REAL-TIME DETECTION OF EXAMINATION MALPRACTICES USING CONVOLUTIONAL NEURAL NETWORKS AND VIDEO SURVEILLANCE: A SYSTEMATIC REVIEW WITH META-ANALYSIS

Adeyemi J. O.[1], Ogunlere S. O.[2], and Akwaronwu B. G.[3]

[1-3]Department of Computer Science, Babcock University, Ilishan-Remo, Ogun State, Nigeria.

Emails:
[1]adeyemi0134@pg.babcock.edu.ng; [2]ogunleres@babcock.edu.ng;
[3]akwaronwu0329@pg.babcock.edu.ng

Cite this article:

Adeyemi, J. O., Ogunlere, S. O., Akwaronwu, B. G. (2025), Real-Time Detection of Examination Malpractices Using Convolutional Neural Networks and Video Surveillance: A Systematic Review with Meta-Analysis. British Journal of Computer, Networking and Information Technology 8(2), 15-50. DOI: 10.52589/BJCNIT-QC5EELJE

Manuscript History

Received: 18 Mar 2025

Accepted: 22 Apr 2025

Published: 13 May 2025

ABSTRACT: *This research project develops a system for automatically detecting cheating and identifying students in order to improve exam integrity while addressing the shortcomings of traditional monitoring methods. The technology detects and captures cheating pupils in real time using both machine learning and manual tactics. A study and analysis were conducted to provide evidence-based recommendations for designing effective automated cheating detection systems in educational settings. According to the PICOS framework, the research is aimed at students who struggle with exam cheating (Population), focuses on developing a detection system (Intervention), compares traditional monitoring techniques to the new system (Comparison), seeks to improve accuracy and fairness in identifying cheating (Outcome), and collects evidence using systematic review and meta-analysis methods (Study Design). The literature search followed PRISMA criteria and includes papers from the Scopus and Google Scholar databases from 2013 to 2024. The inclusion criteria included research papers that investigated exam participants, instances of cheating, and the application of new technologies such as deep learning and machine learning. Articles that were not about examination malpractices or did not use advanced technological tools were rejected based on particular criteria. A total of 37 articles were reviewed. The findings demonstrate how new technology may significantly increase the credibility and dependability of tests, ensuring academic honesty.*

KEYWORDS: Examination malpractice detection, machine learning, convolutional neural networks (CNNs), systematic review, meta-analysis, academic integrity, cheating prevention, data augmentation, real-time surveillance.

Article DOI: 10.52589/BJCNIT-QC5EELJE
DOI URL: https://doi.org/10.52589/BJCNIT-QC5EELJE

INTRODUCTION

The study of tests and their mechanics is becoming more popular. Modern tools for spotting exam cheating and guaranteeing an environment free of cheating are being sought after by universities and other academic institutions across the world in a fierce competition. Exam management and anti-cheating measures often involve the hiring of experienced proctors to supervise the whole examination procedure. They are passionate about using state-of-the-art instruments to detect exam cheating. Universities and other academic institutions all across the world have been working on this idea for the past several years. There's no denying that cheating is a dishonourable and dangerous activity. The profession of education is concerned about the problem of exam cheating. In order to fulfil this objective, we prioritize the automated detection of exam cheating, responding to teacher and educator concerns about the pervasiveness of cheating and the shortcomings of existing detection techniques. Cheating is increasingly more prevalent in secondary and elementary schools as well as in universities [1]. Students use a variety of methods to cheat on traditional examinations, including talking to classmates, hiding cell phones, writing on their hands or arms, and using cheat sheet [2]. Specifically, manual student supervision is essential to the traditional test monitoring techniques used to identify any instances of cheating. Since an examiner cannot keep an eye on every student at all times, there may be distractions that allow students to act dishonestly [3].

In order to direct, safeguard, regulate, or influence conduct, surveillance is keeping an eye on activities, anomalous behaviour, or behaviour. In order to investigate crimes, obtain intelligence, and safeguard protocols, people, or property, government organizations employ surveillance. Robust video surveillance systems function by detecting unusual or suspicious activities. These technologies have recently proven to be useful in spotting unusual or suspicious behaviour, which aids in preventing security lapses. Even though there are numerous research that use computer vision techniques to detect cheating, the solutions that have been suggested are rigid and impractical outside of a strictly supervised learning setting. While there has been significant advancement in image processing and computer vision tasks, deep learning has not yet been applied to real-world cheating detection. Continuous research in human pose estimating problems has led to the development of trustworthy real-time systems that could potentially tackle cheating. Furthermore, there are no exam monitoring systems that can identify and display evidence of cheating.

A person's identity is mostly determined by visual cues found in human faces and behaviours. An individual's physical characteristics are captured in the surveillance footage, which can be seen live or replayed while the activity is being recorded. In every sphere of life, including video analytics, the influence of the contemporary "automation" movement is palpable. Numerous applications, including human identification, behaviour prediction, motion detection, anomalous activity detection, and vehicle and person counting in busy locations, can benefit from the use of video analytics. People can be identified in two ways: by their appearance and gait. When it comes to automatic facial recognition through video surveillance, different people have different levels of proficiency. By using facial recognition technology, one can forecast an individual's activities by anticipating their head position. Combining movement detection with face detection can help achieve good results in a number of tasks, including person identification, presence or absence of a person at a given location and time, and person verification. Additionally, by utilizing estimation, subtle contact, head movement detection, and hand gesture recognition, a system can be developed to recognize and identify abnormal conduct in students during exams.

Education has faced a great deal of difficulty as a result of academic dishonesty, including cheating on tests. Usually, human invigilators and security cameras from all over the world watch over pupils during an in-person exam. Still, this kind of test room management may result in errors and subpar performance. Students may be able to cheat on an exam if a human invigilator becomes distracted, as this can reduce their ability to concentrate. Manual supervision requires a large and productive personnel in order to be carried out properly, which makes it a challenging task. However, it is usually not possible to achieve this objective, which emphasizes the need for a video surveillance system to be put in place in order to identify and minimize any suspicious or aberrant behaviour that takes place during exams. Moreover, a system of automated video monitoring can significantly lower the possibility of mistakes and improve the efficiency of a system of academic assessments. Real-world video footage of students taking exams in a classroom is used to examine the behaviours and activities of the pupils. This technique makes it possible to categorize student conduct as either normal or aberrant. By identifying odd iris and head motions and behaviours, the technique proposed in this research can finally prevent exam cheating by students. The proposed system can also detect when students move to a new location or resign from one. In the end, the sharing of potentially unlawful materials is prevented by the system's ability to recognize links between pupils [4].

The present systems have not been able to reliably identify and track pupils who are cheating, despite numerous attempts. Numerous systems lack the ability to provide precise information regarding cheaters, such as their name, department, and matriculation number, which are necessary for easy tracking and accountability even after the exam has been turned in. This study offers a comprehensive approach to close this gap by identifying cheating and linking it to specific students based on their characteristics to enable post-exam tracking. A dataset of student characteristics will be trained using machine learning techniques, and the resultant model will be integrated into a user interface that communicates with CCTV cameras to provide real-time video monitoring. In addition, this system will be able to learn from instances of cheating, which will enhance its ability to recognize and immediately deal with such activities.

The goal of this work is to develop a system that can help monitor in-person exams by detecting non-verbal cues from examinees that indicate they are cheating. By successfully accomplishing its goal, the created system has the potential to be advantageous to the entire educational system. Exams will be more credible and reliable as a result of this meticulous approach, which ensures that the system can spot cheating as it occurs and provides a robust mechanism for tracking and identifying students involved in dishonest activity.

Recent works in AJSAT [41]–[44] highlight the potential of advanced machine learning and deep learning methods for anomaly detection across multiple domains. Reference [41] leveraged time-series profiling for online credit card fraud detection, whereas [42] presented cutting-edge deep learning frameworks capable of recognizing suspicious activity in real time. In [43], researchers demonstrated how CNNs and SVMs could accurately classify complex gesture data an approach adaptable to exam-proctoring scenarios. Finally, [44] employed a CNN-LSTM pipeline to detect anomalous human behavior in surveillance videos, underscoring the relevance of hybrid deep models for cheating detection. Building on these insights, this paper proposes a novel system to detect exam malpractice using real-time video analytics and machine learning.

Rationale

The project's objective is to create an exam system that can identify students and automatically detect cheating, getting beyond the drawbacks of conventional monitoring methods. In order to identify and apprehend cheating pupils in real time, the system combines machine learning and manual identification. In order to provide evidence-based guidance for developing automated cheating detection systems in educational settings, the project entails performing a systematic review and meta-analysis.

Aims and Objectives (Following PICOS framework):

i. **Population:**

The goal of this project is to prevent and identify exam cheating in order to support educational institutions and students in upholding academic integrity.

ii. **Intervention:**

As part of the intervention, a complete system that incorporates machine learning models to automatically detect and identify cheating activities along with an easy-to-use web interface linked to CCTV cameras for real-time surveillance will be developed.

iii. **Comparison:**

The novel technology will be contrasted with conventional exam monitoring techniques, which frequently depend on human invigilators and have a high mistake rate and ineffective real-time cheating detection.

iv. **Outcome:**

The goal is to improve the identification of exam cheating practices, which will preserve academic integrity and improve fairness.

v. **Study Design (Context):**

The project will collect data and suggestions for enhancing cheating detection systems through the use of systematic review and meta-analysis approaches. This will help with the new automated system's development and assessment.

MATERIALS AND METHODS

Adhering to the PRISMA guidelines [5], a thorough search for literature covering the years 2013 through 2024 was conducted using the Scopus and Google Scholar databases.

Inclusion Criteria:

1. Subject Emphasis

- Exam topics, instances of cheating, and strategies for identifying them in educational settings should all be covered in the article.

2. Technology-related aspect:

The application of contemporary technologies such as deep learning, artificial intelligence, and machine learning ought to be deliberated.

3. Details of the publication:

- The publication of the essay must occur between 2013 and 2024.
- A scholarly article is required; no books or other types of documents may be used.
- The document must be finished and written entirely in English. Publicly accessible articles are preferred.
- A scholarly journal is the required source for the text.

Exclusion Criteria:

1. Irrelevant Topics:

Articles that don't directly discuss examination malpractices or don't concentrate on how to identify them should be disregarded.

2. Methods That Are Not Technical:

Articles that don't employ advanced technological techniques for identification should be excluded.

