A Systematic Review on AI-based Proctoring Systems: Past, Present and Future

Article *in* Education and Information Technologies · September 2021

DOI: 10.1007/s10639-021-10597-x

4 authors, including:

Rhitvik Pasricha
Narsee Monjee Institute of Management Studies
2 PUBLICATIONS **84** CITATIONS

SEE PROFILE

Prathamesh Churi
Narsee Monjee Institute of Management Studies
78 PUBLICATIONS **635** CITATIONS

SEE PROFILE

Education and Information Technologies (2021) 26:6421–6445
https://doi.org/10.1007/s10639-021-10597-x

A Systematic Review on AI-based Proctoring Systems: Past, Present and Future

Aditya Nigam[1] · Rhitvik Pasricha[1] · Tarishi Singh[1] · Prathamesh Churi[2]

Received: 24 March 2021 / Accepted: 19 May 2021 / Published online: 23 June 2021

Abstract

There have been giant leaps in the field of education in the past 1–2 years.. Schools and colleges are transitioning online to provide more resources to their students. The COVID-19 pandemic has provided students more opportunities to learn and improve themselves at their own pace. Online proctoring services (part of assessment) are also on the rise, and AI-based proctoring systems (henceforth called as AIPS) have taken the market by storm. Online proctoring systems (henceforth called as OPS), in general, makes use of online tools to maintain the sanctity of the examination. While most of this software uses various modules, the sensitive information they collect raises concerns among the student community. There are various psychological, cultural and technological parameters need to be considered while developing AIPS. This paper systematically reviews existing AI and non-AI-based proctoring systems. Through the systematic search on Scopus, Web of Science and ERIC repositories, 43 paper were listed out from the year 2015 to 2021. We addressed 4 primary research questions which were focusing on existing architecture of AIPS, Parameters to be considered for AIPS, trends and Issues in AIPS and Future of AIPS. Our 360-degree analysis on OPS and AIPS reveals that security issues associated with AIPS are multiplying and are a cause of legitimate concern. Major issues include Security and Privacy concerns, ethical concerns, Trust in AI-based technology, lack of training among usage of technology, cost and many more. It is difficult to know whether the benefits of these Online Proctoring technologies outweigh their risks. The most reasonable conclusion we can reach in the present is that the ethical justification of these technologies and their various capabilities requires us to rigorously ensure that a balance is struck between the concerns with the possible benefits to the best of our abilities. To the best of our knowledge, there is no such analysis on AIPS and OPS. Our work further addresses the issues in AIPS in human and technological aspect. It also lists out key points and new technologies that have only recently been introduced but could significantly impact online education and OPS in the years to come.

Keywords AI · AIPS · Artificial Intelligence · Exams · Online proctoring · Online learning · Proctoring system

Extended author information available on the last page of the article

1 Introduction:

Over the last few years, online education has advanced rapidly. More students are taking advantage of Massive Open Online Courses (MOOCS) and other online certificate courses. Colleges are also transitioning online to provide more resources to their students. There has also been a rise in individuals rolling out their courses. All of this gives students more opportunities to learn and improve themselves. (Li et al., 2015).

In the past year, during the pandemic situation, almost all educational institutions have been forced to transition to an online education form (Moreno-Guerrero et al., 2020). Colleges started taking classes and tests online, for courses in all fields. The COVID-19 Pandemic also affected entrance exams and the hiring process, which filters students by taking a written test. We acknowledge that maintaining academic discipline and the sanctity of testing in the exams is imperative. This sudden shift to online learning has different effects on students of each level. One cannot expect the same level of seriousness and focus from a graduate-level student and a school student. Each student would have their learning, understanding, and information retaining capabilities. In this situation, malpractice during academic work would be on the rise, be it in the form of plagiarism or cheating during tests. We believe the implementation of an Artificial Intelligence Based Proctoring System (AIPS) is the need of the hour. We also believe that it would soon become the norm to use such systems for continuous monitoring for digital exams, ranging from MOOCs to exams taken during hiring. The quality of one's online certificate is dependent directly on the quality of the testing process that one undergoes to obtain it.In the same way that exams would be monitored when taken in schools and colleges, they need to be proctored when being conducted online. An AIPS is needed to keep a check on all students, as when giving exams online, there are more ways and opportunities for a student to cheat. The exact ratio of teachers to students that used to be in place for physical exams to monitor them would not be practical in this scenario. (Bilen & Matros, 2020), (Peterson, 2019).

This understanding has led to the development of different types of digital proctoring systems in the market. These systems use the hardware such as webcams and mics already present in the student's laptops to monitor them and ensure academic integrity. Many factors must be taken into consideration while designing a digital proctoring system. The AIPS must run on all systems without any issues, and it must not be an overly intrusive system. The system could be entirely human-based. The students are monitored during the exams by faculty through the online meeting's webcam and mic, with no extra software involved. This system can be implemented using a better student-to-faculty ratio and multiple cameras to get a better view of the student's exam environment. Another way to proctor online exams is a fully digital AIPS.

The students would give their exams in a secure browser to ensure no other computer resources are being used to cheat. The question paper would be designed to reduce the number of common questions the students have. They would also be monitored via their webcams and mic to check their behaviour. All activities would be recorded and analysed by the AIPS to flag any attempts at cheating. When a student tries to cheat, the system would flag such behaviour and

take action appropriately. The system could either suspend the exam or generate a report for review by the institution. The third way of designing a system would be a blended system.

The software would assist the human proctor in keeping track of the student activities. In this way, whenever a student is suspected, they would be brought to the forefront of the human proctor's screen, and their suspicious activity flagged for later review. This way, a single human proctor can focus their attention on students most likely to cheating. It also provides an extra layer to the monitoring system. This way, false positives can also be reduced, and the workforce required to monitor the exam also reduces. The system's selection depends on the preferences of the university and the resources of the majority of the student body. If the students are giving the exams from a location where they have a weak net connection or electricity cuts, a human proctor system might not work since any issues with the student's live stream would lead to them being flagged. The digital secure browser-based system would work better; for as long as the computer is running, the exam can be conducted while ensuring the student is monitored. (Butler-Henderson & Crawford, 2020; O'reilly & Creagh, 2016; Weiner & Hurtz, 2017).

In all these systems, the privacy of the user is a significant concern. When such a system is in use, it has access to the audio and video input of the students. Some systems also operate to detect other programs running in the background and restrict their actions. While this is all done to maintain a secure and fair test-taking environment, an institution having access to all this data of any user may be considered by some a major breach of privacy. Therefore, when designing such a system, steps must be taken to ensure that the user feels safe when they are in the test-taking environment. The various companies that exist in the market have different safeguards in place to ensure this. Governing bodies like the EU have also come out with guidelines to regulate the data access and the storage of such user-generated data. Taking into consideration the introduction of biometric verification for the exam in newer systems, it is a given that data security must be implemented. Not only during the examination but also of the sensitive data that is stored and transmitted during the examination process. (Coghlan et al., 2020; Draaijer et al., 2018; Slusky, 2020).

The objective of the paper is as follows:

- This paper discusses the multiple systems that exist in Online Proctoring. It also covers the main parameters to be considered while designing such a system. We have also taken into consideration the user side technological and emotional factors.
- In our literature review of over 43 papers, we have covered all the bases in this field. Our paper has a comparative review between the AI and non-AI-based proctoring systems.
- The existing research is focused more on advancing and improving the individual parameters of Online Proctoring systems. To the best of our knowledge, there is no complete review of the work that has been done in the field. We have used this opportunity to also identify the trends that have appeared in the research done while developing AIPS.

