International Journal of Scientific Research and Engineering Development-– Volume 8 Issue 2, Mar-Apr 2025

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Pariksha Nirikshak: Anti Cheating System for examination Hall

Miss.Sonawane S.M.[1], Patel Alisha[2], Ambale Yashswini[3], Shirole Suruchi[4]

*1 Ass.Prof Department of Computer Technology, Rajgad Dnyanpeeth Technical Campus Pune,Maharashtra, India

*2,3,4 Department of Computer Technology, Rajgad Dnyanpeeth Technical Campus Pune,Maharashtra, India

----------**********----------

Abstract:

The educational system is facing a growing problem with the proliferation of exam cheating as a result of new forms of electronic communication and enjoyment. Most students nowadays are too busy worrying about getting a passing grade to put in the time and effort necessary to really prepare for the test. Classical exam surveillance has become outdated as a result of the emergence of multiple cheating strategies. This means that automated cheating case identification using cutting-edge tech is an absolute need. By utilizing deep learning and computer vision techniques to analyze the student's posture in real-time, this research presents an anti-cheating strategy that focuses on behavior analysis. To do this, we employ YOLO-Facial-landmark and media pipe models to extract domain information from video frames at a high level. The next step in predicting cases of cheating is to employ a decision tree classification model.

Keywords: Decision Tree, Deep learning, Computer vision techniques, Anti-cheating model, Convolution Neural network.

----------**********----------

I. INTRODUCTION

Teachers and schools face a formidable problem in the modern digital era when it comes to ensuring the authenticity of online exams. To combat this, we have developed state-of-the-art online exam software that will make cheating extremely difficult, if not impossible. To ensure that the testing process is both fair and reliable, our program has a comprehensive set of features.

An important feature is the ability to use advanced proctoring capabilities to watch test-takers through their webcams. This helps to ensure that only students who have registered for the course are taking the test and that they are not utilizing any unapproved materials or getting help from others. The use of question randomization in our program further reduces the likelihood of cheating by making each exam unique.

Secure browser technology, which the platform supports, locks down the test takers' browsers so they can't access other websites or apps while they're taking the exam. This, in conjunction with analytics and real-time monitoring, enables teachers to immediately notice any anomalies.

The anti-cheating features of our online exam software aren't the only ones we've thought of; we also made sure that both administrators and test-takers would have an easy time using it. Our platform gives schools the peace of mind that comes from knowing they are giving their students a level playing field when they administer tests and penalize those found endorsing such practices.

[1] The following findings have been evaluated based on the activities, tests, and data collected as described by Bancud et al.: a) The assistive monitoring device prototype makes use of the Jetson Nano and the Jetson Nano AI Camera, both manufactured by NVidia. For the purposes of surveillance and inference-based cheat detection, the device records video and transmits it to a computer over Wi-Fi. b) On a PC with the following specifications: Intel I5-9300H CPU, NVidia RTX 2060 GPU, and 16 GB of RAM, the monitoring system achieves an optimal pose estimation using Open Pose's 25-keypoint model, which provides maximum accuracy and real-time performance of slightly under 10 FPS. c) A model for detecting cheating was created by utilizing the XGBoost library and the gradient boosting technique. After hyper-tuning the model's parameters to achieve peak performance, the Optima library was used for processing. d) Vidgear, Starlette, and Django are three Python web development frameworks that were utilized to construct the monitoring system. In particular, a web app was created to enable browser-based monitoring, modular control, and database analysis. e) The system's performance was assessed using a validation dataset consisting of 30 photographs that were produced and labeled by genuine proctors. With a 90% accuracy rate, a f1-score of 89.65%, and an AUROC of 90.32% f), the system is clearly performing well. Based on their responses to the system evaluation questionnaire, the proctors have reached a unified verdict regarding the system's overall effectiveness. Specifically, the majority of respondents to all eleven survey questions had agreed or strongly agreed that the system is useful.

