1-1-2023

Computational Intelligence and Soft Computing Paradigm for Cheating Detection in Online Examinations

Sanaa Kaddoura
Zayed University, sanaa.kaddoura@zu.ac.ae

Shweta Vincent
Manipal Institute of Technology

D. Jude Hemanth
Karunya Institute of Technology and Sciences

Hindawi
Applied Computational Intelligence and Soft Computing
Volume 2023, Article ID 3739975, 23 pages
https://doi.org/10.1155/2023/3739975

Review Article

Computational Intelligence and Soft Computing Paradigm for Cheating Detection in Online Examinations

Sanaa Kaddoura,[1] **Shweta Vincent**,[2] **and D. Jude Hemanth**[3]

[1]*College of Technological Innovation, Zayed University, Abu Dhabi, UAE*
[2]*Department of Mechatronics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal 576104, Karnataka, India*
[3]*Department of ECE, Karunya Institute of Technology and Sciences, Coimbatore, India*

Correspondence should be addressed to Sanaa Kaddoura; sanaa.kaddoura@zu.ac.ae

Received 31 May 2022; Revised 30 October 2022; Accepted 8 April 2023; Published 4 May 2023

Academic Editor: Imran Ashraf

Covid-19 has been a life-changer in the sphere of online education. With complete lockdown in various countries, there has been a tumultuous increase in the need for providing online education, and hence, it has become mandatory for examiners to ensure that a fair methodology is followed for evaluation, and academic integrity is met. A plethora of literature is available related to methods to mitigate cheating during online examinations. A systematic literature review (SLR) has been followed in our article which aims at introducing the research gap in terms of the usage of soft computing techniques to combat cheating during online examinations. We have also presented state-of-the-art methods followed, which are capable of mitigating online cheating, namely, face recognition, face expression recognition, head posture analysis, eye gaze tracking, network data traffic analysis, and detection of IP spoofing. A discussion on improvement of existing online cheating detection systems has also been presented.

1. Introduction

Online learning has been in demand for the past couple of years. However, the COVID-19 pandemic, since late 2019 to early 2020, has thrusted the need for online learning in a very significant manner. With schools and higher education institutions which closed down around the world, there was a dire need for classroom-like engagement of around 1 billion students, to provide continuous learning. Engaging online classes without much practical exposure for students was a huge challenge. However, a bigger challenge has been to evaluate the performance of such students through online examinations. Fakhroddin et al. [1] have performed a systematic review on the various behaviours of cheating during online examinations. They provide a comprehensive view on methods of cheating detection, prevention, and mitigation. Kaddoura et al. [2] have presented a study on the steep rise of online learning portals which indirectly poses the challenge of fair conduction of online examination. In comparison to an offline examination, it is easier to cheat during an online examination.

Monitoring of online examinations through human proctors is a common methodology to prevent cheating. However, the con of this methodology is the cost borne to employ individuals to monitor the examinations taken. There is a requirement of high bandwidth for communication in such cases and there further exists no metric to evaluate the efficiency of the proctor in cheating detection. Semiautomated proctoring has also been proposed in several research studies such as the ones presented by presented by Rosen and Carr [3] and Li et al. [4], where a desktop robot transmits videos to a proctor for monitoring any suspicious motion in the video. Proctoring through authentication, keystroke recognition, and through webcams offer a level of security in online exams (Xiong and Suen) [5]. Various researchers have performed online proctoring using webcams for face recognition and text detection [6, 7]. Many research studies have also been conducted to monitor the

variation of head posture of students to detect possible cheating [8, 9]. Time-to-time authentication and eye tracking have been adopted in [10, 11] to ensure detection of online cheating. The advances in computer networking have also been leveraged to detect cheating through tracing malicious data packets or data sent to blacklisted URLs [12, 13].

However, these exists a lot of other literature to improve techniques for the detection of cheating in online examination. The motivation behind writing this research article is to analyse what are the categories of methods used for the detection of online cheating using soft computing. Furthermore, we explore the potential techniques that could be employed for online cheating detection which have not been used yet for the same. The main contribution of our article is towards presenting a comprehensive literature review of state-of-the-art soft computing techniques available for the detection of cheating during online examinations. We also present possible solutions using varied methods to mitigate cheating during online examinations. The scope of the article is to present the various methods available for the detection of cheating in online examinations. The next section presents the research gap and methodology followed to address the research gap.

2. Systematic Literature Review for Identifying the Research Gap and Methodology

2.1. Process of Systematic Literature Review. SLR is a method that makes it possible to gather pertinent data about a specific subject that meets the preestablished eligibility requirements and provides a solution to the research questions that had been posed [14]. Our review article presents the existing techniques available for the detection of cheating in online examinations and further proposes the usage of improved techniques with better efficiency for the same task. Figure 1 presents the SLR and meta-analysis diagram which has been followed in our literature review for the process of screening and evaluation. Table 1 further elaborates on the steps followed, outcomes, and methods adopted at every level of the SLR process.

2.2. Research Gap. With the advent of online learning during Covid-19, a need has arisen to monitor cheating behaviour during online examination. In spite of considerable research related to the modes of online learning, there is no comprehensive review of the techniques available or which could be adopted to mitigate cheating during online exams.

Our research article answers the following research questions:

(i) What are the categories of methods used for detection of online cheating using soft computing?

(ii) What are the potential techniques that could be employed for online cheating detection which have not been used yet for the same?

Therefore, our research article addresses this research gap and satisfies the following objectives pertaining to detection of cheating during online examinations:

(i) To present a comprehensive literature review of state-of-the-art soft computing techniques available for the detection of cheating during online examinations

(ii) To present possible solutions using varied methods to mitigate cheating during online examinations.

2.3. Methodology. Table 1 presents the overall methodology of selection and categorization of the articles for our review. Figure 2 showcases the broad categorization of methods followed for the detection of online cheating. They are broadly classified under the categories of the following subsections:

2.3.1. Face Tracking. This technique usually employs a camera to detect the face of the subject taking the online examination. By monitoring his gestures, researchers can develop systems to alert proctors during online cheating.

2.3.2. Face Expression Detection. On the same lines of face tracking, the face expression detection technique is used to monitor stressful or sly expressions on the face of the student while taking an online exam and this can be used to alert the proctor.

2.3.3. Head Posture Analysis. Head posture analysis detects if the subject taking the exam bends his head in a certain direction beyond a threshold value which could suggest that he is involving in cheating.

2.3.4. Eye Gaze Tracking. Eye gaze tracking systems are used to monitor the alertness of drivers and pilots while driving and flying aircrafts, respectively. The same mechanism is employed to detect if a person is fixing his gaze in a particular direction for an unusually long time. It can also detect the chances of a person passing sly glances to his neighbour or surrounding persons during an online exam.

2.3.5. Network Data Analysis and Traffic Classification. While taking an online exam, the student is free to access any resource over the internet. In spite of blocking of essential websites which may lead to copying, there is still a possibility of the student accessing the internet in search for answers.

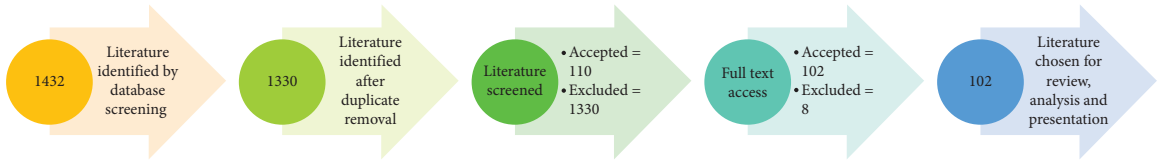

Figure 1: SLR and meta-analysis diagram.

The technique of network data traffic analysis and classification can be used to detect the type and content of traffic emanating from a student's system while taking the examination online.

2.3.6. IP Spoofing Detection. IP spoofing is the mechanism of one computer system masquerading as another. There could be cases where the genuine student registered to take the online exam would allow a proxy user to take the exam in his place. This can be detected via advanced online IP spoofing detection mechanisms.

This article has been divided into the following sections: Section 3 deals with face detection and facial expression detection systems. Section 4 highlights the techniques used for the detection of change in head posture. Section 5 of this article lays emphasis on the literature available for eye gaze tracking. Section 6 of the article presents the state-of-the-art techniques for network data traffic analysis and classification. Section 7 presents the mechanisms used for the detection of IP spoofing. Section 8 presents a brief discussion of the usage of an ensemble of all the techniques to model a robust online cheating detection mechanism to aid authentic online learning.

3. Face Tracking and Facial Expression Detection Systems

3.1. Existing Techniques for Detection of Cheating Using Face Tracking and Facial Expression Detection. Image processing techniques have been used for tracking faces and facial expressions to classify and predict behaviours in people. This section of the article describes some of the literature that uses face tracking and facial expression detection algorithms to detect cheating during online examinations.

Figure 3 adapted from Kaddoura and Gumaei [6] showcases the usage of a webcam and backcam to detect malicious activity by the student. The webcam provides a front view of the face of the student, and the data retrieved from this can be used to monitor his expressions, whereas the backcam gives view of the material he is accessing (second column of images), which in this case is a text book and a cheat sheet.

Fan et al. [7] presented the usage of Microsoft Kinect, a webcam device for gesture detection, by measuring head roll and yaw angles. Under the table, hand movement can also be detected using this device. The classification of images is performed by thresholding. Any roll or yaw movement beyond a certain threshold is treated as malicious activity and referred to as cheating. Unfortunately, this methodology may prove to be less effective when considering a large population of students, each of whom would have different postures of seating. Many students may have the tendency to lean forward or sideways while writing, and this could get misclassified as cheating. The benefits of high accuracy have been leveraged in [15] where a CNN coupled with a Haar Cascade classifier and Viola–Jones feature extractor has been used for the detection of cheating in students.