In human-based and AI-based systems, we have covered the different types that are now in use in the market and the ones suggested in various research papers. (O'reilly & Creagh, 2016) Multiple new hardware and software-based improvements have been noted. These are in addition to the various parameters that are already accepted as the standard for designing an AIPS. The pandemic situation has established an urgent need for a working, user-friendly AIPS. This rise in demand also means that the research and development of AIPS will now be accelerated. This is another reason why a complete review of all the existing literature is so important.

This paper also covers some issues that have been identified, technological and social. Technological issues cover points such as the available bandwidth and peripheral devices. Cameras, mics, and fingerprint scanner are now a regular part of the newer laptops. Older laptops and the majority of desktop systems do not include these. At the same time, for a system like this to run, the internet strength must be strong and constant throughout the test period. Taking this into consideration, users must be informed in advance so that they can take the necessary steps. Other than this, the Pandemic and academic pressure's social and psychological influence has also been touched upon. Teachers and students both have different outlooks when it comes to cheating. (Alessio et al., 2017; Bilen & Matros, 2020; Butler-Henderson & Crawford, 2020) Our paper covers this difference in mindset and the subsequent approach taken by both sides when it comes to the examination process. We believe this must be taken into account while designing the system. Any system that appears too oppressive or too lax will affect the acceptance of it. This will then affect the examination and test results. This is must be considered in systems that involve a human during the proctoring process. The students are greatly influenced by their peers. They may feel that if others get away with cheating and receive higher marks, it is unfair for them. They may feel pressured to get higher marks, as during this Pandemic they have been at home, with more time available to them. They may also be wary and uncomfortable with this new exam system. Lack of understanding in its working would lead to misconceptions and create panic amongst a student body. (Rios & Liu, 2017; Weiner & Hurtz, 2017) These points have also been discussed in our paper.

The following section is the discussion of AIPS. Section 2 discusses an overview of OPS. Section 3 has search criteria and research questions. In the same section, we have also added a concept map that describes the main points identified in the literature review. Section 4 subsequently covers our findings based on research questions. Section 5 gives the future of AIPS and Section 6 summarize our survey work.

2 Online Proctoring System (OPS): an Overview

Online Proctoring in education is not a new area of research. Even before the Pandemic, many universities/institutions were using proctoring systems for online courses. The competitive and adaptive exams like GRE, GMAT, CAT are purely proctor-based exams. Online proctoring makes use of virtual tools for monitoring activities (such as

tab change, timestamp, background noise etc.) for assessing the students appearing for exams. Such exams are generally happening online and remote location so that any student from any location can give exams to ensure the integrity (Caveon et al., 2013).

Online proctoring system focusses on two major components viz. Web camera for recording the video of the student appearing for the exam which can be later on viewed by examiner/proctor. Examiner/proctor can potentially look at any mischievous things, cheating happening during exam or not. The second component is Locking which prevent students from opening other tabs in the web browsers. This is also known as Computer or Browser Lockdown (Alessio et al., 2017). According to (Hussein et al., 2020) there are following features of proctoring, they are being tabulated (Table 1) below:

There are three types of proctoring system identified by (Hussein et al., 2020). Figure 1 shows the types of proctoring systems:

There are various technological advancements that have occurred in online proctoring system. The (Hussein et al., 2020) exclusively covers and overview of proctoring tools. An investigative study was conducted on proctoring system and its evaluation. Based on the investigation, the paper offers recommendations for educational institutions about use of proctoring system. (Prathish et al., 2016) proposes an intelligent online proctoring system. The said proctoring system is based upon audio and video parameters. However, the paper lacks in evaluating their own research work. (Chua et al., 2019) implemented a system which can detect and prevent cheating using tab locking and question bank randomization. (Pandey et al., 2020) develops e-Parakh which is online examination proctoring system exclusively used for mobile devices. (Slusky, 2020) explores various cybersecurity issues in online proctoring system. the paper discusses methods and techniques of multi-factor authentication and authorizations, including the use of challenge-response, biometrics (face and voice recognition), and blockchain technology. The discussion of operational controls includes the use of

Table 1 Features of Online Proctoring System

Features	Description	Newer Technologies
Authentication	Authentication includes verifying the identity of both candidate and proctors who are the part of proctoring software	Two factor authentication, OTP, Face recognition is used to authenticate entity in proctoring system
Browsing tolerance	This is restriction provided by proctoring system software about usage of other resources (such as other tabs of browsers, other face detection during live proctoring etc.)	This is done by log tracking and analysis, Face detection, Object Detection etc
Remote authorizing and control	It gives authority to the proctor to take control over proctoring system (like he/she can start/pause/stop the examination of a particular student remotely)	This is generally done by giving administrative rights and using multilevel security models
Report generation	It is about creating the student's report and activity log during the exam	This is normally done by the technologies like Python, ASP.net or any other open-source programming language

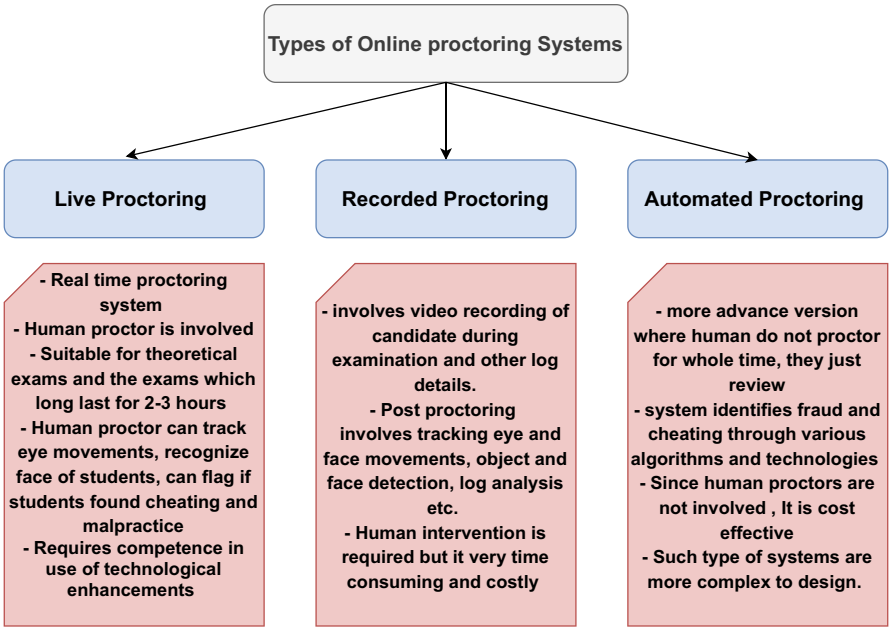

Fig. 1 Types of Online Proctoring Systems

lockdown browsers, webcam detection of behavioural signs of fraud, endpoint security, VPN and VM, screen-sharing and keyboard listening programs, technical controls to mitigate the absence of spatial (physical area) controls, compliance with regulations (GDPR), etc. (Alessio et al., 2017) examines the effect of proctoring on the performance of the student.

