International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET229428

A Systematic Review of Deep Learning Based Online Exam Proctoring Systems for Abnormal Student Behaviour Detection

Muhanad Abdul Elah Abbas*[1], Saad Hameed[2]
*[1]Iraqi Commission for Computers and Informatics, Informatics Institute of Postgraduate Studies, Baghdad-Iraq
[2]Al-Mansur University Co, Baghdad, Iraq

Article Info
Volume 9, Issue 4

Page Number : 192-209

Publication Issue :
July-August-2022

Article History
Accepted : 05 July 2022
Published: 22 July 2022

ABSTRACT

In the last years, educational technology has advanced tremendously. Increasing numbers of schools and universities are embracing online learning to serve their students better. As a result of the COVID-19 epidemic, students now have more flexibility in their study schedules and may work at their speed to better themselves. AI-based proctoring solutions have also grabbed the industry by storm. Online proctoring systems (OPS) generally employ online technologies to ensure that the examination is conducted in a secure environment. A survey of current proctoring systems based on artificial intelligence, machine learning, and deep learning is presented in this work. There were 41 publications listed from 2016 to 2022 after a comprehensive search on Web of Science, Scopus, and IEEE archives. We focused on three key study questions: current approaches for AI-based proctoring systems, techniques/algorithms to be employed, datasets used, and cheating detection methods suggested in such systems. Analysis of AI-based proctoring systems demonstrates a lack of training in using technologies, methodologies, and more. To our knowledge, Machine Learning or Deep Learning-based proctoring systems have not been subjected to such a study. From a technology standpoint, our research focuses on detecting cheating in AI-based proctoring systems. New recently launched technologies are included in this review, where these technologies potentially substantially influence online education and the online proctoring system.

Keywords: Deep Learning, Machine Learning, Artificial Intelligence, Online Exams, Online proctoring, Online learning.

I. INTRODUCTION

It is becoming more common to see the impact of Information technology on people's lives as they become more integrated into society. Several crucial situations, including natural disasters, conflict, and pandemics, have demonstrated encouraging outcomes for e-learning [1]. The development of online education has been fast. Students are increasingly turning to online credential programs like Massive Open Online Courses (MOOCs). Universities are also moving to the internet in order to provide their students with more resources. In addition, a growing number of individuals are now publishing their own

courses. As a consequence, students have more opportunities to learn and develop their skills [2]. Several technical breakthroughs allow for the use of sophisticated image processing and machine learning methods for the actual achievement of educational tasks via E-learning [1]. According to a recent study, course evaluation has been a significant focus of online learning research since 2009. Since there is no direct interaction between students and teachers, course evaluation is complicated in online learning [3]. During the epidemic, almost all educational institutions have been obliged to switch to online education [4]. There has been an increase in colleges offering online lessons and exams for all courses. The COVID-19 Pandemic also impacted college admission tests and the employment procedure, which is based on a written test [5]. For college students, the abrupt transition to online education has varying results. Graduate students are not expected to take their studies as seriously as high school students [5]. Machine Learning (ML) principles like feature selection, classification, etc., are used to offer a specific approach/technique for online tests [1]. For online tests, such as MOOCs and those completed during the recruiting process, using an AI-based proctoring system will soon be the standard, and it is a need. In order to earn a high-quality online certificate, one must endure a rigorous assessment procedure. Similar to how tests are proctored in schools and universities, online exams must be overseen. All students need to be monitored by an AI-based system since there are more methods and possibilities for students to cheat when tests are given online [5]. A precise match between instructors and students for physical examinations would not work in this situation [6], [7].

Students' laptops and PCs already have cameras and microphones that these technologies may employ to keep tabs on them and guarantee academic honesty. Many things must be taken into account while building a system. There must be no problems with the AI-based system running on any system, and it must not be an obtrusive system at all [5]. As protection against exam tampering, students would take their tests through a private web browser, and webcam and microphone monitoring would also be used to monitor their behavior. The Artificial Intelligence Based System would monitor all actions and report any efforts at cheating [5].

The system would flag attempts to cheat, and appropriate action is taken. The test might be halted, or a report could be generated for the institution's evaluation. In order to maintain track of the student's actions, a human proctor might benefit from the use of the software. A human proctor would be alerted if a student is suspected, and their questionable behavior would be noted for subsequent examination. One person may concentrate on students who are most likely to cheat by using this method. In addition, it adds a layer of protection to the surveillance system. False positives may be decreased as well as the number of people needed to supervise the test if done in this manner [5].

In online exams, the verification and identification of anomalous conduct by the examinee are critical characteristics. Static and continuous verification are the two methods available. Only once throughout the online test does the examinee undergo static verification. Examinees are authenticated at regular intervals throughout an online test using continuous verification [1]. The university's preferences and the resources of the majority of students influence the choice of such systems. A human proctor method may not function if the students take the tests from a place with a poor internet connection or power outages, as any faults with the student's live video will signal them. Since the test may be administered as long as the computer is operating, a digital secure browser-based solution is preferable. [8],[5], and [9].

Preventing cheating via the identification of aberrant activity is crucial for ensuring the integrity of online assessments. The ideas of examinee verification and anomalous behavior identification are closely

connected. For instance, biometric identifiers often verify and detect anomalous examinee behavior [1]. When unwanted access to various system components is ensured, the security of online examinations is crucial. The studies examine several facets of online test security. Organizations such as the EU have issued recommendations to control the access to and storage such user-generated data. It is a given that data security must be addressed, given the use of biometric authentication for the test in newer systems. Not just during the test but also for the sensitive information that is kept and communicated throughout the examination procedure [10], [11], and [1].The paper has the following objectives: This article examines the many methods, strategies, and algorithms used in Online Proctoring System-based AI and machine learning methodologies. In addition, it discusses the datasets suggested or employed for such a system, as well as the cheating detection algorithms used in every publication. In this almost 41-paper literature study, we have covered every aspect of this topic.

Existing research is mainly concerned with developing and enhancing Online Proctoring systems. There are no comprehensive assessments of the work done on machine learning-based proctoring systems from existing reviews. We have used this chance to determine the research conducted when designing MLPS (Machine Learning-Based Proctoring System). In terms of convenience, online exam cheating is superior to traditional offline exam cheating. For online assessment, detecting and preventing online cheating is vital. As a result, Massive Open Online Courses summative assessment faces one of its most serious challenges yet. Academic dishonesty and cheating are major issues in online education, according to recent research. In order to protect online exams, proctoring methods such as identity verification, keystroke recognition, and video proctoring have been used [12]. Other tactics include controlling the Browser, restricting test duration, randomizing questions and answers, etc. However, it seems that cheating in distance learning is rather prevalent [13]. While dealing with cheating is one of the most pressing issues in online education [3].

The discussion of AI-based proctoring systems will take place in the following section. Online Proctoring Systems are discussed in Section 2. There are research topics and search criteria in Section 3. Section 4 and Section 5 summarize and explain our survey findings, respectively.