[2] in According to Kamalov F et al., the global spread of the COVID-19 pandemic has resulted in the majority of educational institutions shifting to online programs. The administration of exams has been carried out remotely with minimal oversight, in particular. Consequently, there is a far higher chance of students cheating on exams. The primary goal of this study was to investigate a novel method for identifying possible instances of cheating by use of machine learning. The difficulty of detecting instances of cheating on the final test was specifically addressed by the author. The author suggests a new approach to finding possible instances of exam cheating by analyzing student grades after the test. We base our decision-making on students' pre-final exam grades, their final exam grades, and the class's overall performance. The author uses LSTMs along with an outlier detection method based on KDE to find possible instances of cheating. Researchers hope that administrators and educators might use the study's findings to protect the credibility of course evaluations.

[3] K-nearest neighbor along with the Pearson correlation factors can enhance the deep learning models in identification of the nearest or look alike objects according to the Shubham gade et al. Here author In order to redistribute dynamic power among the charging ports in electric vehicle charging stations, the dataset is first thoroughly examined to preprocess the attributes according to their needs. Author employ the Pearson correlation matrix to establish correlations and delete unwanted columns during the preprocessing step. Author's planned system is structured to reroute power to the charging port, which might completely recharge the battery in the vehicle. To choose the fast charging port with the lowest battery % remaining, the designed model employs the K- Nearest neighbor technique. With the use of the pre-existing data-based deep belief neural network model. This model will help in identifying the nearest cheating objects based on K- nearest neighbors effectively.

The study is structured into five parts. We present a comprehensive overview of ITS in the second section. A concise introduction to deep learning and its uses is given in Section 3. Section 4 details how smart cities and ITS make use of deep learning to detect pedestrians, summarizes the work of several academics in the area, and lays out the obstacles to further study in each subfield. Next, in Section 5, we shall present the final verdict.

II. LITERATURE SURVEY

[4] In a positive development, Sanaa Kaddoura et al. describe how a mix of computer vision techniques and deep learning models were employed to identify instances of online exam cheating. It is a strong and useful training module, but there is still a need for a lightweight detection method that can effectively identify cheating. In this study, we offer a compact strategy for detecting cheating in real time using deep convolutional neural networks (CNNs) and decision fusion with a Gaussian basis for density-functional theory (DFT). The method is primarily composed of three detection modules that, when combined, use a soft voting process to provide scores indicating the likelihood of cheating. In order to test the suggested method using various metrics, we ran extensive tests on a publicly available large-scale database. An evaluation using 30% of the datasets for testing and an evaluation using 40% of the datasets for testing have both been conducted. In the first kind, training uses half of the dataset, validation uses 20%, and testing uses 30%. The second method of evaluation involves training the models on 40% of the datasets, validating them on 20%, and testing them on 40%. The created front camera deep CNN model attained accuracy rates of 99.83% and 99.81% on 30% and 40% test sets, respectively. Additionally, on a 30% test set size, the accuracy rate for the back camera deep CNN model is 98.78%, and on a 40% test set size, it drops to 96.78%. At 0.028 seconds for identifying a single sample image and 0.082 seconds for detecting one second of audio, the computing expenses of the approaches offered by the approach are low. The results and trials validate the usefulness and efficacy of the suggested method for detecting online exam cheating in real-time. An empirical investigation with big recorded datasets and metrics exhibiting various forms of cheating behavior will be conducted by the author in future work.

[5] In a study conducted by Al_airaji et al., an automated approach was introduced to identify students who had unusual behavior while taking tests. When it comes to spotting suspicious activity (cheating) on a test, this system's implementation is crucial. Due to the fact that human invigilators are susceptible to fatigue and illness, which impair their effectiveness, this technology is superior to humans. Various methods for recognizing and tracking students' eye, hand, and head motions are presented in this study. Whether a student's actions are considered normal or not is a function of the system. In particular, the system uses green squares to identify specific facial features, hands, and eyes; however, when these areas of the body exceed a predetermined threshold, the squares' color turns to red, signifying abnormal behavior.

