Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 3, 3929 – 3941

Cloud based LMS Security& Exam Proctoring Solution

Paramita Chatterjee[1] [0000-0001-7989-3574],
Department of Computational Science, Brainware University, India,
Rajesh Bose[2] [0000-0002-0967-455X],
Department of Computational Science, Brainware University, India,
Subhasish Banerjee[3] [0000-0003-1920-1913]
National Institute of Technology, Arunachal Pradesh, India
Sandip Roy[4] [0000-0002-5447-803X]
Department of Computational Science, Brainware University, India,

Abstract

These days, education is rapidly expanding, and each of its core procedures and techniques is rapidly altering. The global education system is transitioning to a cloud-based learning model. Educational institutions have no choice but to use cloud-based learning when the socioeconomic situation is dire, such as during a global epidemic. Because of its adaptability, variety, user acceptance, economics, and structure, cloud-based learning methods are becoming heavily dependent on the future of the worldwide education system. Learning from home and then taking online tests is the latest craze in education and its evaluation culture in this Covid-19 pandemic situation. It is, of course, a preventative strategy to avoid disease infection. Proctoring has become a new difficulty in this Learning Management System (LMS) era, as online tests have become the new trend. In this next stage of education's scalability, the opportunity to completely proctor remote online tests is a critical limiting issue. The most common technique of assessment is human proctoring, which entails either requiring examinees to visit the examination center or observing them visually and vocally throughout exams through a webcam. However, such methods are time consuming and costly. Internet proctored tests are commonly employed in all kinds of academic education and skills. In proctored online assessment verification, authorization, and operational management, modern technology is critical.The study conducts literature review to better understand academic fraud and the security mechanisms in place to combat it. This study goes on to depict a paradigm for proctoring virtual exams in different universities based on contextual factors. The proposed proctoring framework can offer universities with preliminary recommendations for implementing online exams.

Keywords : LMS, Cloud Computing, Online Proctoring System, Virtual Reality, Dynamic Learning, academic integrity, operational security, information security, authentication, visual analytics

Introduction

The CORONA virus outbreak in 2019 has heightened awareness of digital teaching and learning, that's been on the upswing for some time.Most of these online courses also incorporate online assessment activities, which poses a lot of concerns and challenges in terms of plagiarism and overall academic integrity. Utilization of online proctoring solutions for online tests is one method to deal with some of these issues.The use of virtual tools for measuring students' progress during evaluations is known as online proctoring. As they continue to resolve their limitations, the technology has the ability to enable students to participate an online assessment from a distant location while assuring the safety (security and reliability) and trustworthiness of the online exam [1].This includes securing and preserving the standards of an exam and its management by authenticating the student and their identity. Educators who are actively engaged in online education are worried about the protection of eLearning technology and online examinations [2]. According to certain estimates, the global eLearning business has surpassed the $100 billion mark. As the shift to online education progressed, the security risks of virtual learning technology became more obvious and raised greater concerns, particularly about privacy and integrity

issues.There are two primary components to online proctoring. To begin, turn on a webcam on the student's computer to video capture the real learning environment including everything the student accomplishes during the exam session [3].This video footage can be monitored remotely by the examiner or proctor. The examiner or proctor can identify potential cheating, suspicious actions, and attitude, such as speaking to someone in the room or checking for answers in a booklet, smart phone, or other printed media [4].The second option is lockdown, which prevents students from accessing any other computer software, along with the Internet browser, as well as user-computing procedures (such as copying, pasting, or printing), which could lead to exam cheating. This study's author aims to create a multimodal intelligence system that can also provide for exam continual online proctoring system (OPS).The general purpose of this system is to ensure exam academic integrity by offering real-time proctoring in order to catch the bulk of test taker cheating behaviours.

The sections of the research work are as follows: Section 2 covers Cloud Based LMS Security and Online Exam Proctoring System in detail. Section 3 went over all of the connected works that have been published to date by reading a lot of related publications and researches. Section 4 discussed the proposed works and methodology in detail, with the best explanations possible. Result Analyses were briefly discussed in Section 5. Finally, Section 6 describes the Conclusion and Next Steps.

Cloud Based LMS Security and Online Exam Proctoring System

The cloud system, also known as cloud technology, is a specific technological method that allows members to engage in virtual learning or e learning sessions via an internet connection from any location at any time [2]. Cloud computing and e-learning work together to create a virtual space where students and faculty or learners can exchange ideas. In today's world, the educational system has been totally changed into a digital paradigm, with cloud-based learning management systems serving a key role in improving system optimization, cost reduction, reliability, and stability. Various types of cloud computing are advancing at breakneck speed all around the world. Figure 1 depicts the various levels of services supplied by cloud computing service providers.

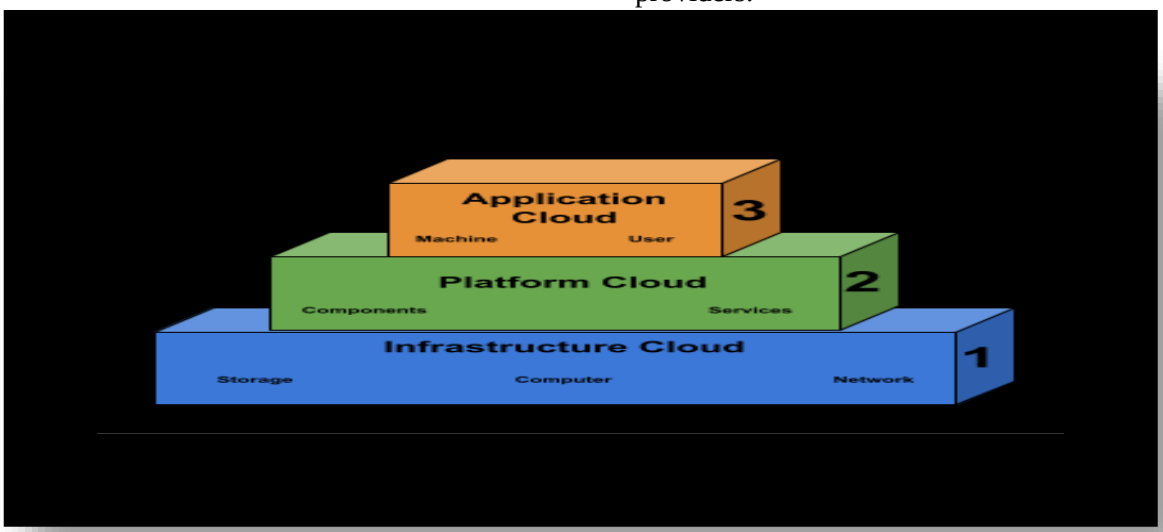

Fig. 1. Cloud computing Services [2]