He et al. [16] have presented a face tracking system with a database of faces of all students writing the exam. They claim to detect "ghost writers," i.e., students/individuals whose faces are not registered in the system. This system typically prevents a proxy writer from taking an online exam on behalf of another student. Though the system may prove to be efficient for small numbers, as the number of students get scaled up, the system may fail to perform. Furthermore, a large dataset of all faces of individuals taking the exam would be required which leads to a huge storage capacity requirement.

Most techniques discussed in Section 3.1 are rudimentary and pose a scope of improvement. Section 3.2 outlines novel techniques used for face tracking and the detection of facial expressions which could be potentially adapted to design systems for the detection of online cheating.

3.2. Potential Techniques for Face Tracking and Expression Detection for Online Examinations. Articles from the literature by Ren et al. [17], Liu et al. [18], and Yuankai et al. [19] have explored the usage of deep neural networks for the extraction of facial features for image recognition (Table 2). For instance, Ren et al. [17] have used the Chinese whisper algorithm for extraction of facial features and double triplet NN for classification of the images. Gan and C. P. [18] have been able to overcome the problem of a person writing an exam in various poses by developing a pose invariant face recognition (PIFR) algorithm. This would be of great help for students who have diverse postures while writing the exam as various profiles of their faces would be registered and facial feature matching would be done. In Jianwen et al.' study [20], a globally optimized modular boosted ferns (GoMBF)-cascade regression model has been constructed to prove its superiority in feature detection when compared to the classical explicit shape regression (ESR) algorithm (Figure 4).

Apart from general face detection, soft computing algorithms have also been used for the detection of various facial expressions. There are various biomarkers/biological indicators of stress, panic, grief, joy, and others that are displayed by a human body. When these markers are detected, tagged, and classified appropriately, they could prove

Table 1: Steps, outcomes, and methods of the SLR process.

S. no	Step	Outcome	Methods
1	Protocol search	Definition of scope of review and search strategy	(i) The scope of the review is fixed to soft computing techniques (automated) used for cheating detection during online examinations (ii) Literature studies on physical modes of detection of cheating and behavioural analysis of students while cheating are excluded (iii) Keywords used for the search strategy are "machine learning for online cheating detection" and "AI for online cheating detection" (iv) Sources of articles are IEEE, Springer, Elsevier, Taylor and Francis, and other top quartile journals
2	Appraisal	Qualitative selection of articles for review	(i) Articles are selected based on novelty of the technique used for online cheating detection (ii) Abstracts of the articles are read, and only the novel ones are selected under each methodology of online cheating detection (Figure 2)
3	Synthesis	Extraction and categorization of articles for review	(i) Full texts are downloaded under each category of online cheating detection (ii) Categorization is performed on the basis of various soft computing techniques available for the task (Figure 2)
4	Analysis	Conduction of article analysis and formulation of discussion	(i) An in-depth study of performance metrics of the soft computing techniques used in each category for online cheating detection is performed
5	Report	Presentation of discussion and final review article	(i) Further studies on potential techniques which could be used for cheating detection under each category are performed and presented in the discussion (ii) The performance metrics of these techniques have also been presented in the discussion

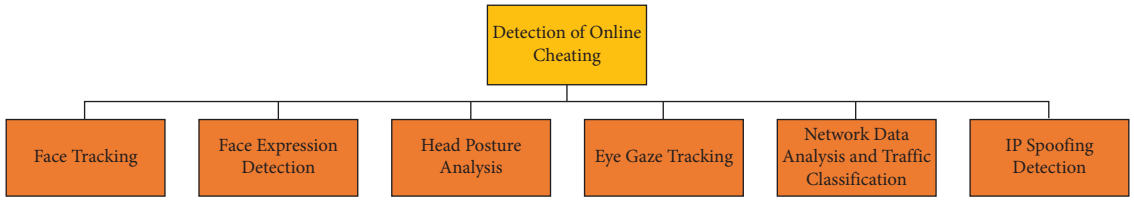

Figure 2: Broad categorization of methods of detection of online cheating.

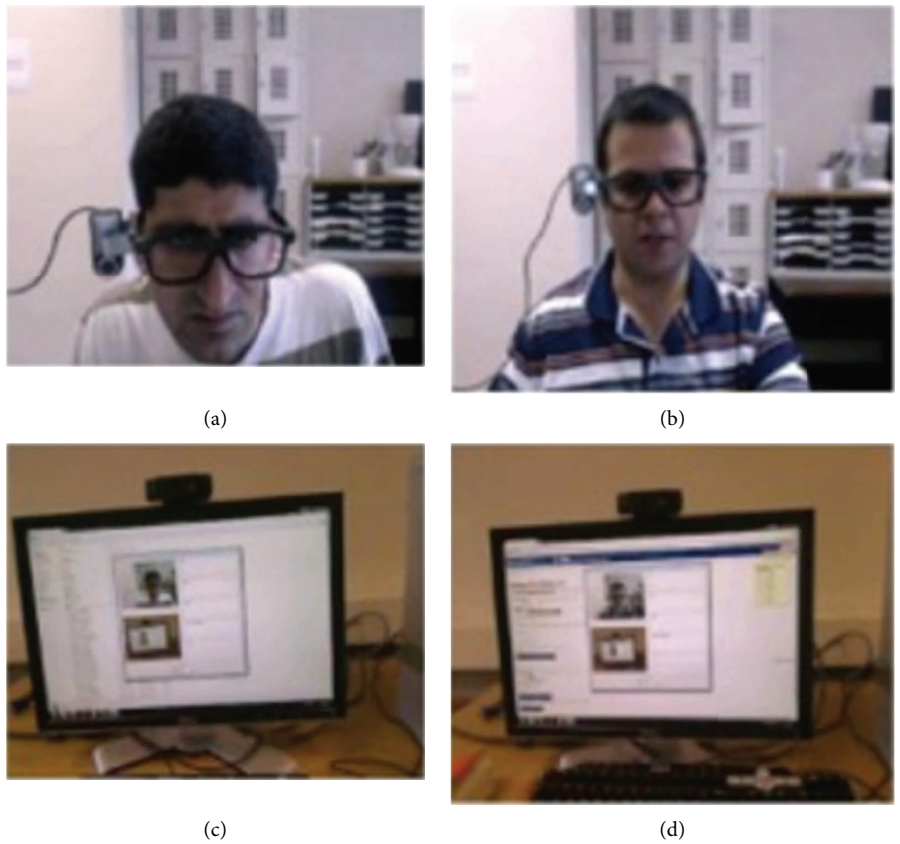

Figure 3: Sample image of cheating [6].

to be very useful for detecting a malicious behaviour during an online exam. Table 3 presents a comparison of the latest literature, apart from conventional image processing techniques, for detection of facial expressions.

Mohammad et al. [22] have devised a novel technique for the detection of facial expressions using EEG signals along with the long-short-term memory recurrent neural network (LSTM-RNN) for the purpose of classification. Figure 5 illustrates the power spectral density of the alpha, beta, gamma, and theta waveforms of a human subject while experiencing varied emotional states of fear, anger, calm etc. For the purpose of online examinations, this technique could prove to be helpful as whenever a student would have thoughts of cheating or involve in the act of cheating, the behaviour could be extracted from the PSDs of the EEG signals. These data could be used to supplement the image data being gathered by a webcam and fed to a neural network for accurate facial expression recognition.

Xinyu et al. [23] used yet another biomarker of oxygen saturation levels in the facial tissues during stressful situations. Hyperspectral imaging is used to detect these stress levels and can be appropriately mapped to classes of behaviours. This could prove to be of great help for cheating detection. On similar lines of [23], Lanxin et al. [24] used the linear discriminant analysis (LDA) for the classification of facial expressions.

Apart from detection over a local system, the transference of data through the internet to remotely placed proctors is also a key area of research. Jiannnan et al. [25] described a novel technique of detection of facial expressions using facial action unit (AU), which is a unit assigned to the expressions based on the change of muscles of the face while feeling the assigned emotion. The authors have also presented a light-weight method (using Raspberry Pi) to transfer these data from the client (student) system to any remote server (proctor) by leveraging the low latency

Table 2: Comparative analysis of face detection techniques.

Ref. no	Title	Methodology	Dataset used	Performance metrics			Year of publication
[6]	Towards effective and efficient online exam systems using a deep learning-based cheating detection approach	Devices used: front and back webcam, microphone User verification, voice and text detection, gaze estimation, and phone detection Technique: deep convolutional neural networks (CNNs) and the Gaussian-based discrete Fourier transform (DFT) statistical method	Audio visual data collected from 24 subjects	Text	True detection rate (TDR) False alarm rate (FAR)	3% 1%	2022
				Speech	Accuracy FAR	98.78% 43.9%	
				Phone	TDR FAR	100% 5.3%	
[7]	Gesture-based misbehavior detection in online examination	Device: Microsoft Kinect for gesture detection and classification Classification: threshold selection for pitch, yaw, and hand under the table actions	Audio visual data from subjects	Action only Frequency only 2 D	100% 74% 89%	82% 23% 4%	2016
[15]	Convolutional neural network-based virtual exam controller	Device: camera Classification: Haar cascade classifier with deep learning to apply constraints Face detection using the Viola–Jones algorithm Classifier learning: Adaboost	50 subjects dataset	TDR FAR	93% NA		2020
[16]	Using face recognition to detect "ghost writer" cheating in examination	Device: webcam to detect "ghost writer" and student face recognition	PubFig83 dataset with 100 pictures of 83 students and rest ghost writers	Student Ghost writer	Accuracy Precision Accuracy Precision	92.9% 91.45% 95.9% 95.06%	2019
[17]	A crosscamera multiface tracking system based on double triplet networks	Device: Classification: a Chinese whisper clustering algorithm for feature extraction Double triplet neural network (DTN) with margin sample mining loss (MSML) function	Yolov3 network and WIDER FACE dataset	Accuracy of DTNCNN 16 with a feature size of 128 Accuracy of DTNCNN 16 with a feature size of 1024	99.26% 99.47%		2021
[18]	CP-GAN: a cross-pose profile face frontalization boosting pose-invariant face recognition	Device: camera Classification: crosspose generative adversarial networks (CP-GAN)	CASIA 3D FACE dataset IJB-A dataset	Accuracy on the CASIA 3D FACE dataset Accuracy on the IJB-A dataset	98.5% 95.2%		2020
[20]	Real-time 3D facial tracking via cascaded compositional learning	Device: monocular RGB camera Classification: globally-optimized modular boosted ferns (GoMBF) -cascade regression model	300 W-3D dataset, FaceWarehouse dataset, multi-PIE dataset	Tracking error Run time	0.04 15.5 ms		2021
[19]	Siamese local and global networks for robust face tracking	Device: camera Classification: Siamese CNN	50 reannotated videos from OTB100, TC128, and VOT2017 datasets	Area under the curve (AUC) for the OTB100 dataset AUC for the face tracking dataset	0.70 0.53		2020