[6] A dataset of cheating video sequences was developed by Hussein, F et al. to identify instances of exam cheating using paper-based assessments. There are a lot of difficult video sequences in the dataset because a lot of the activities seem to be extremely similar and some of the acts don't rely on body movement at all. Impressive and considerable findings were obtained from the experiments conducted on the framework. A whopping 91% of the time, the cheating recognition model got the cheating behaviors right. There are a number of ways our work could be improved, given that the outcomes were positive and noticeable. For instance, better features and classifiers for classification and more advanced algorithms like deep learning for learning are both viable options. Future updates to the system could even make it possible to use it to identify instances of cheating on multi-subject online tests. In addition, the examination environment varies from country to country, and the suggested dataset was only collected in one of those countries. Hence, additional movies can be added to the dataset by including more dynamic characteristics like: other settings; lighting (dim, normal, brilliant); camera angle (low, face-level, on-looking, top-down); presence of varied motions; blurriness; resolution (SD, HD, 4K), etc.

[7] In order to detect online exam cheating, Ambi Singh et al. devised a smart system that can monitor

a student's head orientation and poses in addition to tracking their eye gaze. The use of external equipment to record the student's or test-taker's back-view and side-view could greatly improve this task. The ability to detect spoofing is crucial for verifying the authenticity of test takers. It is possible to enhance this system overall by incorporating procedures for fingerprint or voice identification.

[8] Dr. Mohammadreza VALIZADEH et al. [8] brought attention to the ways in which, causes of, and recommendations for reducing cheating on online learning programs among Turkish college students. More than half of those who took the survey think that cheating is easier and more common in online courses, and they do it anyhow. They plagiarized by copying and pasting answers from websites like Google, consulting with others, and utilizing their own class notes or textbook. For reasons including "exam stress," "getting higher marks," "some technical problems," "lack of knowledge," and "lack of proctoring," they cheated. The majority of respondents felt that institutions should remove the ability to copy and paste in order to combat cheating. A variety of alternatives to traditional forms of assessment, including differentiated quizzes, online tests that demand pupils turn on their webcams, essay-style questions designed to stimulate critical thinking, and increased public awareness of the issue, should be considered by educators. On the other hand, a number of students have made it quite plain that, whether it's because of incompetent faculty or faulty technological infrastructure, nothing can be done.

[9] According to Chaitanya Thombare et al. [9], Flask is in charge of the entire model. A web page's transmission to a client browser is the first step. The proctoring system can see the student's actions on the camera and browser (tab switching, key presses, etc.) through these web pages, which candidates use to take the exam. Information about the observed behavior is transmitted to the Flask Server in the form of data (Starting Point and End Point of Looking Away, Starting Point and End Point of Person Missing). Every time a candidate takes an action, the data they provide is recorded in a database.

[10] According to Bashar H. Asker et al. [10], electronic tests are a crucial component of online education, which has recently seen a surge in popularity. The validity of these exams depends on the presence of guardians who keep an eye out for signs of cheating. To keep tabs on the student while they took the test online, this study developed a system that uses deep learning algorithms. For the system to work as intended, certain conditions must be met, such as adequate lighting and the prohibition of certain student motions that could be construed as cheating attempts. A laptop and an external webcam with a minimum resolution of 2.1 MP (1920 * 1080 @ 30 FPS) are all that's needed for decent results. During operation, the system records video in real-time from the webcam and processes it to extract six features, including: detecting no face, one face, multiple faces, and the examinee's face recognition; tracking the examinee's head movement by following the pupil's movement; and detecting attempts to use a cell phone. The exam supervision center receives a report regarding instances of cheating that are addressed by various algorithms. According to the findings, the suggested solution helped greatly decrease efforts at cheating on the electronic exam and did a good job of supervising the test. The suggested technique detected the six benefits listed above with an average accuracy of about 93.9%.