LMS stands for learning management system, so it is platform that allows an e-learning platform run smoothly. Students acquire knowledge and skills using the internet as a tool. It gives instructors or mentors a way to evaluate pupils by giving them online exams and evaluating the outcomes [2]. The focus of the LMS is mostly on rapidly changing information technologies. Security, appropriate equipment, infrastructure, price, quality, and accuracy are just a few of the technological challenges that users or learners

face. As a consequence, the user's technological learning becomes a problem.Users can access a large and diverse database through the internet thanks to this cloud-based technology. A data storage center and its related management system are now unavoidable because users are continuously dealing with massive amounts of data. The infrastructure is made up of storage devices, software, physical interfaces, and a communication network. In this cloud service paradigm, there are three types of participants. The three groups are solution provider, programmers, and end users. Maintenance and monitoring of the service, as well as the infrastructure components, are the responsibility of service providers.Programmers are in charge of providing end users with infrastructure-based services. End users use the full range of cloud service functionalities to perform personal and corporate tasks from a number of places over the internet. There is a big security risk now that multiple customers are using the same platform in a cloud service. Because the cloud computing system is reliant on a number of technicalities, there are a number of security-level protocols, such as SaaS, PaaS, and IaaS, that efficiently manage the security system. The dangers connected with cloud-based LMS are listed in Table 1.

Threats and other issues associated with Cloud Based LMS				
Data Privacy	Internet	Application	Personal Devices	CCE
Malfunctioning Loss Copying Quality Availability	Availability Traffic Service	Technology Infrastructure Service	Infected old devices Malware Hacking	Data Storage IT Infrastructure Cost

Table 1. VariousThreats [2]

Learning platforms are vulnerable to the same kinds of flaws that affect all information systems. Among the tactics used include XSS (Cross-Site Scripting), SQL code injection into internet sites, malware as well as worms, trojan files, computer hacking, and others [1].The CIA triad (confidentiality, integrity, and availability) as well as additional security elements like evidence of identification, remote access, approval, financial analysis, command, non-repudiation, and monitoring of online examination processes constitute the cornerstone of a reliable Online Proctoring System (OPS).To achieve these goals, administrative, technological, and physical controls might be applied. Basic security principles can be applied to LMS and OPS in general (privacy, reliability, availability, integrity, operational procedures, and so on). Breach of access control and data (information) "leakage," for instance, are also both violations of confidentiality. Plagiarism and theft are both attempts to undermine one's credibility. Availability attacks on OPS are denial of service attacks.The removal of exam logs and video recordings before they are completed is an attack on accountability [1]. Integrating online proctoring with the other applications could lead to security flaws. It can be obtrusive if an OPS is established on an independent platform or a generalized LMS platform, for example. The LMS may include sensitive or confidential information that must be protected (for instance, learner profiles and proprietary learning content). In addition, to expand functionality, current LMS are linked to additional third-party software tools like cloud-based lab projects (for instance, short movies, hacking simulators, short writings, questionnaires), plagiarism checking, and so on.Security capabilities and additional controls are necessary for security problem identification, protection, detection, enquiry, mitigating, response, and documentation in

order to remove or mitigate the impact of these vulnerabilities. The "leakage" of examination content is another key problem for teachers. Screen scanner (holders) can capture an image and store it as a PDF file, even if a word cannot be copied and pasted.The PDF file can be converted into editable text utilizing optical character recognition (OCR) software. By preventing screen scanners, security mechanisms, on the other hand, can prohibit it. Data leakage can take several forms, including access to preliminary studies' content, a proxy impersonating the users, the use of fake identity, a breach of the students' records' integrity, and so on. Other forms of content theft, including such "Brain Dumping" (memorizing examination content using human memory) ,use of hidden cameras to duplicate exam materials, are more difficult to detect. Static, repeated passwords are the most common method of user authentication. It has a number of flaws that are well-known. Technologies like such a one-time password may be able to help large-scale OPS. Authentication systems based on challenge-response are regularly investigated by small-scale OPS developers. Traditional one-time authentication mechanisms used in face-to-face examinations are inadequate for a secure OPS.A test-taker may have to be re-authenticated continuously or on a frequent basis all through the examination in OPS to identify a proxy impersonation. The way to manipulate behavioral indications is another differentiator. During face-to-face assessments, the proctor observes the student's behaviour visually, whereas computer activities are normally unmonitored. A webcam is a popular and effective tool for observing and recording activity. Screen-sharing technology as well as a keyboard listener application can be used to manage user activity on the computer. Dual surveillance distinguishes two types of theft: illegal money transactions and unlawful behavioral conduct (fake identity, multiple computers, books).The behavioral behaviours could be observed in real time or asynchronously (as a preventive measure) (as a detective measure, after-exam recordings are viewed). The three types of online examination proctoring are available through a variety of online proctoring platforms. However, universities in the procedure of selecting and deploying an OPS should evaluate following considerations first are depicted in table 2:

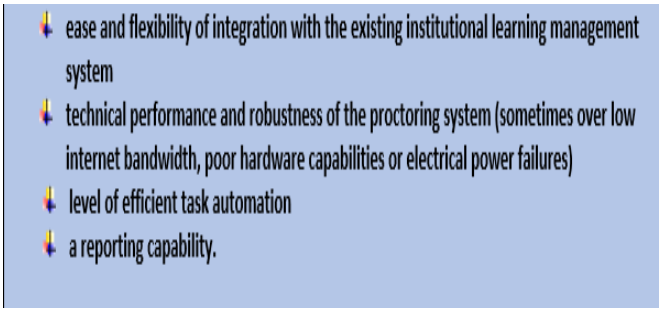

Table 2 Features of OPS [5]

Confidentiality and administration, security and anti-fraud procedures, and their associated expenses are all important aspects to consider when implementing an online proctoring system. Table 3 shows the characteristics of each of the several systems:

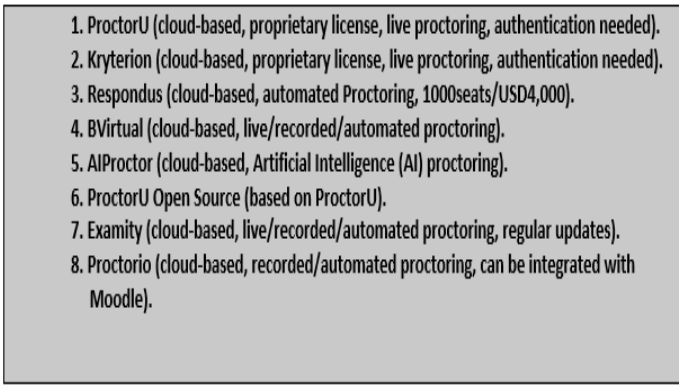

Table 3 Capabilities of each of different OPS **[5]**

Two well-known technologies, Xproctor and ProctorU, can be used to combat different fraud. Xproctor (n.d.) authenticates students and tracks their participation over time using facial recognition, behaviour video-streaming, speech, and photography technology.Xproctor simplifies synchronization with the LMS (Canvas, Blackboard, Moodle, Desire2Learn), offers a limitless quantity of photo captures, screenshots per test, and video capture time when installed on the user's computer (Windows or Mac OS).ProctorU (n.d.) offers an AI-based autonomous OPS that can be used separately or in tandem of Pearson's MyLab product line. The fully automated solution includes multivariate regression identity verification (includes ongoing biometric authentication), video capturing, and AI-powered behaviour analysis.

The basic architecture of such an OPS and an exam room shows users (test-taker, proctor, and unauthorized collaborator), unauthorized information sources, WIFI device, computing devices, and data storage (Fig. 2 **).**

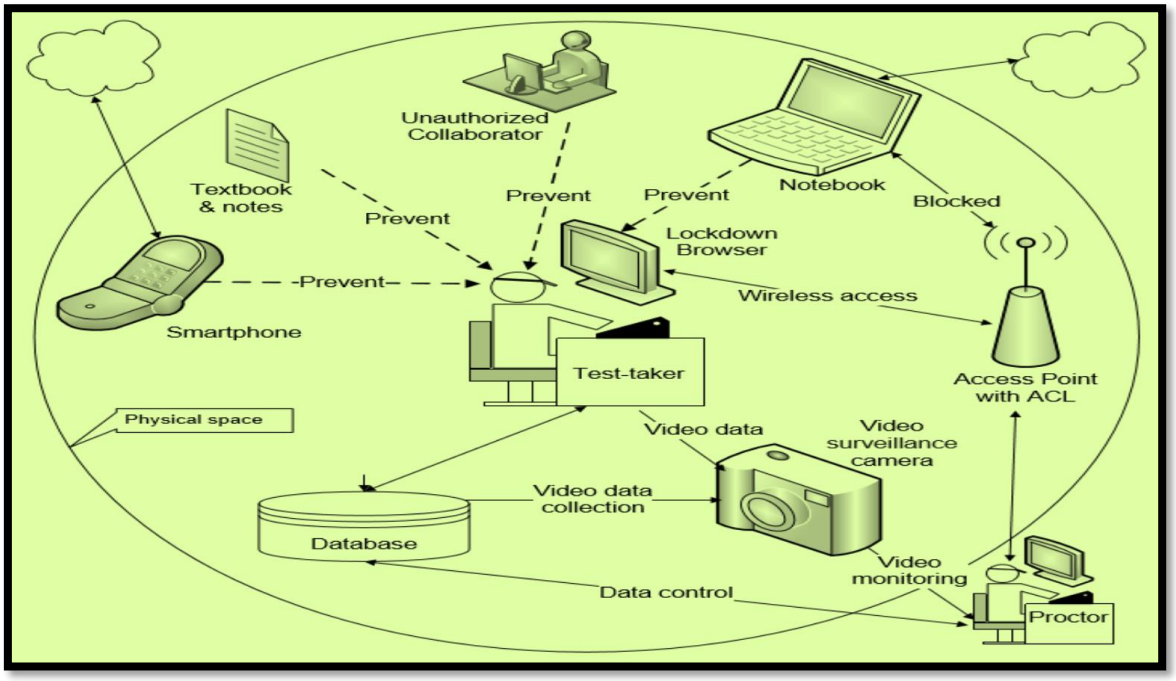

Fig. 2. Online proctoring system [1]

Related Work

Following an examination of several studies and papers on the subject, it was determined that ongoing research and studies are being conducted to increase the accessibility of cloud-based LMS while preserving optimum security in OPS. The perspectives of certain papers and studies are presented below.:

According to paper [1], online proctored exams are commonly employed in all types of professional and academic training. AI with Machine Learning technology can assist mitigate the cybersecurity vulnerabilities of online proctoring systems by enabling identification, authorization, and effective control of proctored online exams, and also maintaining administrative, physical, and technological controls (OPS).In article [2,] a secure loopback connection structure is examined and attempted, which blocks access to every webpage,after an encrypted channel to the primary approach for monitoring software deployments has been established.In paper [3,] a multimodal analytics method for intelligent online test proctoring is presented. Webcams, wearcams, and microphone are needed in the system hardware for monitoring the visual and auditory environment of the testing area.The paper [4] proposes an online test system based on the landmark features of South African universities. The suggested scheme can offer universities the basic recommendations for implementing online exams. According to paper [5,] a slew of new online proctoring systems are hitting the market, promising to address some of the key issues. However, they have yet to be tried and proven on a wide basis. This comprises the service's pricing as well as its technical needs. This paper details one of several attempts to thoroughly assess a variety of these tools and make suggestions to educational institutions. One of the most significant difficulties facing online learning today is identity authentication and taking exams of online students.The training organizations must authenticate that the current learners who finished the educational process and obtained academic credits would be those who enrolled for the courses, associated with online quality assurance system. They must also guarantee that such students complete all of the online training exercises without cheating or engaging in improper behaviour. The COVID-

19 epidemic has hastened (in some cases, dramatically) the migration and deployment of online education initiatives, necessitating the development of secure mechanisms to verify as well as proctor online students. There are a variety of technologies available today, each with varying degrees of automation.Authors detail a particular proposal depending on the verification of various sensor authentication and an automated proctoring process (system workflow and AI algorithms) in article [6], which includes features to address the key problems.Paper [7] detects and visualizes alleged student body and mouse movements in three degrees of detail, allowing program instructors and teachers to proctor online tests in a convenient, quick, and trustworthy manner.The paper [8] examines user ratings of browser extensions used by proctoring providers and then conducts an internet questionnaire (n = 102).The goal of the paper [9] is to develop a web-based automated examination system that can detect and report harmful activities in order to verify that exams are administered fairly.The purpose of this study [10] was to use a readability evaluation approach that also included five usability criteria on the students' learning platforms, along with LMS software recommendations, to identify the key myCourseVille interface issues.The research [11] looked into user happiness levels, as well as the importance of adopting a cloud-based LMS during pandemic circumstances and what factors should be used to improve user satisfaction.In paper [12], the behavioural goal of LMS inside a COVID setting is stated and investigated. It offers a moderated look at the adoption of e-learning with Corona Virus-affected students.The study [13] focused on cloud applications and its digital system technologies, including its advantages and disadvantages.The evolution of LMS as a service or product, as well as how it assists the educational system, was studied in research [14].The proposed cloud computing infrastructure based on LMSs for building a digital e-learning environment was investigated in this study [15].The author of [16] is attempting to develop a suggested e-learning architecture that will aid in the correction of the current cloud-based learning system's flaws. The five largest e-learning technologies discussed in this article are likely to gain in popularity as the proportion of students expands in the next years. To every single day, the population of e-learners increases, and there are only a few software packages, each with a set of benefits and drawbacks, with some systems being overly complicated.Cloud computing's key qualities, including its privacy and security, were covered in [17].The paper [18] explains the impact of the Covid-19 outbreak on Cloud Computing.

Various papers, spanning education systems, students, and teachers, have depicted the technical implementation and suitability of digital learning and exam proctoring systems in the twenty-first century. The LMS paradigm is discussed in several publications, covering course content, distribution, tracking, and technological augmentation, as well as usability, exam proctoring, and security analysis. In order to continue the investigation, a few relevant papers are investigated in this study.

Proposed work and Methodology

The goal of this project is to create a secure and web-based cloud-based LMS security and exam proctoring solution. Exams are an important part of any educational program, and online schools are no exception. Cheating is a possibility in each exam, so detecting and preventing it is crucial. In order to maintain their worth in society, educational qualifications must reflect actual learning. Exam data integrity require technical security safeguards. Computers, networks, data sources, software, and physical space all are impacted in some way. For online exam proctoring, there are two sorts of technical controls: static and dynamic. Fixed measures, such as user’s biometric data, do not change considerably during an examination and remain generally consistent.Dynamic controls are associated with operations that change over time, such as recording live photos and logging comprehensive information for a number of activities [1].OPS compatibility and connectivity with LMS are required. Any proctoring system should have the ability to record a test session.

- Simultaneous synchronous (real-time monitoring) and

- asynchronous (after test detection review) proctoring can be done with the recorded sessions.

  It's also possible to add video-streaming, image-capturing, and sound-capturing features.The purpose of gathering information on test-takers' computer behavioural patterns is to discover and log security incidents (which may indicate fraudulent activity) that occur when they depart from the standard online procedure.In the log file, "markings" are used to detect and note occurrences. The information gathered throughout the examination (including video streaming, images, audio, screenshots from the pupil's desktops) is saved and can be used for exam validation and storage.Within OPS, there are two types of technical controls in place: endpoint (computer-based) security protection and cheaters detection based on behaviour. A variety of procedures and strategies are used as controls for both.A computer security plan determines the amount of information protection for various groups (or responsibilities) of users, with the administrator community having the most control. Endpoint security prevents an authorized user (examiners) from accessing unauthorized system resources, programs, or keyboard operations that could jeopardize the integrity of the online exam.Hackers can access online proctoring systems, much as other university information resources. To minimize the effect of these assaults, organizations employ monitoring, preventative, and restoration mechanisms.It's also vital to keep in mind that students' technical (and basic hacking) skills are improving over time. As a result, a teacher's ability to assess a student's level of Capacity, Motive, and Opportunities and match it to the appropriate controls is crucial.The various online examination frameworks work with [4], assuming that students, examiners, and administrators would all fall into place naturally. As a result, the suggested online exam framework is made up with four modules, as shown infigures 3 and 4.
- **Authentication and continuous monitoring module** -The component enrolls, authenticates, and then keeps a real-time eye on the learner taking the exam for assistance and fraud detection.
- **Student enrolment and standardization**-The enrolment of factors or attributes that will be used in the identification process is required by the most of authentication mechanisms. These will be used as learner's sign when they access the virtual exam.This study suggests that multimodal biometrics be used for identity management. Fingerprints and facial detection software will be taken to verify learners' identities. Learners should also be informed of the recommended minimum connection speeds for sitting an online assessment. As a result, at this phase, testing will be performed to assess the whether internet connection in the student's immediate vicinity meets the acceptable minimum speed. As a result, determining a pupil's internet speed before to enrollment is crucial. Learners having slow internet speeds will be requested to choose a location where they may take the exam with the minimal internet connection required. An online exam should only be taken by people who have the required minimum network speed.Moreover, the learner's remoteposition should be automatically determined and recorded [4]. This information could be useful in cases of academic cheating or other administrative matters regarding learners who have reported about their environment.Students are entitled to features that allow them to alter their connection speed and geographic area if necessary. The information gathered in this stage should be delivered over a secured connection and stored in an encryption-oriented format.Students will log in with a username and password. Then there are testing for visual, audio, and bandwidth. The student then downloads, installs, and runs software that allows remote proctor to access the learner's computer and enables these webcam and microphone.In this time, a learnermay produce a form of identification and exhibit this to the online proctor withthe camera. These data on the given identificationcard should be compared with the data on this examination registration form by the remote proctor. To establish his or her identity, the student should use fingerprints