Figure 4: 3D facial tracking where GoMBF-cascade tracks faces (globally optimized modular boosted ferns) better than the explicit shape regression (ESR) model [20].

provided by edge computing. This methodology would be a boon for our application of cheating detection, considering that several real-time facial expressions would have to be classified and transferred to the proctor in real time for him to take further action.

This section presented the state-of-the-art and novel image processing and soft computing techniques for face tracking and facial expression detection. As discussed, several of these techniques can be employed for better accuracy of detection of cheating, lower false positive rates, and most importantly, less network transmission overhead.

Section 4 of this article presents various techniques for the detection of cheating in online examinations using head posture analysis.

4. Head Posture Analysis Systems

There are several studies which have been performed to monitor the posture of a person's head while he sits before a computer/laptop. These studies have helped in detection of potential cheating activity by noticing the change in the roll, pitch, and yaw angle of the head (Figure 6) beyond a certain

Table 3: Comparative analysis of facial expression detection techniques.

Ref. no	Title	Methodology	Dataset used	Performance metrics		Year of publication
[22]	Analysis of EEG signals and facial expressions for continuous emotion detection	Device: camera and EEG Classification: long-short-term memory recurrent neural network (LSTM-RNN) and continuous conditional random fields (CCRF)	MAHNOB-HCI database	RMSE of EEG RMSE of LSTM-RNN	0.053 ± 0.029 0.043 ± 0.026	2016
[23]	Evolution of facial tissue oxygen saturation and detection of human physical stress	Hyperspectral imaging for physical stress detection by extracting oxygen saturation in facial tissue Classification: linear discriminant (LD), logistic regression (LR), K-nearest neighbour (KNN), decision tree (DT), and ensemble	20 subjects within ages of 18 to 25	LD accuracy LR accuracy KNN accuracy DT accuracy Ensemble accuracy	80% 79% 72% 72.5% 77.5%	2020
[24]	Facial emotion recognition based on LDA and facial landmark detection	Device: camera Classification: linear discriminant analysis (LDA) and facial landmark detection (FLD)	Cohn–Kanade dataset	LDA accuracy FLD accuracy	73.9% 84.5%	2021
[25]	Real-time facial expression recognition based on edge computing	Device: NVIDIA Jetson TX2, camera, raspberry pi Classification: facial action unit (FAU)	CK + dataset, RAF-DB dataset, pose-RAF-DB dataset, and AffectNet dataset	Run time Accuracy Bandwidth RTT	200 s 94% <20 mbps 80 ms	2021

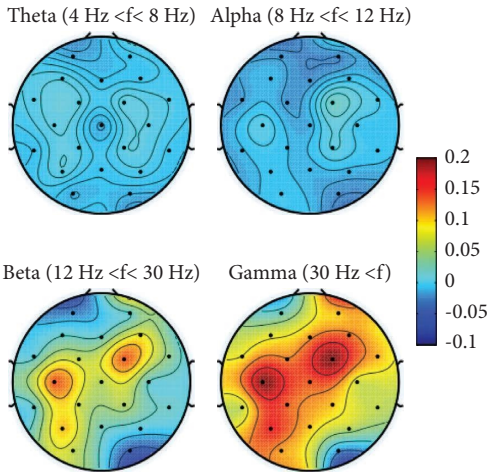

Figure 5: Correlation between power spectral density and continuous valence bands of alpha, beta, theta, and gamma with frontal lobe and nose on the top position [22].

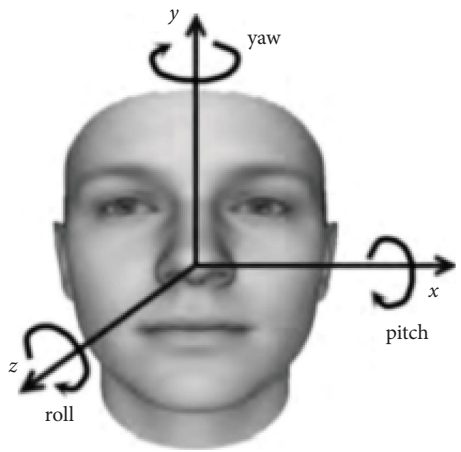

Figure 6: Roll, pitch, and yaw angle of the head [26].

threshold. When the threshold gets crossed, the activity of the person may be deemed as malicious and suitable methods could be applied to tackle the same.

Hu et al. [26] used a method where a webcam is attached to the monitor of the computer or laptop on which the student is expected to take the online examination. From the same, an image of the person is input which is passed through the Adaboost algorithm with the Haar classifier to detect the movement of the head beyond a certain threshold degree. Once the threshold is crossed, a malicious activity is detected. A similar principle of thresholding using various other classification algorithms using multivalued variables has been proposed by Prathish and Bijlani [27], Zhu and Ramanan [28], and Geng and Xia [29].

Donghoon et al. [30] have leveraged the benefits of convolutional neural networks along with the random forest algorithm to perform the classification of head postures beyond a posture. Due to the dense layers of features extracted using the CNN model, the authors have been able to achieve accuracies of the order beyond 97%.

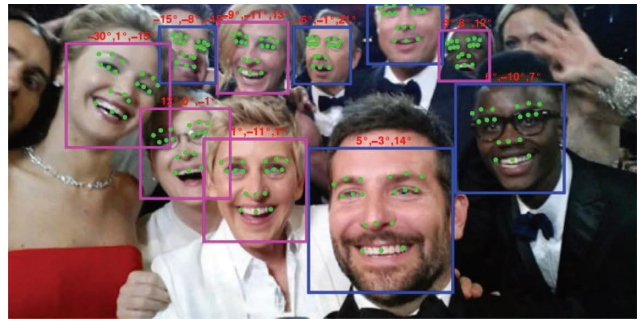

Figure 7: Feature detection and gender classification using ResNet [35].

Yu et al. [31] presented interesting results for creating a 3D morphable model using ResNet. The novelty of this system stems from the fact that not just is a thresholding mechanism used for head pose analysis, but even a 3D model which changes according to the change in head posture of the student, has been created. This could be a revolutionary technique for monitoring students during an online examination. Hu et al. [32], Bouaziz et al. [33], and Taigman et al. [34] have presented their results of 3D modelling of faces on the same lines as Yu et al. [31], which can be explored for their usage in cheating detection during online exams.

Rajeev et al. [35] have presented the usage of ResNet for classification of facial features, head poses, and gender of the student using the CelebA dataset (shown in Figure 7). Similar approaches with varied accuracies have been proposed and proven by Hu et al. [32], Bouaziz et al. [33], and Taigman et al. [34].

Hobeom et al. [36] have presented the development of magnet-magnetometer pairs for monitoring the change in head posture. Based on the craniovertebral angle of the person, a Gaussian regression model is generated to estimate further changes in CVA. Based on these changes, the decision tree and support vector machine classification algorithms have been explored to classify the changing head postures.

Various other methods used for head posture analysis have been described in Table 4.

Therefore, this section presented the possibilities of usage of various head posture analysis techniques to combat the problem of cheating detection in online examinations. Section 5 of this article presents a review of various eye gaze tracking systems that are available in the literature. The usage of the eye gaze tracking systems also proves as one of the methods for online exam cheating detection.

5. Eye Gaze Tracking Systems

The technique of eye tracking computes the eye gaze point of a student as he looks at his surroundings. Based on where he is looking, the rectangular coordinates of the form (x, y) are computed for the subject with the screen as a reference point [42]. Several applications of this technology have been explored, namely, active and passive applications. Active

Table 4: Comparative analysis of head posture analysis techniques.