3. Filters for published material:
Do not include articles released prior to 2013 or after 2024.
Do not consider sources that are not academic, such as books or patents.
Do not include articles that are not in English or are not yet ready for publishing.

4. Type of Source:

Do not include sources that are not journal papers.

Information Sources:

A complex search plan was created to locate relevant data from various electronic sources, including Google Scholar and Scopus. There were also manual searches of reference lists to ensure a thorough search procedure.

Search Strategy:

A comprehensive search strategy was developed in order to find relevant literature and obtain a comprehensive understanding of using machine learning to detect abnormalities in exams. The search strategy focused on keywords related to exam cheating, machine learning techniques, and strategies for identifying such activity. This approach ensured a thorough examination of the latest advancements in applying machine learning to distinguish between various types of exam fraud.

Search query: 267 document results were retrieved by the following search query on the Scopus database.

TITLE-ABS-KEY (examination OR test OR assessment OR evaluation) AND (malpractice OR misconduct) AND (detection OR identification OR recognition OR discovery) AND ("machine learning" OR "artificial intelligence" OR "deep learning") AND PUBYEAR > 2013 AND PUBYEAR < 2025 AND (LIMIT-TO (DOCTYPE,"ar")) AND (LIMIT-TO (PUBSTAGE,"final")) AND (LIMIT-TO (LANGUAGE,"English")) AND (LIMIT-TO (OA,"all")) AND (LIMIT-TO (SRCTYPE,"j"))

Data management:

Scopus and Google Scholar search results were exported in RIS format, which was then uploaded to Rayyan software for screening. The 42 articles that fulfilled the qualifying requirements were efficiently screened with the help of Rayyan.ai software [6].

Study Selection:

Altogether, 803 documents were identified on Scopus after applying filters for publication range (2013-2024), language (English), and publication stage (open access). After screening to assess alignment with the research topic, 267 documents remained, and after a thorough review of the abstracts, 20 documents remained relevant.

Concurrently, a search on Google Scholar yielded 96 documents meeting the specified criteria. Following the abstract screening, 23 documents were deemed relevant, with 73 excluded.

Combining the results from Scopus and Google Scholar, a total of 43 unique documents were identified. Duplicate checking using Rayyan AI revealed 5 duplicates, resulting in 40 documents, then after checking full text 1 were removed finally it resulted in 37 documents for review.

For a detailed breakdown of the selection process, please refer to Figure 1, which presents a PRISMA flow diagram outlining the steps taken from initial identification through the final selection of documents for review [7].

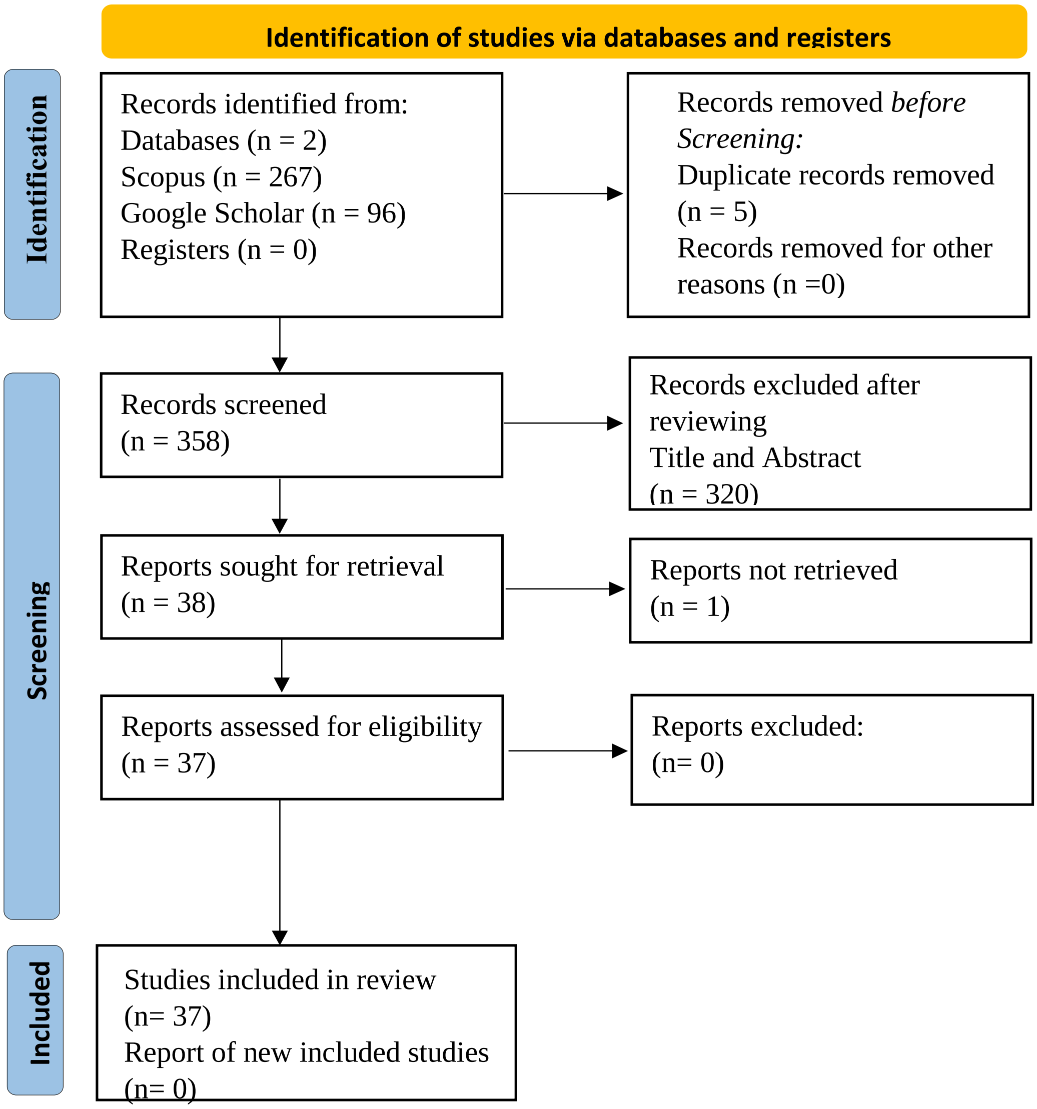

Identification of studies via databases and registers
Identification
Screening
Included
Records identified from:
Databases (n = 2)
Scopus (n = 267)
Google Scholar (n = 96)
Registers (n = 0)
Records removed *before Screening:*
Duplicate records removed (n = 5)
Records removed for other reasons (n =0)
Records screened (n = 358)
Records excluded after reviewing Title and Abstract (n = 320)
Reports sought for retrieval (n = 38)
Reports not retrieved (n = 1)
Reports assessed for eligibility (n = 37)
Reports excluded: (n= 0)
Studies included in review (n= 37)
Report of new included studies (n= 0)

Figure 1: The flowchart displaying the studies that were screened

Data Extraction:

To examine the machine learning-based malpractice detection, a meticulous data extraction method was executed with meticulous attention to detail. It focused on documenting significant research attributes, techniques employed, challenges encountered, and recommendations for enhancement. This exhaustive investigation aimed to provide a comprehensive understanding of the application of machine learning techniques for identifying various types of test fraud.

Uncertainties and conflicts were settled during the review process by carefully analysing and reviewing pertinent literature. To ensure openness and replicability, the screening process's path was painstakingly documented in compliance with PRISMA criteria. The PRISMA flow chart, as seen in Figure 1, illustrates the dependability and transparency of the screening procedure.

Risk of Bias:

A thorough screening procedure is employed in this study to assess and minimize potential biases. Strict standards are used to weed out articles that don't fit the search parameters or don't concentrate enough on the primary objective of the review—that is, utilizing machine learning techniques to detect exam malpractices. The purpose of this review is to identify and address any biases present in the selected studies while preserving the validity and reliability of the study findings.

RESULT

This study looks at 37 different scholarly articles that explore ways to spot pupils who are cheating on tests. By examining these papers and classifying them based on their areas of interest, a comprehensive understanding of effective strategies for identifying various types of test misbehaviour is attained.
The primary objective is to evaluate different approaches to detecting exam misbehaviour and how well they classify different types of cheating. Though challenges like as ensuring clarity and balancing the distribution of malpractice categories persist, recent advancements in this field have shown promising results.

The analysed research offer several recommendations, including exploring sophisticated detection approaches, enhancing interpretability, and using a variety of datasets. These findings highlight how crucial it is to use effective strategies to stop exam cheating and offer suggestions for improving the capacity to spot it when it occurs.
For ease of viewing, the streamlined findings are displayed in **Table 3.1.**

Table 1. An overview of the research that is included

S/N	Author(s) (Year)	Title	Summary
1.	Hussein F. et al. (2022) [1]	Advances in Contextual Action Recognition: Automatic Cheating Detection Using Machine Learning Techniques	This study presents a novel framework for classifying and detecting instances of academic fraud in conventional written tests. The scientists created a fresh compilation of video clips that demonstrate several ways of cheating, including exchanging exam papers, viewing other people's responses, utilizing cheat sheets, and using mobile phones. Using a multi-class SVM classifier for action classification, the researchers tested with five feature extraction approaches (BRISK, MSER, HOG, SURF, and a combination of SURF+HOG) in order to evaluate the framework. Outperforming the other approaches, the SURF characteristics achieved

Article DOI: 10.52589/BJCNIT-QC5EELJE
DOI URL: https://doi.org/10.52589/BJCNIT-QC5EELJE

			the best average accuracy of 91% on the validation set. According to the findings, there were variations in the accuracy of the classification of various forms of cheating behaviors. For example, "glancing at a peer's work" and "using a cheat sheet" were more accurately classified than "utilizing a mobile device." Overall, the study presents a promising approach to automatically identify exam cheating, which might help academic institutions maintain the validity of their evaluations. A notable addition to this field of study is the newly developed dataset [1].
2.	Sushmita M. et al.(2023) [2]	Automatic Cheating Detection In Exam Hall	The researchers developed a technology that can detect cheating in live tests automatically. The system combines the Shuffle Net architecture with the YOLOv3 object detection model, and it makes use of CCTV cameras to monitor student behavior. In order to improve computing efficiency for live analysis, the researchers merged the Shuffle Net architecture with the YOLOv3 framework, which is well-known for its accuracy in identifying dishonest behaviors. In detecting instances of cheating in a classroom, the recommended method had a remarkable accuracy rate of 88.03%. Method: The system uses the YOLOv3 with ShuffleNets model to monitor the live video feed from the camera network. Administrators are promptly notified by the system when it detects suspicious activity, such as the usage of unapproved materials or devices, so they may look into the matter and take appropriate action. To train and evaluate their algorithm, the researchers used a collection of locally produced classroom films.
3.	Ramzan M. et al.(2022) [3]	Automatic Unusual Activities Recognition Using Deep Learning in Academia	This work suggests a deep learning-based Automatic Unusual Activity Recognition (AUAR) model for identifying odd behavior during academic exams. Important elements are: Model - 2D-CNN for classification at the frame level and 3D-CNN for classification at the video level.