II. AN OVERVIEW OF ONLINE PROCTORING

Research on online proctoring in learning is not new. Even prior to the Pandemic, several colleges and organizations used proctoring systems for online classes. Competitive and adaptive examinations, such as the GRE, GMAT, and CAT, are proctored exclusively. Online proctoring employs virtual monitoring techniques (such as tab switching, timestamps, background noise, etc.) to evaluate students taking tests. Exams of this kind are often administered online and in a distant location, allowing students from any area to participate. [14].

For the online proctoring system, the examiner/proctor uses a web camera to record the student taking the test and a secure server to save the video, which the examiner can then see. The examiner or proctor may investigate any questionable action. Pupils cannot open new tabs in their web browsers due to the second feature, Locking. Computer or browser lockdown are other names for this technique [15]. According to [16], the following characteristics of proctoring are listed in Table(I). Three kinds of proctoring systems are recognized by [16]. Fig. 1. depicts the several proctoring system types. The online proctoring method has seen several technical developments. The [16] provides an exhaustive review of proctoring tools. The assessment and investigation of the proctoring system were undertaken. The document provides suggestions for educational

institutions regarding implementing the proctoring system based where some examples of these methods listed here. Where in [17] an intelligent online proctoring system is proposed, the aforementioned proctoring method utilizes audio and visual characteristics. However, there is no assessment of their study in the publication. Using tab locking and question bank randomization [18] developed a method to identify and prevent cheating. [19] creates the online test proctoring system e-Parakh, which is only accessible through mobile devices.[20] focuses on numerous cybersecurity problems in the online proctoring system. In addition to challenge-response and biometrics (such as facial and voice recognition), the study explores blockchain technology and other multi-factor authentication and authorization technologies. When talking about operational controls, it is common to utilize. Lockdown browsers (webcam fraud detection), endpoint security (VPN and virtual machine), screen-sharing and keyboard listening programs, technical controls to counteract spatial (physical) limits, and compliance with the law (GDPR) are some examples of these security methods.[15] Investigates the impact of proctoring on a student's performance.

Table I : Online Proctoring System

No.	Characteristics	Summary	Techniques
1	Authenticity	The verification of the identities of applicants and proctors, who are built into the proctoring software, is included in the authentication process.	Face recognition and two-factor authentication are employed for entity authentication in the proctoring system.
2	Examining tolerance	This restriction on the use of extra resources, such as browser tabs, face recognition during live proctoring, etc., is one that is enforced by the software that is used to proctor examinations.	This is achieved by log monitoring and analysis, Face recognition, Object Detection, and other techniques.
3	Remote authorizing and control	There is an ability to take over a proctoring system (such as starting/stopping an exam for one student remotely) using this feature.	In most cases, this is accomplished by granting administrative privileges and using a multi-tiered security paradigm.
4	Report generation	It involves preparing the student's test report and activity record.	This is often accomplished using tools such as Python and PHP.

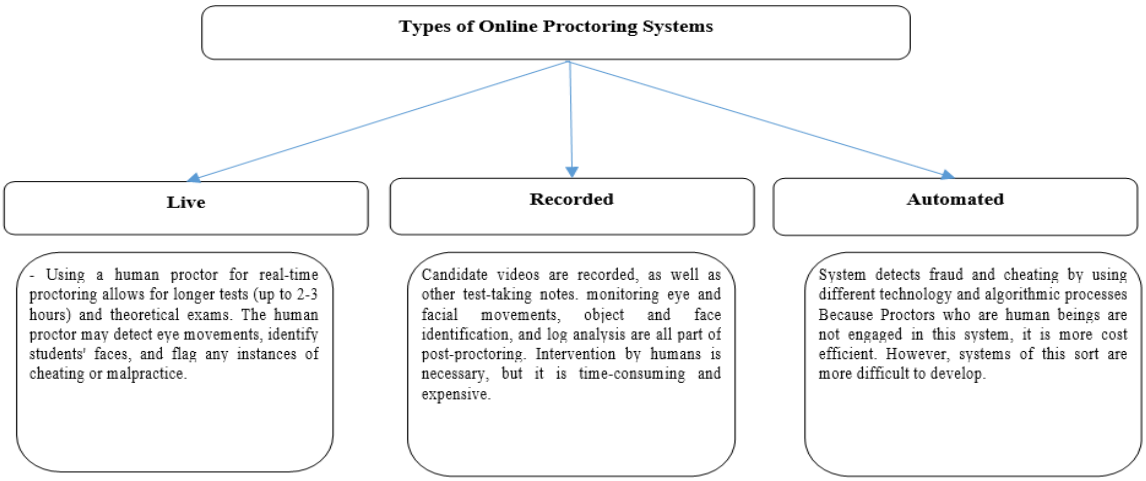

Fig. 1. Online Proctoring Systems: Types and Features

III. RESEARCH QUESTIONS, SEARCH CRITERIA, AND INCLUSION/EXCLUSION CRITERIA

We searched and compiled a selection of the most relevant publications for the literature review in this article. Publications (the majority were Springer, IEEE, Elsevier), Indexed papers (Scopus, Web of Science, including ESCI, SCI, SSCI, and SCIE), and conference numbers were used to identify and choose these works (mainly containing a good number of citations). A total of 137 documents were obtained from the databases, and

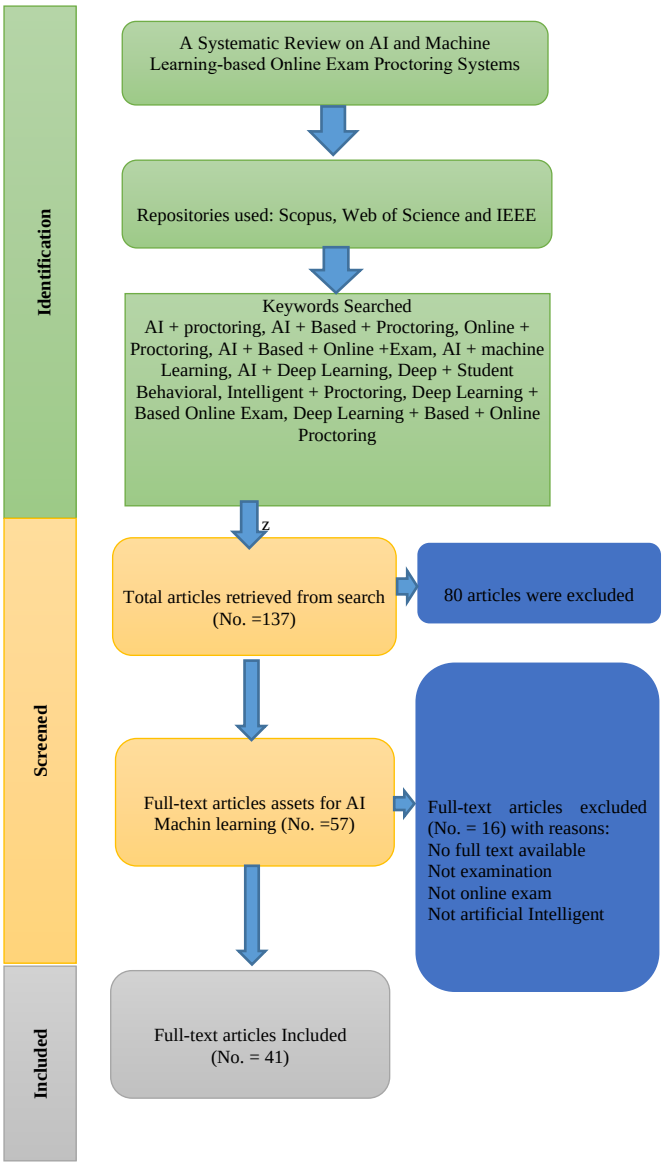

Fig. 2. exhaustive research search process.