3 Search Criteria, Inclusion/Exclusion Criteria and Research Questions

For the literature review carried out in this paper, we have searched and shortlisted the most relevant papers. These papers were identified and selected based on the Publications (Majority of them were Springer, IEEE, Elsevier, Taylor and Francis, Sage, Inderscience, IGI Global etc.), Indexed paper (Scopus, Web of Science such as ESCI, SCI, SSCI, SCIE, and available in ERIC Database), and the conference number (mostly containing good number of citations). Total 56 documents were retrieved from the databases out of which few papers were removed as they were not relevant to our study. The papers which are based on legal aspect and psychological aspect of online proctoring system were removed from the literature study. These papers, totalling 43 are distributed over 6 years (from 2015 to 2021). This was done intentionally to help us identify the new technologies and advancements that have been implemented in proctoring systems. Figure 2 depicts the search methodology of our extensive research work.

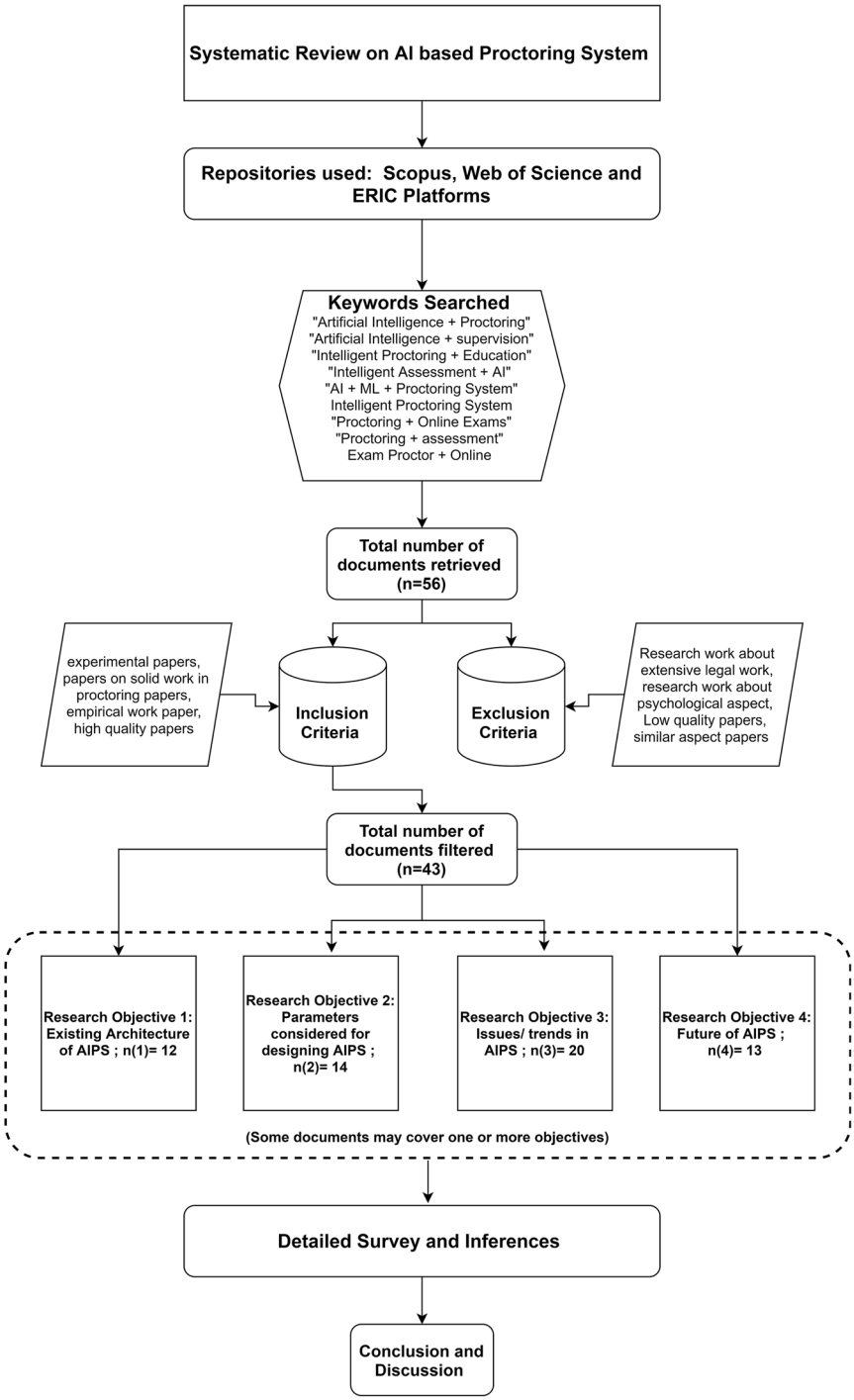

Fig. 2 Search Criteria, Inclusion/exclusion criteria of systematic review work

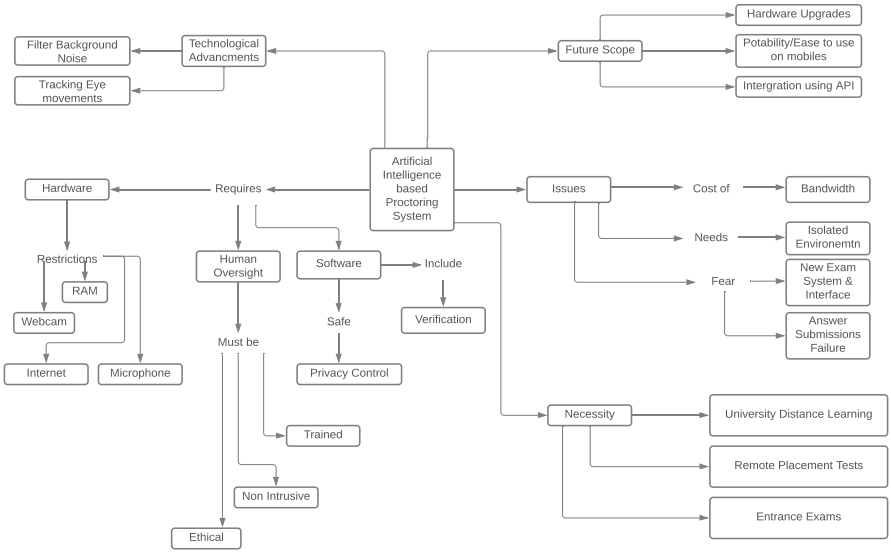

Fig. 3 Concept map of AIPS (Based on searched papers)

The papers cover topics such as new hardware and software designed for the systems and human factors that influence the use and design of such systems. Studying the previous work done in this field, we framed four research questions and identified the main points of our review, which we have laid out in the concept map below (Fig. 3).

The concept map shows us the key points that need to be considered while designing the AIPS. All of these points have been covered in greater detail in their respective sections as per the related research question. This allows us to give a clearer and detailed analysis of the work done. Topics such as Requirements and Necessity cover the points related to the existing architectures of such systems. Hardware, Software and Human Oversight are related with the discussion over the parameters that are considered when designing the proctoring systems. Issues in itself is covers a large focus of our literature review, and is related to the Technological Advancements that are discussed. Technological Advancements and Future Scope deal with the trends and advancements of the proctoring system.