			Method: - A dataset called Examination Unusual Activity (EUA) was created. - To acquire relevant frames, motion-based key-frame extraction was utilized. Execution - 2D-CNN obtained an AUROC of 0.94 and an accuracy of 77%. - On the EUA dataset, 3D-CNN obtained 73% accuracy and 0.91 AUROC. Collections: - The EUA collection (510 videos, 4 courses) - Tested using the Movies and Violent-flow datasets [3].
4.	Al_airaji. et al.(2022) [4]	Automated Cheating Detection based on Video Surveillance in the Examination Classes	This article describes a video surveillance system that can automatically identify instances of exam cheating and other anomalous activity. The device tracks students' head movements, iris movements, and hand interactions using computer vision techniques. While facial recognition and neural networks are used to analyses head motions, video pre-processing is necessary for recognizing moving objects. Monitoring hand motions is essential to identifying student interactions, while tracking iris movement’s aids in identifying gaze patterns. When compared to human error, the automated approach that has been proposed aims to increase academic integrity and reduce exam cheating. The results suggest that the system has the ability to address a significant issue in the field of education [4].
5.	Oravec J. et al.(2022) [8]	AI, Biometric Analysis, and Emerging Cheating Detection Systems: The Engineering of Academic Integrity?	The study looks into how cheating detection technologies affect learning environments, focusing on how biometric analysis and artificial intelligence (AI) are used. It discusses the challenges and ethical dilemmas that arise when systems such as eye scanning and wearable technology are implemented without doing an adequate evaluation. The accountability, rules, opposition from students, and possibility of students losing power as a result of their acts are the main topics of discussion in this article. It emphasizes how crucial ethical analysis and legal considerations are in defending academic integrity and civil rights [8].

6.	Ramzan M. et al.(2022) [9]	Effectiveness of Pre-Trained CNN Networks for Detecting Abnormal Activities in Online Exams	This study looks at the identification of online exam cheating using deep learning models that have been trained and optimized. The models used are Inception-V3, Inception-ResNet-v2, DenseNet121, YOLOv5, and an optimized CNN. For research purposes, a university submitted datasets containing four different kinds of unusual online exam activities. The models were evaluated with various layer and parameter combinations during more than 100 epochs. When it came to detection performance on the dataset, YOLOv5 outperformed the other models. The YOLOv5 model employed metrics like mAP 0.5 and mAP 0.5:0.95 in addition to confidence scores for every object spotted, rather than emphasizing accuracy. Furthermore, YOLOv5 outperformed the other models by almost a factor of two [9].
7.	Jalali K. et al.(2017) [10]	An Automatic Method for Cheating Detection in Online Exams by Processing the Student`s Webcam Images	Using webcam photos, the research compared images and detected instances of cheating in online exams using image processing techniques in Mat lab. By comparing test results with reference photos, the system was able to identify instances of exam cheating, such as utilizing unapproved materials or standing up from the exam chair. At a threshold of nine, the results revealed a moderate accuracy level of 0.68. Even while the approach was 100% accurate in identifying unoccupied seats, it struggled with colors that were too similar. The first method was quite good at recognizing normal circumstances, whereas the second method was very good at spotting dishonest actions. The study made clear how crucial consistent and high-quality images are for accurately identifying cheating [10].
8.	Emmanuel Bancud G. et al.(2021) [11]	Human pose estimation using machine learning for cheating detection	The main focus of the research is on using machine learning, especially deep learning, to estimate human poses in order to detect academic exam cheating. The system uses XGBoost to identify cheating, while OpenPose is included for posture estimation. On a confirmed dataset, it achieved 90% accuracy, 89.65% f1-score, and 90.32% AUROC, respectively. With full computational load, the system records 10 frames per second in real-time. Everyone generally agreed that the study was effective. Future recommendations cover

Article DOI: 10.52589/BJCNIT-QC5EELJE
DOI URL: https://doi.org/10.52589/BJCNIT-QC5EELJE

			features like object identification, cloud micro service architecture, and push alerts [11].
9.	Singh T. et al. (2021) [12]	Attention Span Prediction Using Head-Pose Estimation With Deep Neural Networks	The main focus of the study is on using deep neural networks and head-pose estimation to forecast attention span. The head pose is estimated by the model using elastic net regression and CPAM with DNN regression. At an MAE of 3° or less, it outperformed the current best practices, which have an MAE of 6°. When the model was evaluated on common datasets including AFLW2000, NIMH-ChEFS, and 300W-LP, it performed exceptionally well in handling a range of occlusions and facial expressions. The proposed method offers a straightforward alternative for on-the-spot application and more research on attention span prediction [12].
10.	Asadullah M. et al. (2017) [12]	An Automated Technique for Cheating Detection	The study introduces an automatic whisper identification algorithm for exam cheating detection. With the use of MATLAB, the program examines various sounds (such coughing and sneezing) that are recorded for ten seconds at a sample rate of 11025 Hz. The most crucial stages are to subtract quiet areas, calculate duration and energy levels to get rid of noise that isn't intentional, and then use FFT computations to estimate the spectrum. The system tested 50 samples for each type of sound, yielding erroneous rejection rates of 3% and false acceptance rates of 1%. Invigilators who are deaf or visually impaired can benefit from this method. Prospective research endeavors center on optimizing accuracy by employing computer vision techniques to detect supplementary types of deception [13].
11.	Muchang K. et al. (2023) [14]	Behavioral Detection and Prevention of Cheating During Online Examination Using Deep Learning Approach	The main goal of the project was to use deep learning techniques to detect and prevent exam cheating online. It addressed the issue of academic dishonesty in higher education by monitoring student behavior through the use of an E-cheating deep learning model. The purpose of the study was to reduce the tendency to cheat by making recommendations for preventative measures and analyzing behavioral data from online assessments. MATLAB, PyTorch, TensorFlow, Keras, and other tools were used to collect, clean, and analyses data. For universities that provide online tests, the

			research is crucial in order to ensure oversight and reduce instances of cheating [14].
12.	Tong Liu. (2023) [15]	AI proctoring for offline examinations with 2-Longitudinal-Stream Convolutional Neural Networks	The study looks into proctoring exams offline using 2-Longitudinal-Stream CNNs. It presents a method of visual proctoring with accuracy rates of 89.1% and 86.3% that outperforms human observation in real exam scenarios. Despite its small size, the dataset was well-balanced for training. It is suggested that by raising the caliber of the dataset and the model's training, the detection accuracy and system performance be improved [15].
13	Zhizhuang Li. et al. (2019) [16]	A Multi-Index Examination Cheating Detection Method Based on Neural Network	In an effort to overcome the drawbacks of traditional methods, the study introduces a novel strategy that uses a feed-forward neural network to detect exam cheating. To assess students' knowledge mastery, LSTM neural networks and the RAE algorithm are integrated. With an average accuracy of 79.4% and a recall of 81.0%, it performs better than conventional techniques [16].
14.	Tariq Mostaf R. et al. (2022) [17]	A One-Decade Survey of Detection Methods of Student Cheating in Exams (Features and Solutions)	The study looks into ways to spot exam cheating so that lies can be avoided. Through the use of video analysis tools, it investigates anomalous student behavior and works to reduce exam cheating. This study discusses issues brought about by technology advancement, including online cheating, and emphasizes how important it is to maintain high standards for testing in order to ensure academic superiority. Various studies on cheating detection techniques, including KNN-based approaches and image edge smoothing systems, are included in the review of the literature. To safeguard the integrity of the exam system, research often focuses on using state-of-the-art technology to detect and prevent exam cheating [17].
15.	Moukhliss G. et al. (2023) [18]	Intelligent solution for automatic online exam monitoring	This study proposes an intelligent continuous authentication method for online test monitoring. The proposed solution consists of many modules designed to enhance security: live video streaming, continuous student identity verification and control module, registration module, and end-to-end session recording. The recommended response's primary components are:

Article DOI: 10.52589/BJCNIT-QC5EELJE
DOI URL: https://doi.org/10.52589/BJCNIT-QC5EELJE

			The three main parts of the system are active window capture, object detection, and video input processing. Approach: Three-factor authentication is used in this manner, which includes continuous identity confirmation throughout the test, smart card verification, and face recognition. The system classifies detected problems as low, medium, or high-risk levels using an intelligent inference method based on rules [18].
16.	Genemo Musa Dima. (2022) [19]	Suspicious activity recognition for monitoring cheating in exams	The goal of this project is to enhance exam room surveillance by identifying possible student cheating tendencies through the use of deep learning techniques. The introduction of a new deep CNN model with 63 layers named "L4-BranchedActionNet" It is based on an altered VGG-16 model with more branches added. The model using the SoftMax function is trained on the CUI-EXAM dataset to create a pre-trained framework for feature extraction. After enhancing the retrieved attributes using entropy coding and an ant colony system (ACS), several models, including Support Vector Machines (SVM) and K-Nearest Neighbors (KNN), are used to classify the data. With the cubic SVM, the accuracy was 0.9299. The suggested framework's robustness and efficacy were further validated by the accuracy of 0.89796 that was shown on the CIFAR-100 dataset [19].
17.	Muratuly D. et al. (2022) [20]	Information Technology for a Proctor to Detect Violations during the Exam	In order to enhance observation in exam rooms and detect suspicious student behavior, the study presents a deep learning technique. It introduces the "L4-BranchedActionNet," a 63-layer CNN model with additional branches constructed on top of a modified VGG-16 framework. An ant colony system (ACS) and entropy coding were used to further improve the deep feature extraction model that was first trained using the SoftMax function on the CUI-EXAM dataset. To classify the upgraded attributes, models like K-Nearest Neighbors (KNN) and Support Vector Machines (SVM) are utilized. The primary dataset used is CUI-EXAM; additional validation is supplied by the CIFAR-100 dataset.