80 were omitted since they were irrelevant to our research. In the literature review, the publications based on legal, psychological, and non-AI-based online proctoring systems were eliminated, resulting in 41 publications. These 41 publications are scattered over six years (from 2016 to 2022). This was done to assist us in detecting the newly implemented technologies and improvements in AI-based proctoring systems. Fig. 2. displays our exhaustive research search process.

The articles include issues such as software design, methodologies, techniques, algorithms, datasets presented or used for such a system, and the cheat detection techniques applied in these studies. We are examining prior research on this topic. This paper provides an overview of the current state of AI and machine learning research in online examination proctoring. The following are the research questions:

RQ1: What are the suggested approaches?

RQ2: What datasets are suggested or utilized?

RQ3: How can cheating in online exams be detected?

IV.ARTIFICIAL INTELLIGENCE-BASED PROCTORING

A. What are the suggested approaches (RQ1)?

Webcam, microphone, and other hardware are often used in online proctoring systems. Before the test begins, proctors must confirm that there are no unlawful items in the exam room. It is a requirement that students submit their ID cards as proof of identification [21]. The online proctoring system based on artificial intelligence is shown as follows:

AI-ProctorU, the AI module of the same-named non-AI-based proctoring system, is not very safe and may be tricked. Hence the firm suggests a hybrid approach to ensure high security. This hybrid method combines automatic proctoring with live proctors who are highly trained and can act if they detect cheating [17]. Proctor is an additional well-known online proctoring solution that authenticates students and continuously follows and monitors them using face recognition, behavior

video streaming, audio, and photographic techniques. It also supports many learning management systems (LMS), which allow for limitless picture grabs, screenshots, and video captures when installed on a user's PC.

[20] TeSLA, an EU-funded project, is another example of a proctoring system. TeSLA intends to create strategies for the biometric verification of test-takers. This includes face recognition, voice recognition, keystroke analysis, and fingerprint analysis to confirm that no impersonation is occurring and that the genuine test-taker is providing the answers [11]. Lockdown browsers and self-authentication schemes are used by the PSI Bridge platform, which ensures compliance while protecting student privacy and reducing security concerns. It is a very safe platform that does not need access to the student's computer to check the test's integrity. In a cloud-based Software as a Service, the exam session is recorded and kept on an LMS server (SaaS); in addition, the proctor has access to exam records and infractions that have been highlighted for review. Using a 360-degree monitoring system, ProctorExam enhances spatial controls. Webcam, screen sharing, and a camera on a smartphone are all used to watch the test surroundings. Taker's Facial recognition technology is also included in the system to detect instances of cheating [20].

In addition, online examination services have presented a spectacular multi-factor authentication system that is both secure and user-friendly. Face recognition, OTP verification, and fingerprint authentication are part of the three-part system. For the user to begin using the system, they must first register. User identification consists of a unique ID issued by the institution, an imprint of the right forefinger, and an OTP-verified phone number. A user's credentials are checked before they can log in to a system. There are three modules included in this login module. The user may only take the exam after passing all of these courses. During the inspection, the system does a fingerprint match regularly to check the user's validity; if this fails, the new fingerprint is compared to the database to determine who is aiding and abetting the crime. After that, a report containing information on the malicious users is forwarded to the Controlling Authority [22].

In [17], a webcam-based monitoring system maintains track of the candidate's behaviors, facial movements, and the device's use and audio information. To record voice and video, they have used webcam hardware and active window capture. An intelligent rule-based inference system may use this information to determine whether or not any malpractices have occurred. Face detection and feature extraction from the examinee's face is utilized to estimate the examinee's head posture. Based on yaw angle fluctuations, audio, and active window capture, misbehavior is recognized.

[23] Propose a unique computer vision-based video content analysis system for the automated generation of video summaries of online examinations to aid remote proctors in post-exam evaluations. Using head posture estimates and a semantically relevant two-state hidden Markov model, the approach predicts typical and deviant student behavior patterns. Video summaries are generated from sequences of anomalous activity that have been observed. Another suggested multimedia analytics system [24] does online test proctoring automatically. The system hardware consists of a webcam, a wearable camera, and a microphone to monitor the testing area's visual and aural surroundings. The system consists of six fundamental components that constantly estimate the important behavioral cues: user verification, text detection, voice detection, active window detection, gaze estimation, and phone detection.

A multimodal biometric architecture is proposed by [25] to combat the threat by continuously authenticating users. The proposed multimodal framework combines facial, mouse, and keystroke dynamics biometric technologies. No predetermined

activities are required from the test taker to gather and process any of the three modalities. ExamShield, a new platform for complete test monitoring, includes the architecture we presented as one of its significant features. The significance of time delay and head posture in detecting cheating in a lab-based online assessment session was examined in another research. There is a statistical correlation between the position of a student's head regarding the computer screen and the likelihood of cheating on a test [26].

Using a structural model that combines B/S and C/S, JSP technology, and SSH frames, [27] presents a method for implementing an Intelligent Examination subsystem in an Internet Plus environment. Student examination terminal enables automated capture and keeping of test candidate's facial image for automatic verification of its identity, automatic collecting of examination papers' information, automatic uploading of answers, and automatic feedback on wrong responses. Others suggest obtaining information about the examinee's head position and oral condition through a webcam and identifying examiners' abnormal conduct during online examinations. The system has been tested online, making monitoring the test simple [28]. [29] Implement continuous authentication on an online test system so that exam actions may be observed remotely. The system comprises two modules: the authentication module and the supervision module. Integrating the two modules allows for creating an examination system that can authenticate test participants and monitor exam circumstances. In another research, classification and identification of the impact were suggested using gesture modeling head positions as a gesture during an online test; the study identifies the student disengagement effect. The use of the divide-and-conquer method on object recognition utilizing Haar Cascade feature extraction and HMM classification resulted in an accurate categorization of disengaged behavior during an online evaluation. The experimental findings demonstrate that head-poses may be utilized to identify effects concerning inspection behavior [30].

In [31], describe a method that enables instructors to snap a picture and obtain a visual response after our deep learning program analyzes handwriting patterns, evaluates exam answers, and identifies identities and IDs. Consequently, the system provides instructors with a more efficient computational tool for creating and grading examinations in various forms. An online test management system shown in [32] allows for automated and ongoing monitoring. Face-recognition technology ensures that students are whom they say they are. In order to improve the proposed system's performance, various criteria have been created to identify any fraudulent activity by the applicant.