Our detailed survey paper ought to solve following research questions:

RQ1: What are the existing architectures in AIPS?
RQ2: What are the different parameters to be considered in AIPS?
RQ3: What are the issues in designing and using AIPS?
RQ4: What is the future of AIPS?

4 AI based Proctoring System: Current Scenario

4.1 Existing Architectures on AIPS (RQ1)

ProctorU is an example of an OPS that uses a microphone and webcam. It is a live proctoring system in which the proctor guides students through the entire process of an online exam, and also monitors them using the webcam. Proctors are required to ensure that no unauthorized materials are present before the start of the exam. They are also required to verify the student's identity by asking them to present their ID cards. Students are required to maintain an uninterrupted audio-visual connection to the proctor throughout the session. (Milone et al., 2017) Kryterion, a widely-used commercial OPS uses an approach very similar to the one used by ProctorU. (Prathish et al., 2016) The AI module of ProctorU, however, isn't highly secure and can be deceived, which is why the company recommends using their hybrid solution to maintain high security. This hybrid solution augments automated proctoring with professionally trained live proctors, who have the ability to interrupt the test and intervene in case they suspect something. (Slusky, 2020).

Xproctor, another popular OPS, authenticates students & constantly tracks and monitors them via facial recognition, behavior video streaming, audio and photographic methods. It also supports various LMS, which when installed on the person's computer, paves way for unlimited photo captures, screenshots, and video captures. (Slusky, 2020).

Another example of a proctoring system is the EU-funded project TeSLA. TeSLAaims at developing techniques for the verification of test-takers via biometrics. This involves facial recognition, voice recognition, keystroke analysis and fingerprint analysis to ensure that no impersonation is taking place, and that the answers are being given by the actual test-taker. (Draaijer et al., 2018).

The PSI Bridge platform makes use of a proprietary lockdown browser and a self-authentication scheme, to ensure proper compliance, while also maintaining student privacy and minimizing security risks. It is a highly secure platform that doesn't need any access to the student's computer to verify the exam's integrity, hence making it non-invasive. The exam session is recorded and stored in an LMS server that is integrated with a cloud-based Software as a Service (SaaS) Exam logs and flagged violations are also stored along with it, where the proctor can review it later. In ProctorExam, spatial controls are augmented by utilizing a highly innovative 360-degree monitoring. This monitoring includes webcam, screen-sharing, and a smartphone camera positioned in such a way so as to view everything around the test-taker. It also uses facial recognition to flag cheating attempts. (Slusky, 2020).

A brilliant multi-factor authentication scheme specifically designed for securing online examination services without comprising user-friendliness has also been proposed. It is a three-fold scheme featuring face-recognition, OTP verification, and fingerprint authentication modules. The system deploys a hierarchical structural methodology where the user starts off with a proper Registration process. The registration process involves the user registering themself with a unique ID provided by the institution, right forefinger impression and phone number verified using OTP.

The system then proceeds to the login module, that screens users trying to access the system. This login module contains the three above-mentioned modules. Only on passing all of these modules is the user allowed to undertake the test. To ensure the authenticity of the user during the examination, the system does a fingerprint match on a periodic basis, at any given instance. On failing this, the new fingerprint is tested against the database to acquire the details of the person who is abetting. After acquiring this, a report is sent to the Controlling Authority with the details of the users involved in the malicious activity. (Joshy et al., 2018).

In another proposed system, the student needs to have a webcam equipped computer and is asked to show the whole room in which they are seated. The first module is face detection, post which the detected face is tracked to ensure the continuous presence of the student throughout the examination. Along with continuous audio–video capture, active window capture also takes place simultaneously to detect whether the student is trying to access some other folder or additional browsers in the computer. Other characteristics like hand movements can also be detected. All these are then given as input to the heuristic-based inference system. It is by analyzing all of these results that the inference system decides whether there is any malpractice or not. (Raj et al., 2015).

The Safe Exam Browser is a software that works with an LMS platform. It is a kiosk application & a browser. The Kiosk Mode locks down the device and prevents the user from browsing other tabs and applications, and lets them communicate inly with the LMS and exam software. It also disables shortcuts and copy/paste. (Slusky, 2020).

Respondus has an OPS that is compatible and well-integrated with an LMS. It offers two tools, a Lockdown Browser and a Monitor. The Browser allows only one browser tab to remain open and disables everything else. The Monitor works hand-in-hand with the Browser and monitors student's behaviour using a webcam. It performs video analytics on this video input to determine behavioral events that indicate cheating. (Slusky, 2020).

There are several AI-based software that help bridge the gap between online lectures and online examinations. One such software is Examus, that offers the ability to obtain student's behavioral characteristics during online lectures, and then provide them to proctoring services for better monitoring in online exams. (Slusky, 2020).

The table below (Table 2) provides a list of OLP vendors. Each vendor has a very different and unique approach to OLP. Live OLP is where the proctor can see and communicate with the student, and fully automated OLP is where the webcam and microphone are able to start recording on its own, without the need of a live proctor. (O'reilly & Creagh, 2016).

4.2 Parameters Considered for Designing AIPS (RQ2)

After reviewing the research done on various AIPS the necessary parameters have been identified (Atoum et al., 2017; O'reilly & Creagh, 2016; Slusky, 2020). These parameters are selected based on ease of implementation based on hardware that is accessible to the students. While using the available resources, it is important to ensure that at

Table 2 Various AIPS (Live OLP or Fully automated OLP)

Company Name	Live OLP	Fully Automated OLP
BVirtual	✓	✓
Examity	✓	✓
Global Campus Proctoring	✓	
Kryterion	✓	
Loyalist	✓	
Mettl	✓	
PearsonVUE	✓	✓
Proctorfree		✓
Proctorio		✓
Proctortrack		✓
ProctorU	✓	
Respondus	✓	
SoftwareSecure	✓	
Tegrity		✓

no point is the user's privacy being violated. The software and image processing algorithms that are designed to work in tandem with the same hardware. The AIPS parameters are restricted to input devices that come attached to the majority of user systems, such as webcams and microphones. Commercially designed systems cannot expect students or institutions to purchase additional equipment, even if it helps increase the accuracy of the system (Li et al., 2015). Any such systems will be passed over in favor of companies that can deliver similar results with no extra cost and/or equipment.

The parameters are:

Camera: This is an input device comes as a part of almost all laptops and is an easily available add-on for desktop systems. The webcam is used to provide the proctoring authority (PO) with a live view of the user. This way the user can be monitored to ensure that they are attentively giving the examination, while simultaneously checking for any attempts at cheating. Using face recognition technology, the system can make sure that only the registered in user is giving the exam and this way prevent impersonation (Joshy et al., 2018; Sinha et al., 2020). The webcam can also be used to check for any other people in the background that try to help in cheating (Raj et al., 2015).

Mic: This is again an input device that comes attached to most systems. The mic can be used to record audio and analyze it. The analysis can then be used to determine whether the user is being assisted by someone out of the field of camera view or via a call on another device (Sinha et al., 2020). As background noises can also be considered as dishonest activities, the software needs to be trained to prevent false positives accordingly (Prathish et al., 2016; Raj et al., 2015).