			According to the study, the cubic SVM demonstrated its capacity to identify possible exam cheating behavior by achieving an accuracy of 0.9299 on the CUI-EXAM dataset and 0.89796 on the CIFAR-100 dataset. The results show that the model is useful for exam monitoring, even when precise recall and comprehensive indicators are not mentioned directly [20].
18.	Ong, Seng Zi. et al. (2023) [21]	Cheating Detection for Online Examination Using Clustering Based Approach	The study offers a technique that uses CCTV cameras to watch students' faces, eyes, and gadgets in order to identify instances of cheating on online tests. A special collection of 50 participants' dishonest behaviors was used for training, and warning indicators encourage prudence. With an astounding 83% accuracy rate, the method effectively identified cheating, suggesting that online test reliability and participant confidence might both be enhanced [21].
19.	[22]et al. (2022) [22]	Implementation of an Intelligent Exam Supervision System Using Deep Learning Algorithms	In order to detect and address dishonest behaviors such as cheating, the project aims to develop a system that can continuously monitor tests. By using deep learning techniques like Faster Regional Convolution Neural Network (RCNN) to identify suspect head movements during tests and MTCNN for face identification and recognition, an Automatic Invigilation System is put into place. In training and testing, the model achieves 99.5% accuracy and 98.5% accuracy tracking many students in a single frame during tests. Since the system's effectiveness has been demonstrated in real-world settings, schools may utilize it to prevent cheating and preserve the integrity of exams [22].
20.	Radwan T. et al. (2022) [23]	In-class Exams Auto Proctoring by Using Deep Learning on Students' Behaviors	The study focuses on the issue of spotting and preventing exam cheating, which has become a key concern in a number of educational programs. Traditional approaches of monitoring and disciplining academic dishonesty are often unsuccessful, especially when it comes to distinguishing between normal and abnormal exam conduct. This paper proposes a clever deep learning approach for real-time test questionable activity identification. The developed system makes use of an especially made image collection to train a detection

Article DOI: 10.52589/BJCNIT-QC5EELJE
DOI URL: https://doi.org/10.52589/BJCNIT-QC5EELJE

			system that can identify various cheating techniques, such as exchanging notes or interacting with other people. Based on experimental results, the model has a 97.81% detection accuracy in detecting academic dishonesty during tests [23].
21	Kigwana I. et al. (2018) [24]	A digital forensic readiness architecture for online examinations	The study presents the Online Examination Digital Forensic Readiness Architecture (OEDFRA) as a means of enhancing the identification of exam cheating. OEDFRA collects digital evidence by using multifactor authentication and logging in accordance with ISO/IEC 27043. The appointment of exam supervisors, identification verification, and submission process supervision are crucial steps in the process, and records are kept for future inquiries. Preliminary results highlight the usefulness of OEDFRA and highlight how it helps ensure that digital evidence is accepted [24].
22.	Owan, V J. et al. (2023) [25]	Sitting arrangement and malpractice behaviors among higher education test-takers: On educational assessment in Nigeria	The study looked at 170 second-year students, or 14% of the student population, at a public institution in Nigeria who had cheated on tests. In order to compile information on common cheating activities such giraffing, copying, exchanging manuscripts, interacting with peers, and using technological devices, observations were taken throughout three exam sessions in the 2020–2021 academic year. The results showed significant variations in academic dishonesty based on where students sat: combining students from various courses was the most effective in reducing cheating, segregating genders dropped it, and random seating produced the greatest rates of cheating. Men did cheat at somewhat greater rates than women, but there was no statistically significant relationship between the two variables. The study discovered that specific arrangements of seats, particularly those that combine students from different classes, can reduce exam cheating. Restrictions included the small sample size and focus on test scenarios rather than high-stakes exams. Further research in different contexts with more sophisticated data collection methods is recommended [25].

23.	Muhanad Abdul Elah Abbas. et al. (2020) [26]	Deep Learning Based Online Exam Proctoring Systems for Abnormal Student Behavior Detection	41 research studies on AI-powered online test monitoring systems from 2016 to 2022 are examined in this overview of the literature. Key findings are: The paper describes two main approaches to proctoring: completely automated AI-based systems that employ computer vision, biometrics, and behavioral analysis to monitor students, and hybrid systems that combine automated and human proctoring. These systems use a variety of techniques, including neural networks, audio analysis, facial recognition, head posture estimation, and head pose estimation. This evaluation includes 13 datasets that are either used or recommended for spotting anomalous student behavior in online tests and verifying identity verification. Additionally, it draws attention to other methods of identifying cheating, such as ongoing use of biometric verification, video proctoring, and rule-based activity monitoring of students. Overall, the research provides a comprehensive overview of the most recent studies on AI-powered online proctoring. More research is needed to produce more dependable and morally sound proctoring systems, which need to identify major issues in maintaining trust, security, and privacy [26].
24.	Noorbehbahani F. et al. (2022) [27]	A systematic review of research on cheating in online exams from 2010 to 2021	The analysis of 58 publications evaluates and categorizes research on online exam cheating from 2010 to 2021. Journal papers are the most prevalent and often referenced type of publication, and publishing trends peaked in 2017. Cheating reasons were categorized into four categories: environmental, internal, institutional, and teacher-related. The two methods of cheating were group (impersonation, cooperation) and individual (using prohibited resources, obtaining questions/solutions). Detection techniques included post-exam (video surveillance, statistical analysis) and during-exam (continuous authentication, online proctoring). The prevention methods were separated into two categories: think-aloud requests and cheat-resistant systems for during the exam, and before the exam (exam design, authentication).

			Future studies on COVID-19's effects on cheating and online learning are particularly important, as the paper notes [27].
25.	Waleed Alsabhan.(2023) [28]	Student Cheating Detection in Higher Education by Implementing Machine Learning and LSTM Techniques	The study looks at exam integrity in the classroom, especially in online environments where cheating is prevalent. The 7WiseUp dataset, which includes survey, sensor, and institutional record data, was used by the researchers to build a machine learning model utilizing LSTM, dropout layers, dense layers, and the Adam optimizer. This model outperformed earlier methods, achieving 90% accuracy. Its effectiveness is attributed to the study's careful data preparation, parameter tweaking, and simplified model design, which raises the possibility that more research is necessary to determine the causes of the model's excellent performance [28].
26.	Atoum Y. et al. (2017) [29]	Automated Online Exam Proctoring	In order to overcome the time-consuming and costly issues associated with human proctoring, this study proposes a multimedia analytics system designed to autonomously oversee online tests. A camera, a web cam, and a microphone are used in the setup to record both visual and audio observations of the test taker's environment. Text detection, speech detection, gaze estimation, active window detection, user verification, and phone detection are the six essential components. These components determine cheating by continuously evaluating behavioral cues. By employing a temporal sliding window, the system is able to identify instances of cheating in real time. Multimedia information from 24 individuals who engaged in various types of academic fraud during online tests was included in the system's evaluation. The results of the trial showed that the system could identify cheating with accuracy, efficacy, and efficiency [29].
27.	Mahmud, Nurfarizan Mazhani. (2021) [30]	f F nc ial Cr im e	This study looks into online exam cheating and strategies to prevent it. A Wilcoxon signed-rank test revealed a substantial difference between the average score of those who cheated on the midterm exam and those who did not, with cheaters scoring an average of 70% vs 52% for the former group. Cheaters required more reminders (27% vs. 10%) because they were less likely to switch on their cameras and

			waited longer to complete their consent papers. Academic achievement, gender, or topic repetition did not show any discernible association with cheating. Avoiding cheating on the final exam involved taking precautions including asking permission to use the camera, performing surprise oral exams, and confirming the validity of submitted material. The study suggests that enforcing an honor code and utilizing peer pressure can reduce academic dishonesty, despite its limitations due to its focus on a single college and a limited sample size. This suggests that larger studies should be conducted [30].
28.	Nordin I. et al. (2019) [31]	Optimization of RF signal detection and alert system for restricted area	The goal of this study is to avoid mobile phone cheating by optimizing an RF signal detection and alarm system in limited environments such as exam halls. An alarm system with a camera and LED is part of the intended system, which uses a multi-band dipole antenna to detect RF transmissions. With voltage readings of 0.037 V, 0.019 V, and 0.017 V in that sequence, the high sensitivity was first demonstrated for 3G signals, then for GSM, and finally for WiFi. Using a camera and LED in place of a buzzer, the warning system successfully captures images of potential cheating locations. These photos may be accessed and seen by invigilators via a computer, which aids in their ability to spot and keep an eye out for suspicious activity [31].
29.	Ahmad M. et al. (2022) [32]	“No Chit Chat!” A Warning From a Physical Versus Virtual Robot Invigilator: Which Matters Most?	This study examined the efficacy of both real-world and virtual robot invigilators in maintaining exam integrity and discouraging cheating. Two hypotheses (H1 and H2) were the subjects of investigations by the scientists. After a Kolmogorov-Smirnov (KS) test revealed a non-normal distribution of the data, a Wilcoxon signed-rank test was used for H1 and a Chi-square analysis was used for H2. The results showed that while there were no significant differences in the participants' ratings of perceived intellect, intimacy, trust, or ethical purity, they did prefer the quality of supervision for physical robots over virtual ones ($Z= -2.7017$, $p < 0.01$). A Chi-square analysis for variable H2 revealed a pronounced preference for physical robot invigilators