[32] Suggested a way to improve the resilience of posture and illumination fluctuations by employing m-learning online lecture sessions as training data. E-Parakh is an application that enables both supervised and unsupervised remote monitoring of the examination via a variety of techniques, such as live video and audio streaming of not only the candidate but also the candidate's surrounding environment, liveliness check of the candidate, facial comparison of the candidate's photograph [33].

By capturing the whole video and audio, this program allows the evaluator to cross-check the candidate's activities at any moment throughout the assessment and after the examination. [34] In order to keep tabs on the test taker's actions and halt any unethical activity, a camera-based tracking system is being considered. Haar Cascade Classifier and deep learning will be used to monitor (detect), tag, and identify the student's face. Certain restrictions will be applied to stop these activities (e.g., Multiple face detection). A cheating detection pipeline for online interviews and tests is presented by [35]; for the system to work, all that is needed is a video of the applicant taken during the test. Afterward, a cheating detection pipeline is used to identify another person, electronic device use,

and the absence status of a candidate. Face detection, face recognition, object detection, and face tracking algorithms make up the system's backbone. There will be no need to add additional steps to face recognition training because of the incremental training method [36].

They have tried four different face detectors, including Haar-cascade, LBP, MTCNN, and Yolo-face, as well as a Facenet model for face identification to achieve high accuracy. While a deep learning face detector outperforms the others, incremental training of facet models leads to a reduced dataset size by 1% and quicker training times of 7 percent for the Yolo-face face detector and 64 percent for MTCNN compared to batch training. [37] Detects widespread student wrongdoing using a range of machine learning algorithms, freeing up administrative resources. In order to ensure that the test participants are whom they claim to be, the model validates and authenticates them. Students' honesty is verified by recognizing the video and audio that the model analyzes. The system's constant examination of the inputs ensures academic integrity in eLearning by verifying the candidate's honesty. This includes user identification, audio processing, gaze detection, the number of people detected, and the detection of items and phones. Using a temporal sliding window and integrating continuous estimate components, they generate higher-level features to identify whether the test taker is cheating at any time throughout the exam.

[38] E-cheating intelligence agents have been used to identify online cheating behaviors, which are built of two key modules: an internet protocol (IP) detector and a behavioral detector. The intelligence agent keeps a close eye on the kids and can spot any unethical activity before it occurs. Respondus's OPS is well-suited for use in conjunction with an LMS. Both the Lockdown Browser and the Monitor are included. Allows one browser tab to stay open simultaneously while all other tabs are closed. The Monitor uses a camera to keep tabs on pupils' activities in conjunction with the Browser. Analyzing the camera data allows us to spot patterns that may point to cheating [20]. The paper [40] suggests an innovative technique based on process mining to assess students' computer-based performance. Process mining and similarity analysis are the two critical steps of the proposed method. Students' final grades are determined by an automated process that takes six phases. Additionally, the similarity analysis allows for cheat detection and prevention at the final stage. A real-world implementation of the suggested technique is shown in a course on Enterprise Resource Planning (ERP).

[39] The knowledge base, question encoder, question generating module, and question analysis module are the key conceptual components of the proposed system, which focuses on administering written examinations on online education platforms. An ontology for the format ontology is built on text fragments representing sections of the course. These text fragments are also used in the question generation module to generate fact-based questions and in the question analysis module to create dependency trees for response assessment. In addition, [40] suggests a unique way of creating test papers based on a forecast of exam results. As a result, they use genetic algorithms and dynamic programming to improve the quality of the questions they create continuously. They used Deep Knowledge Tracing for the prediction job. The weight, difficulty, and distribution of test results were considered in the method.

Several artificial intelligence-based tools are available to assist students in transitioning smoothly from online lectures to online exams. For example, Tests software may collect students' behavioral traits during online lectures and then provide them with proctoring services for improved supervision during online exams. [20]. The following Table II provides a breakdown of the various approaches used in the various studies.

Table II: Online Proctoring System

No.	Category	References	Total
1	Artificial Intelligent (Machine &Deep Learning)	[23], [24], [25], [26], [27], [28], [31], [41], [32],[33],[34],[35], [36], [38],[39]	15
2	Artificial Intelligent (No Machine Learning)	[17], [20], [11], [22], [26], [29], [30],[42],[43],[40]	10

Several techniques/algorithms have been presented in the chosen publications to attain a certain target for enhancing online tests. Table 3 provides an overview of the top techniques/algorithms suggested in the chosen studies. Researchers demonstrated CNN-based machine learning and deep learning algorithms for examinee verification. [32], cheating prevention [28], [34], and online examination-based ways to strengthen verification / aberrant behavior features (i.e. [32], [28], [34] and automated assessment [31]).

In the same vein, academics have developed a variety of methods and algorithms for recognizing faces and estimating and detecting head poses, as seen in Table 3's numbers #2 and #3. Furthermore, several NLP-based approaches are suggested in # 4 and 5 of Table 3, respectively. In independent research [26], online test cheating is predicted using a normal logistic regression model with no significant variance. Therefore, such simple approaches are omitted from Table 3. In several of the research, relevant information on the suggested approach or algorithm is lacking. [29] designed a two-component authentication and monitoring method for online examinations. However, the authors did not give meaningful information on the methodologies and algorithms used to create the system. Consequently, such research is excluded from Table III.

Table III: Online Proctoring System

No.	Techniques / Algorithms	References
1	Convolution neural network CNN	[23], [24], [25], [26], [27], [28], [31], [41], [32],[33],[34],[35],[36], [38],[39].
2	Face Recognition, Face Detection	[41], [24], [44], [25], [41], [35],[32],[27], [36],[45],[44].
3	Head Pose Estimation and Detection	[23],[17],[30],[46],[26].
4	Natural Language Processing NLP	[47],[43].
5	Voice Recognition	[24].

B. What datasets are suggested or utilized (RQ2)?

For the accurate validation of a proposed approach, datasets are vital. Authenticating the consequences of a proposal requires hence the use of dependable datasets. As shown in Table 4, we were able to identify 13 datasets that were either utilized or suggested in the AI-based research that were chosen for validation. Only DS #1 was freshly produced in [24], but the other six publicly accessible datasets, which are presented in # 1 to 7 of Table 4, are all considered benchmark datasets. These datasets were used in [38], [48], [28], [40] and [25]. On the other hand, the availability

information for the remaining six datasets (# 8 to #13 of Table 4) was not provided; these datasets are denoted by (NO) in the table. This is because the link to download the dataset was not present.

[33] Developed a dataset for the online test on Verification & Abnormal Behavior. However, the contents of the produced dataset were not well described, and there was no mention of its availability. In the same way, writers [23] However, the availability information was missing from the sample of six videos with 25311 frames. According to another research [35], a dataset had been created, but crucial information such as the total number of records was not provided. According to Table 4, ten datasets were used for the Verification & Abnormal Behavior feature, two datasets were used for the Question Bank Generation & Evaluation feature, one dataset was recommended for the Security feature, and two datasets included audio. Three of these datasets use a textual format. Moreover, as shown in Table IV, six datasets are based on video format. It is essential to note that other chosen research did a variety of experiments, surveys, and test scenarios for the validation of the idea without using a specific dataset. For instance, Rajala [48] confirmed the suggested method with the involvement of 478 students who took the test four times.