and facial detection technologies.The powerful authenticated system using an online proctor, fingerprint, and facial recognition can prevent impersonation and the entrance of banned material into the exam environment. Students' nervousness is expected to be reduced by the appearance of a remote proctor, allowing them to focus on their tests. Students can now write the exam while being monitored and terminated once they've been authenticated.Browsing tolerance is also taken account, which is the practice of restricting a student's ability to use their web browser for other purposes.

- **Continuous monitoring and termination** - This study recommends using true automating background sound assessments, face detection, time lag, and the head posture for ongoing observation. A distant virtual proctor, keyboard dynamic, question and challenge, biometric, or a mix of these approaches can be used to provide continuous monitoring.Throughout the exam, visual recordings taken with a camera may be used to do facial detection. The recordings may also be used for monitoring time lag and head movement while answering questions. Information from background sound assessments as well as the webcam should be pooled and supplied into a real-time exam cheating prediction algorithm.These strategies have been found to reduce the options of test fraud through this use of illegal material, impersonation, support, distant verbalcommunication, and whispering. Test cheating threat can be ranked so that if it's medium or high, an alert may be sent to a faraway proctor with immediate intervention.At this point, this faraway proctor can issue a caution to the learner or begin the exam termination process, ensuring those enough evidences have been collected. Similarly, technological defects must be evaluated with the possibility of cheating for taking appropriate actions. Once this test has been done, the learner can save and submit thisvirtual answer scripts.The whole examination is digitally recorded and made accessible to teachers or assessors for evaluation either immediately or later [5].
- **Phone Detection**---During the online exam, the usage of any type of mobile device is prohibited. As a consequence, the presence of a cellular phone in the test room may be a sign of suspected cheating. There are several ways to cheat now that mobile phone technology has advanced, including reviewing saved notes, mobile messaging friends, browsing the Web, and taking a picture of the examination to share with other students.Phone detection is tough due to the variety of sizes, types, and forms of phones (a tablet could always be regarded a kind of phone). Some test takers use large touch screens, while others use a flip phone with buttons. Furthermore, occlusions like as holding a phone under the table or shielding part of the gadget with their hand are regularly used when stealing on a phone [3].

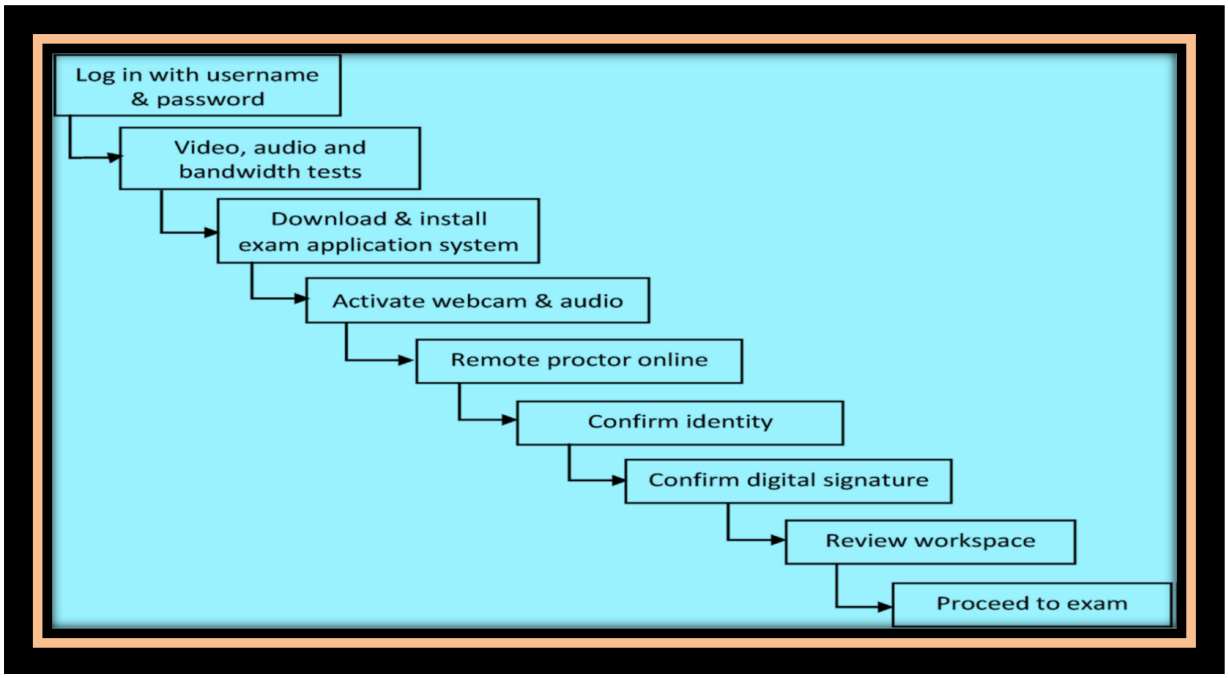

Fig. 3. Proper Authentication [4]