Ref. no	Title	Methodology	Dataset used	Performance metrics		Year of publication
[8]	Detecting probable cheating during online assessments based on time delay and head pose	Device: camera Method: visual focus of attention (VFOA) analysis Classifier: constrained local model (CLM) with a generalized view-based appearance model (GAVAM)	42 students (28 males and 14 females)	Accuracy	75.6%	2017
[9]	Video summarization for remote invigilation of online exams	Device: webcam (logitech quickcam 9000 pro) Classifier: hidden Markov model	Dataset of videos acquired on different days to analyse head pose	Accuracy	81%	2016
[26]	Research on abnormal behaviour detection of online examination based on image information	Device: webcam Classifier: AdaBoost with Haar classifier	Dataset of 30 independent videos	Roll accuracy Pitch accuracy Yaw accuracy	96.66% 95.24% 96.47	2018
[37]	An application to discover cheating in digital exams	Device: FLEXauth, application Classifiers: deep neural networks (DNNs), random forests (RFs), and support vector machines (SVMs)	12 assignments of 13 students each	Accuracy RF SVM DNN	67.15% 57.69% 37.78%	2018
[38]	An intelligent system for online exam monitoring	Device: webcam for audio and video capture Classifier: yaw angle threshold	Dataset of 39 videos with frame rate of 25 frames per second	Accuracy	90%	2016
[39]	Categorizing the students' activities for automated exam proctoring using proposed deep L2-GraftNet CNN network and ASO-based feature selection approach	Device: Classifier: L2-GrafNet CNN with 46 layers Softmax classifier along with SVM and KNN	Dataset of 2268 pictures of students	KNN classifier accuracy	92.43%	2021 (look at references)
[40]	Face-from-depth for head pose estimation on depth images	Device: depth camera Classifier: CNN termed POSEidon with a deterministic conditional GAN	Biwi kinect head pose, ICT-3DHP, and pandora datasets	Accuracy of POSEidon on pandora dataset test	73.6%	2020
[30]	Head and body orientation estimation using convolutional random projection forests	Device: webcam Classifier: convolutional random projection forest (CRPF)	HIIT dataset with 24000 images of 6 head poses	HIIT dataset image of 15×15 size HIIT dataset image of 25×25 size HIIT dataset image of 50×50 size	97.9% 98.2% 98.3%	2019
[31]	HeadFusion: 360 head pose tracking combining 3D morphable model and 3D reconstruction	Device: webcam Classifier: 3D morphable model (3DMM) with 3D head model	BIWI, UbiPose dataset	BIWI dataset accuracy	96.4%	2018

Table 4: Continued.

Ref. no	Title	Methodology	Dataset used	Performance metrics		Year of publication
[35]	HyperFace: A deep multitask learning framework for face detection, landmark localization, pose estimation, and gender recognition	Device: webcam Classifier: HyperFace CNN along with HyperFace-ResNet and Fast-HyperFace variations	CelebA and LFWA datasets	HyperFace on CelebA dataset HyperFace on LFWA dataset HF-ResNet on CelebA dataset HF-ResNet on LFWA dataset	97% 94% 98% 94%	2019
[41]	MR-CapsNet: a deep learning algorithm for image-based head pose estimation on CapsNet	Device: webcam Classifier: multistage regression-capsule network (MR-CapsNet)	AFLW2000 and BIWI datasets	Mean absolute error on AFLW2000 dataset Mean absolute error on AFLW2000 dataset	4.26% 3.95%	2021
[36]	Novel wearable monitoring system of forward head posture assisted by magnet-magnetometer pair and machine learning	Device: forward head posture (FHP) sensor Classifier: linear classification (LC), decision tree (DT), support vector machine (SVM), and Gaussian process regression (GPR)	Experimental dataset created	RMSE for LC RMSE for DT RMSE for SVM RMSE GPR	6.03 5.82 4.37 4.73	2020

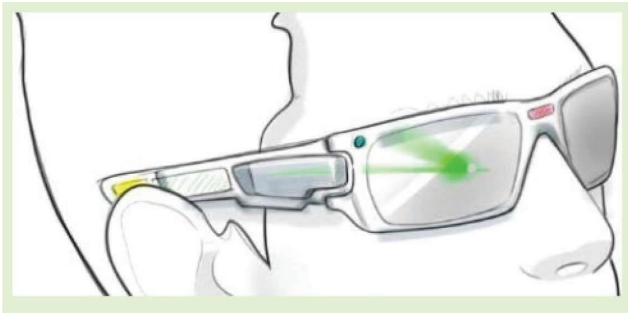

Figure 8: Eye gaze sensor with AR [21].

applications include control of devices using eye gaze, login using eye activation, etc. Passive applications include analysis of design, vehicular safety, medical diagnosis, etc. [43]. Based on Bawarith et al. [10], eye gaze tracking with the usage of logistic regression has been utilized for the detection of malicious activity by a subject during an online examination. Similar approaches have been followed by Curran et al. [44], Kerkvliet and Sigmund [45], Keresztury and Cser [46], and Yee and MacKown [47].

Complex eye gaze tracking systems have been developed by researchers for various other purposes, and the same can be utilized for the detection of cheating during online examinations.

Johannes et al. [21] have proposed the development of an eye gaze tracking sensor coupled with an augmented reality system (Figure 8). A gaze angle resolution of 2.3° has been achieved using this system. Therefore, any minute change in the eye gaze can be detected using this system. Crossing the eye gaze threshold by a large margin may be deemed as a malpractice in the case of online examinations by utilizing such as system.

Bazrafkan et al. [48], Braunagel et al. [49], Corcoran et al. [50], and Bissoli et al. [51] have also presented the development of eye gaze tracking systems for estimation of drivers' attention while driving, consumer electronic applications, development of HMI systems, etc. Table 5 reviews different state-of-the art systems available for eye gaze tracking which may be useful for cheating detection in online examinations.

Apart from the aforementioned techniques for tracking cheating in online exams, one of the major methods followed for the same could be classification of computer network traffic arising from the subject's computer. Section 6 presents various methodologies applied for detection and classification of computer network traffic which could serve as a major breakthrough for cheating detection.

6. Network Data Analysis and Traffic Classification

During an online examination, the student has free internet access to various sources of information and related study material. The detection of the content that he is browsing on the internet while taking the exam is a critical technique to classify his behaviour as malicious or not. A simple method to check the content of his screen would be to mount a camera behind the subject to monitor his screen all the time. However, such a system would create a lot of overhead in terms of data captured and relayed to the proctor who would also be monitoring the face of the student. Therefore, the need arises to develop a mechanism to monitor the browsing activity of the student and analyse the data traffic generated from his system while he takes the exam. This would include the websites he tries to visit, the amount of time those websites are open, and any content that he might have downloaded during the examination.

This section of the article presents literature on various techniques used for the classification of network traffic and analysis of the same. This presents the possibility of building such a system for monitoring online examinations and detection of cheating.

Lizhen and Qusay [64] have developed a phishing detection system using machine learning classification algorithms, namely, random forest, logistic regression, and RNN-BLSTM. Based on what the user browses, the algorithm detects if the site trying to be accessed is a phishing site and alerts the network administrator. In a similar manner, in the case of online examinations, websites posting content that could help a student cheat could be termed "phishing" sites and could be detected if the student tries to browse through them.

A deep learning algorithm has been proposed for the detection of phishing websites in Kaddoura et al. [65] along with classical classification algorithms such as SVM and C4.5. This leads to a comparatively higher accuracy of detection in comparison to conventional algorithms. Furthermore, Chiew et al. [66], Sahingoz et al. [67], and Kaddoura et al. [68] have also explored the detection of phishing sites using machine learning approaches. Table 6 tabulates the state-of-the-art mechanisms followed for the detection of phishing using machine learning. It also provides an insight into the possibility of using these techniques to detect malpractice and malicious activity during online examinations.

Apart from trying to access content from the internet, another major form of cheating could be when another person masquerades as a student to take an online examination from another location. This may go undetected, especially if the examination system is automated (e.g., CourseEra) and does not involve a proctor. Section 7 of this article presents recent developments in research for the detection of IP spoofing that could be a pathbreaker in the detection of masquerades during online examinations.

7. IP Spoofing Detection Mechanisms

IP spoofing refers to the mechanism of using false IP addresses to impersonate another computer system. This is a great threat to the security and authenticity of any computer network. However, in the scenario of online examinations, IP spoofing could be even more dangerous as the actual registered student who is supposed to take the exam is impersonated by another individual who can take the examination on his behalf. Therefore, for efficient detection of cheating during an online exam, it would be very beneficial if

Table 5: Comparative analysis of eye gaze analysis techniques.

Ref. no	Title	Methodology	Dataset used	Performance metrics		Year of publication
[10]	Exam cheating detection system	Device: finger print reader and eye tribe tracker Classifier: logistic regression	Dataset of 30 participants, 15 cheating and 15 noncheating	Accuracy Specificity Precision	97.78% 95.56% 95.74	2017
[11]	Novel solution based on face recognition to address identity theft and cheating in online examination systems	Device: authentication system and webcam Classifier: thresholding	8 instructors and 32 students' data	NA		2014
[52]	A smart approach of E-exam assessment method using face recognition to address identity theft and cheating	Device: finger print authentication, encryption, and webcam Classifier: thresholding	Dataset of 29 students	NA		2016
[53]	A complete system for analysis of video lecture based on eye tracking	Device: VLEYE comprising an eye movement recorder, a dynamic AOI module, and a video analyser Classifier: thresholding	12 subjects in survey	The fixation time rate is calculated for various texts on the screen		2018
[21]	A novel camera-free eye tracking sensor for augmented reality-based on laser scanning	Device: low power eye tracking sensor	Laboratory set up with single subject	Gaze angle resolution	2.3°	2020
[54]	A privacy-preserving approach to streaming eye-tracking data	Device: camera Classifier: radial basis function (RBF) network	ET-DK2 dataset	Error angle	Less than 1.5 degree	2021
[55]	An improved classification model for depression detection using EEG and eye tracking data	Device: camera and EEG Classifier: content-based ensemble method (CBEM)	36 subjects for resting 34 subjects for eye gaze tracking	SVM out of the ensemble	70.28% ± 2.5%	2020
[56]	Automatic pupil detection and gaze estimation using the vestibuloocular reflex in a low-cost eye-tracking setup	Device: low cost head-mounted webcam	1 subject with various gaze angles	Mean absolute angle difference	Less than 1°	2020
[57]	Deep convolutional neural networks and transfer learning for measuring cognitive impairment using eye-tracking in a distributed tablet-based environment	Device: front camera Classifier: CNN	250 subjects	Test accuracy	76%	2021
[58]	GazeVisual: a practical software tool and web application for performance evaluation of eye tracking systems	Device: camera system System developed: GazeVisual	20 subjects	Gaze accuracy Standard deviation	2.1 to 4.4 degrees 0.9 to 2.0	2019
[59]	Quantifying gaze behavior during real-world interactions using automated object, face, and fixation detection	Device: eye tracking glasses Classifier: CNN with Viola–Jones framework to detect faces	5 subjects	Accuracy	77.83%	2018
[60]	Real-time eye tracking for bare and sunglasses-wearing faces for augmented reality 3D head-up displays	Device: webcam Classifier: iris recognition algorithm	Wider facial landmarks in-the-wild (WFLW) database	Accuracy for bare eye Accuracy with sunglasses	1.5 mm 6.5 mm	2021

Table 5: Continued.