Table IV: datasets suggested or utilized

Dataset No.	Type	Count of Documents	Aim	is publicly	Rel. References
DS_1	Audio & Video	(72) (movies and audio)	Abnormality & Verification	YES	[24]
DS_2	pictures	(21997)	Abnormality & Verification	YES	[28]
DS_3	pictures	(6) datasets group	Generating and Evaluating Question Banks	YES	[48]
DS_4	pictures	(16128)	Abnormality & Verification	YES	[25]
DS_5	Text	(7) CSV files	Security	YES	[49]
DS_6	Text	(3) CSV files	Generating and Evaluating Question Banks	YES	[40]
DS_7	Text	(94) CSV file	Abnormality & Verification	YES	[38]
DS_8	Video	(6) movies	Abnormality & Verification	NO	[23]
DS_9	Video	(30) movies	Abnormality & Verification	NO	[17]
DS_10	video	(43) movies	Abnormality & Verification	NO	[35]
DS_11	pictures	(1295) images	Abnormality & Verification	NO	[36]
DS_12	Audio & Video	(2) movies or audio for Group	Abnormality & Verification	NO	[33]
DS_13	Video	(39) movies	Abnormality & Verification	NO	[17]

C. How cheating in online exams be detected (RQ3)?

Detecting cheating during an online test is vital to ensuring academic integrity. Continuous authentication and online proctoring are the two primary methods for detecting cheating. Online proctoring keeps an eye on test-takers to catch any misconduct, while continuous verification mechanisms confirm their identity. Each of these strategies will be discussed in more detail in the following sections.

Impersonation is one of the most common methods of cheating. In order to prevent illegal candidates from taking the test, it is necessary to verify students before they register for the exam. It is also vital to continually confirm the test identity taker's during the exam. Biometric or behavioral metric modalities are the most common in continuous authentication systems, which may be divided into unimodal and multimodal methods. Unimodal authentication is the automated detection and identification of candidates based on a single feature. For example, a person's face, fingerprints, hand geometry, and iris might be static (physiological) or dynamic (behavioral) characteristics, such as their voice and handwriting [50].

As a unimodal authentication method, [51] developed a non-AI facial recognition system that randomly takes pictures of the test taker. By matching the acquired photographs to the image from the exam registration procedure, the face recognition module ensures the test taker's identification at all times. In [29], an Android-based online test application is built that captures images of the examinee at random intervals. A web-based application enables the administrator or supervisor of the examination to check participant photos. In addition, [41] uses the idea of utilizing a camera to collect faces, then using an automated learning algorithm to translate them into digital data, and finally comparing the resulting data to a database was offered. [45] Face recognition algorithms were proposed as a possible anti-ghostwriter solution, or they alter their look to fool the examiner into believing that a ghostwriter is a natural person.

In [52], an eye tracker is used to verify the examinees at all times. So that various screen regions may be examined for the presence or absence of eyeballs, eye tracking data is converted into pixel coordinates. This makes it more difficult for someone to impersonate you by using many biometric or behavioral attributes simultaneously. According to [52], a fingerprint and eye-tracking authentication system was presented. Using the eye tribal tracker, researchers can verify that the people taking the tests are the people they claim to be. For security reasons, a test-taker must be re-authenticated every time he or she is no longer present in front of the screen. Using an artificial facial recognition algorithm, [41] suggested a continuous online authentication system to authenticate the user's identity and identify inappropriate actions continually during the online assessment process.

[25] Proposed a system that continually verifies examinees utilizing three complementing biometric technologies: face, keyboard, and mouse dynamics. In this method, test-takers are verified continually in the background during the exam, and alerts are generated and forwarded to the teacher through the proctoring panel. In [50], classification of various sorts of high-stakes tests, cheating methods, and which forms of cheating are more pertinent for which types of examinations are provided. It also analyzes which risks biometric authentication is most successful against and which dangers it is least effective against.

To maintain academic integrity, online proctoring is crucial. In automated online proctoring, the proctoring technology flags or detects cheating actions automatically. Recent technological advancements have enabled remote proctoring of online examinations. Kryterio, ProctorU, and Real-Time Video Monitoring, for instance, enable users to be supervised via a webcam by a human proctor during examinations [53]. In [54], considerable online proctoring help is given. The data demonstrate a large gap between both the exam scores of those that are not proctored and those that were proctored utilizing the ProctorU tool. Some systems may take random screenshots of applicants' laptops during an examination [55]. Therefore, if an examinee uses a prohibited resource on their computer, it will be shown to the proctor. [56] Implemented webcam-based video proctoring at Miami University. The findings indicate that students are less likely to cheat on online exams when supervised using a camera. Diverse automated proctoring technologies are offered

to monitor students during examinations and identify inappropriate activity. Following is a discussion of numerous automated approaches.

[26] Proposed a semi-automatic method of proctoring that uses two criteria to identify suspicious behavior: the time it takes to answer questions and how different people hold their heads when answering them. To determine whether an individual student has cheated, a human proctor might utilize further evidence. [34] suggested a technique that uses deep learning and the Haar Cascade Classifier to recognize the candidate's face. There will be an immediate termination of the test and communication to the administrator if the examinee's head disappears from view or if more than one person is identified. The suggested method in [28] employs a camera to monitor applicants' head position and mouth condition to identify aberrant behavior. Using the concept of rule-based reasoning, the system may identify suspicious conduct during an online test, such as turning the head or conversing.

[17] built a multimodal online proctoring system. The system records the applicants' voices and videos and their active windows. Variations in yaw angle, the existence of audio, or window changes noticed in any period may be indicative of cheating. As a result, a rule-based inference mechanism analyzes the video, sound, and system use data to look for any indications of improper behavior. Using facial and voice identification, body motion track, and computer activity monitoring, ProctorTrack is a full automation online test proctoring solution that may detect any suspicious conduct throughout the exam. [57]. Using a camera, wear cam, and microphone, [24] has built a system that can identify a broad range of cheating actions during an online test. A wearable camera enables the monitoring of the student's observations. It helps identify any banned phone or text message in the testing room. In addition, the system may identify various types of cheating, such as reading from books, notes, etc., by using the worn cam. In addition, the system can predict the test-head taker's look by merging data from the camera and wear cam. Receiving verbal aid from another player in the same room or remotely through the phone is also considered cheating. The system can use the microphone and voice detection to identify this kind of cheating; the suggested multimedia system is capable of performing automated online test proctoring. [58] developed an automated test activity detection system that uses security cameras to monitor the body movements of students and a deep learning method to classify their activities into six categories. The activity categories include typical behavior, looking back, gazing forward, making motions to other individuals, glancing to the left or right, and other questionable behavior. [59] PageFocus is a JavaScript program that may be placed on the test page and executed in the background. A defocusing event is logged whenever the examinee navigates away from the test page. The script records the occurrence and frequency of defocus and refocus occurrences on the test page. To combat internet protocol (IP) cheating, an intelligent agent with an IP detector and a behavior detector was proposed [38]. The first module might keep track of each student's IP address and send an alarm whenever a device or location changes. The second module monitors the pace at which users respond to questions to look for signs of abnormality. It is also possible to determine whether two participants are at the exact location by comparing their IP addresses [60]. Each work's method of cheating detection is summarized in the table V.