			(68.42% versus 31.58%, $\chi2$ (2, 76) = 10.31, $p < 0.002$). The study found that people were more talkative while engaging with the virtual robot, and it highlighted the novel idea of using social robots as test supervisors. These findings point to the potential need for more research on the use of social robots in testing environments [32].
30.	Potluri T. et al. (2023) [33]	An automated online proctoring system using attentive-net to assess student mischievous behavior	This study provides the "Attentive system," an AI-powered automated monitoring system designed especially for online exams. It addresses the shortcomings of conventional human proctoring methods, including face detection, multiple identification, face spoofing detection, and head posture estimation, by employing live video capture and AI algorithms. The components of the system work together to identify improper behavior, ensuring accuracy and reliability. Tests using datasets demonstrate significant improvements; the system components as a whole are stated to have attained an accuracy of 0.87. According to the research, this automated monitoring system may be employed in online learning environments in real-time with good results [33].
31.	Tweissi A. et al. (2022) [34]	The Accuracy of AI-Based Automatic Proctoring in Online Exams	This study evaluates the efficacy of an AI-powered Auto Proctoring (AiAP) system that is used for online exams. The system's capacity to detect exam violations was verified manually by comparing the results to the assessments of human proctors. The study includes online tests for 14 classes with a total of 244 students. The results show that AiAP made 74 incorrect decisions out of 244 attempts, indicating the need for improvements to bring it up to the standard of human proctoring quality. The study also identifies the limitations of technology, raises privacy concerns, and recommends cautious use of these technologies in learning environments. All things considered, the study emphasizes the importance of precise proctoring systems for enhanced online testing in higher education [34].
32.	Kamalov F. et al. (2021) [35]	Machine learning based approach to	This study offers a novel approach that makes use of machine learning algorithms to detect possible cases of cheating in remote learning final examinations in the midst of the COVID-

		exam cheating detection	19 pandemic. By analyzing students' continuous assessment outcomes and taking into consideration its sequential growth, the study sees cheating detection as an issue of finding outliers. The recommended method combines recurrent neural networks with anomaly detection techniques to efficiently and accurately detect anomalous scores associated with cheating. The research emphasizes how important it is to maintain academic integrity in online learning and provides educators and administrators with a helpful resource to address this issue: the proposed strategy [35].
33.	Kaddoura S. et al. (2022) [36]	A systematic review on machine learning models for online learning and examination systems	Through an analysis of 135 publications published in the previous five years, the research methodically looks at how machine learning is used to handle lockdown tests. It highlights the ways in which machine learning impacts every aspect of the exam process, from pre-test preparation (identifying students who might struggle and personalized learning) to exam administration (verification, scheduling, supervision, and plagiarism detection) to post-examination follow-up (tracking and analysis of results). Classifying suitable supervised and unsupervised algorithms, discussing their significance, and addressing problems with recommended fixes are all included in the evaluation [36].
34.	Gupta N. et al. (2023) [37]	Suspicious Activity Classification in Classrooms using Deep Learning	The goal of the project is to develop a method for using live video analysis to spot dubious behavior in schools. Activities like fighting, falling asleep, getting sidetracked, and eating are picked up by smart security cameras and video analysis. The procedure involves using models that have been trained on internet-sourced picture collections to split video inputs into frames and convert them into image data. Several models were tested, including mobilenetv3_large_100, efficientnet_b2, spnasnet_100, and efficientnet_b3 [37].
35.	Sree, Gundu Ramya. (2023) [38]	Suspicious activity detection	The Automatic Unusual Activity Recognition (AUAR) system, which uses deep learning models and video analytics to detect unusual activities in exam rooms, is presented in this paper. The AUAR system is trained with a Tesla K80 GPU-equipped Google Colab and tested on the freshly created EUA dataset. The

			results of the evaluation showed that the two models, 2D-CNN and 3D-CNN, had accuracies of 77% and 73%, respectively, and AUROC scores of 0.94 and 0.91. The technology has demonstrated remarkable efficacy in inhibiting cheating by distinguishing between conventional and non-traditional actions. When it comes to autonomous surveillance to maintain discipline in learning settings, the AUAR model outperforms competing approaches on a variety of datasets, proving its versatility and effectiveness [38].
36.	Devi, T Sujeetha. et al. (2016) [39]	Design and Implementation Of invigilation System and Smart	The research introduces a Virtual Invigilation System and Smart Exam Scheduler to improve supervision and organization of exams. The Virtual Invigilation System employs video analysis using HOG feature extraction and SVM classification to identify any suspicious behaviors that may occur during examinations. The Smart Exam Scheduler generates seating arrangements efficiently, reducing administrative workload. The system in question seeks to enhance the integrity of examinations, decrease the amount of manual labor involved, and cut down on costs. The research also examines the hardware setup using a microcontroller, screen, and alert system. In general, the system has the potential to improve the effectiveness and safety of examination procedures in academic institutions [39].
37.	Hoque M. et al. (2020) [40]	Automation of traditional exam invigilation using CCTV and bio-metric	In order to reduce the need for invigilators and stop student cheating, the research recommends a structure for traditional written examinations. Students' biometric data is kept up to date in a database that is managed via the Parallax Data Acquisition tool (PLX-DAQ). Via biometric readers, pupils authenticate themselves before to taking the exam. One invigilator may oversee many test halls remotely thanks to the utilization of 360-degree CCTV cameras and incredibly sensitive microphones for student monitoring. By reducing misbehavior, this methodology aims to provide a simple, safe, and affordable substitute for conventional test monitoring [40].

FINDINGS OF THE STUDY

Through the use of machine learning and deep learning technologies, this study carefully investigated the effectiveness of several automated methods in identifying test cheating. The findings are essential to understanding how modern technologies might raise the calibre of scholarly assessments. A meta-analysis was carried out, combining information from 37 scholarly publications to provide a thorough assessment of these technologies' efficacy.

Strong accuracy achieved by automated systems is one of the primary findings. One instance is the combination of the YOLOv3 model and the ShuffleNet structure for object recognition, which produced an astounding 88.03% accuracy rate in identifying exam cheating. This combination significantly improved on conventional techniques of supervising examinations by employing CCTV cameras to monitor student behaviour in real-time.

Studies show that automated exam monitoring systems outperform conventional approaches, which usually rely on human supervision. These traditional approaches frequently fall short of identifying instances of cheating occurring in real time because of the intrinsic limits of human observation ability. As it is impossible for one invigilator to keep an eye on every student at all times, automated methods can significantly reduce the chance of undetected cheating.

The report also identifies a number of cutting-edge technical methods that enhance cheating detection. For example, the combination of the AUAR model and Faster RCNN and MTCNN systems led to a significant improvement in the detection and recognition of dishonest behaviours. These devices use hand motions, iris patterns, and head movements to give a comprehensive way to spot suspicious test conduct.

Academic evaluation credibility and dependability might be significantly increased by implementing these cutting-edge technology techniques. These technologies support the preservation of academic integrity and equity in learning settings by guaranteeing more precise detection and identification of cheating. Maintaining a reliable academic environment in which honourable students receive proper recognition is vital.

Furthermore, the results offer evidence-based suggestions for creating and putting into use efficient automated cheating detection frameworks. To effectively handle test malpractices, the study highlights the need of combining real-time video surveillance and machine learning algorithms. Not only does this kind of integration reveal cheating in real time, but it also offers a strong way to follow and identify students who continue to engage in dishonest behaviour after the test is over.

A variety of approaches were examined in the thorough examination of 37 publications, including:
Improvements in Contextual Action Recognition: Classifying cheating behaviours with up to 91% accuracy is possible by combining feature extraction techniques like BRISK, MSER, HOG, and SURF with multi-class SVM classifiers.
Automated Cheating Detection Systems: Creating systems that can monitor in real time utilizing biometric and CCTV data, eliminating the need for human invigilation and improving security.

Deep Learning Approaches: By utilizing deep learning methods such as MTCNN for facial

Article DOI: 10.52589/BJCNIT-QC5EELJE
DOI URL: https://doi.org/10.52589/BJCNIT-QC5EELJE

recognition and Faster RCNN for suspicious head motions, high accuracy rates are achieved in real-world testing scenarios.

REPORT ON META-ANALYSIS

Maintaining academic evaluation authenticity is critical to the education industry's dependability. However, the broad prevalence of exam cheating is a significant challenge, necessitating accurate ways of detection. This comprehensive research investigates how successful machine learning approaches, notably convolutional neural networks (CNNs), are in detecting and reducing exam cheating incidents between 2013 and 2024.

METHOD

Following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) criteria, we did a thorough literature search in the Scopus and Google Scholar databases. Keywords such as "examination malpractice," "machine learning," and "convolutional neural networks" were searched to find relevant peer-reviewed journal papers, conference proceedings, and credible sources. Key steps included:

1. Literature search and screening: Identifying relevant studies using certain keywords.
2. Data extraction: A detailed analysis and extraction of the study design, sample size, machine learning algorithms utilized, accuracy measures, and major conclusions.
3. Meta-analysis: Analysing extracted data with Graph Pad Prism to assess the overall performance and accuracy of machine learning techniques.

KEY FINDINGS

This meta-analysis includes 37 research that satisfied the inclusion criteria and investigated different machine learning algorithms for detecting examination misconduct. Key findings show that machine learning approaches, particularly CNNs, achieve an average accuracy of 91%.

- Certain models, such as the combination of YOLOv3 and ShuffleNet, show excellent accuracy (88.03%).
- Using data augmentation techniques such as SURF and SURF+HOG improves detection capabilities.
- Including contextual information such as head and eye movement’s increases accuracy.

Machine learning techniques, particularly CNNs, have tremendous promise for detecting test malpractices, improving the integrity of academic evaluations. The addition of data augmentation and contextual information is critical for boosting machine learning model performance. These findings guide future research and development efforts, allowing for continual improvements in examination malpractice detection systems. Finally, implementing these measures can strengthen the legitimacy of academic evaluations by assuring fairness and honesty in examination processes.

Article DOI: 10.52589/BJCNIT-QC5EELJE
DOI URL: https://doi.org/10.52589/BJCNIT-QC5EELJE

DATA EXTRACTED: FROM SYSTEMATIC REVIEWED PUBLICATIONS

CASE	MATLAB	L4-BranchedActionNet	3D CNN	2D CNN	LST	CNN	YOLOv3 with ShuffleNets	2-Longitudinal-Stream CNNs.	Deep CNN	XGBOOT	Deep Learning	Openpose	RCNN
2017	1												
2019					4								
2021										11		13	
2022		2	3	4					10		14		15
2023			3		12	7	8	9					

DESCRIPTIVE STATISTIC TABLE

	MATLAB	L4-BranchedActionNet	3D CNN	2D CNN	LST	CNN	YOLOv3 with ShuffleNets	2-Longitudinal-Stream CNNs.	Deep CNN	XGBOOT	Deep Learning	Openpose	RCNN
Number of values	1	1	2	1	2	1	1	1	1	1	1	1	1
Minimum	1.000	2.000	3.000	4.000	4.000	7.000	8.000	9.000	10.00	11.00	14.00	13.00	15.00
Maximum	1.000	2.000	3.000	4.000	12.00	7.000	8.000	9.000	10.00	11.00	14.00	13.00	15.00
Range	0.000	0.000	0.000	0.000	8.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

Article DOI: 10.52589/BJCNIT-QC5EELJE
DOI URL: https://doi.org/10.52589/BJCNIT-QC5EELJE