[11] Recognizing suspicious activity has been a significant focus of research in recent years, as described by Genemo et al. [11]. The invigilator can better ensure fairness and accuracy in disciplinary action if they can automatically detect when pupils are engaging in suspicious behavior and act accordingly. The goal of this work is to use a proposed 63-layer convolutional neural network (CNN) called L4-Branched-ActionNet to categorize suspicious activities. The data collection used to train the network is the CUI-EXAM dataset. An entropy-coded ACS technique is used to decrease the features after that. Various variants of SVM and

KNN classifiers are used for training and validating the features chosen for the dataset. These classifiers get the results again when the feature selection process involves changing the feature count. The Cub-SVM classifier achieves poorer performance on 100 features with an accuracy of 0.9299. Using a Cub-SVM classifier with an accuracy of 0.9299, the best classification results are taken into consideration with 1000 features. With superior performance across the board, the CSVM emerges as the clear winner. Furthermore, the findings are cross-referenced with more current research and verified on the CIFAR-100 dataset. The validity of the proposed method is proven by the acceptable and comparable outcomes. By incorporating features from another convolutional neural network (CNN), feature fusion can be accomplished. In this respect, previous works have demonstrated better results. This task should be investigated in the near future, though, according to the author.

[12] Using data from 38 studies with a total of 24,181 participants and an effect size of up to 43, Li Zhao et al. conducted a meta-analysis that looked at the correlation between students' perceptions of cheating by their classmates and their own self-reported cheating behavior [12]. Perceived effects of peer cheating were statistically significant, with a mean effect size that fell somewhere in the middle (Cohen, 1988). This effect size was among the strongest of all known characteristics connected with students' academic cheating; it was even stronger than factors like gender, age, conscientiousness, and achievement drive. In addition, evaluations of moderators showed that some cultural factors, such as collectivism, power distance, long-term orientation, restraint, uncertainty avoidance, and religion, were associated with a greater perceived peer cheating effect. These results point to the importance of students' peers in encouraging academic dishonesty, the exact nature of which may vary according to cultural norms. These results shed light on the causes of academic dishonesty and show that measures to encourage students to be truthful in the classroom need to take cultural norms and students' social circles into account. Future directions and limitations-The sample's characteristics are one area where this study falls short. Despite a big overall sample size (N = 24,181), only 43 effect sizes were used to estimate the mean effect size of the link between perceived peer behavior and academic cheating. This meta-analysis does not cover all of the research on the perceived peer cheating effect; in fact, there are many more. The effect sizes were not published or were given in a non-standard form, which led to the exclusion of several of these studies. Future research should adhere to a consistent protocol in order to report the required statistical data for meta-analyses.

[13] For the purpose of detecting cheating on online exams, Kaddoura et al. provided a thorough overview of the ways in which the soft computing paradigm has been and can be used more effectively. The research found that while some systems do a good job of detecting cheating on online exams, there is room for improvement by including cutting-edge technologies for user identification and motion detection. There are models that can detect biomarkers for unexpected spikes in emotions like fear and perplexity, and there are also models that can follow faces in three dimensions. Not only can these systems offer very accurate identification, but they can also pick up on the tiniest changes in face expression. Several studies have been provided in this article about the analysis of head posture systems. The ones that use ResNet CNN to extract many features and detect minute changes in head posture that could be considered malevolent conduct are the most promising. The next topic that has seen a lot of research and presentation is the use of eye gaze tracking systems. Systems that can be used to build systems for online exam cheating detection have a very high resolution of up to 2.3°. In this paper, we delve into a hitherto uncharted area of study concerning system-generated network traffic in the context of online examinations. Data created by computers may now be clearly classified using a number of methods that have been proposed. With the use of these cutting-edge resources, we can build a reliable model for detecting cheating on online tests. In addition, research on IP spoofing

detection has been conducted and showcased as a significant method for identifying instances of online exam cheating.

