Suspicious Activity Detection in Online Exams

Prof. Trupti Rajput[1], Rutuja Sandip Gangane[2] ,Rutuja Rajabhau Kadu[3] , Rashmi Vilas Yeole[4], Dhanashri Ramdas Gaikwad[5]

Dept. of Computer Engineering, Siddhant College of Engineering, Maval, Pune, Maharashtra 411062

Abstract- **The rise of online exams has made it necessary to ensure their integrity and fairness. This project focuses on detecting cheating during online examinations without the need for physical supervision. Our goal is to develop a system that can analyze video feeds of exam takers in real time to identify any suspicious activities that may indicate dishonest behaviour. We will collect data from video streams, which will be processed to detect any suspicious actions. Using advanced techniques like o ensure exam integrity, including PHP for web development, Flask for proctoring, and YOLOv8 for real-time person detection. which are effective for understanding sequences of events over time. Additionally, Support Vector Machines (SVM) and Random Forest algorithms will be used for analysing structured data, providing reliable models for identifying abnormal behaviour. Hidden Markov Models (HMM) will be utilized to monitor audio data, capturing any verbal cues that could suggest cheating. To build this system, we will use programming languages such as Php, Mysql and Html,Css, JavaScript, along with frameworks like flask and OpenCV. Our methodology includes several steps: data collection, preprocessing, feature extraction, model selection, real-time detection, and rigorous training and testing of the models. Ultimately, this project aims to ensures a secure online examination environment by integrating advanced monitoring technologies. The combination of PHP, Flask, and YOLOv8 enhances security, making cheating difficult. Future enhancements could include AI-based behavior analysis and voice detection.**

I. INTRODUCTION

The paper "Suspecious Activity Detection in Online Exams" seeks to uphold academic honesty in the increasingly digitalized world of online assessments. With the shift towards virtual exams, the risk of academic misconduct has become more prominent. This solution leverages machine learning and computer vision to monitor various indicators like student attention, video feeds, and keyboard usage, enabling the detection of activities that might signal cheating or unauthorized assistance. By creating a secure online exam environment, the project aims to strengthen the credibility of digital assessments, ultimately fostering a trustworthy and fair online education space. With online education's rise, maintaining exam integrity without physical invigilation is challenging. In order to foster a controlled and equitable exam environment, this work proposes a real-time monitoring system that employs auditory cues, video, and keystroke tracking to identify suspect activity and notify examiners.

The necessity for a reliable and effective online exam system is what motivates the idea. As remote exams become standard in many institutions, preventing dishonest behaviors without physical supervision remains a challenge. Traditional methods like live video proctoring require considerable resources and may not always be effective. By developing an automated, real-time monitoring system that recognizes anomalous activity.

II. LITERATURE SURVEY

A deep learning-based framework for detecting anomalous exam behavior, notably cheating and misconduct, is presented in this work [1]. The suggested technique analyzes students' odd online behavior by extracting keyframes from a video stream or sequence based on human motion. To identify instances of cheating, deep learning models, pre-trained models, such as YOLOv5, and a proposed CNN are used. By analyzing the video, the proposed system [2] finds unusual behaviors like fighting, stealing, abuse, etc. that deviate from typical or expected behavior. The video frames are quickly divided into two categories: those with human activity and those without. The proposed system is applied to 11 classes of abnormal behaviors and has a very high degree of applicability in recognizing and classifying aberrant behavior. Nowadays, security officers are notified via CCTV (Closed Circuit Television) cameras when there is any malfunction or unusual activity. Stealing, violence, and explosions are examples of abnormal behavior. To help detect crime and improve public safety, CCTV cameras are installed in public areas such as parks, city streets, and neighborhoods. A number of approaches for detecting aberrant activity under deep learning and the handmade approach are explained in this study [3]. Modern surveillance systems need to be clever in order to automatically detect strange behavior in both public and private settings. Due to the industrial 4.0 revolution, intelligent algorithms based on machine learning and deep learning are becoming increasingly important in the current decade. These algorithms provide efficient performance in a variety of applications, surpassing automatic detection and identification. This study [4] primarily looks at the numerous intelligence algorithms that are used to effectively identify aberrant activity through surveillance, as well as their main benefits, drawbacks, and contributions to a range of applications. By using the browser to access the candidate's device's microphone and video stream, this system [5] offers real-time detection of suspicious occurrences including the presence of another person, the use of an electronic device, or the candidate's absence status. Using cutting-edge deep learning algorithms, the cheating detection system can identify candidates who are not present, electronic device use, speech activity, and candidate absence status. This article [6] introduces relevant research on the analysis of anomalous human behavior, including numerous cutting-edge real-world initiatives. The benefits and drawbacks of the three human target detection techniques are then examined. The inter-frame difference method is used in the design of the detecting process. Area identification, feature extraction, abnormality assessment, and a clear summary of the algorithm stages are the three areas from which a specific realization is finally suggested. In order to address the authentication issue and anticipate exam cheating, we present a Proctoring of Online Test (POT) model in this paper [7] that is based on an embedded system that integrates artificial intelligence algorithms. The system's capacity to automatically and continually monitor in real time during the online exam is its main feature. Paper [8] focuses on features including voice-to-text detection, eye tracking, face spoofing, mouth opening detection, phone and person detection, and number of people detection. The proposed system collects, processes, and trains a face key point model using the Dlib library's model, which recognizes 68 facial key points. The suggested approach, which uses a webcam and microphone for automated proctoring, performs better than current systems when tested in an online test environment. The system that is suggested with e-Parakh [9] , candidates can take the test online using a mobile app, which drastically lowers the amount of resources needed and, consequently, the candidate's expenses. Through a number of methods, such as live video and audio streaming of the candidate and their surroundings, a liveliness check, a facial comparison with their photo, and more, the application also makes it easier to administer the test remotely under supervision or without it. This application allows the assessor to record the entire video and audio of the candidate's activities, allowing them to cross-check their performance at any point during the test and after. Using a camera, the authors of the paper [10] used many modalities to identify the student's activities during the online test and reported the suspected student to the proctor. These modalities include eye-gaze estimation, object detection, and head-pose. To verify the efficacy of suggested solution, 29 students participate in a total of four exam sessions for testing and evaluation.