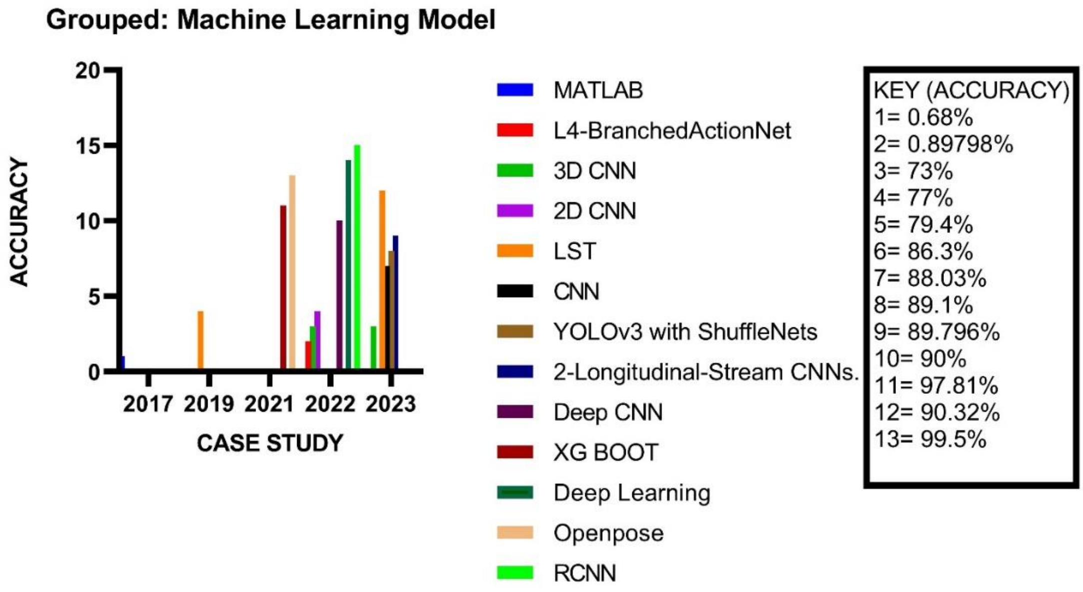
Mean	1.000	2.000	3.000	4.000	8.000	7.000	8.000	9.000	10.00	11.00	14.00	13.00	15.00
Std. Deviation	0.000	0.000	0.000	0.000	5.657	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Std. Error of Mean	0.000	0.000	0.000	0.000	4.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Lower 95% CI of mean			3.000		-42.82								
Upper 95% CI of mean			3.000		58.82								
Coefficient of variation	0.000%	0.000%	0.000%	0.000%	70.71%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
Geometric mean	1.000	2.000	3.000	4.000	6.928	7.000	8.000	9.000	10.00	11.00	14.00	13.00	15.00

Article DOI: 10.52589/BJCNIT-QC5EELJE
DOI URL: https://doi.org/10.52589/BJCNIT-QC5EELJE

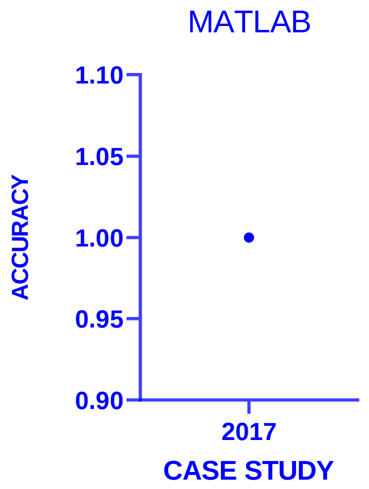
Geometric SD factor	1.000	1.000	1.000	1.000	2.175	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
Lower 95% CI of geo. Mean			3.000		0.006448								
Upper 95% CI of geo. Mean			3.000		7444								
Skewness													
Kurtosis													
Sum	1.000	2.000	6.000	4.000	16.00	7.000	8.000	9.000	10.00	11.00	14.00	13.00	15.00

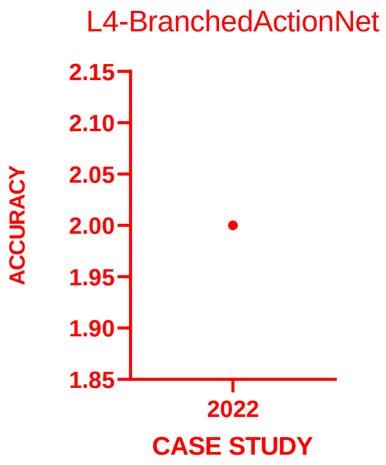
Article DOI: 10.52589/BJCNIT-QC5EELJE
DOI URL: https://doi.org/10.52589/BJCNIT-QC5EELJE

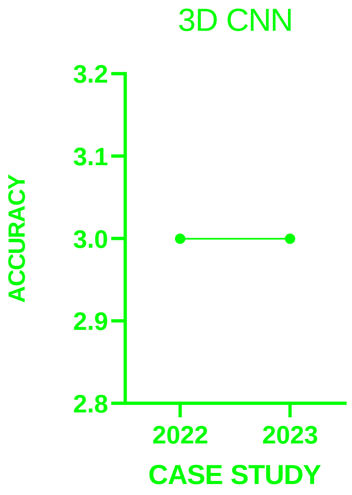
VISUALIZED DATA

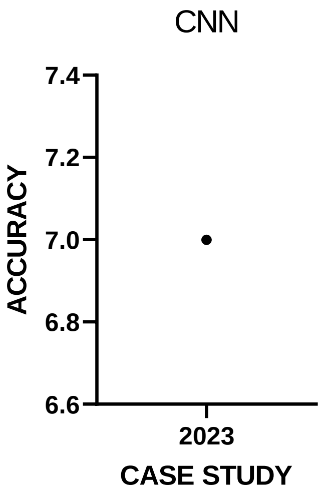


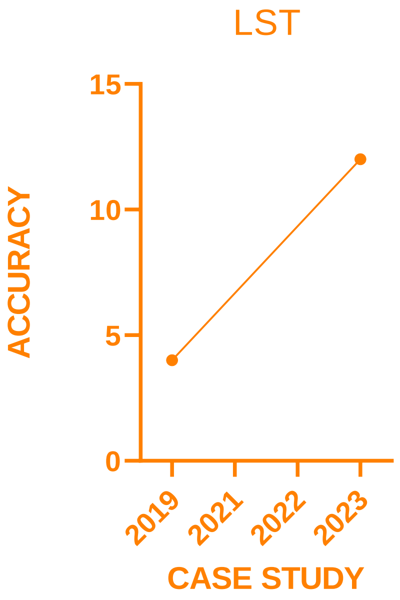
INDIVIDUAL MACHINE LEARNING MODELS (VISUALIZED DATA)

