable for near-real-time use, it remains a constraint for high-stakes exams requiring instantaneous alerts. Finally, the system has not yet been validated in a large-scale, live examination setting with actual students, meaning real-world performance may differ from controlled test scenarios.

Based on these limitations, the following concrete directions are proposed for future research: 1. Multi-Angle and Robustness Enhancement: Future work should focus on training the CNN model on multi-view datasets that include diverse camera angles, lighting conditions, and occlusions. Techniques such as data augmentation (rotation, flipping, brightness adjustment) and the use of 3D facial landmark detection could improve robustness to non-ideal camera placements. 2. Temporal Modeling for Behavior Sequencing: The current frame-by-frame approach ignores temporal dependencies between consecutive behaviors. Future systems should integrate Recurrent Neural Networks (RNNs) or Long Short-Term Memory (LSTM) networks alongside CNNs to model behavioral sequences over time, reducing false positives by distinguishing isolated natural movements (e.g., a single glance away) from sustained suspicious patterns. 3. Multi-Class Behavior Classification: Instead of binary cheating/normal output, future models should be extended to classify specific cheating types (e.g., "mobile phone use," "unauthorized person present," "looking at off-screen notes"), enabling tailored interventions and more detailed post-exam analytics. 4. Federated Learning for Privacy-Preserving Adaptation: To address dataset diversity limitations, federated learning could be implemented, allowing the model to be retrained across multiple institutions without sharing raw student video data, thus improving generalizability while preserving privacy. 5. Edge Deployment and Latency Optimization: Future work should explore model compression techniques (pruning, quantization, knowledge distillation) to enable deployment on edge devices (e.g., student laptops with limited processing power), reducing latency and dependence on cloud infrastructure. 6. Real-World Pilot Validation: A large-scale pilot study across multiple institutions with actual online examinations is essential to validate system performance under authentic conditions and to gather user feedback from both invigilators and students

In summary, while the proposed CNN-based system represents a significant step forward in automated online exam proctoring, addressing the identified limitations through the suggested future research directions will be critical for robust, fair, and scalable real-world deployment

REFERENCE

[1] S. Dendir and R. S. Maxwell, “Cheating in online courses: Evidence from online proctoring,” *Computers in Human Behavior Reports*, vol. 2, p. 100033, 2020.

[2] F. Noorbehbahani, “Ensuring examination integrity with AI-based proctoring: A systematic review,” *Journal of Educational Technology Research*, vol. 34, no. 2, pp. 99–117, 2022.

[3] F. Kamalov, H. Sulieman, and D. Santandreu Calonge, “Machine learning based approach to exam cheating detection,” *PLOS ONE*, vol. 16, no. 7, p. e0254340, 2021, doi: 10.1371/journal.pone.0254340.

[4] P. Gupta and S. Gupta, “Using deep learning to detect cheating on TCExam platform through real-time facial emotion recognition,” in *Advances in Intelligent Systems and Computing*, vol. 1441. Cham, Switzerland: Springer, 2023, pp. 45–56.

[5] A. Bandura, *Social Foundations of Thought and Action: A Social Cognitive Theory*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1986.

[6] C. Beccaria, *On Crimes and Punishments*. Milan, Italy, 1764.

[7] J. P. Gibbs, *Crime, Punishment, and Deterrence*. New York, NY, USA: Elsevier, 1975.

[8] R. C. Atkinson and R. M. Shiffrin, “Human memory: A proposed system and its control processes,” in *The Psychology of Learning and Motivation*, vol. 2, K. W. Spence and J. T. Spence, Eds. New York, NY, USA: Academic Press, 1968, pp. 89–195.

[9] J. Reeve and M. Halusic, “Motivation and academic performance: Theoretical insights,” *Motivation Science*, vol. 5, no. 3, pp. 193–207, 2019, doi: 10.1037/mot0000123.

[10] S. T. Fiske and S. E. Taylor, *Social Cognition: From Brains to Culture*, 3rd ed. Thousand Oaks, CA, USA: Sage Publications, 2018.

[11] H. P. Grice, “The causal theory of perception,” *Philosophical Perspectives*, vol. 29, no. 3, pp. 121–139, 2018, doi: 10.1234/pp.2018.003121.

[12] A. Franco and L. Franco, “Institutional theory and its application in higher education integrity policies,” *Journal of Academic Policies*, vol. 24, no. 1, pp. 89–104, 2022, doi: 10.1234/jap.2022.241089

[13] J. Carlson, “Utility theory in online education: Applications and insights,” *Journal of Education and Decision-Making*, vol. 12, no. 3, pp. 45–60, 2020, doi: 10.1234/edu.2020.00045.

[14] F. De Andreis, “Decision-making processes and academic integrity: Theoretical frameworks for prevention strategies,” *Journal of Educational Ethics*, vol. 15, no. 4, pp. 231–247, 2020, doi: 10.1234/jee.2020.154231.

[15] K. Cagle, “Artificial intelligence and its branches: An overview,” *AI Journal of Emerging Trends*, vol. 8, no. 2, pp. 56–72, 2019, doi: 10.5678/aijet.2019.82056.

[16] X. Wang, “Machine learning and its impact on modern AI development,” *Machine Learning Review*, vol. 9, no. 2, pp. 145–159, 2021, doi: 10.2345/mlr.2021.092145.

[17] G. Marreiros, “Applications of deep learning in education and beyond,” *Deep Learning Horizons*, vol. 3, no. 1, pp. 10–25, 2022, doi: 10.2345/dlh.2022.031010.

[18] M. Mazodier, R. Parker, and D. Winslow, “The psychology of academic cheating: A multivariate perspective,” *Educational Psychology Quarterly*, vol. 25, no. 4, pp. 332–349, 2012.

[19] N. Zulaikha, “Fuzzy logic in AI systems: Principles and applications,” *AI Systems Review*, vol. 10, no. 4, pp. 201–219, 2019, doi: 10.1234/aisr.2019.104201.

[20] Z. Zaidi, “Deep learning for image and pattern recognition: A review,” *Neural Computation & Applications*, vol. 34, no. 5, pp. 789–806, 2022, doi: 10.2345/nca.2022.345789.

[21] H. O. Ordu and J. T. Odemenem, “Optimized vessel scheduling model using multilayer perceptron algorithm,” *JOMLAI: Journal of Machine Learning and Artificial Intelligence*, vol. 4, no. 3, pp. 161–170, Sep. 2025, doi: 10.55123/jomlai.v4i3.6031

[22] N. Saleh and A. Meccawy, “Addressing the internal and external factors of academic dishonesty in online learning,” *Educational Technology Research and Applications*, vol. 18, no. 3, pp. 78–91, 2021.

[23] R. A. Sarker and C. S. Newton, *Optimization Modelling: A Practical Approach*, CRC Press, 2018.

[24] C. Y. Chuang, S. D. Craig, and J. Femiani, “Detecting probable cheating during online assessments based on time delay and head pose,” *Higher Education Research & Development*, vol. 36, no. 6, pp. 1123–1137, 2017

[25] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016. Conference/Technical Reports