Table V: summarized cheating detection Methods

No.	Research Purpose	Cheating detection	References
1	Examining cheating strategies and developing an e-exam administration platform	yes	[52]
2	Automated video proctoring, which may save human work and increase digital evaluation,	yes	[55]

	is being presented as early findings.		
3	Comparing the results of online proctored tests with those of onsite proctored tests.	yes	[9]
4	Face-recognition technology might be used to authenticate users.	yes	[51]
5	An online test proctoring and automatic cheating detection system was developed.	yes	[17]
6	Exam cheating may now be detected using an image and audio analytics technology.	yes	[24]
7	Several strategies for preventing students from cheating on electronic examinations were discussed.	yes	[61]
8	Created a computerized examination supervisor that can classify how pupils move their bodies throughout the test.	yes	[58]
9	Detection of dishonesty by recording of webcam activity automatically.	yes	[34]
10	Identifying the behaviour of test takers in order to identify cheating, with a particular emphasis on time delay and head posture.	yes	[26]
11	A method of continuous authentication for an online learning application based on Android was created.	yes	[29]
12	It was possible to create a program called "page focus" that can identify whether the exam window is being opened by an unauthorized party.	yes	[59]
13	A cheating detection system based on two modules, the IP detector model and the behavior detector model, was created.	yes	[38]
14	Online test cheating is examined, notably via continuous authentication and online proctoring, in this study.	yes	[62]
15	Suggested a system which uses facial, keyboard, and mouse dynamics to continually verify test takers.	yes	[25]
16	For online assessments, a massive open online proctoring architecture has been proposed that incorporates both automated and collaborative ways to identify cheating.	yes	[2]
17	High-stakes tests, cheating methods, and which sorts of cheating are more important for which assessments were outlined in the presentation.	yes	[50]
18	High-stakes tests, cheating methods, and which sorts of cheating are more important for which assessments were outlined in the presentation.	yes	[28]
19	Developed a three-tiered architecture for spotting test takers who are posing as other people.	yes	[45]
20	For remote proctoring, we're specializing on video summary of anomalous behavior.	yes	[23]

V. CONCLUSION AND DISCUSSIONS

This article includes a systematic literature review to discover and examine 41 research (published between January 2016 and December 2022) on AI-based online tests. This leads to presenting two substantial AI-based methods and five suggested methodologies and algorithms. In addition, 13 datasets and 20 significant cheating detection approaches are given. The COVID-19 Pandemic has increased demand for online testing,

which is the next wave of acceptance following online learning. There are no reliable online proctoring systems, but they are altering the way people think about online testing from home, a concept that was formerly considered absurd.

New forms and technologies of cheating arise in tandem with the advancement of detection and prevention strategies. No system can prevent all forms of cheating in online tests. Hence newer approaches are needed. A system that integrates biometrics with a high degree of accuracies, such as user authentication, surveillance of movement, sound, or keystrokes, should be sought by institutions. Other elements that should be included are the ability to shut down the system or Browser, cloud-based technology that eliminates the need for local upgrades, and an easy user interface. Another point of view on a universal AI-based system is the extent to which it is ubiquitous and how much people trust it. The most pressing issue is how to create AI-based proctoring systems that can be trusted. No articles that compared the trustworthiness of proctoring systems based on human or artificial intelligence to those based on existing classroom-based systems [63]. In conclusion, it is challenging to determine if the advantages of these Online Proctoring systems exceed their hazards. The most plausible conclusion we can draw at this time is that the ethical justification of these technologies and their different capacities needs us to carefully ensure, to the best of our ability, that a balance is achieved between concerns and potential advantages. This research may be expanded in numerous ways in the future. For instance, one strategy is to do a comprehensive examination of online test cheating prevention tactics, strategies, and algorithms.

VI. REFERENCES

[1]. A. W. Muzaffar, M. Tahir, M. W. Anwar, Q. Chaudry, S. R. Mir, and Y. Rasheed, "A systematic review of online exams solutions in e-learning: Techniques, tools, and global adoption," IEEE Access, vol. 9, pp. 32689–32712, 2021, doi: 10.1109/ACCESS.2021.3060192.

[2]. X. Li, K. M. Chang, Y. Yuan, and A. Hauptmann, "Massive open online proctor: Protecting the credibility of MOOCs Certificates," CSCW 2015 - Proc. 2015 ACM Int. Conf. Comput. Coop. Work Soc. Comput., pp. 1129–1137, 2015, doi: 10.1145/2675133.2675245.

[3]. F. Noorbehbahani, A. Mohammadi, and M. Aminazadeh, A systematic review of research on cheating in online exams from 2010 to 2021, no. 0123456789. Springer US, 2022. doi: 10.1007/s10639-022-10927-7.

[4]. A. J. Moreno-Guerrero, C. Rodríguez-Jiménez, G. Gómez-García, and M. R. Navas-Parejo, "Educational innovation in higher education: Use of role playing and educational video in future teachers' training," Sustain., vol. 12, no. 6, 2020, doi: 10.3390/su12062558.

[5]. A. Nigam, R. Pasricha, T. Singh, and P. Churi, "A Systematic Review on AI-based Proctoring Systems: Past, Present and Future," Educ. Inf. Technol., vol. 26, no. 5, pp. 6421–6445, 2021, doi: 10.1007/s10639-021-10597-x.

[6]. E. Bilen and A. Matros, "Online cheating amid COVID-19," J. Econ. Behav. Organ., vol. 182, pp. 196–211, 2021, doi: 10.1016/j.jebo.2020.12.004.

[7]. J. Peterson, "An analysis of academic dishonesty in online classes," Mid-Western Educ. Res., vol. 31, no. 1, pp. 24–36, 2019.

[8]. K. Butler-Henderson and J. Crawford, "A systematic review of online examinations: A pedagogical innovation for scalable authentication and integrity," Comput. Educ., vol. 159, no. September, p. 104024, 2020, doi: 10.1016/j.compedu.2020.104024.

[9]. J. A. Weiner and G. M. Hurtz, "A comparative Study of Online Remote Proctored Vs Onsite Proctored," J. Appl. Test. Technol., vol. 18, no. 1, pp. 13–20, 2017.

[10].S. Coghlan, T. Miller, and J. Paterson, "Good Proctor or 'Big Brother'? Ethics of Online Exam Supervision Technologies," Philos. Technol., vol. 34, no. 4, pp. 1581–1606, 2021, doi: 10.1007/s13347-021-00476-1.

[11].S. Draaijer, A. Jefferies, and G. Somers, Online proctoring for remote examination: A state of play in higher education in the EU, vol. 829. Springer International Publishing, 2018. doi: 10.1007/978-3-319-97807-9_8.