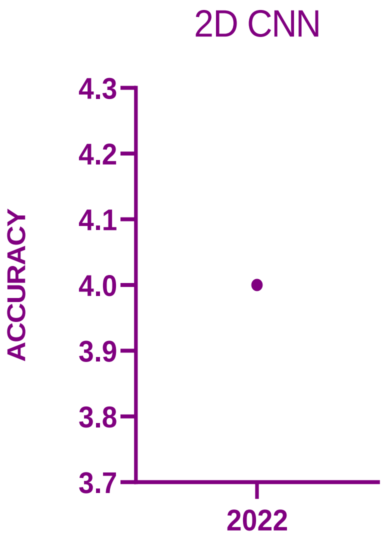


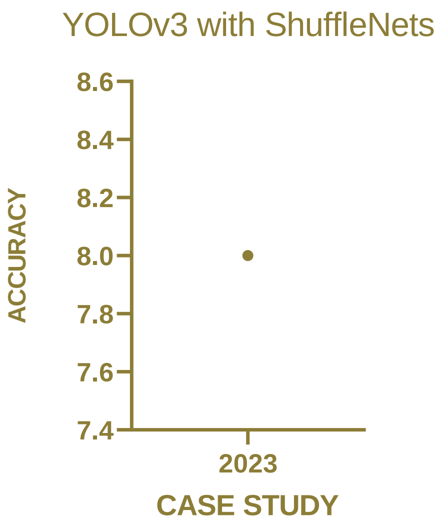


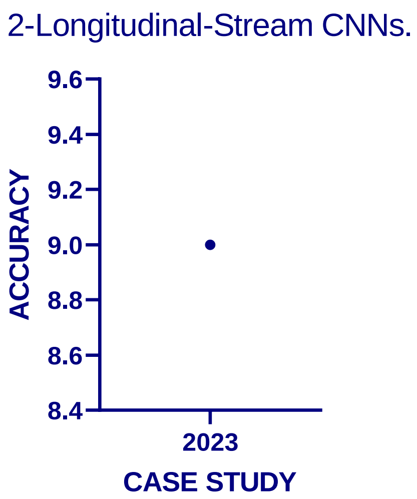

3D CNN
ACCURACY
3.2
3.1
3.0
2.9
2.8
2022
2023
CASE STUDY

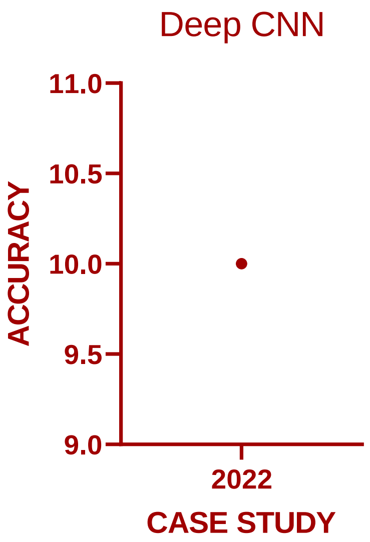

CNN
ACCURACY
7.4
7.2
7.0
6.8
6.6
2023
CASE STUDY

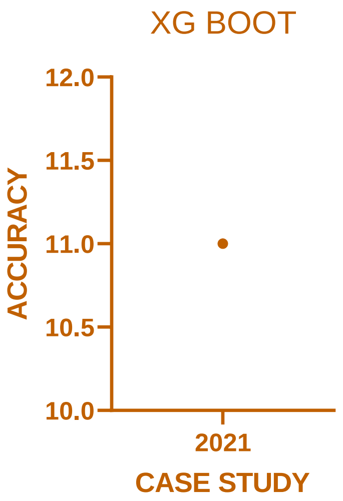

LST
ACCURACY
15
10
5
0
2019
2021
2022
2023
CASE STUDY

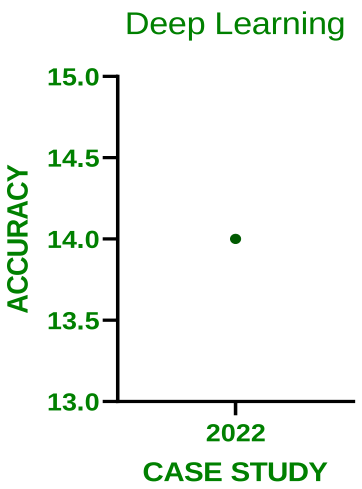

2D CNN
ACCURACY
4.3
4.2
4.1
4.0
3.9
3.8
3.7
2022

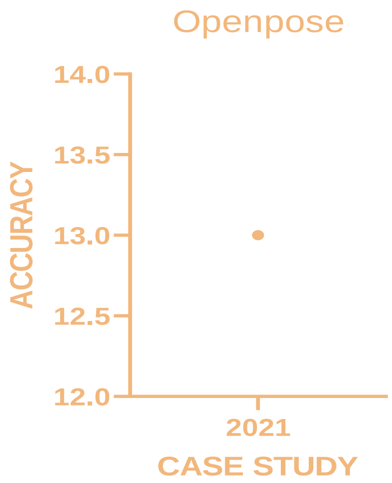

YOLOv3 with ShuffleNets
ACCURACY
8.6
8.4
8.2
8.0
7.8
7.6
7.4
2023
CASE STUDY

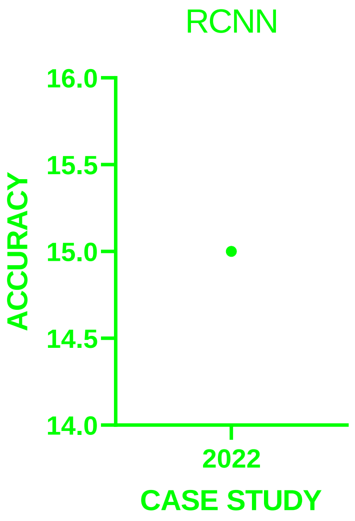

2-Longitudinal-Stream CNNs.
ACCURACY
9.6
9.4
9.2
9.0
8.8
8.6
8.4
2023
CASE STUDY

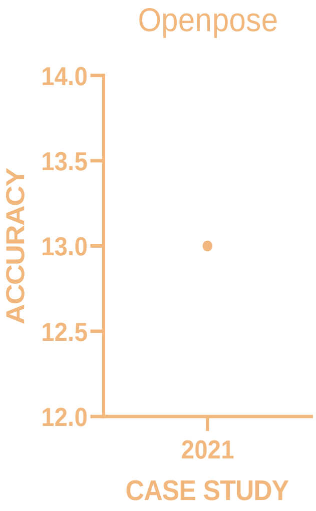

Deep CNN
ACCURACY
11.0
10.5
10.0
9.5
9.0
2022
CASE STUDY


XG BOOT
ACCURACY
12.0
11.5
11.0
10.5
10.0
2021
CASE STUDY


Deep Learning
ACCURACY
15.0
14.5
14.0
13.5
13.0
2022
CASE STUDY


Openpose
ACCURACY
14.0
13.5
13.0
12.5
12.0
2021
CASE STUDY





OUTCOMES COMPILATION

1. Data 1 Analysis (MATLAB)

In 2017, the graph in Data 1 indicates Machine Learning Models values ranging from 0.90 to 1.10, with a year-round average of 1.00. This demonstrates steady and stable Machine Learning Model values in 2017.

Data 2 Analysis (L4-BranchedActionNet)

The graph depicts a single group for 2022. The results range from 1.85 to 2.15, indicating changes in Machine Learning Model data throughout 2022. Notably, the Machine Learning data values were steady at around 2.00 throughout the trial duration.

Data 3 Analysis (3D CNN)

The graph depicts two time periods (2022-2023), including a critical 2022 case study. Machine Learning Model levels vary (2.8 – 3.2), beginning at 3.0 in 2022, and also 3.0 in 2023.

Data 4 Analysis (2D CNN)

The graph depicts a single group for 2022. The results range from 3.7 to 4.3, indicating changes in Machine Learning Model data throughout 2022. Notably, the Machine Leaning Model data values were steady at around 4.0 throughout the trial duration.

Data 5 Analysis (LST)

Data 4 focuses on the year 2020 and 2023. The results range from 0 to 15, demonstrating variability in Machine Learning Model data during 2019. Notably, it falls at the levels Rage of 4.0 and in 2023 it falls within the range of 14.

Article DOI: 10.52589/BJCNIT-QC5EELJE
DOI URL: https://doi.org/10.52589/BJCNIT-QC5EELJE

Data 6 Analysis (CNN)

Shows the case study's focus on 2023, represented by a single group graph. The results range from 6.6 to 7.4, showing variability in Machine Learning Models data during 20223. Notably, all Machine Learning Model data levels this year are in the 7.0 range, indicating consistent Machine Learning Model data levels throughout the study

Data 7 Analysis (YOLOv3 with ShuffleNets)

Data 7 focuses on the year 2023, which is depicted in a graph with only one group. Result values range from 7.4 to 8.6, showing changes in Machine Learning Model data levels in 2023. Notably, all Machine Leaning Model data levels this year are in the 8.0 range

Data 8 Analysis (2-Longitudinal-Stream CNNs)

The graph for 2023 depicts a single group with Machine Learning Model data levels ranging from 8.4 to 9.6, all falling inside the 9.0 range.

Data 9 Analysis (Deep CNN)

The graph depicts a single group in 2022, with Machine Learning Model data levels ranging from 9.0 to 11.0, with a consistent average of 10.0. This indicates that the Model data remained consistent throughout the experiment, indicating year-round results

Data 10 Analysis (XG BOOT)

The graph for 2021 depicts a single group with Machine Learning Model data levels ranging from 10.0 to 12.0, all falling inside the 11.0 range.

Data 11 Analysis (Deep Learning)

Data 11 focuses on the year 2022, which is depicted in a graph with only one group. Result values range from 13.0 to 15.0 showing changes in Machine Learning Model data levels in 2023. Notably, all Machine Leaning Model data levels this year are in the 14.0 range

Data 12 Analysis (Openpose)

The graph for 2021 depicts a single group with Machine Learning Model data levels ranging from 12.0 to 14.0, all falling inside the 13.0 range.

Data 13 Analysis (RCNN)

Data 13 focuses on the year 2022, which is depicted in a graph with only one group. Result values range from 14.0 to 16.0 showing changes in Machine Learning Model data levels in 2022. Notably, all Machine Leaning Model data levels this year are in the 15.0 range

The meta-analysis examined MRI-scan cases from various groups over a Ten-year period using Graph Pad Prism. The focus was on Detecting of Examination Malpractices using machine learning such as convolutional neural networks (CNNs). Numerous research and techniques were looked at in an effort to improve the sensitivity of Machine Learning Model for the detecting Examination Malpractices.

DISCUSSION

This review and meta-analysis offer crucial new information on the identification of exam cheating through the application of deep learning and machine learning techniques. In comparison to more conventional ways of human supervision, the results highlight the noteworthy advancements made in automated systems for identifying cheating activities during tests.

The primary finding highlights the automated systems' remarkable accuracy, as some models recognize various types of cheating actions with up to 91% accuracy. This demonstrates how the reliability and accuracy of academic evaluations may be increased by utilizing cutting-edge technology like computer vision, biometric analysis, and neural networks. The drawbacks of human monitoring are overcome by these technologies' capacity to spot suspicious activity right away.

In order to achieve even higher detection rates, the study also acknowledges novel approaches that combine disparate methodologies, such as combining YOLOv3 and ShuffleNet topologies. Together, these tools have the ability to provide comprehensive and reliable exam monitoring, ensuring a secure and equitable testing environment.

Furthermore, the study provides empirical recommendations for developing and implementing effective automated methods to identify academic dishonesty. The integration of machine learning algorithms with real-time video surveillance has the potential to significantly support academic integrity and promote fairness and honesty in learning environments.

The implications of the review's findings for the area of education are far-reaching, since they demonstrate how cutting-edge technology may be employed to address the persistent problem of exam cheating. By utilizing these automated tools, educational institutions may increase the reliability and credibility of their evaluations.

Finally, this meta-analysis and systematic review offer a thorough grasp of the state-of-the-art in automated exam misconduct identification. The encouraging outcomes and research-backed suggestions provide educational institutions with a road map for putting into practice sensible tactics for upholding academic integrity and encouraging an impartial and open assessment environment.

CONCLUSION

This meta-analysis and review provides an in-depth understanding of the most recent developments in automated exam misconduct detection. Positive results and evidence-based suggestions offer schools a roadmap for implementing effective strategies for maintaining academic integrity and creating a fair and transparent evaluation environment.

The assessment demonstrates the remarkable potential of deep learning and machine learning techniques to raise the fairness and consistency of academic evaluations. There is potential for comprehensive and real-time cheating behaviour detection with the development of hybrid systems that integrate computer vision, biometric analysis, and neural networks.

By putting these automated methods into place, educational institutions can ensure that students' academic achievements accurately reflect their knowledge and abilities and significantly improve the reliability of their assessments. Students and the academic community at large stand to gain in the long run from the implementation of these systems, which can support the development of an ethical and equitable culture in education.

For academics, decision-makers, and educational institutions attempting to address the problem of test misconduct, the findings and recommendations presented in this study are a helpful resource. Upholding the integrity of academic assessments and fostering a more transparent and trustworthy educational system depend on the continuous development and application of these cutting-edge technologies.

REFERENCES

[1] F. Hussein, A. Al-Ahmad, S. El-Salhi, E. Alshdaifat, and M. Al-Hami, “Advances in Contextual Action Recognition: Automatic Cheating Detection Using Machine Learning Techniques,” *Data*, vol. 7, no. 9, 2022, doi: 10.3390/data7090122.

[2] R. Saravanan, S. M. S, S. Roopikha, S. Roshini, and S. Rithika, “Automatic Cheating Detection In Exam Hall,” 2023, [Online]. Available: https://doi.org/10.36227/techrxiv.24538150.v1

[3] M. Ramzan, A. Abid, and S. M. Awan, “Automatic Unusual Activities Recognition Using Deep Learning in Academia,” 2022, doi: 10.32604/cmc.2022.017522.