III. MOTIVATION

The primary motivation behind this project is the need for a secure and reliable online examination system. As online education becomes the norm, many institutions are conducting exams remotely, which presents the challenge of ensuring that students do not engage in unfair practices. Traditional methods of online proctoring, such as live video supervision, can be resource-intensive and may not always be effective. Therefore, the motivation of this project is to create an automated system that can provide accurate and real-time detection of abnormal behaviors during online exams, making online education more credible. -19 pandemic, online exams have become a standard practice for assessing students. However, the absence of physical supervision poses significant challenges in maintaining the integrity of these exams. Students may resort to dishonest practices such as using unauthorized materials or getting help from others during the exam. Our motivation is to create a system that can automatically monitor students during online exams and detect any cheating behavior without the need for a physical proctor. By ensuring fair practices, we can enhance the credibility of online assessments and support educational institutions in maintaining academic integrity.

PROBLEM STATEMENT

The problem addressed by this project is the inability to ensure that students are not cheating during online exams without the physical presence of invigilators. Cheating behaviors such as using multiple devices, switching between applications, or getting help from another person can compromise the integrity of the exam. The goal is to create a system that can detect these behaviors in real time using various data sources like video, keystrokes, and audio, ensuring that online exams are conducted fairly. The challenge faced in online examinations is the lack of supervision, which can lead to various forms of cheating. Students may engage in activities such as looking up answers online, using notes, or receiving assistance from others.

The existing monitoring systems often rely on manual oversight, which is impractical for large-scale examinations. This project addresses the problem of detecting abnormal activities in online exams by creating an automated system that utilizes video analysis and machine learning techniques to ensure that examinations are conducted fairly and with integrity.

IV. SYSTEM ANALYSIS

The system architecture consists of several modules that work together to detect abnormal activities. Each module performs a specific task, such as capturing video data, analyzing keystroke patterns, or monitoring audio. The architecture of the system consists of various components that work together to detect abnormal activities.

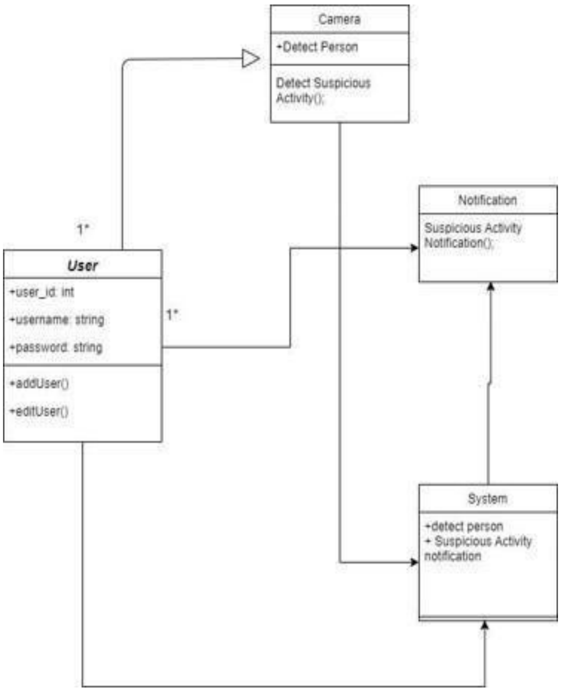

Figure 1.1: system Architecture

V. MODULES

5.1 Admin Module

Secure login for administrators. ItCreate and manage courses. It Add students, assign them to courses, and set credentials. It Add multiple-choice questions (MCQs) to exams and link them to courses.

5.2 Student Module

Students authenticate with email and password.Displays available exams and allows students to take them.Includes real-time proctoring and activity monitoring.