Human Proctor: The systems in use today do not have a hundred percent accuracy rate. These require human oversight for dealing with false positives and to assist with grievance redressal (Li et al., 2015). This way the systems can be continuously trained to better the AI working in the backend. The PO will also analyse the report generated by the AIPS to render final judgement regarding the malpractice (Metzger & Maudoodi, 2020). The AIPS processes multiple inputs such as Audio and Video, and background application data. In case there is a false positive logged in any of these inputs, the PO can compare the inputs from all these sources to get a better idea before declaring it a copy case. There could be an instance where the AI might flag a calculator as a phone, and report the user as a "copy case" considering it to be a mobile device. In this case human oversight will be required to prevent a student from being wrongly accused.

Screen Share / Recording: This way the user's screen is shared with the PO. The proctor can then view the tabs that are open on the student's screen to ensure that they do not open other web pages or notes to search for answers (Beust et al., 2018). This can also be recorded by the AIPS for future reference in case there is a dispute on the flag raised by the system regarding suspicious activity. This also goes hand in hand with the Application Lock parameter, by recording the evidence of other applications being used to cheat (Slusky, 2020).

Application Lock: The application lock parameter is to ensure that no user access other programs in the background of the exam. The AIPS ensures that no other communication applications or documents are accessible during the duration of the test. This can be done via the "secure browser" method that does not allow tab switching (Chua et al., 2019). The user is also prevented from searching online for the answers via this method (Slusky, 2020). Any attempts to do so will also be flagged as a copy case by the system (Metzger & Maudoodi, 2020). A simpler way to implement this concept is to use a regular browser and flag the user whenever they do make a tab switch (Raj et al., 2015).

Biometrics: Using biometric verification, the system can verify that the user is not cheating via impersonation. It also adds another layer of security over a simple User ID and password combination that can be easily shared. This can also be used during the paper to make sure that the user does not switch places with someone during the paper (Joshy et al., 2018). Facial recognition can also be implemented to act simultaneously throughout the duration of the examination (Ghizlane et al., 2019; Zhang et al., 2016).

Gaze Tracking: Using gaze tracking, the student behaviour can be monitored for copying using external resources like notes or textbooks. The student can be monitored using hardware add-ons like a gaze tracker (Atoum et al., 2017; Li et al., 2015). It can also be done by training the AIPS to identify when the user is looking away from the screen (Prathish et al., 2016; Zhang et al., 2016). The system must allow for small movements of the user, as it is not reasonable to assume, they will sit still for the entire duration of the paper.

Random Question Banks: The paper can comprise of questions randomly selected form a pre-prepared question bank. In this manner the users will all get a paper unique to themselves (Chua et al., 2019; Norris, 2019). This method will also help nullify the attempts to copy by sharing the answers to a particular question as no two students would have a question bearing the same question number.

The Table 3 is designed to show the research work done on AIPS systems over the years of 2015–2020. In this we see the rising trend of implementation of better software like tab locking. The research on older systems was focused more on developing AIPS that have a high accuracy based only on video input. This way we see that gaze tracking research has been carried out and implemented from 2015 onwards itself. With fingerprint scanners now becoming a standard part of modern systems for security, more AIPS can be designed to utilize them for verification. While using randomly generated papers from test banks is relatively new research, it is quite promising on the cheating prevention front. If a user is somehow able to avoid the AIPS safeguards and communicate with someone else, the mix up and/or unique questions will make this attempt fruitless.

4.3 Issues in AIPS (RQ3)

One major consideration to be made when designing any software is of the issues which may occur at any stage of execution. For any proctoring software, we must primarily consider two factors where a user may face problems: technological and human response.

A major Security factor which can be misused easily is user privacy (Beust et al., 2018). Since, user authentication is necessary before allowing the student to attempt the exam; they are required to verify their personal details to the proctor. This can be done by scanning their User Identity Cards like College ID, Aadhar Card etc. (Butler-Henderson & Crawford, 2020; Caveon et al., 2013; Slusky, 2020). Such documents are often linked to sensitive user details and can be misused easily. The mobile numbers linked can also lead to phishing calls and serious offences like catfishing, harassment and so on. A proctor may end up indulging in immoral activities with the information at hand (Coghlan et al., 2020). Hence, a lot of emphasis must be given to ensuring that any Proctoring Software is robust, secure and ensures privacy of the test-taker.

Impersonation by candidates is another security flaw which needs to be avoided (Hylton et al., 2016). Since Proctoring Software give us the liberty to attempt any exam at home, this facility can be misused by users as they may make any other person attempt the test using their credentials (Ghizlane et al., 2019). User Authentication, therefore, becomes a necessity before permitting anyone to begin with the exam.

For ensuring fair assessments, various security measures are applied by Proctoring software. Some applications involve gaining control of the candidate's device. This includes webcam, microphone and even gaining screenshare access of the Desktop/Laptop/Mobile Phone (Coghlan et al., 2020). Such level of control over a

Table 3 Parameters considered for designing AIPS

Paper	Camera	Mic	Human Proctor	Screen Share / Recording	Application Lock	Biometrics	Gaze Tracking	Random Question Banks
(Zhang et al., 2016)	✓					✓	✓	
(Prathish et al., 2016)	✓	✓					✓	
(Raj et al., 2015)	✓	✓			✓			
(Li et al., 2015)	✓		✓				✓	
(Atoum et al., 2017)	✓	✓			✓	✓	✓	
(Beust et al., 2018)	✓	✓	✓	✓				
(Joshy et al., 2018)	✓					✓		
(Ghizlane et al., 2019)	✓			✓		✓		
(Golden & Kohlbeck, 2020)								✓
(Chua et al., 2019)					✓			✓
(Slusky, 2020)	✓	✓	✓	✓	✓	✓		
(Sinha et al., 2020)	✓	✓			✓			
(Norris, 2019)	✓	✓	✓		✓	✓	✓	✓
(Metzger & Maudoodi, 2020)	✓		✓		✓			

device can lead to numerous privacy problems and makes the device more susceptible to hacking attacks. Any Proctoring System must ensure that the device security is ensured using various Security Protocols and the data being stored at their data centers is well-protected from malware attacks (Ilgaz & Afacan Adanır, 2020).

Proctor Authenticity is one important aspect which should not be neglected. Since the proctors are hired separately by the companies providing the solutions and not the organizations which administer the exams, steps should be taken to ensure that well-qualified people are given the role after rigorous interviews and relevant background checks (Furby, 2020). Presence of any miscreant as a proctor can be harmful for the candidate's safety and privacy as the details at their disposal can be misused and lead to dire consequences. Both the organization and the company involved will face negative reviews in public which will be a great deterrent to their future prospects.

Proctoring Systems also have to deal with and work around several infrastructure issues. Since their main goal is to ensure fairness and closeness to offline pen-and-paper exams, they require certain minimum specifications and hardware components to be present in devices of all candidates who are going to avail their facility. Implementing a combination of Artificial Intelligence and Human Proctoring inadvertently increases the cost for the company delivering the software (Atoum et al., 2017). Doing cost-analysis is integral to ensure that the entity doesn't become a loss-making proposition but is instead a sustainable venture (Furby, 2020).

The IP Addresses of candidate's devices (Both Desktops/Laptops and Mobile Phones) are accessible by several software to prevent misconduct. However, they can be easily manipulated nowadays using VPNs which cannot be tracked easily. This can be misused by candidates to indulge in malpractices which dilutes the efficiency of the application (Joshy et al., 2018).