[14] By combining YOLOv8 with an attention mechanism, Yan Zuo et al. overcame the difficulties of identifying suspicious conduct in online testing centers. In particular, five attention mechanisms and YOLOv8 models were evaluated for their performance in order to optimize the algorithm. In order to make this optimization process easier, the author created datasets that are tailored to examine unusual behavior. Specifically, the suggested method processes inspection movies using an improved YOLOv8l model with an ECA mechanism, allowing for the assessment of detection speed and accuracy. The results show that the YOLOv8l model with ECA allows for real-time automatic cheating detection when combined with exam room video monitoring. Automated methods to prevent cheating can benefit greatly from the enhanced YOLOv8 algorithm's ability to identify suspicious exam activity. The technique improved its ability to detect abnormal behavior by achieving accuracy rates surpassing 85% in each subclass, with a focus on detection accuracy. The suggested method has a wide range of possible uses. The primary use case is in the realm of education, namely for the purpose of remote proctoring of online exams in an effort to maintain academic honesty in this age of ubiquitous digital tools. Educational institutions can improve test fairness and reduce the likelihood of misconduct by using this method. Furthermore, this method is not limited to the realm of education. One such use case is in business settings, where it might be utilized to monitor online certification or training sessions for compliance with ethical standards. The security business may also employ it for surveillance purposes, with the goal of identifying questionable actions that could be suggestive of criminal or rule-breaking behavior. The exam as a whole is intricate, so keep in mind that not all strange actions point to cheating. As a result, judgment calls for human intervention in this process. Certain limitations exist in the methodology used in this study, suggesting that there is potential for additional improvement. Rather than focusing on action types, future studies will use multimarket tracking technologies to accurately forecast people's behaviors. An improved method for identifying instances of cheating is to track the nature and frequency of irregular behavior displayed by test takers. Improving the model's performance could be as simple as tweaking the attention mechanism. To be more precise, further research might look at how to incorporate transformer-based models, like vision transformers, that use self-attention mechanisms to prioritize various aspects of the image. To create a more all-encompassing system for detecting cheating, it could be helpful to incorporate extra sensory data like audio or infrared imaging.

[15] In light of the clear limitations of existing dual-perspective systems for detecting cheating behavior, Hu, Z. et al. proposed a system that incorporates three cameras: one for overhead viewing, one for face detection, and one for horizontal monitoring. A three-perspective adaptive behavior detection system that is driven by candidate gaze direction was proposed to increase the scope of examination monitoring while ensuring real-time system performance. Every one of nine possible eye orientations was classified as either a normal, horizontal, or above view. The best-perspective cheating tool detection model and the cheating behavior determination model were automatically chosen based on the results of the gaze direction identification. We presented Lightweight-YOLOv5-CA, a model for a lightweight object detection network, to efficiently and precisely detect cheating tools. It was confirmed through online testing results that the three-perspective capture and evidence gathering method may successfully widen the surveillance area and provide clear descriptions of cheating conduct. With the use of gaze direction recognition, an adaptive model can detect dishonest behavior in real time and expand the surveillance area. Some of these metrics include a mAP50 of 97.4% for overhead object detection and 98.8% for horizontal object identification, as well as an accuracy of 92.4% for the gaze direction recognition model when viewed from the face perspective. The

accuracy reached 95.4% in the final model for determining cheating behavior. After verification, the system's application effect is good at a given school where it has been implemented. This enables intelligent monitoring, significantly decreases student cheating, and saves resources for invigilators. Promoting the system in more schools, investigating any issues with practical implementation, and expanding the resources of the three-perspective dataset will all be part of the future plans to make the system more ubiquitous.

METHODOLOGY

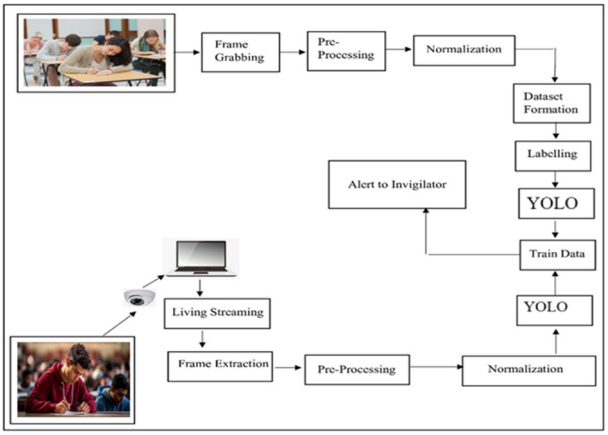

Figure 1: System Overview Diagram

The method that has been suggested to establish a Anti-Cheating system depicted in the system overview in Figure 1 up top. The suggested method was based in part on the execution of the procedures detailed below.