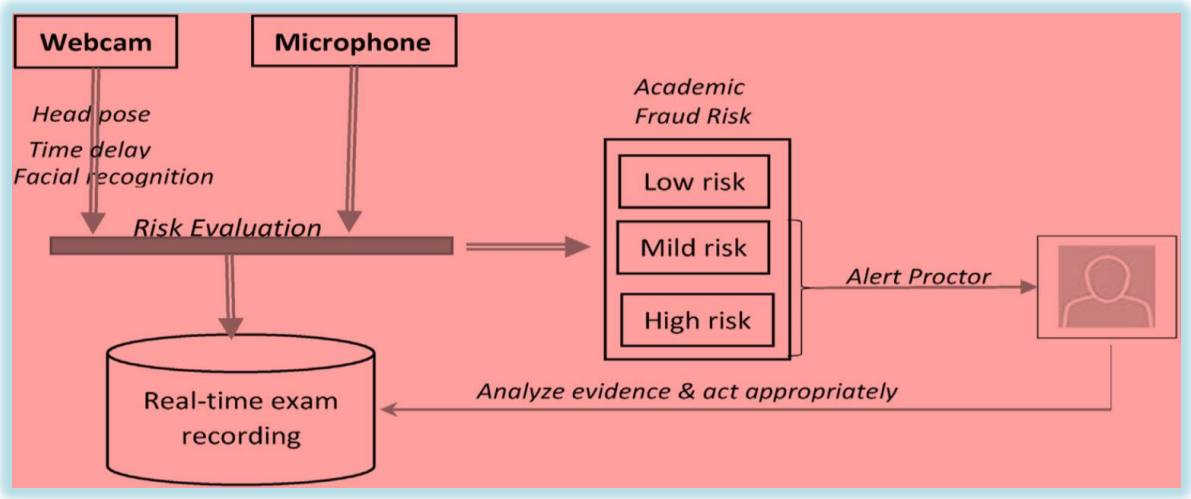

Fig. 4. Monitoring [4]

Result

In an online exam session, a multimedia diagnostic system is employed to detect a wide range of cheating actions. Warm-up and online-exam phases are included in the proposed online test process. Before commencing the exam, the examiner must authenticate himself using a password and facial authentication during the warm-up phase. Calibration steps are also included in this process to make sure that all sensors are attached and working properly. The examiner also learns and verbally accepts the OPS's regulations, such as no two people in the same room, the inspector not leaving the room during the test phase, and so on.The inspector takes the exam while being "monitored" by the OPS for genuine fraudulent behaviour detection during the online exam phase. The audiovisual cues of the test environment and examiner are captured using OEP system hardware (i.e., a webcam, wearcam, and microphone). To extract the distinct properties listed in table 4, the detected data is first analyzed using six components.

- user verification
- text detection,
- speech detection,
- active window detection
- gaze estimation, and
- phone detection

Table 4. Six Components

The higher-level features generated from these extraction characteristics within a temporal frame are then utilized to train and test a cheat classifier as seen in fig.5. Factor features, such as the quantitative variables within a window, and features based on component interaction, such as covariance features, are among the higher-level features [3]. Because the identification of some cheating activities requires the firing of many behaviour cues, it is critical to use a varied and extensive set of features to increase the OPS' overall detection effectiveness.

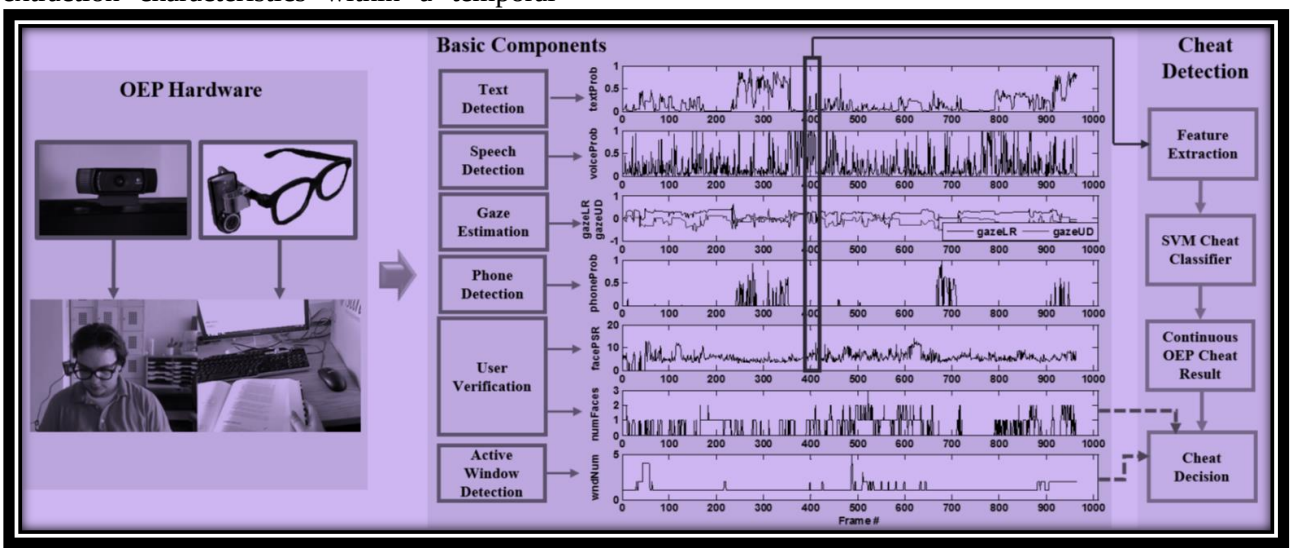

Fig. 5. Working features of the Online Proctoring system. [3]

Conclusion and Way Forward

In this case, where online learning is the only method to keep the entire school system running while the Covid -19 pandemic continues to spread over the globe, it is critical to have sufficient security measures in place to ensure safe log-in and access to the online medium. The best protocol for this is to change it. To keep the security and usability in mind, the author has tried to include a few elements of the Online Exam Proctoring System to allow for safe internet access and online education.