Candidates' devices need to have certain minimum specifications like a working webcam and microphone, certain free storage in RAM. They also need to give control access to proctors and need to ensure an efficient internet bandwidth (Slusky, 2020). All this has to be working throughout the duration of the examination. Failure of any one of these components leads to the examination getting temporarily suspended until they are fixed and working again (Ilgaz & Afacan Adanır, 2020). Any candidate who goes through these issues has to shift his/her focus from the exam towards fixing the problem which isn't ideal in such a stressful scenario.

The Interface of the application also needs to be not too complex but rather easy to understand (Butler-Henderson & Crawford, 2020). When we consider various National/International level exams, people from all sections of society appear for them. Many of them cannot afford to own such devices and hence, they end up without an opportunity to appear for the examinations. A complex User Interface also ends up perplexing candidates even before their exam has started which isn't ideal.

The logistics of setting up data-centers to store candidates' personal information as well as examination data isn't cheap either (Caveon et al., 2013). Any exam is given by thousands of people together at any given time. Hence, robust servers need to be created and used so as to ensure that no candidate faces any technical issue from the server-side of the application. Low internet connectivity can also lead to

problems during the exam and hence, arrangements need to be made to ensure a stable network connection (Sinha et al., 2020).

Apart from the above technical factors, we also need to consider issues pertaining to human psychology and other socio-cultural factors like acceptance of the new methodology. Various studies have been conducted to test how cheat-proof any proctoring software is. A common theme has been observed in the results where candidates end up scoring more marks in an online exam compared to an offline exam (Ilgaz & Afacan Adanır, 2020). Inflated marks can be deceptive for not only outsiders but even the candidate who scores them since they may get an impression of possessing abilities to an extent within them which is not the case in reality (Langenfeld, 2020). Making any proctoring software cheat-proof has to be the first priority for any company to ensure they replace pen-and-paper based examinations in the future (Beust et al., 2018; Butler-Henderson & Crawford, 2020; Ghizlane et al., 2019; Weiner & Hurtz, 2017).

Present-day Proctoring Softwares not being cheat-proof (O'reilly & Creagh, 2016) evoke polarizing opinions amongst the society. Faculties of Schools/Colleges/Universities still prefer the traditional mode of examinations over online examinations as it is easier for them to keep a check on students and prevent cheating and other malpractices (Dendir & Maxwell, 2020; Norris, 2019; Peterson, 2019). Academic Dishonesty is one big drawback which hasn't allowed more organizations switching to the new methods of conducting examinations (Peterson, 2019). Marks scored by the examinee cannot be considered as a true testament of their knowledge and hence, the apprehensions still remain.

E-Proctoring is expensive to implement and has to respect a candidate's autonomy and liberty. Trust is an important aspect during examinations for both the examinee and the examiner (Coghlan et al., 2020). Flagging any candidate inappropriately of indulging in wrongdoing can be detrimental for them. It will also not be correct on the proctor's end to miss out on obvious evidences of cheating.

Anxiety amongst examinees has been a long-prevalent issue even when giving exams in the traditional method (Butler-Henderson & Crawford, 2020; Woldeab & Brothen, 2019). Societal/Parental pressure, Desire to be the highest-scorer and so on, all these psychological factors contribute to raised stress levels and anxiety among the candidates. Compounded with the stress of giving exams on a completely new medium with numerous technicalities involved, any examinee would feel drained during the process (Beust et al., 2018; Sinha et al., 2020). It is the responsibility of both the organization which administers the examination as well as the company providing the Proctoring Software to ensure that the examinees have a hassle-free experience while giving their examination.

Continuous Surveillance can also be an issue for the examinees as the thought of being monitored consistently for long durations can impact their mental health and sow seeds of doubt in their mind when instead they should be focusing on their own examination. This stigma should never creep into a candidate's mind (Joshy et al., 2018).

Proctoring Systems must also ensure that candidates do not possess cheat sheets (Furby, 2020) or indulge in collusion while giving a proctored exam. This defeats the entire purpose of using such an application in the first place. Since mobile phones are a necessary accessory for conducting any proctored exam (except those

involving Multiple Choice Questions), it becomes an easy tool at an examinee's disposal to indulge in cheating using social media platforms, search engines or even accessing study material of the relevant subject (Ullah et al., 2017). Hence, any Proctoring Software must also be able to take into account this and provide the necessary breakers to prevent misuse and cheating by the examinees.

The Table 4 below provides a list of the various categories of issues as identified by us related to an AI-based Online Proctoring System. We have categorized the issues into two broad categories: Technological and Human. These have been further divided into two sub-sections each: Technological factors include the Security (Candidate Privacy etc.) and Infrastructure (Hardware, Software, Internet Bandwidth) problems while Human factors include Psychological (Stress, Anxiety, Cheating and so on) and Socio-Cultural (Acceptance of new Technology, Score Integrity etc.) issues.

4.4 Trends and Technological changes in AIPS (RQ3):

Remote Proctoring enables candidates to appear for an assessment from a remote location while ensuring the integrity of the exam. Online Examinations have been conducted for several years where the organizers use designated testing centers or

Table 4 Factors affecting designing AIPS

Paper	Technological Factors		Human Factors	
	Security	Infrastructure	Psychological	Socio-Cultural
(O'reilly & Creagh, 2016)				✓
(Woldeab & Brothen, 2019)			✓	
(Hylton et al., 2016)			✓	
(Weiner & Hurtz, 2017)			✓	✓
(Atoum et al., 2017)		✓		
(Beust et al., 2018)	✓		✓	✓
(Joshy et al., 2018)		✓	✓	
(Ullah et al., 2017)	✓	✓		✓
(Ghizlane et al., 2019)	✓			✓
(Butler-Henderson & Crawford, 2020)	✓	✓	✓	✓
(Coghlan et al., 2020)	✓		✓	✓
(Peterson, 2019)			✓	✓
(Dendir & Maxwell, 2020)			✓	
(Slusky, 2020)	✓	✓		
(Langenfeld, 2020)	✓			✓
(Ilgaz & Afacan Adanır, 2020)	✓	✓	✓	✓
(Furby, 2020)	✓	✓	✓	✓
(Sinha et al., 2020)		✓		✓
(Norris, 2019)			✓	
(Caveon et al., 2013)	✓	✓		

require that the students report to their college campus to appear for the exam. A growing range of digital tools are trying to fill this void by allowing people to appear for their exams from the comfort of their homes. These include web-based services that provide real-time remote monitoring of a human being or a video recording of student behaviour throughout the duration of a test. This is done to ensure authenticity of people who are appearing for the test and also to ensure that they do not indulge in cheating. (*Remote Proctoring*, 2020).

A gradual rise was being observed in the demand of Online Proctoring Solutions since the beginning of the previous decade. Initial users of such solutions were universities who had to conduct exams for their distance learning courses. The pen-and-paper based approach was employed majorly by them. However, logistical constraints of candidates began surfacing as they couldn't travel to the city where the university was located to appear for their exams. This inadvertently led them to not being able to give the exam and hence, miss out on achieving their certification for which they had worked throughout the Academic Year.

Universities began taking notice of this problem and began implementing remote proctoring solutions provided to them by third-party organizations. This allowed the candidates the liberty to appear for their exams without having to worry about the logistics involved. These solutions, however gave rise to major problems like hacking of the technologies, dwindling academic integrity and so on. Since then, major research is being conducted to make Online Remotely-Proctored Exams as academically fair, safe and secure as possible. (*Remote Proctoring*, 2020), (*Emerging Technology and the Future of Online* Proctoring, 2020).