Step 1: Dataset preparation: As an initial step in the proposed system, several models are used to obtain their own images for training. Approximately 598 of these anti-cheating visuals are gathered using the opencv library, which is a part of the python programming language. It is necessary to divide the acquired images into training and testing sets in order to teach the suggested system to distinguish between the various Pariksha nirikshak types.

Step 2: pre-processing : An image data generator object for the Keras Python library class is constructed using a number of factors, including rescaling with a ratio of 1:25. The training and testing items in each dataset are subjected to a categorical class mode, and each image is scaled with a particular size for 64 batches. We train the dataset using a convolutional neural network with 25 adjusted epochs, as we'll see later on.

S. no	Layer Type	Parameters
1	Convolutional Layer	7x7x64 Stride-2
2	Maxpool Layer	2x2 Stride 2
3	Convolutional Layer	3x3x192
4	Maxpool Layer	2x2 Stride 2
5	Convolutional Layer	1x1x128
6	Convolutional Layer	3x3x256
7	Convolutional Layer	1x1x256
8	Convolutional Layer	3x3x512
9	Maxpool Layer	2x2 Stride 2
10	Convolutional Layer	1x1x256
11	Convolutional Layer	3x3x512
12	Convolutional Layer	1x1x256
13	Convolutional Layer	3x3x512
14	Convolutional Layer	1x1x256
15	Convolutional Layer	3x3x512
16	Convolutional Layer	1x1x256
17	Convolutional Layer	3x3x512
18	Convolutional Layer	1x1x512
19	Convolutional Layer	3x3x1024
20	Maxpool Layer	2x2 Stride 2
21	Convolutional Layer	1x1x512
22	Convolutional Layer	3x3x1024
23	Convolutional Layer	1x1x512
24	Convolutional Layer	3x3x1024
25	Convolutional Layer	3x3x1024
26	Convolutional Layer	3x3x1024 Stride 2
27	Convolutional Layer	3x3x1024
28	Convolutional Layer	3x3x1024
29	Fully Connected Layer	
30	Fully Connected Layer	

Figure 2 : Model summary

Step 3: Anti-cheating detection: The technique of detecting cheating in an image starts with locating the student and then moves on to cropping the area around them. The method employs the picture as a means of identifying instances of exam cheating. The student identification module does this by utilizing the Yolov8 technique, which successfully recognizes students as objects. Installing ultralytics and collecting the roboflow dataset are the initial stages in training the Yolov8 model for student identification. To access the cheating detection dataset, follow these steps: https://universe.roboflow.com/srp/anticheating-detection-aiauu/dataset/3/download/yolov8.

Make sure to connect Roboflow with an API key before continuing. A directory index of the files included within the downloaded dataset is created by conducting a full search on it. The total number of files in the folder can then be determined using the file list. There are a total of 598 files, with 478 files being used for training purposes. The 120 files will be alphabetized and then randomly jumbled after they have been transferred to the destination directory. Based on the revised count of files in the directory, there are 478 in the training folder and 598 in the extra folder. The yolov8 object recognition model can be launched after the roboflow dataset and anticheating dataset have been successfully integrated and shuffled. Using the learned weights, the detection algorithm is launched after 50 epochs of training with 478 photos and 32 batches. A zip file containing the project runs is created and saved in the designated location once the training of the yolov8 model is finished. In order to test the application, we take still images from the camera at various points throughout the test and run them through the cheating class. In line with the pariksha nirikshak policy, disciplinary action will be taken whenever it is determined that the student has engaged in exam cheating. Additionally, the department head is being notified of each student's image so that appropriate action can be taken.

III. RESULTS AND DISCUSSIONS

Pariksha Nirikshak: Anti Cheating System for Examination Hall was developed with the help of Python, the Anaconda framework, and the Spyder IDE. Eight gigabytes of primary RAM and one terabyte of secondary memory are available on the development machine. A variety of elements have been taken into account to assess the viability of the suggested plan. Here, we describe in detail the experimental study's findings.