Reference

1. Slusky, L.: Cybersecurity of Online Proctoring Systems. Journal of International Technologyand Information Management: 29 (1),56-83(2020).

2.Chatterjee, P., Bose, R., Banerjee, S., Roy, S.: Enhancing Security of Cloud based LMS by deploying secure Loopback Protocol. International Journal of Mechanical Engineering. Vol. 7(1), 1474-1481(2022).

3.Atoum, Y., Chen, L., Liu, A., Hsu, S., Liu, X.: Automated Online Exam Proctoring. IEEE Transactions on Multimedia. 19(7),1-15 (2017).

4. Ngqondi, T.,Maoneke, P.,Mauwa, H.: A secure online exams conceptual framework for South African universities. Social Sciences & Humanities Open.Elsevier.3(1),1-12(2021).

5. Hussein, M.J.,Yusuf, J., Deb, A.S., Fong, L.,Naidu, S.: An Evaluation of Online Proctoring Tools. Open Praxis.12(4), 509–525(2020).

6.Labayen, M., Vea, R., Florez , J., Aginako, N., Sierra, B. : Online Student Authentication and Proctoring System Based on Multimodal

Biometrics Technology. IEEE Access. 9 ,72398-72411(2021).

7.Li, H., Xu, M., Wang, Y., Wei, H., Qu, H.: A Visual Analytics Approach to Facilitate the Proctoring of Online Exams. Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI ’21), May 8–13, 2021, Yokohama, Japan. ACM, New York, NY, USA, pp. 1-17 (2021).

8.Balash, D.G., Kim, D.,Shaibekova, D.: Examining the Examiners:Students’ Privacy and Security Perceptions of Online Proctoring Services. Proceedings of theSeventeenth Symposium on Usable Privacyand SecurityAugust 9–10,USENIX Association, pp.633-652.(2021).

9.Chandra M, N.,Sharma, P.,Tripathi, U.,Kumar, U.,BhanuPrakash, G. C.: AUTOMATING ONLINE PROCTORING THROUGH ARTIFICIAL INTELLIGENCE.International Research Journal of Engineering and Technology (IRJET).8(1),1894-1896 (2021)

10. Phongphaew, N., Jiamsanguanwong, A.: Usability Evaluation on Learning Management System. Proceedings of the AHFE 2017 International Conference on Usability and User Experience, July 17-21, 2017, The Westin Bonaventure Hotel, Los Angeles, California, USA, pp. 39-48. Springer (2018).

11. Pandey, D., Ogunmola, G.,Enbeyle, W., Abdullahi, M., Pandey, B.,Pramanik, S.: COVID-19: A Framework for Effective Delivering of Online Classes During Lockdown. Human Arenas,Springer 1-15(2021).

12. Raza, Syed A., Qazi, W., Khan, K., Salam, J.: Social Isolation and Acceptance of the Learning Management System (LMS) in the time of COVID-19 Pandemic: An Expansion of the UTAUT Model. Journal of Educational Computing Research. 59(2),183-208 (2020).

13. Aldheleai,H. F.,Ubaidullah,M,Alammari, A.,:Overview of Cloud –based Learning Management System,. International Journal of Computer Applications (0975-8887).Vol.162, No.11 , pp. 41-46 .DOI:10.5120/ijca2017913424 (2017).

14.Turnbull, D.,Chugh, R., Luck ,J.,: Learning Management Systems: An Overview,A.Tatnall (ed.), Encyclopedia of Education and Information Technologies. DOI: 10.1007/978-3-319-60013-0_248-1(2019).

15.Qwaider,W. , :A Cloud Computing Based Learning Management Systems (LMSs) Architecture. International Journal of Computing and Network Technology .Int.J.Com.Net.Tech.5, No. 2 pp. 51-58.ISSN(2210-1519 (2017).

.

16.Siddiqui,S.T.,Alam, S., Khan,Z. A.,Gupta A.:Cloud-Based E-Learning: Using Cloud Computing Platform for an Effective E-Learning.Proceedings of ICSICCS-2018. DOI:10.1007/978-981-13-2414-7_31(2018).

17. Brandao,P.R.: Cloud Computing Security.International Journal of Computer Science And Technology(IJCST). Vol.10,Issue 1, pp 26-32.ISSN: 0976-8491(2020).

18. Alashhab, R., Anber,M.,Singh ,M. M. ,Leau,Y,Al-Sai Z,Alhayja’a,S.A.,:Impact of coronavirus pandemic crisis on technologies and cloud computing applications.,Journal of Electronic Science and Technology.100059.ISSN: 1674-862X.Elsevier(2020).

19. Ajayi, A., Akai, S.: Effect of Cloud Based Learning Management System on The Learning Management System Implementation Process. SIGUCCS '19: Proceedings of the ACM SIGUCCS Annual Conference, pp. 176–179. ACM (2019).

20.Chatterjee, P., Bose, R., Roy, S.:A Review on Architecture of Secured Cloud Based Learning Management System .Journal of Xidian University 14(7), 365-376 (2020).

21.Kacha, L., Zitouni ,A., :An Overview on Data Security in Cloud Computing.Advances in Intelligent Systems and Computing 661,pp 250-260.DOI: 10.1007/978-3-319-67618-0_23.(2018).