History teaches us that times of crisis can lead to rapid societal and technological change. As a direct result of the COVID-19 Pandemic, organizations have been forced to explore new tools for remote collaboration, learning, working and assessment (Pozo Sánchez et al., 2020). Schools and Universities have had to adopt the new methods of online teaching and then conducting virtual exams to assess the students. Corporate Organizations also have had to conduct virtual hiring of people and hence, have had to resort to conducting online tests before the Interviews. The need to balance security needs as well as ensure a good, stress-free experience of candidates – all while staying within budget is the current need of Remote Proctoring Technologies. (*Emerging Technology and the Future of Online* Proctoring, 2020).

A large number of online proctoring services – live, automated, or hybrid—rely on uninterrupted audio-visual streaming. The student can appear for the exam at any given location, provided they have a fast and stable internet connection. This has made appearing for exams extremely convenient for students. (Milone et al., 2017).

Maintaining academic integrity is a crucial part of an examination, and it plays an even bigger role in online proctoring. This explains why over the years, many OPS have ditched single-factor authentication for the more advanced and secure, multi-factor authentication schemes. These vary from very simple ones, such as verification of student identity using school/college ID cards, to more complex ones, that require OTP authentication, and fingerprint verification. However, some of these schemes, although implemented with the benefit of students in mind, are impractical if the exam is being taken by the student at their homes – which was a very common sight in the Pandemic. Therefore, fingerprint authentication schemes are

usually restricted to kiosk-based exams. (Draaijer et al., 2018; Joshy et al., 2018; Milone et al., 2017).

Perhaps one of the biggest additions to the world of OPS would be the advent of 360-degree proctoring, which can be achieved using a webcam, a smartphone, and screen-sharing. Many OPS also indulge in active widow capture and tab locking, that doesn't allow students to switch applications while the exam is on. Active window capture periodically takes screenshots of the test-taker's screen and saves them on the cloud, to be reviewed later. Another leap in the world of online proctoring was made when many OPS started periodically saving student's progress during the exam, in case their internet connection breaks down. This allowed students to be able to continue their exam right where they left off, when their internet connection was restored to normalcy. It has proven to be a huge boon for students in developing countries. (Slusky, 2020), (Milone et al., 2017), (Raj et al., 2015).

When most OPS began operations, they relied only on live proctoring services, where trained proctors would sit on the other end, invigilating the examination, with the ability to pause the exam and intervene if they suspected any illicit activity. However, with the recent advancements in artificial intelligence, hybrid systems have now come into play, where the OPS automatically flags the student in case of some background noise, or if the student attempts switching to a new application. It also has the ability to flag the student in case a mobile phone is captured on the webcam. These flags can be reviewed by live proctors, since AI is fully capable of making mistakes, and the models aren't perfect yet. (Milone et al., 2017; Prathish et al., 2016; Slusky, 2020).

A few other technologies that have come into picture are iris tracking, disabling of cut/copy/paste operations, video analysis, hand movement tracking, keystroke analysis, etc. All of these are implemented by some OPS or the other to ensure maximum academic integrity at all times during the exam. Many AI-based services are also attempting to combine online lectures and online examinations This helps them form dynamic profile questions and gain better insights into a student's behaviour, hence improving their invigilation capabilities. (Draaijer et al., 2018; Raj et al., 2015; Slusky, 2020; Ullah et al., 2019).

While technology is becoming more and more advanced day by day, it has become extremely important for us to find ways to maintain our privacy while being connected to the internet. Hence, sustaining student privacy is also a matter of concern, and many OPS have begun to prioritize it. Students are hesitant to give out data that they believe won't be protected properly. Videos, identity cards, IP addresses, fingerprints, etc. are very sensitive details that should be preserved properly, if at all. To address these apprehensions, a few OPS have started releasing lockdown browsers and other softwares, that rely on self-authentication and are non-invasive. These do not record and store data anywhere, and are hybrid which means that a proctor can interrupt the test at any time in case they suspect malicious activity. They only allow the exam browser to remain open and disable most other activities on the PC, which means that the student only can communicate with the proctor and vice-versa. (Slusky, 2020), (Prathish et al., 2016).

Technology has advanced tremendously in the last few years, and the COVID-19 Pandemic has resulted in a surge in online proctoring. Schools and universities are constantly enlisting newer third-party programs to prevent academic dishonesty and cheating in their examinations. A significant boom is expected in the demand of Remote Proctoring Solutions as this decade progresses. A robust, secure and easy-to-use Proctoring Software is the need of the hour which ensures that academic integrity is ensured whilst also maintaining stringent security standards.

5 Future of AIPS (RQ4):

Educational institutions and corporate organizations across the world had gradually begun the process of adopting online proctoring software over the past decade to conduct remote examinations in a fair manner and ensuring that the candidates gave the exam in a known environment. Due to the COVID-19 Pandemic, it has become the need of the hour to leverage remote proctoring platforms to conduct seamless tests while also ensuring that the candidates do not indulge in malpractices during these online exams. (*Remote Proctoring*, 2020).

There are numerous benefits to any organization when they conduct any assessment via remote proctoring instead of the traditional pen-and-paper based method. Scheduling exams becomes easier as there is no need to set up specific testing centers to conduct examinations. Communication between the examiner and the examinee is more streamlined, hassle-free and faster. Results of the examination can be generated faster and, in some cases, almost instantly. Online examinations also give the organization the liberty to conduct the exam on a massive scale without worrying about maxing out the capacity of the examination centers. (Arora, 2021).

However, a sincere effort needs to be made for developing proctoring technologies to ensure that the level of online examinations is at par with offline examinations in all aspects; be it integrity of marks scored, ensuring candidates do not get involved in wrongdoings etc. Social perception of the masses towards online exams also needs to be changed and they must be made aware of the benefits for the same. The issues while designing an AI-based proctoring system as discussed by above need to be tackled with the use of existing technologies. Advancement of technologies will no doubt be beneficial for constructing more robust and secure systems but currently, anticipating the growing need for these software; a conscious effort needs to be made to enable existing technologies in mitigating the issues that exist. (Pimple, 2021).

Any proctoring software needs to accurately establish the identity of the person giving the examination. Impersonation is a big threat to the sanctity of the online exams and hence, various methods are being employed to ensure that the designated person is the one giving the examination. Proctoring software ask every candidate to submit some personal information or proof of identity which is then verified before allowing the candidate to proceed. Certain systems have begun employing biometric authentication via fingerprints through the fingerprint scanner which is now readily available on mobile phones or laptops nowadays.

This mode of authentication is more readily available in today's world but it still is not 100% foolproof in determining the identity of the candidate. A more secure method of biometric authentication would be using iris scanning as a tool. However, the hardware capabilities for the above method are not commercially available in devices and hence, candidates will have to spend money to get the required hardware components. Any attempt at forcing a person to buy something specifically for using a remote proctoring software would defeat the efforts made to achieve global acceptance of the technology. Hence, continued human proctoring throughout the exam duration is a "necessary evil" which needs to be employed while designing a proctoring software.