The following figures show the confusion matrix results that were obtained.

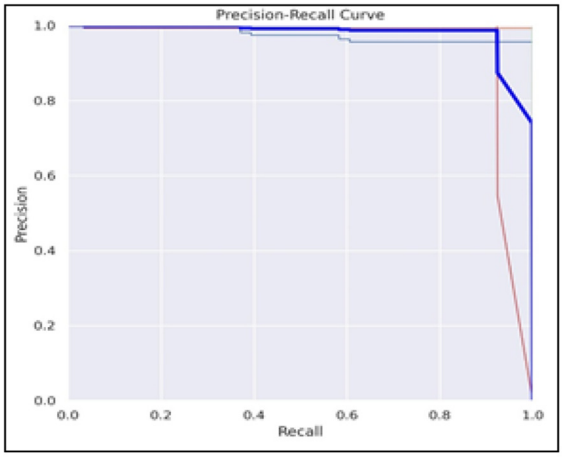

Figure 3: Precision-Recall Curve

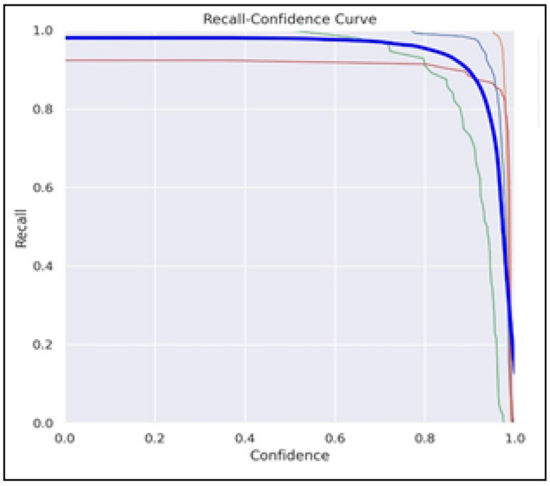

Figure 4:Precision-Confidance Curve

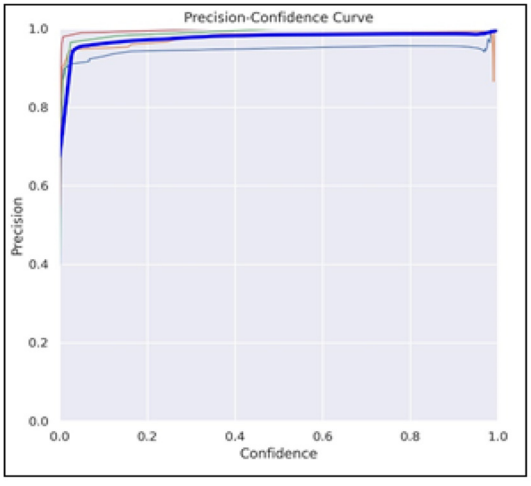

Figure 5: Recall-Confidence Curve

IV. CONCLUSION AND FUTURE SCOPE

Online test systems are expanding in popularity and use because to the rapid rise of digitization and globalization. This is particularly true in situations where infectious diseases, such as a pandemic, are spreading rapidly. In order to keep the test honest and provide fair results, detecting cheating in online exam systems is a big and important job. At now, systems for online exams equip examiners with capabilities to identify instances of cheating by utilizing vision-based classical ML algorithms. Traditional ML approaches, on the other hand, rely on manually-created features and are unable to learn object hierarchies from data, which hinders the efficacy and efficiency of such systems. By analyzing students' posture in real-time using deep learning and computer vision techniques, this paper proposes an anti-cheating model that focuses on behavior analysis. The goal of this research is to develop an efficient and effective approach for online exam systems that uses these models for real-time cheating detection. To do this, we employ the YOLO-Facial-landmark and media pipe models to extract domain-level information from video frames. The next step in predicting cases of cheating is to employ a decision tree classification model. Looking Ahead To ensure that exams are administered fairly and without cheating, this system can be put into action in real-time in educational institutions.