Ref. no	Title	Methodology	Dataset used	Performance metrics		Year of publication
[61]	Tracking the progression of reading using eye-gaze point measurements and hidden Markov models	Device: commercial eye trackers Classifier: Kalman filter with a hidden Markov model	Gazepoint GP3 device used to collect gaze data of a single subject	Line detection accuracy	Increase in 27.1% in comparison to conventional systems	2020
[62]	Training a camera to perform long-distance eye tracking by another eye tracker	Device: learning-based single camera eye tracker (LSC) Classifier: deep neural network	100K samples of 6 subjects	Distance error at 1.2 m distance	4.58	2019
[63]	Wavelet method for automatic detection of eye-movement behaviors	Device: webcam Classifier: nonlinear wavelet threshold denoising method	6 participants	Error Accuracy	1.47 76.33%	2019

Table 6: Comparative analysis of network data and classification techniques.

Ref. no.	Title	Methodology	Dataset used	Performance metrics		Year of publication
[12]	Cheating detection in online examinations	Device: 2 laptops running on ubuntu for proposed kismet server Algorithms: blacklist URL, SVM, and URL frequency analysis technique	San Jose State University CS department with 60 students	Accuracy	92%	2015
[13]	E-cheating prevention measures: detection of cheating at online examinations using deep learning approach: a case study	Device: intelligence agent and IP behaviour detector Algorithm: deep neural network (DNN), long-short-term memory (LSTM), dense LSTM, and recurrent neural network (RNN)	Self-generated database	DNN accuracy LSTM accuracy DenseLSTM accuracy RNN accuracy	68% 92% 95% 86%	2021
[64]	A deep learning-based framework for phishing website detection	RNN-GRU model	Phish storm, phish tank, ISCX-URL2016, and Kaggle datasets	RNN-GRU accuracy	99.18%	2021
[69]	A fuzzy ontology and SVM-based web content classification system	SVM with fuzzy-based ontology system	4646 webpages of normal, adult, and medical content	False positive rate Precision Accuracy	5.2% 98% 94%	2017
[70]	An efficient antiphishing method to secure eConsume	Resource request-based phishing discovery (RRPD)	200 zero-hour phishing sites	Recall	88%	2019
[71]	An explainable multimodal hierarchical attention model for developing phishing threat intelligence	Multimodal hierarchical attention mode (MMHAM)	4396 legitimate and illegitimate websites	Accuracy Precision Recall F1	0.9726 0.9784 0.9666 0.9724	2022
[72]	Generalized outlier Gaussian mixture technique based on automated association features for simulating and detecting web application attacks	Association rule mining followed by the outlier Gaussian mixture technique	Webattack and UNSW-NB-15 datasets	Accuracy for the webattack dataset False alarm ratio for the webattack dataset Accuracy for the UNSW-NB-15 dataset False alarm ratio for the UNSW-NB-15 dataset	98.96% 1.04% 95.68% 4.32%	2021
[73]	OFS-NN: an effective phishing websites detection model based on optimal feature selection and neural network	Optimal feature selection-neural network (OFS-NN)	Dataset 1	Accuracy Precision Recall F1 score	96.44% 94.78% 99.02% 96.85%	2019
[65]	Particle swarm optimization-based feature weighting for improving intelligent phishing website detection	Particle swarm optimization with ensemble machine learning models	11055 websites	SVM with PSO accuracy C4.5 with PSO accuracy BPNN with PSO accuracy	92.19% 96.28% 96.43%	2020
[74]	Phishing website detection based on multidimensional features driven by deep learning	CNN-LSTM algorithm	PhishTank dataset	Accuracy False positive rate	98.99% 0.59%	2019

Table 6: Continued.

Ref. no.	Title	Methodology	Dataset used	Performance metrics		Year of publication
[75]	A fuzzy ontology and SVM-based web content classification system	SVM with fuzzy-based ontology system	4646 webpages of normal, adult, and medical content	False positive rate Precision Accuracy	5.2% 98% 94%	2017
[76]	Adversarial network traffic: towards evaluating the robustness of deep learning-based network traffic classification	Injection attacks, AdvPay, AdvBurst, and AdvPad on a DL-based network	Chat, e-mail, file transfer, streaming, torrent, and VoIP datasets	Precision Recall F-score	85.35% 76.45% 80.66%	2021
[77]	Classification and forecasting of real-time server traffic flows employing long-short-term memory for hybrid E/O data center networks	LSTM	File sever dataset	Accuracy	99%	2021
[78]	Edge computing intelligence using robust feature selection for network traffic classification in internet-of-things	Ensemble weighted approach (EWA) for feature selection	Datasets from the University of Cambridge	Increase in overall accuracy	1.3%	2020
[79]	Evolutionary algorithm-based and network architecture search-enabled multiobjective traffic classification	Neural architecture search (NAS) on multiobjective evolutionary algorithms (MOEAs)	IDS2012 and ISCX VPN dataset	F1 score for IDS2012 dataset F1 score for ISCX VPN dataset	99.8% 99.4%	2021
[80]	FlowPic: A generic representation for encrypted traffic classification and applications identification	FlowPic using CNN for data classification	ISCX VPN and ISCX Tor datasets	VoIP class accuracy Video class accuracy File transfer class accuracy Chat class accuracy Browsing class accuracy	99.7% 99.9% 77.4% 89.3% 90.2%	2021
[81]	FPGA-based network traffic classification using machine learning	FPGA-based random forest classifier	UNIBS and UNB datasets	Accuracy F1 score	98.5% 0.932	2020
[82]	PCCN: parallel cross convolutional neural network for abnormal network traffic flows detection in multiclass imbalanced network traffic flows	Parallel cross convolutional neural network (PCCN)	CICIDS2017 dataset	PCCN test time	34932 seconds	2019
[83]	Security analysis of network anomalies mitigation schemes in IoT networks	Ensemble machine learning models, naïve bayes, K-NN, and J48 algorithms	UNSW-NB15 dataset	Accuracy NB Accuracy J48 Accuracy K-NN	85% 93% 94.5%	2020
[84]	Semisupervised encrypted traffic classification with deep convolutional generative adversarial networks	Deep convolutional generative adversarial network (DCGAN)	QIC, ISCX VPN, and non-VPN datasets	QIC dataset accuracy ISCX VPN and non-VPN dataset accuracy	89% 78%	2019
[85]	Sequential message characterization for early classification of encrypted internet traffic	Sequential message characterization (SMC) with LSTM network	Network protocol datasets	Classification accuracy	97%	2021

Table 6: Continued.

Ref. no.	Title	Methodology	Dataset used	Performance metrics		Year of publication
[86]	SETA++: real-time scalable encrypted traffic analytics in multi-Gbps networks	SETA++	165,000 flows of data	Accuracy of service provider classification Content classification accuracy	99% 90%	2021
[87]	Traffic density classification using sound datasets: an empirical study on traffic flow at asymmetric roads	CNN model	Custom dataset	Accuracy	95%	2020
[88]	VoIP traffic detection in tunneled and anonymous networks using deep learning	MLP, CNN, LSTM	VPN VoIP and TOR VoIP datasets	MLP precision CNN precision LSTM precision	96% 97.1% 95.2%	2021

Table 7: Comparative analysis of IP spoofing detection techniques.

Ref. no	Title	Methodology	Dataset used	Performance metrics		Year of publication
[105]	An ensemble intrusion detection method for train ethernet consist network based on CNN and RNN	LeNET-5, AlexNet, VGGNet, SimpleRNN, LSTM, and GRU	ECN test bed	Accuracy	97.5	2021
[106]	Enhanced intrusion detection system for an EH IoT architecture using a cooperative UAV relay and friendly UAV jammer	Monte Carlo approach	UAV data	Detection time	0.7s	2021
[107]	Hardware trojan detection in behavioral intellectual properties (IP's) using property checking techniques	AES algorithm	Sobel, UART	Assertion of target trojan	75%	2017
[108]	SASA: source-aware self-attention for IP hijack detection	Source-aware self-attention (SASA) algorithm	78 solid agents dataset and 7 noisy agents dataset	Accuracy False alarm	99.24% 0.80%	2022
[89]	Symmetry degree measurement and its applications to anomaly detection	Thresholding	CERNET dataset	Precision Recall	63.6% 93.3%	2020
[109]	Using scan side channel to detect IP theft	Pipeline-associated watermark algorithm	Bitcoin SHA-256 accelerator	Area overhead	16%	2017
[93]	Watermarch: IP protection through authenticated obfuscation in FPGA bitstreams	Watermarch watermarking algorithm				2021

an IP spoofing detection mechanism was in place. This section of the article presents a review of the final possible method that could be used to combat cheating, namely, the detection of IP spoofing.

Tao et al. [89] have presented a novel technique for spoofing detection. A symmetry degree is proposed for the identification of incomplete sessions of data transfer and other sessions that may exhibit unusual behaviours. Furthermore, based on the method of thresholding, dynamic traffic analysis is performed using the Chinese remainder theorem.