[12].Y. Xiong and H. K. Suen, "Assessment approaches in massive open online courses: Possibilities, challenges and future directions," Int. Rev. Educ., vol. 64, no. 2, pp. 241–263, 2018, doi: 10.1007/s11159-018-9710-5.

[13].S. Dendir and R. S. Maxwell, "Cheating in online courses: Evidence from online proctoring," Comput. Hum. Behav. Reports, vol. 2, no. October, p. 100033, 2020, doi: 10.1016/j.chbr.2020.100033.

[14]."Online & Proctoring & Systems & Compared &," 2013.

[15].H. M. Alessio, N. Malay, K. Maurer, A. J. Bailer, and B. Rubin, "Examining the effect of proctoring on online test scores," Online Learn. J., vol. 21, no. 1, 2017, doi: 10.24059/olj.v21i1.885.

[16].M. J. Hussein, J. Yusuf, A. S. Deb, L. Fong, and S. Naidu, "An Evaluation of Online Proctoring Tools," Open Prax., vol. 12, no. 4, p. 509, 2020, doi: 10.5944/openpraxis.12.4.1113.

[17].S. Prathish, A. N. S, and K. Bijlani, "An intelligent system for online exam monitoring," 2016 Int. Conf. Inf. Sci., pp. 138–143, 2016, doi: 10.1109/INFOSCI.2016.7845315.

[18].S. S. Chua, J. B. Bondad, Z. R. Lumapas, and J. D. Garcia, "Online Examination System with Cheating Prevention Using Question Bank Randomization and Tab Locking," Proc. 2019 4th Int. Conf. Inf. Technol. Encompassing Intell. Technol. Innov. Towar. New Era Hum. Life, InCIT 2019, pp. 126–131, 2019, doi: 10.1109/INCIT.2019.8912065.

[19].A. K. Pandey, S. Kumar, B. Rajendran, and B. B S, "E-parakh: Unsupervised online examination system," IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON, vol. 2020-Novem, pp. 667–671, 2020, doi: 10.1109/TENCON50793.2020.9293792.

[20].L. Slusky, "Cybersecurity of online proctoring systems," J. Int. Technol. Inf. Manag., vol. 29, no. 1, pp. 56–83, 2020.

[21].A. S. Milone, A. M. Cortese, R. L. Balestrieri, and A. L. Pittenger, "The impact of proctored online exams on the educational experience," Curr. Pharm. Teach. Learn., vol. 9, no. 1, pp. 108–114, 2017, doi: 10.1016/j.cptl.2016.08.037.

[22].N. Joshy, M. Ganesh Kumar, P. Mukhilan, V. Manoj Prasad, and T. Ramasamy, "Multi-Factor Authentication Scheme For Online Examination," Int. J. Pure Appl. Math., vol. 119, no. 15, pp. 1705–1712, 2018, [Online]. Available: http://www.acadpubl.eu/hub/

[23].M. Cote, F. Jean, A. B. Albu, and D. Capson, "Video summarization for remote invigilation of online exams," 2016 IEEE Winter Conf. Appl. Comput. Vision, WACV 2016, May 2016, doi: 10.1109/WACV.2016.7477704.

[24].Y. Atoum, L. Chen, A. X. Liu, S. Hsu, and X. Liu, "Automated Online Exam Proctoring," IEEE Trans. Multimed., vol. 19, pp. 1609–1624, 2017, doi: 10.1109/TMM.2017.2656064.

[25].I. Traoré, A. Awad, and I. Woungang, "Information security practices: Emerging threats and perspectives," Inf. Secur. Pract. Emerg. Threat. Perspect., pp. 1–104, 2017, doi: 10.1007/978-3-319-48947-6.

[26].C. Y. Chuang, S. D. Craig, and J. Femiani, "Detecting probable cheating during online assessments based on time delay and head pose," High. Educ. Res. Dev., vol. 36, no. 6, pp. 1123–1137, 2017, doi: 10.1080/07294360.2017.1303456.

[27].L. D. Zhou, H. Li, H. Gu, and J. Shi, "Research and development of intelligent online examination monitoring system," ICCSE 2017 - 12th Int. Conf. Comput. Sci. Educ., no. Iccse, pp. 57–62, 2017, doi: 10.1109/ICCSE.2017.8085463.

[28].S. Hu, X. Jia, and Y. Fu, "Research on Abnormal Behavior Detection of Online Examination Based on Image Information," 2018 10th Int. Conf. Intell. Human-Machine Syst. Cybern., vol. 02, pp. 88–91, 2018, doi: 10.1109/IHMSC.2018.10127.

[29].S. Aisyah, Y. Bandung, and L. B. Subekti, "Development of Continuous Authentication System on Android-Based Online Exam Application," 2018 Int. Conf. Inf. Technol. Syst. Innov. ICITSI 2018 - Proc., pp. 171–176, Jul. 2018, doi: 10.1109/ICITSI.2018.8695954.

[30].M. B. Abisado, B. D. Gerardo, L. A. Vea, and R. P. Medina, "Towards academic affect modeling through experimental hybrid gesture recognition algorithm," ACM Int. Conf. Proceeding Ser., pp. 48–52, 2018, doi: 10.1145/3239283.3239305.

[31].B. Wagstaff, C. Lu, and X. A. Chen, "Automatic exam grading by a mobile camera: Snap a picture to grade your tests," Int. Conf. Intell. User Interfaces, Proc. IUI, pp. 3–4, 2019, doi: 10.1145/3308557.3308661.

[32].H. S. G. Asep and Y. Bandung, "A Design of Continuous User Verification for Online Exam Proctoring on M-Learning," 2019 Int. Conf. Electr. Eng. Informatics, pp. 284–289, 2019, doi: 10.1109/ICEEI47359.2019.8988786.

[33].S. P. Saurav, P. Pandey, S. K. Sharma, B. Pandey, and R. Kumar, "AI Based Proctoring," Proc. - 2021 3rd Int. Conf. Adv. Comput. Commun. Control Networking, ICAC3N 2021, pp. 610–613, 2021, doi: 10.1109/ICAC3N53548.2021.9725547.

[34].K. Garg, K. Verma, K. Patidar, and N. Tejra, "Convolutional Neural Network based Virtual Exam Controller," 2020 4th Int. Conf. Intell. Comput. Control Syst., pp. 895–899, 2020, doi: 10.1109/ICICCS48265.2020.9120966.

[35].A. C. Ozgen, M. U. Öztürk, O. Torun, J. Yang, and M. Z. Alparslan, "Cheating Detection Pipeline for Online Interviews," 2021 29th Signal Process. Commun. Appl. Conf., pp. 1–4, 2021, doi: 10.1109/SIU53274.2021.9477950.

[36].A. H. S. Ganidisastra and Y. Bandung, "An Incremental Training on Deep Learning Face Recognition for M-Learning Online Exam Proctoring," Proc. - 2021 IEEE Asia Pacific Conf. Wirel. Mobile, APWiMob 2021, pp. 213–219, 2021, doi: 10.1109/APWiMob51111.2021.9435232.