22. Chatterjee, P., Mukherjee, S.,Bose, R., Roy, S.:A Review on Information Security in Cloud Based System during Covid -19 pandemic .Brainwave, Brainware University 2(1), 60-69 (2021).

23. Favale, T., Soro, F., Trevisan, M., Drago, I., Mellia, M.:Campus traffic and e-learning during Covid-19 pandemic. Computer Networks (2020).

24. Cornetto, G., Mateos, J., Touhafi, A. et al.:Design ,simulation and testing of a cloud platform for sharing digital fabrication resources for education. Journal of Cloud Computing 8(12) (2019).

25. Guo,Y., Mohamed, I., Abou-Sayed, O. et al.: Cloud Computing and Web Application Based remote real-time monitoring and data analysis : slurry injection case study, Onshore USA. Journal of Petroleum Exploration and Production Technology 9, 1225-1235 (2019).

26. He, G., Xu, B., Zhu, H.: AppFA: a novel approach to detect malicious android applications on the network. Security and Communication Networks. (2854728), 1-15 (2018).

27.KirangeS. , Dr. Sawai D.,: A Comperative Study Of E-Learning Platforms And Associated Online Activities, The Online Journal of Distance Education and e-Learning, 9(2),194 -199(2021).

28. Kabassi, K., Dragonas, I., Ntouzevic, A., et al.: Learning management systems in higher education in Greece: Literature review. 1-5. (2015).

29.Tan, C., Lin, J. A new QoE-based prediction model for evaluating virtual education systems with COVID-19 side effects using data mining. Soft Computing, Springer Nature,1-15 (2021).

30. Caballé, S.,Miguel M. J., JosepPrieto,. : Security in Learning Management Systems: Designing collaborative learning activities in secure information systems. Enhancing ICT education through Formative assessment, Learning Analytics and Gamification28, 1-3, Spain(2017).

31. Desai, V., Oza, K., Kamat, R.,: PREFERENCE BASED E-LEARNING DURING COVID-19 LOCKDOWN: AN EXPLORATION. The Online Journal of Distance Education and e-Learning, 9(2), 285-292 (2021).

32. Mohammadi, M.,Mohibbi, A., Hedayati, M., : Investigating the challenges and factors influencing the use of the learning management system during the Covid-19 pandemic in Afghanistan. Education and Information Technologies. Springer Nature,1-35(2021).

33. Ahmeda,F.R.A. ,.Ahmedb,T.E., Saeedc,R.A.,Alhumyanic,H.,et al.: Analysis and challenges of robust E-exams performance under COVID-19. Results in Physics. ScienceDirect Elsevier 23, 1-7 (2021).

34. Adzovie ,E. D., Jibril, A. B., Holm, R., Nyieku, I., :E-Learning Resulting from Covid-19 Pandemic: A Conceptual Study from a Developing Country Perspective. Proceedings of the 7th European Conference on Social Media ECSM Larnaca, Cyprus,pp.19-27 (2020).

35.Ferreira P., Antunes F.O., Gallo H., Tognon M., Pereira H.M. : Design Teaching and Learning in Covid-19 Times: An International Experience. In: Reis A., Barroso J., Lopes J.B., Mikropoulos T., Fan CW. (eds) Technology and Innovation in Learning, Teaching and Education. TECH-EDU 2020. Communications in Computer and Information Science, vol 1384. Springer, Cham pp. 263-278(2021).

36. Jandrić, P., Hayes, D., Levinson, P. et al. :Teaching in the Age of Covid-19—1 Year Later. Postdigital Science and Education. Springer Nature Switzerland AG 2021.pp.1-151(2021).

37.Huang, R., Tlili, A., Chang, TW. et al. :Disrupted classes, undisrupted learning during COVID-19 outbreak in China: application of open educational practices and resources. Smart Learning Environments, Springer open,7, 19 (2020).

Authors Profile

1. Paramita Chatterjee : Research Scholar of Computational Science Department of Brainware University,Kolkata,WestBengal,India.
Faculty of CharuChandraCollege,University of Calcutta,Kolkata,India.
M.Phil in Computer Science from The Global Open University,Nagaland.
M.Sc. in Computer Science from North Orissa University.
B.Sc . in Computer Science from University of Calcutta.

2. Dr.Rajesh Bose:Ph.D. (CSE),Postdoc (CSE), M.Tech, B.Tech

Associate Professor, Dept. Of Computational Science, Brainware University, 398 Ramkrishnapur Road,Barasat, Kolkata, West Bengal 700125, India.

Awarded PhD from the University of Kalyani following submission of doctoral thesis titled “A New Paradigm in Cloud Computing to Extend Multiple Services through a Common Gateway Based on Secure Virtualization”.

Total number of publications: 100,Publications in the Journals: 67 ,Publication in the International Conferences: 12,Book Chapters :8,Book Published by International Publishers:13

3. Dr. Subhasish Banerjee :National Institute of Technology, Arunachal Pradesh
Assistant Professor, Computer Science & Engineering
Ph.D: National Institute of Technology, Arunachal Pradesh, India
M.Tech : Indian Institute of Technology (ISM), Dhanbad, India
M.Sc : Indian Institute of Technology (ISM), Dhanbad, India
Research Areas:Computer Networks, Data Structure, Data
Base Management System, Algorithm Design and
Analysis, Cryptography

4. Dr. Sandip Roy :Ph.D. (CSE), Postdoc (CSE), M.Tech, B.Tech.
Associate Professor & Head of Department of Computational Science of Brainware University, Kolkata, West Bengal, India.
He has awarded his Ph.D. in Computer Science & Engineering from
University of Kalyani, India .
He has authored over 60 papers in peer-reviewed journals, conferences, and is
a recipient of the Best Paper Award from ICACEA in 2015. He has also
authored of six books and also granted two patents. His main areas of research
interests are Data Science, Internet of Things, Cloud Computing, and Smart
Technologies.