On the same lines as Tao et al. [89], Tankard [90], Liu et al. [91], and Barford et al. [92] have proposed advanced machine learning approaches for IP spoofing and malicious behaviour detection.

Olney and Karam [93] present a novel technique of watermarking traffic being generated from a computer system by obfuscating the same at the FPGA level. Therefore, an extra layer of security is added to the data being generated from the computer system, as every system has a unique watermark which cannot be copied through spoofing.

Similar approaches to Olney and Karam [93] have been followed by Kahng [94], Moradi et al. [95], Moradi et al. [96], Schmid et al. [97], and Zhang et al. [98] research studies to watermark IP addresses to mitigate spoofing.

The state-of-the-art mechanisms for countering cyber attacks have also been presented by Kaddoura et al. [99], Abrham et al. [100], Kaddoura et al. [101], Balobid et al. [102], Haraty et al. [103], and Haraty et al. [104]. Table 7 describes the state-of-the-art systems used for IP spoofing detection.

8. Discussion and Conclusion

This article presented a comprehensive review of how the soft computing paradigm has been and can be more effectively employed for the detection of cheating during online examinations. From the study, it has been concluded that though there are a few mechanisms in place for the detection of cheating during online examinations, there is still a great possibility to enhance these mechanisms by using state-of-the-art systems for user identification and motion detection.

In the case of face tracking and facial recognition systems, there are models available which can perform 3D tracking of faces (Jianwen et al.) [20] or use biomarkers (Xinyu et al.) [23] to detect sudden surges of emotions such as fear and confusion. These systems not only provide detection of minute details of facial expression change but also give high accuracy of detection. In the case of the analysis of head posture systems, several studies have been presented in this article. The most promising ones are the ones utilizing ResNet CNN [30, 31, 35], resulting in multiple feature extraction and minute change detection in head posture which may be termed as malicious activity. Moving on to the usage of eye gaze tracking systems, much literature has been studied and presented in this area too. A very high resolution of up to a change of 2.3° has been detected [21] in systems which can be employed to create systems for cheating detection in online examinations. An unexplored domain of research in the online examination realm which is related to network traffic emanating from the systems has been explored in our article. Several systems [64, 65] have been presented which clearly classify the data being generated from computer systems. A robust model for cheating detection in online exams can be created utilizing these state-of-the-art facilities. Furthermore, the area of IP spoofing detection [93, 105] has also been explored and presented as one of the major techniques to detect cheating during online exams. The issues and challenges in online learning and exams including cheating detection problems were presented by Itani et al. [110].

Therefore, a comprehensive system comprising of the aforementioned verticals can be created to effectively monitor and report malicious activity and cheating during online examinations. This would also serve as a robust methodology to help proctors conduct online exams and make online learning a more authentic and rewarding process.

Nomenclature

AUC:	Area under the curve
3D MM:	3D morphable model
AOI:	Area of interest
CBEM:	Content-based ensemble method
CCRF:	Continuous conditional random field
CLM:	Constrained local model
CNN:	Convolutional neural network
CP-GAN:	Camera classification: crosspose generative adversarial network
CRPF:	Convolutional random projection forest
DNN:	Deep neural network
DT:	Decision tree
DTN:	Double triplet neural network
EEG:	Electroencephalogram
ESR:	Explicit shape regression
FAR:	False alarm rate
FAU:	Facial action unit
FHP:	Forward head posture
FLD:	Facial landmark detection
GAVAM:	Generalized view-based appearance model
GoMBF:	Globally-optimized modular boosted ferns
GPR:	Gaussian process regression
K-NN:	K- nearest neighbour
LC:	Linear classification
LDA:	Linear discriminant analysis
LR:	Logistic regression
LSC:	Learning-based single camera
LSTM-RNN:	Long-short-term memory recurrent neural network
MR-CapsNet:	Multistage regression-capsule network
MSML:	Margin sample mining loss function
PCA:	Principal component analysis
PIFR:	Pose invariant face recognition
RBF:	Radial base function
RF:	Random forest

RMSE: Root mean square error
RTT: Round trip time
SVM: Support vector machine
TDR: True detection rate
VFOA: Visual focus of attention analysis
WFLF: Wider facial landmarks in-the-wild.

Data Availability

Since this is a review article, the data pertaining to this review are available in the references.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was funded by the Zayed University Research Incentive Fund (RIF) Grant (grant no.: R20128).

References

[1] N. Fakhroddin, M. Azadeh, and A. Mohammad, "A systematic review of research on cheating in online exams from 2010 to 2021," *Education and Information Technologies*, vol. 27, pp. 8413–8460, 2022.

[2] S. Kaddoura, D. E. Popescu, and J. D. Hemanth, "A systematic review on machine learning models for online learning and examination systems," *PeerJ Computer Science*, vol. 8, p. 986, 2022.

[3] W. Rosen and M. Carr, "An autonomous articulating desktop robot for proctoring remote online examinations," in *Proceedings of the 2013 IEEE Frontiers in Education Conference (FIE)*, pp. 1935–1939, Oklahoma, OK, USA, October 2013.

[4] X. Li, K. M. Chang, Y. Yuan, and A. Hauptmann, "Massive open online proctor: protecting the credibility of MOOCs certificates," in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, pp. 1129–1137, New York, NY, USA, February 2015.

[5] Y. Xiong and H. K. Suen, "Assessment approaches in massive open online courses: possibilities, challenges and future directions," *International Review of Education*, vol. 64, no. 2, pp. 241–263, 2018.

[6] S. Kaddoura and A. Gumaei, "Towards effective and efficient online exam systems using deep learning- based cheating detection approach," *Intelligent Systems with Applications*, vol. 16, Article ID 200153, 2022.

[7] Z. Fan, J. Xu, W. Liu, and W. Cheng, "Gesture based misbehavior detection in online examination," in *Proceedings of the 11th International Conference on Computer Science & Education*, pp. 234–238, NagoyaF, Japan, Augest 2016.

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

[9] M. Cote, F. Jean, A. B. Albu, and D. Capson, "Video summarization for remote invigilation of online exams," in *Proceedings of the 2016 IEEE Winter Conference on Applications of Computer Vision*, pp. 1–9, Lake Placid, NY, USA, March 2016.

[10] R. Bawarith, A. Basuhail, A. Fattouh, and P. S. Gamalel-din, "E-exam cheating detection system," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 4, pp. 176–181, 2017.

[11] A. Fayyoumi and A. Zarrad, "Novel solution based on face recognition to address identity theft and cheating in online examination systems," *Advances in Internet of Things*, vol. 04, no. 02, pp. 5–12, 2014.

[12] G. Kasliwal, "Cheating detection in online examinations," M.Sc. thesis, San Jose State University, San Jose, CA, USA, 2015.

[13] 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," 2021, https://arxiv.org/abs/2101.09841.

[14] W. Mengist, T. Soromessa, and G. Legese, "Method for conducting systematic literature review and meta-analysis for environmental science research," *MethodsX*, vol. 7, no. 7, Article ID 100777, 2020.

[15] K. Garg, K. Verma, K. Patidar, N. Tejra, and K. Petidar, "Convolutional neural network based virtual exam controller," in *Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS)*, pp. 895–899, Secunderabad, India, May 2020.

[16] H. He, Q. Zheng, R. Li, and B. Dong, "Using face recognition to detect "Ghost Writer" cheating in examination," in *Edutainment, Lecture Notes in Computer Science*, vol. 11462, pp. 389–397, Springer International Publishing, Heidelberg, Germany, 2018.

[17] G. Ren, X. Lu, and Y. Li, "A cross-camera multi-face tracking system based on double triplet networks," *IEEE Access*, vol. 9, no. 9, pp. 43759–43774, 2021.

[18] J. Liu, Q. Li, M. Liu, and T. Wei, "CP-GAN: a cross-pose profile face frontalization boosting pose-invariant face recognition," *IEEE Access*, vol. 8, no. 8, pp. 198659–198667, 2020.

[19] Q. Yuankai, Z. Shengping, J. Feng, Z. Huiyu, T. Dacheng, and L. Xuelong, "Siamese local and global networks for robust face tracking," *IEEE Transactions on Image Processing*, vol. 29, pp. 43759–43774, 2020.

[20] L. Jianwen, C. Xiaoxu, D. Junyu, and Y. Hui, "Real-time 3D facial tracking via cascaded compositional learning," *IEEE Transactions on Image Processing*, vol. 30, p. 202, 2020.

[21] M. Johannes, S. Thomas, F. Wolfgang, and K. Enkelejda, "A novel camera-free eye tracking sensor for augmented reality based on laser scanning," *IEEE Sensors Journal*, vol. 20, no. 24, pp. 1–9, 2020.

[22] S. Mohammad, A. Sadjad, F. Yun, and P. Maja, "Analysis of EEG signals and facial expressions for continuous emotion detection," *IEEE Transactions on Affective Computing*, vol. 7, no. 1, pp. 43759–43774, 2016.

[23] L. Xinyu, X. Xiao, C. Ranlei, and C. Tong, "Evolution of facial tissue oxygen saturation and detection of human physical stress," in *Proceedings of the Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC)*, Dalian, China, April 2020.

[24] S. Lanxin, S. Xunbing, and D. JunBo, "Facial emotion recognition based on LDA and facial landmark detection," in *Proceedings of the 2021 2nd International Conference on Artificial Intelligence and Education (ICAIE)*, Dali, China, June 2021.

[25] Y. Jiannnan, Q. Tiatian, Z. Fan, and U. K. Samee, "Real-time facial expression recognition based on Edge computing," *IEEE Access*, vol. 11, pp. 1–13, 2021.

[26] S. Hu, X. Jia, and Y. Fu, "Research on abnormal behaviour detection of online examination based on image information," in *Proceedings of the 10th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC)*, vol. 2, pp. 88–91, IEEE, Hangzhou, China, Augest 2018.