5.3 Image-Based Proctoring (Flask + YOLOv8)

The system captures a frame from the student's webcam every 5 seconds.The frame is sent to a Flask server where YOLOv8 processes the image.The model detects if no person or multiple persons are present.If a violation is detected, a warning is issued.If a student receives 5 warnings, their exam is terminated.

5.4 Mouse and Keyboard Activity Monitoring

JavaScript monitors user activity within the exam page.Detects tab switching, mouse movement outside the exam window, and keyboard usage unrelated to the exam.Unauthorized actions trigger a warning.

5.5 Deployment

The PHP web application is hosted on a server to ensure accessibility.The Flask server is deployed separately and communicates with the PHP system.The YOLOv8 model runs on the Flask server for real-time monitoring.

VI. CONCLUSION

The implementation of an Suspicious Activity Detection System for online exams represents a significant advancement in maintaining the integrity of digital assessment environments. By leveraging deep learning techniques, specifically the combination of Convolutional Neural Networks (CNNs) and YOLO (You Only Look Once networks, the system is capable of analysing real-time video feeds to identify behaviours that may indicate cheating or misconduct. Through extensive data collection and preprocessing, the CNN model effectively extracts spatial features from individual frames, while the YOLO model analyses the temporal sequences of these features to discern patterns of behaviour over time. This dual approach ensures a robust detection mechanism, minimizing false positives and providing educational institutions with a reliable tool for online proctoring.

The system's design prioritizes usability and efficiency, enabling seamless integration into existing online examination platforms. By providing educators and institutions with the ability to monitor students in real-time, this project contributes to enhancing academic integrity and fostering a fair assessment environment.

Future work may involve refining the model to adapt to diverse examination settings and incorporating additional data sources for improved accuracy. Furthermore, addressing ethical considerations and privacy concerns will be crucial in ensuring the responsible deployment of such technologies.

In conclusion, the development of this abnormal activity detection system not only showcases the potential of deep learning in educational settings but also lays the groundwork for future advancements in automated monitoring and analysis, making online assessments more secure and trustworthy.

REFERENCES

[1] A. A. Al-Halabi, Y. H. Al-Badawi, and N. H. Al-Sharif, "Real-Time Abnormal Behaviour Detection in Surveillance Videos Using Deep Learning," IEEE Access, vol. 9, pp. 51093-51105, 2021. DOI: 10.1109/ACCESS.2021.3064004.

[2] P. Zhang, Y. Zhan, and X. Wang, "A Novel Deep Learning Model for Abnormal Activity Detection in Surveillance Systems," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 357-372, 2021. DOI: 10.1109/TIFS.2020.3027754.

[3] R. K. Gupta, A. Kumar, and P. Singh, "Deep Learning for Action Recognition: A Survey," IEEE Access, vol. 8, pp. 106889-106906, 2020. DOI: 10.1109/ACCESS.2020.3001237.

[4] H. Zhang, Z. He, and W. Li, "Real-time Abnormal Behaviour Detection Using Convolutional Neural Networks," IEEE Transactions on Multimedia, vol. 22, no. 2, pp. 405-416, Feb. 2020. DOI: 10.1109/TMM.2019.2926876.

[5] C. Chen, H. Yu, and L. Zhang, "An Efficient Method for Abnormal Behaviour Detection Using 3D Convolutional Neural Networks," IEEE Transactions on Neural Networks and Learning Systems, vol. 32, no. 5, pp. 2046-2057, May 2021. DOI: 10.1109/TNNLS.2020.2982204.

[6] F. Wang, J. Zhang, and W. Chen, "An Enhanced Video-Based Abnormal Behaviour Detection Framework Using Deep Learning Techniques," IEEE Transactions on Cybernetics, vol. 52, no. 4, pp. 2357-2369, April 2022. DOI: 10.1109/TCYB.2021.3057065.

[7] M. G. K. Alzahrani, A. Alhassan, and H. R. F. Alsharif, "Combining Optical Flow and CNNs for Abnormal Behaviour Detection in Surveillance Videos," IEEE Access, vol. 9, pp. 50290- 50301, 2021. DOI: 10.1109/ACCESS.2021.3061778.

[8] X. Wang, H. Lu, and Z. Wu, "A Survey of Deep Learning Techniques for Abnormal Behaviour Detection," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 51, no. 3, pp. 1779-1792, March 2021. DOI: 10.1109/TSMC.2020.2978310.

[9] M. J. B. W. Uddin, A. S. Hossain, and M. A. K. Sarker, "Anomaly Detection in Videos Using Convolutional Neural Networks and Temporal LSTM Networks," IEEE Transactions on Image Processing, vol. 30, pp. 112-126, Jan. 2021. DOI: 10.1109/TIP.2020.2980654.

[10] Y. Zhang, J. Jiang, and T. G. H. Kwan, "Video Abnormal Event Detection Based on Patio-Temporal Feature Learning," IEEE Transactions on Circuits and Systems for Video Technology, vol. 31, no. 4, pp. 1302-1315, April 2021. DOI: 10.1109/TCSVT.2020.2988760