[4] M. Roa’a, I. Aljazaery, A. A.-I. J. of, and undefined 2022, “Automated Cheating Detection based on Video Surveillance in the Examination Classes,” *academia.edu*, Accessed: May 15, 2024. [Online]. Available: https://www.academia.edu/download/88653247/11175.pdf

[5] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, “Preferred reporting items for systematic reviews and meta-analyses: the PRISMA Statement.,” *Open Med.*, vol. 3, no. 3, pp. e123-30, 2009.

[6] M. Ouzzani, H. Hammady, Z. Fedorowicz, and A. Elmagarmid, “Rayyan-a web and mobile app for systematic reviews.,” *Syst. Rev.*, vol. 5, no. 1, p. 210, Dec. 2016, doi: 10.1186/s13643-016-0384-4.

[7] N. R. Haddaway, M. J. Page, C. C. Pritchard, and L. A. McGuinness, “PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis.,” *Campbell Syst. Rev.*, vol. 18, no. 2, p. e1230, Jun. 2022, doi: 10.1002/cl2.1230.

[8] J. A. Oravec, “AI, Biometric Analysis, and Emerging Cheating Detection Systems: The Engineering of Academic Integrity?,” *Educ. Policy Anal. Arch.*, vol. 30, 2022, doi: 10.14507/EPAA.30.5765.

[9] M. Ramzan, A. Abid, M. Bilal, K. M. Aamir, S. A. Memon, and T.-S. Chung, “Effectiveness of Pre-Trained CNN Networks for Detecting Abnormal Activities in Online Exams,” *IEEE Access*, vol. 12, pp. 21503–21519, 2024, doi: 10.1109/ACCESS.2024.3359689.

[10] K. Jalali and F. Noorbehbahani, “An Automatic Method for Cheating Detection in Online Exams by Processing the Student`s Webcam Images Learner assessment View project An Automatic Method for Cheating Detection in Online Exams by Processing the Student`s Webcam Images,” *Researchgate.Net*, no. June, pp. 96170–31805, 2017, [Online]. Available: http://conf.isc.gov.ir/etech2017

[11] G. Emmanuel Bancud, E. Palconit, G. V Emmanuel Bancud, and E. V Palconit, “HUMAN POSE ESTIMATION USING MACHINE LEARNING FOR CHEATING DETECTION,” *researchgate.net*, doi: 10.13140/RG.2.2.12686.28481.

[12] T. Singh, M. Mohadikar, S. Gite, S. Patil, B. Pradhan, and A. Alamri, “Attention Span

Prediction Using Head-Pose Estimation with Deep Neural Networks," *IEEE Access*, vol. 9, pp. 142632–142643, 2021, doi: 10.1109/ACCESS.2021.3120098.

[13] M. Asadullah and S. Nisar, "An automated technique for cheating detection," *2016 6th Int. Conf. Innov. Comput. Technol. INTECH 2016*, pp. 251–255, 2017, doi: 10.1109/INTECH.2016.7845069.

[14] G. Muchangi Kiura, L. Mwenda Muriira, N. Riungu, J. Michael Odhiambo Corresponding Author, and G. Muchangi Kiura ---, "Behavioral Detection and Prevention of Cheating During Online Examination Using Deep Learning Approach," pp. 20–24, 2023, doi: 10.9790/1813-12070105.

[15] T. Liu, "Computers and Education : Artificial Intelligence AI proctoring for offline examinations with 2- Longitudinal-Stream Convolutional Neural Networks," vol. 4, pp. 1–23, 2023.

[16] Z. Li, Z. Zhu, and T. Yang, "A multi-index examination cheating detection method based on neural network," *Proc. - Int. Conf. Tools with Artif. Intell. ICTAI*, vol. 2019-Novem, no. July, pp. 575–581, 2019, doi: 10.1109/ICTAI.2019.00086.

[17] T. M. Radwan, S. Al Abachy, and A. S. Al-Araji, "A One-Decade Survey of Detection Methods of Student Cheating in Exams (Features and Solutions)," *J. Optoelectron. Laser*, vol. 41, no. 4, pp. 355–366, 2022.

[18] G. Moukhliss, R. F. Hilali, and H. Belhadaoui, "Intelligent solution for automatic online exam monitoring," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 5, pp. 5333–5341, 2023, doi: 10.11591/ijece.v13i5.pp5333-5341.

[19] M. D. Genemo, "Suspicious activity recognition for monitoring cheating in exams," *Proc. Indian Natl. Sci. Acad.*, vol. 88, no. 1, pp. 1–10, 2022, doi: 10.1007/s43538-022-00069-2.

[20] D. Muratuly, N. F. Denissova, and I. V Krak, "Information Technology for a Proctor to Detect Violations during the Exam," *Cybern. Syst. Anal.*, vol. 58, no. 6, pp. 983–990, 2022, doi: 10.1007/s10559-023-00533-x.

[21] S. Z. Ong, T. Connie, and M. K. O. Goh, "Cheating Detection for Online Examination Using Clustering Based Approach," *Int. J. Informatics Vis.*, vol. 7, no. 3–2, pp. 2075–2085, 2023, doi: 10.30630/joiv.7.3-2.2327.

[22] F. Mahmood, J. Arshad, M. Ben Othman, M. H.- Sensors, and undefined 2022, "Implementation of an intelligent exam supervision system using deep learning algorithms," *mdpi.com*, Accessed: May 15, 2024. [Online]. Available: https://www.mdpi.com/1424-8220/22/17/6389

[23] T. Radwan, S. Alabachi, and A. Al-Araji, "In-class Exams Auto Proctoring by Using Deep Learning on Students' Behaviors," *Guangdianzi Jiguang/Journal Optoelectron. Laser*, vol. 41, no. June, pp. 969–981, 2022.

[24] I. Kigwana and H. S. Venter, "A digital forensic readiness architecture for online examinations," *South African Comput. J.*, vol. 30, no. 1, pp. 1–39, 2018, doi: 10.18489/sacj.v30i1.466.

[25] V. J. Owan, M V Owan, and J. O. Ogabor, "Sitting arrangement and malpractice behaviours among higher education test-takers: On educational assessment in Nigeria," *J. Appl. Learn. Teach.*, vol. 6, no. 1, pp. 244–258, 2023, doi: 10.37074/jalt.2023.6.1.5.

[26] M. Abdul Elah Abbas Alkhalisy, S. Hameed Abid, M. Abdul Elah Abbas, and S. Hameed, "A Systematic Review of Deep Learning Based Online Exam Proctoring Systems for Abnormal Student Behaviour Detection," *researchgate.net*, 2022, doi: 10.32628/IJSRSET229428.

[27] F. Noorbehbahani, … A. M.-E. and I., and undefined 2022, "A systematic review of

research on cheating in online exams from 2010 to 2021," *Springer*, Accessed: May 15, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s10639-022-10927-7

[28] W. Alsabhan, "Student Cheating Detection in Higher Education by Implementing Machine Learning and LSTM Techniques," *Sensors*, vol. 23, no. 8, 2023, doi: 10.3390/s23084149.

[29] Y. Atoum, L. Chen, A. Liu, … S. H.-I. T. on, and undefined 2017, "Automated online exam proctoring," *ieeexplore.ieee.org*, 2015, doi: 10.1109/TMM.2017.2656064.

[30] N. M. Mahmud, "f F nc ial Cr im e," no. November, 2021.

[31] I. N. A. M. Nordin *et al.*, "Optimization of RF signal detection and alert system for restricted area," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 16, no. 1, pp. 325–332, 2019, doi: 10.11591/ijeecs.v16.i1.pp325-332.

[32] M. I. Ahmad and R. Refik, "'No Chit Chat!' A Warning From a Physical Versus Virtual Robot Invigilator: Which Matters Most?," *Front. Robot. AI*, vol. 9, 2022, doi: 10.3389/frobt.2022.908013.

[33] T. Potluri, S. Venkatramaphanikumar, and K. Venkata Krishna Kishore, "An automated online proctoring system using attentive-net to assess student mischievous behavior," *Multimed. Tools Appl.*, vol. 82, no. 20, pp. 30375–30404, 2023, doi: 10.1007/s11042-023-14604-w.

[34] A. Tweissi, W. A. Etaiwi, and D. A. Eisawi, "The Accuracy of AI-Based Automatic Proctoring in Online Exams," *Electron. J. e-Learning*, vol. 20, no. 4, pp. 419–435, 2022, doi: 10.34190/ejel.20.4.2600.

[35] F. Kamalov, H. Sulieman, D. S. C.-P. one, and undefined 2021, "Machine learning based approach to exam cheating detection," *journals.plos.org*, vol. 16, no. 8 August, Aug. 2021, doi: 10.1371/journal.pone.0254340.

[36] S. Kaddoura, D. Popescu, J. H.-P. C. Science, and undefined 2022, "A systematic review on machine learning models for online learning and examination systems," *peerj.com*, Accessed: May 15, 2024. [Online]. Available: https://peerj.com/articles/cs-986/

[37] N. Gupta and B. Bhushan Agarwal, "Suspicious Activity Classification in Classrooms using Deep Learning," *Eng. Technol. Appl. Sci. Res.*, vol. 13, no. 6, pp. 12226–12230, 2023, doi: 10.48084/etasr.6228.

[38] G. R. Sree, "Suspicious activity detectio n 1 1," vol. 13, no. 06, pp. 95–105, 2023.

[39] T. S. Devi, R. Vinodhini, R. Vishwam, and H. Y. Priya, "Design and Implementation Of Iinvigilation System and Smart," vol. 10, no. 9, pp. 367–373, 2016.

[40] M. J. Hoque, M. R. Ahmed, M. J. Uddin, and M. M. A. Faisal, "Automation of traditional exam invigilation using CCTV and bio-metric," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 6, pp. 392–399, 2020, doi: 10.14569/IJACSA.2020.0110651.

[41] AJSAT, "Time-series profiling for online credit card fraud detection," African Journal of Science, Technology and Innovation, vol. 1, no. 2, pp. 9-15, Dec. 2012.

[42] AJSAT, "Deep learning frameworks for real-time anomaly detection," African Journal of Science, Technology and Innovation, vol. 7, no. S1, pp. 24-28, Nov. 2018.

[43] AJSAT, "CNN and SVM for gesture classification in surveillance," African Journal of Science, Technology and Innovation, vol. 12, no. 1, pp. 11-15, Jun. 2023.

[44] AJSAT, "Hybrid CNN-LSTM models for human activity recognition," African Journal of Science, Technology and Innovation, vol. 12, no. 1, pp. 35-40, Jun. 2023.