REFERENCES

[1] Bancud, Gil Emmanuel & Palconit, Eleonor. (2021). HUMAN POSE ESTIMATION USING MACHINE LEARNING FOR CHEATING DETECTION. 10.13140/RG.2.2.12686.28481.

[2] Kamalov F, Sulieman H, Santandreu Calonge D (2021) Machine learning based approach to exam cheating detection. PLoS ONE 16(8): e0254340. https://doi.org/10.1371/journal. pone.0254340

[3] Shubham Gade, Bhakti M Kholpe, Uday B Paikrao and ,Gauri Jaywant Kumbhar " Enriching redistribution of power in EV ChargingStations through Deep learning". IJSRMST | Vol. 4| Issue 1 | January2025

[4] Sanaa Kaddoura, Abdu Gumaei, Towards effective and efficient online exam systems using deep learning-based cheating detection approach, Intelligent Systems with Applications, Volume 16, 2022, 200153, ISSN 2667-3053, https://doi.org/10.1016/j.iswa.2022.200153.

[5] Al_airaji , R. M. ., Aljazaery, I. A., Alrikabi, H. T., & Alaidi, A. H. M. . (2022). Automated Cheating Detection based on Video Surveillance in the Examination Classes. *International Journal of Interactive Mobile Technologies (iJIM)*, *16*(08), pp. 124–137. https://doi.org/10.3991/ijim.v16i08.30157

[6] Hussein, F.; Al-Ahmad, A.; El-Salhi, S.; Alshdaifat, E.; Al-Hami, M. Advances in Contextual Action Recognition: Automatic Cheating Detection Using Machine Learning Techniques. Data 2022, 7, 122. https://doi.org/10.3390/ data7090122

[7] Ambi Singh, Smita Das, Year: 2022, A Cheating Detection System in Online Examinations Based on the Analysis of Eye-Gaze and Head-Pose, THEETAS, EAI, DOI: 10.4108/eai.16-4-2022.2318165

[8] Dr. Mohammadreza VALIZADEH, "CHEATING IN ONLINE LEARNING PROGRAMS: LEARNERS' PERCEPTIONS AND SOLUTIONS", TOJDE, January 2022, ISSN 1302-6488, Volume: 23, Number: 1, Article 12

[9] Chaitanya Thombare, Kushank Sapate, Aniket Rane, Ankush Hutke, "Exam Proctoring System," DOILink: https://doi.org/10.22214/ijraset.2022.42229

[10] Bashar H. Asker, Ahmad F. Al-allaf, "Detecting cheating in electronic exams using the artificial intelligence approach," International Journal of Mechanical Engineering, Vol.7 No.2 (February, 2022)

[11] Genemo, M.D. Suspicious activity recognition for monitoring cheating in exams. *Proc.Indian Natl. Sci. Acad.* **88**, 1–10 (2022). https://doi.org/10.1007/s43538-022-00069-2

[12] Li Zhao, Haiying Mao, Brian J. Compton, Junjie Peng, Genyue Fu, Fang Fang, Gail D. Heyman, Kang Lee, Academic dishonesty and its relations to peer cheating and culture: A meta-analysis of the perceived peer cheating effect, Educational Research Review, Volume 36, 2022, 100455, ISSN 1747-938X, https://doi.org/10.1016/j.edurev.2022.100455.

[13]Kaddoura, Sanaa, Vincent, Shweta, Hemanth, D. Jude, Computational Intelligence and Soft Computing Paradigm for Cheating Detection in Online Examinations, *Applied Computational Intelligence and Soft Computing*, 2023, 3739975,23 pages, 2023. https://doi.org/10.1155/2023/3739975

[14] Yan Zuo et al., "Cheating Detection in Examinations Using Improved YOLOv8 with Attention Mechanism", Journal of Computer Science 2024, 20 (12): 1668.1680, DOI: 10.3844/jcssp.2024.1668.1680

[15] Hu, Z.; Jing, Y.; Wu, G.; Wang, H. Multi-Perspective Adaptive Paperless Examination Cheating Detection System Based on Image Recognition. Appl. Sci. 2024, 14, 4048. https://doi.org/10.3390/ app14104048.

****