[27] S. Prathish and K. Bijlani, "An intelligent system for online exam monitoring," in *Proceedings of the Information Science (ICIS)*, pp. 138–143, IEEE, Kochi, India, Augest 2016.

[28] X. Zhu and D. Ramanan, "Face detection, pose estimation, and landmark localization in the wild," in *Proceedings of the Computer Vision and Pattern Recognition (CVPR)*, pp. 2879–2886, IEEE, Providence, RI, USA, June 2012.

[29] X. Geng and Y. Xia, "Head pose estimation based on multivariate label distribution," in *Proceedings of the Computer Vision and Pattern Recognition (CVPR)*, pp. 1837–1842, Nanjing, China, June 2014.

[30] L. Donghoon, Y. Ming-Hsuan, and O. Songhwai, "Head and body orientation estimation using convolutional random projection forests," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 41, no. 1, pp. 437–450, 2019.

[31] Y. Yu, A. F. M. Kenneth, and O. Jean-Marc, "HeadFusion: 360 head pose tracking combining 3D morphable model and 3D reconstruction," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 40, no. 11, pp. 437–450, 2018.

[32] J. Hu, X. H. Zhu, X. J. Zhang et al., "Face alignment across large poses: a 3D solution," *Journal of Hepatology*, vol. 64, no. 1, pp. 146–159, 2016.

[33] S. Bouaziz, Y. Wang, and M. Pauly, "Online modeling for real-time facial animation," *ACM Transactions on Graphics*, vol. 32, no. 4, pp. 1–10, 2013.

[34] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "Deepface: closing the gap to human-level performance in face verification," in *Proceedings of the 2014 IEEE Conference on Computer Vision and Pattern Recognition*, pp. 1701–1708, Columbus, OH, USA, June 2014.

[35] R. Rajeev, V. M. Patel, and R. Chellappa, "HyperFace: a deep multi-task learning framework for face detection, landmark localization, pose estimation, and gender recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 41, no. 1, pp. 437–450, 2019.

[36] H. Hobeom, J. Hyeongkyu, and W. Y. Sang, "Novel wearable monitoring system of forward head posture assisted by Magnet-Magnetometer pair and machine learning," *IEEE Sensors*, vol. 20, no. 7, pp. 43578–43590, 2020.

[37] J. Opgen-Rhein, B. Küppers, and U. Schroeder, "An application to discover cheating in digital exams," in *Proceedings of the ACM International Conference Proceeding Series*, Koli, Finland, November 2018.

[38] S. Prathish, S. Athi Narayanan, and K. Bijlani, "An intelligent system for online exam monitoring," in *Proceedings of the 2016 International Conference on Information Science (ICIS)*, pp. 138–143, Dublin, Ireland, Augest 2016.

[39] 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.

[40] B. Guido, F. Matteo, V. Roberto, C. Simone, and R. Cucchiara, "Face-from-depth for head pose estimation on depth images," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 42, no. 3, pp. 1–13, 2020.

[41] F. Hao, L. Jun-qing, X. Kai et al., "MR-CapsNet: a deep learning algorithm for image-based head pose estimation on CapsNet," *IEEE Access*, vol. 5, pp. 440–450, 2021.

[42] B. S. Bagepally, "Gaze pattern on spontaneous human face perception: an eye tracker study," *Journal of the Indian Academy of Applied Psychology*, vol. 41, no. 3, p. 127, 2015.

[43] "The eye tribe," 2016, https://theeyetribe.com.

[44] K. Curran, G. Middleton, and C. Doherty, "Cheating in exams with technology," *International Journal of Cyber Ethics in Education*, vol. 30, pp. 1–15, 2011.

[45] J. Kerkvliet and C. L. Sigmund, "Can we control cheating in the classroom?" *The Journal of Economic Education*, vol. 30, no. 4, pp. 331–343, 1999.

[46] B. Keresztury and L. Cser, "New cheating methods in the electronic teaching era," *Procedia-Social and Behavioral Sciences*, vol. 93, no. 93, pp. 1516–1520, 2013.

[47] K. Yee and P. MacKown, *Detecting and Preventing Cheating during Exams*, Pedagogy, Not Policing, New York, NY, USA, 2009.

[48] S. Bazrafkan, A. Kar, and C. Costache, "Eye gaze for consumer electronics: controlling and commanding intelligent systems," *IEEE Consumer Electronics Magazine*, vol. 4, no. 4, pp. 65–71, 2015.

[49] C. Braunagel, W. Rosenstiel, and E. Kasneci, "Ready for take-over? A new driver assistance system for an automated classification of driver take-over readiness," *IEEE Intelligent Transportation Systems Magazine*, vol. 9, no. 4, pp. 10–22, 2017.

[50] P. Corcoran, F. Nanu, S. Petrescu, and P. Bigioi, "Real-time eye gaze tracking for gaming design and consumer electronics systems," *IEEE Transactions on Consumer Electronics*, vol. 58, no. 2, pp. 347–355, 2012.

[51] A. Bissoli, D. Lavino-Junior, M. Sime, L. Encarnação, and T. Bastos-Filho, "A human–machine interface based on eye tracking for controlling and monitoring a smart home using the Internet of Things," *Sensors*, vol. 19, no. 4, p. 859, 2019.

[52] S. Idemudia, M. F. Rohani, M. Siraj, and S. H. Othman, "A smart approach of E-Exam assessment method using face recognition to address identity theft and cheating," *International Journal of Computer Science and Information Security*, vol. 14, no. 10, pp. 515–522, 2016.

[53] Z. Xuebai, Y. Shyan-ming, C. Ming-dao, and L. Xiaolong, "A complete system for analysis of video lecture based on eye tracking," *IEEE Access*, vol. 1, no. 1, pp. 49056–49066, 2018.

[54] B. David-John, D. Hosfelt, K. Butler, and E. Jain, "A privacy-preserving approach to streaming eye- tracking data," *IEEE Transactions on Visualization and Computer Graphics*, vol. 27, no. 5, pp. 2555–2565, 2021.

[55] J. Zhu, Z. Wang, T. Gong et al., "An improved classification model for depression detection using EEG and eye tracking data," *IEEE Transactions on NanoBioscience*, vol. 19, no. 3, pp. 527–537, 2020.

[56] A. Vered, Y. C. Verushen, L. G. Kyle, and P. Michiel, "IEEE Automatic pupil detection and gaze estimation using the vestibulo-ocular reflex in a low-cost eye-tracking setup," *South African Institute of Electrical Engineers*, vol. 111, no. 3, pp. 120–124, 2020.

[57] R. U. Haque, A. L. Pongos, C. M. Manzanares, J. J. Lah, A. I. Levey, and G. D. Clifford, "Deep convolutional neural networks and transfer learning for measuring cognitive impairment using eye-tracking in a distributed tablet-based environment," *IEEE Transactions on Biomedical Engineering*, vol. 68, no. 1, pp. 11–18, 2021.

[58] A. Kar and P. Corcoran, "GazeVisual: a practical software tool and web application for performance evaluation of eye tracking systems," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 293–302, 2019.

[59] L. Chukoskie, S. Guo, E. Ho et al., "Quantifying gaze behavior during real-world interactions using automated object, face, and fixation detection," *IEEE Transactions on Cognitive and Developmental Systems*, vol. 10, no. 4, pp. 1143–1152, 2018.

[60] D. Kang and L. Ma, "Real-time eye tracking for bare and sunglasses-wearing faces for augmented reality 3D head-up displays," *IEEE Access*, vol. 9, no. 9, pp. 125508–125522, 2021.

[61] S. Bottos and B. Balasingam, "Tracking the progression of reading using eye-gaze point measurements and Hidden Markov Models," *IEEE Transactions on Instrumentation and Measurement*, vol. 69, no. 10, pp. 7857–7868, 2020.

[62] W. Li, Q. Dong, H. Jia et al., "Training a camera to perform long-distance eye tracking by another eye-tracker," *IEEE Access*, vol. 7, no. 7, pp. 155313–155324, 2019.

[63] B. Yan, T. Pei, and X. Wang, "Wavelet method for automatic detection of eye-movement behaviors," *IEEE Sensors Journal*, vol. 19, no. 8, pp. 3085–3091, 2019.

[64] T. Lizhen and H. M. Qusay, "A deep learning-based framework for phishing website detection," *IEEE Access*, vol. 10, pp. 1509–1521, 2021.

[65] S. Kaddoura, O. Alfandi, and N. Dahmani, "A spam email detection mechanism for English language text emails using deep learning approach," in *Proceedings of the 2020 IEEE 29th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, pp. 193–198, IEEE, Bayonne, France, September, 2020.

[66] K. L. Chiew, C. L. Tan, K. Wong, K. S. C. Yong, and W. K. Tiong, "A new hybrid ensemble feature selection framework for machine learning-based phishing detection system," *Information Sciences*, vol. 484, pp. 153–166, 2019.

[67] O. K. Sahingoz, E. Buber, O. Demir, and B. Diri, "Machine learning based phishing detection from URLs," *Expert Systems with Applications*, vol. 117, pp. 345–357, 2019.

[68] S. Kaddoura, G. Chandrasekaran, D. Elena Popescu, and J. H. Duraisamy, "A systematic literature review on spam content detection and classification," *PeerJ Computer Science*, vol. 8, p. 830, 2022.

[69] A. Farman, P. Khan, K. Riaz et al., "A fuzzy ontology and SVM–based web content classification system," *IEEE Access*, vol. 5, pp. 257821–325797, 2017.