[37].F. Detection, O. Detection, and A. Conversion, "Remote online proctoring system 1," vol. 9, no. 5, pp. 559–565, 2021.

[38].L. C. O. Tiong and H. J. Lee, "E-cheating Prevention Measures: Detection of Cheating at Online Examinations Using Deep Learning Approach -- A Case Study," vol. XX, no. Xx, pp. 1–9, 2021, [Online]. Available: http://arxiv.org/abs/2101.09841

[39].A. Matveev et al., "A Virtual Dialogue Assistant for Conducting Remote Exams," Conf. Open Innov. Assoc. Fruct, vol. 2020-April, no. July, pp. 284–290, 2020, doi: 10.23919/FRUCT48808.2020.9087557.

[40].Z. Wu, T. He, C. Mao, and C. Huang, "Exam paper generation based on performance prediction of student group," Inf. Sci. (Ny)., vol. 532, pp. 72–90, 2020, doi: 10.1016/j.ins.2020.04.043.

[41].M. Ghizlane, B. Hicham, and F. H. Reda, "A New Model of Automatic and Continuous Online Exam Monitoring," 2019 Int. Conf. Syst. Collab. Big Data, Internet Things Secur., pp. 1–5, 2019, doi: 10.1109/SysCoBIoTS48768.2019.9028027.

[42].A. Baykasoğlu, B. K. Özbel, N. Dudaklı, K. Subulan, and M. E. Şenol, "Process mining based approach to performance evaluation in computer-aided examinations," Comput. Appl. Eng. Educ., vol. 26, no. 5, pp. 1841–1861, 2018, doi: 10.1002/cae.21971.

[43].I. Das, B. Sharma, S. S. Rautaray, and M. Pandey, "An Examination System Automation Using Natural Language Processing," Proc. 4th Int. Conf. Commun. Electron. Syst. ICCES 2019, no. August 2020, pp. 1064–1069, 2019, doi: 10.1109/ICCES45898.2019.9002048.

[44].A. A. Sukmandhani and I. Sutedja, "Face Recognition Method for Online Exams," Proc. 2019 Int. Conf. Inf. Manag. Technol. ICIMTech 2019, vol. 1, no. August, pp. 175–179, 2019, doi: 10.1109/ICIMTech.2019.8843831.

[45].H. He, Q. Zheng, R. Li, and B. Dong, "Using Face Recognition to Detect 'Ghost Writer' Cheating in Examination," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 11462 LNCS, pp. 389–397, 2019, doi: 10.1007/978-3-030-23712-7_54.

[46].L. Fanani, A. H. Brata, and D. P. Riski Puspa Dewi, "An interactive mobile technology to improve the usability of exam application for disabled student," ACM Int. Conf. Proceeding Ser., pp. 302–306, 2019, doi: 10.1145/3345120.3345149.

[47].A. Matveev et al., "Virtual dialogue assistant for remote exams," Mathematics, vol. 9, no. 18, 2021, doi: 10.3390/math9182229.

[48].T. Rajala et al., "Automatically assessed electronic exams in programming courses," ACM Int. Conf. Proceeding Ser., vol. 01-05-Febr, 2016, doi: 10.1145/2843043.2843062.

[49].S. Kausar, X. Huahu, A. Ullah, Z. Wenhao, and M. Y. Shabir, "Fog-Assisted Secure Data Exchange for Examination and Testing in E-learning System," Mob. Networks Appl., 2020, doi: 10.1007/s11036-019-01429-x.

[50].A. Vegendla and G. Sindre, "Mitigation of Cheating in Online Exams," pp. 47–68, 2019, doi: 10.4018/978-1-5225-7724-9.ch003.

[51].J. Achkoski, "Proceedings FINAL VERSION F2," 2019, [Online]. Available: https://www.researchgate.net/publication/337338310

[52].H. R. Bawarith, "Student Cheating Detection System in E-exams." 2017.

[53].K. Hylton, Y. Levy, and L. P. Dringus, "Utilizing webcam-based proctoring to deter misconduct in online exams," Comput. Educ., vol. 92–93, pp. 53–63, 2016, doi: 10.1016/j.compedu.2015.10.002.

[54].T. H. Reisenwitz, "Examining the necessity of proctoring online exams," J. High. Educ. Theory Pract., vol. 20, no. 1, pp. 118–124, 2020, doi: 10.33423/jhetp.v20i1.2782.

[55].G. Migut, D. Koelma, C. G. M. Snoek, and N. Brouwer, "Cheat me not: Automated proctoring of digital exams on bring-your-own-device," Annu. Conf. Innov. Technol. Comput. Sci. Educ. ITiCSE, p. 388, 2018, doi: 10.1145/3197091.3205813.

[56].H. Alessio and K. Maurer, "The Impact of Video Proctoring in Online Courses.," J. Excell. Coll. Teach., vol. 29, pp. 183–192, 2018.

[57].M. Norris, "University online cheating - how to mitigate the damage," vol. 37, pp. 1–20.

[58].T. Saba, A. Rehman, N. S. M. Jamail, S. L. Marie-Sainte, M. Raza, and M. Sharif, "Categorizing the Students' Activities for Automated Exam Proctoring Using Proposed Deep L2-GraftNet CNN Network and ASO Based Feature Selection Approach," IEEE Access, vol. 9, pp. 47639–47656, 2021, doi: 10.1109/ACCESS.2021.3068223.

[59].B. Diedenhofen and J. Musch, "PageFocus: Using paradata to detect and prevent cheating on online achievement tests," Behav. Res. Methods, vol. 49, no. 4, pp. 1444–1459, 2017, doi: 10.3758/s13428-016-0800-7.

[60].J. Backman, "Students ' Experiences of Cheating in the Online Exam Environment," 2019.

[61].D. Von Grünigen, B. Pradarelli, and M. Cieliebak, "with a Special Focus on Cheating Prevention," 2018 IEEE Glob. Eng. Educ. Conf., pp. 899–905, 2018.

[62].R. Bawarith, D. Abdullah, D. Anas, and P. Dr., "E-exam Cheating Detection System," Int. J. Adv.

Comput. Sci. Appl., vol. 8, no. 4, pp. 176–181, 2017, doi: 10.14569/ijacsa.2017.080425.

[63].S. Vincent-Lancrin and R. van der Vlies, “Trustworthy artificial intelligence (AI) in education : Promises and challenges,” OECD Educ. Work. Pap. No. 218, no. 218, p. 17, 2020, [Online]. Available: https://www.oecd-ilibrary.org/education/trustworthy-artificial-intelligence-ai-in-education_a6c90fa9-en

Cite this article as :

Muhanad Abdul Elah Abbas, Saad Hameed, " A Systematic Review of Deep Learning Based Online Exam Proctoring Systems for Abnormal Student Behaviour Detection", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 4, pp. 192-209, July-August 2022. Available at doi : https://doi.org/10.32628/IJSRSET229428
Journal URL : https://ijsrset.com/IJSRSET229428