[70] G. Guang-Gang, Y. Zhi-Wei, L. Jong-Hyouk, J. Xiao-Bo, and J. Dong, "An efficient antiphishing method to secure eConsume," *IEEE Consumer Electronics Magazine*, vol. 8, no. 6, pp. 2162–2248, 2019.

[71] C. Yidong, Z. Yonghang, L. Weifeng, and J. Yuanchun, "An explainable multi-modal hierarchical attention model for developing phishing threat intelligence," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 790–803, 2022.

[72] N. Moustafa, G. Misra, and J. Slay, "Generalized outlier Gaussian mixture technique based on automated association features for simulating and detecting web application attacks," *IEEE Transactions on Sustainable Computing*, vol. 6, no. 2, pp. 245–256, 2021.

[73] E. Zhu, Y. Chen, C. Ye, X. Li, and F. Liu, "OFS-NN: an effective phishing websites detection model based on optimal feature selection and neural network," *IEEE Access*, vol. 7, no. 7, pp. 73271–73284, 2019.

[74] P. Yang, G. Zhao, and P. Zeng, "Phishing website detection based on multidimensional features driven by deep learning," *IEEE Access*, vol. 7, no. 7, pp. 15196–15209, 2019.

[75] F. Ali, P. Khan, K. Riaz et al., "A fuzzy ontology and SVM–based web content classification system," *IEEE Access*, vol. 5, no. 5, pp. 25781–25797, 2017.

[76] A. M. Sadeghzadeh, S. Saeed, and R. Jalili, "Adversarial network traffic: towards evaluating the robustness of deep-learning-based network traffic classification," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1520–1530, 2021.

[77] B. Mihail and S. Pachnicke, "Classification and forecasting of real-time server traffic flows employing long short-term memory for hybrid E/O data center networks," *Journal of Optical Communications and Networking*, vol. 13, no. 5, pp. 85–93, 2021.

[78] M. Bushra, H. Mosab, J. S. Bassi et al., "Edge computing intelligence using robust feature selection for network traffic classification in Internet-of-Things," *Special Selection on Edge Intelligence for Internet of Things*, vol. 8, pp. 224059–224070, 2020.

[79] W. Xiaojuan, W. Xinlei, J. Lei et al., "Evolutionary algorithm-based and network architecture search-enabled multi-objective traffic classification," *IEEE Access. Special Section on Intelligent Big Data Analytics for Internet of Things, Services and People*, vol. 9, pp. 52310–52325, 2021.

[80] T. Shapira and Y. Shavitt, "FlowPic: a generic representation for encrypted traffic classification and applications identification," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1218–1232, 2021.

[81] M. Elnawawy, A. Sagahyroon, and T. Shanableh, "FPGA-based network traffic classification using machine learning," *IEEE Access*, vol. 8, no. 8, pp. 175637–175650, 2020.

[82] Y. Zhang, X. Chen, D. Guo, M. Song, Y. Teng, and X. Wang, "PCCN: parallel cross convolutional neural network for abnormal network traffic flows detection in multi-class imbalanced network traffic flows," *IEEE Access*, vol. 7, no. 7, pp. 119904–119916, 2019.

[83] M. A. Lawal, R. A. Shaikh, and S. R. D. Hassan, "Security analysis of network anomalies mitigation schemes in IoT networks," *IEEE Access*, vol. 8, no. 8, pp. 43355–43374, 2020.

[84] S. I. Auwal and D. Huifang, "Semi-supervised encrypted traffic classification with deep convolutional generative adversarial networks," *IEEE Access*, vol. 8, pp. 118–126, 2019.

[85] W. Chen, F. Lyu, F. Wu, P. Yang, G. Xue, and M. Li, "Sequential message characterization for early classification of encrypted internet traffic," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 4, pp. 3746–3760, 2021.

[86] C. Kattadige, K. N. Choi, A. Wijesinghe et al., "SETA++: real-time scalable encrypted traffic analytics in multi-gbps networks," *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 3244–3259, 2021.

[87] K. H. N. Bui, H. Oh, and H. Yi, "Traffic density classification using sound datasets: an empirical study on traffic flow at asymmetric roads," *IEEE Access*, vol. 8, no. 8, pp. 125671–125679, 2020.

[88] F. U. Islam, G. Liu, J. Zhai, and W. Liu, "VoIP traffic detection in tunneled and anonymous networks using deep learning," *IEEE Access*, vol. 9, no. 9, pp. 59783–59799, 2021.

[89] Q. Tao, L. Zhaoli, W. Pinghui, L. Shancang, G. Xiaohong, and G. Lixin, "Symmetry degree measurement and its applications to anomaly detection," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1–15, 2020.

[90] C. Tankard, "Advanced persistent threats and how to monitor and deter them," *Network Security*, vol. 8, pp. 16–19, 2011.

[91] J. Liu, Y. Xiao, K. Ghaboosi, H. Deng, and J. Zhang, "Botnet: classification, attacks, detection, tracing, and preventive measures," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, Article ID 692654, 2009.

[92] P. Barford, J. Kline, D. Plonka, and A. Ron, "A signal analysis of network traffic anomalies," in *Proceedings of the 2nd ACM SIGCOMM Workshop Internet Measurement*, pp. 71–82, New York, NY, USA, November 2002.

[93] B. Olney and R. Karam, "WATERMARCH: IP protection through authenticated obfuscation in FPGA bitstreams," *IEEE Embedded Systems Letters*, vol. 13, no. 3, pp. 81–84, 2021.

[94] A. B. Kahng, "Watermarking techniques for intellectual property protection," in *Proceedings of the 1998 Design and Automation Conference. 35th DAC. (Cat. No.98CH36175)*, pp. 776–781, San Francisco, CA, USA, June 1998.

[95] A. Moradi, A. Barenghi, T. Kasper, and C. Paar, "On the vulnerability of FPGA bitstream encryption against power analysis attacks: extracting keys from Xilinx virtex-II FPGAs," *IACR Cryptol*, ePrint Archive, Lyon, France, 2011.

[96] A. Moradi, A. Barenghi, T. Kasper, and C. Paar, "Side-channel attacks on the bitstream encryption mechanism of Altera Atratix II: facilitating black-box analysis using software reverse-engineering," in *Proceedings of the ACM/SIGDA international symposium on Field programmable gate arrays*, pp. 91–100, New York, NY, USA, February 2013.

[97] M. Schmid, D. Ziener, and J. Teich, "Netlist-level IP protection by watermarking for LUT-based FPGAs," in *Proceedings of the 2008 International Conference on Field-Programmable Technology*, pp. 209–216, Taipei, Taiwan, December 2008.

[98] J. Zhang, Y. Lin, Q. Wu, and W. Che, "Watermarking FPGA bitfile for intellectual property protection," *Radio Engineering*, vol. 21, pp. 764–771, 2012.

[99] S. Kaddoura, A. El Arid, and A. Al-Dulaimy, "Supervised machine learning techniques to protect IoT healthcare environment against cyberattacks," in *Intelligent Edge Computing for Cyber Physical Applications*, pp. 17–34, Academic Press, Cambridge, Massachusetts, 2023.

[100] T. Abrham, S. Kaddoura, and H. Al Breiki, "Artificial intelligence applications in cybersecurity," in *Handbook of Research on AI Methods and Applications in Computer Engineering*, pp. 179–205, IGI Global, Hershey, Pennsylvania, 2023.

[101] S. Kaddoura, A. E. Arid, and M. Moukhtar, "Evaluation of supervised machine learning algorithms for multi-class intrusion detection systems," in *Proceedings of the Future Technologies Conference (FTC)*, vol. 3, pp. 1–16, Springer International Publishing, Heidelberg, Germany, 2022.

[102] A. M. Balobid, J. S. Binamro, S. T. Yohannes, and S. Kaddoura, "Evaluation of supervised machine learning approaches for credit card fraud detection," in *Proceedings of the 2022 14th Annual Undergraduate Research Conference on Applied Computing (URC)*, pp. 1–6, IEEE, Dubai, United Arab Emirates, November, 2022.

[103] R. A. Haraty, B. Boukhari, and S. Kaddoura, "An effective hash-based assessment and recovery algorithm for healthcare systems," *Arabian Journal for Science and Engineering*, vol. 47, no. 2, pp. 1523–1536, 2021.

[104] R. A. Haraty, S. Kaddoura, and A. Zekri, "Transaction dependency based approach for database damage assessment using a matrix," *International Journal on Semantic Web and Information Systems*, vol. 13, no. 2, pp. 74–86, 2017.

[105] C. Yue, L. Wang, D. Wang, R. Duo, and X. Nie, "An ensemble intrusion detection method for train ethernet consist network based on CNN and RNN," *IEEE Access*, vol. 9, no. 9, pp. 59527–59539, 2021.

[106] N. V. Van, T. Hung, and S. Chakchai, "Enhanced intrusion detection system for an EH IoT architecture using a cooperative UAV relay and friendly UAV jammer," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 11, pp. 1786–1799, 2021.

[107] N. Veeranna and B. C. Schafer, "Hardware trojan detection in behavioral intellectual properties (IP's) using property checking techniques," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 576–585, 2017.

[108] T. Shapira and Y. Shavitt, "SASA: source-Aware Self-Attention for IP hijack detection," *IEEE/ACM Transactions on Networking*, vol. 30, no. 1, pp. 437–449, 2022.

[109] L. Azriel, R. Ginosar, S. Gueron, and A. Mendelson, "Using scan side channel to detect IP theft," *IEEE Transactions on Very Large Scale Integration Systems*, vol. 25, no. 12, pp. 3268–3280, 2017.

[110] M. Itani, M. Itani, S. Kaddoura, and F. Al Husseiny, "The impact of the Covid-19 pandemic on on- line examination: challenges and opportunities," *Global Journal of Engineering Education*, vol. 24, no. 2, p. 16, 2022.