One of the primary approaches that should be taken for authenticating the test-taker's identity, is multi-factor authentication. With biometrics on the rise, devices such as mobile phones, tablets and laptops are now incorporating fingerprint scanners and face scanners. Mass production of such devices results in everyone using at least one biometric service available. While password can serve as the first module, OTP-based verification, facial recognition, and fingerprint authentication can be used at the second stage of any OPS. While a few AIPS have also made use of iris tracking among several other techniques, one must understand that these require high-end hardware that isn't available or affordable for everyone. (Draaijer et al., 2018; Joshy et al., 2018; Raj et al., 2015; Slusky, 2020; Ullah et al., 2019).

Another technology that is creating waves is LIDAR. LIDAR, which stands for Light Detection and Ranging, is a remote sensing method. LIDAR uses a pulsed laser to calculate an object's variable distances from the source. These light pulses generate accurate 3D information about the target object and its surroundings. LIDAR is used extensively in the field of astronomy—NASA's Phoenix Mars Lander used LIDAR technology to detect snow falling – and now, it is finding newer applications in the fields of biology, atmosphere, and autonomous vehicles. LIDAR is now being incorporated in self-driving cars – to help identify nearby obstacles and model the road better, and was introduced in mobile phones. LIDAR helps measure distances more accurately and improves augmented reality (AR) implementation. It gives apps more useful and accurate information about the user's surroundings, for smoother, more reliable AR. While this is a huge boon for AIPS, LIDAR is a highly expensive technology that is yet to hit mass-production in mobile phones to make it more affordable.

Online education and online examinations are two sides of the same coin, and bridging the gap between these is very important. Several software aims to analyze students' behaviors in online classes and obtain their unique behavioral characteristics, and then provide this information to proctoring services for better invigilation in online exams. Many such software will be introduced in the future that would aim to help strengthen the numerous pillars of online education. (Slusky, 2020).

In the years to come, this revolutionary change that has been brought upon us by the Pandemic will not diminish. If anything, it has only reinforced the idea that online education is not only possible, but also highly effective and practical. More and more institutions are offering distance-learning courses and complete

degrees that one can get by studying in the comfort of their homes. In such cases, AIPS are here to stay, and will only make more leaps in the future.

Other parameters considered include using EEG machines (Li et al., 2015), user interface setup (Karim & Shukur, 2016), OTP based verification (Joshy et al., 2018) & anti-plagiarism methods (Norris, 2019). Research conducted on these parameters has shown promising results in identifying cases of misconduct. While these methods may be expensive to implement as of today, with the increase in technological integration, it would soon become feasible to include them in an AI based Proctoring System.

6 Conclusion and Discussions

Online testing is the next wave of adoption after online learning which has seen a significant rise in demand due to the problems posed by the ongoing COVID-19 Pandemic. OPS do not claim to be completely fool proof but are rapidly changing the adoption of online testing from home, a scenario that previously would have been thought to be preposterous amongst the masses.

With the advent of Online Proctoring Software, security issues associated with it are multiplying and are a cause of legitimate concern. Highly sensitive biometric data can be collected and stored on the pretext of verification purposes. Hence, personal data collected during OPS operations need to be carefully identified, classified, and labeled according to its sensitivity level for storage to maintain its confidentiality, integrity, and availability; irrespective of the medium of storage. Debate and disagreement about the appropriateness of remote proctoring technologies is bound to continue into the future. There are definite considerations that speak in favor of such technologies despite their drawbacks. It is not unfair to acknowledge here that in-person proctoring is not ethically perfect either: it too can miss cases of cheating and hence, result in unfair accusations of academic dishonesty. Furthermore, we have to accept the fact that it is vital to maintain academic integrity to protect both students and institutions.

Nonetheless, the above analysis revealed that Remote Proctoring platforms raise ethical concerns over-and-above those affecting live and in-person exam invigilation. These concerns include an uncertain risk of academic unfairness associated with AI-informed judgement (Singh et al., 2021), further diminution of student privacy and autonomy, and increased distrust towards institutions that are bastions of social values. Another fear, partially dependent on these former fears, is that these platforms could contribute to the issues of growing surveillance, liberty and privacy loss, mining of massed personal data, and dubious instances of AI decision-making.

Another viewpoint about general AI based system is it's pervasiveness and trust level. AIPS system more over works on human values (such as cheating prediction, sanctity of exams etc.). The central question that arise is that how we can developed trust enabled AIPS. From the available papers, no papers were reflecting the difference between trust value of human to AIPS and real classroom based proctoring systems. Trustworthy Artificial Intelligence is a buzzword in the future

(Vincent-Lancrin & van der Vlies, 2020).The cost of AIPS software is too high to be afford by many universities and organizations specially who are resides in under-developed and developing countries (Coghlan et al., 2020).

To sum up, it is difficult to know whether the benefits of these Online Proctoring technologies outweigh their risks. The most reasonable conclusion we can reach in the present is that the ethical justification of these technologies and their various capabilities requires us to rigorously ensure that a balance is struck between the concerns with the possible benefits to the best of our abilities.

Acknowledgements The author would like to thank the anonymous reviewers and editors for taking valuable time to go through the paper. Author would like to thank Mr. Omkar Pimple, Founder and CEO of Cerebranium (EdTech Company), Berlin, Germany for valuable inputs and feedback about the paper.

Funding Authors of this paper confirm that there is no funding received for this research work.

Declarations

Conflict of Interest The authors of this research study declare that there is no conflict of interest.

References:

Alessio, H. M., Malay, N., Maurer, K., John Bailer, A., & Rubin, B. (2017). *Examining the Effect of Proctoring on Online Test Scores*.

Arora, P. (2021). *Is Remote Proctoring The Future Of Academia? - eLearning Industry*.

Atoum, Y., Chen, L., Liu, A. X., Hsu, S. D. H., & Liu, X. (2017). Automated Online Exam Proctoring. *IEEE Transactions on Multimedia, 19*(7), 1609–1624. https://doi.org/10.1109/TMM.2017.2656064

Beust, P., Duchatelle, I., & Cauchard, V. (2018). *Exams taken at the student's home*.

Bilen, E., & Matros, A. (2020). *Online Cheating Amid COVID-19*.

Butler-Henderson, K., & Crawford, J. (2020). A systematic review of online examinations: A pedagogical innovation for scalable authentication and integrity. *Computers and Education*, *159*. https://doi.org/10.1016/j.compedu.2020.104024

Caveon, D. F., Security, T., & Layman, H. (2013). *Online Proctoring Systems Compared*.

Chua, S. S., Bondad, J. B., Lumapas, Z. R., & Garcia, J. D. (2019). *Online Examination System with Cheating Prevention Using Question Bank Randomization and Tab Locking*.

Coghlan, S., Miller, T., & Paterson, J. (2020). Good proctor or "Big Brother"? AI Ethics and Online Exam Supervision Technologies. *ArXiv Preprint*.

Dendir, S., & Maxwell, R. S. (2020). Cheating in online courses: Evidence from online proctoring. *Computers in Human Behavior Reports, 2*, 100033. https://doi.org/10.1016/j.chbr.2020.100033

Draaijer, S., Jefferies, A., & Somers, G. (2018). Online proctoring for remote examination: A state of play in higher education in the EU. *Communications in Computer and Information Science, 829*, 96–108. https://doi.org/10.1007/978-3-319-97807-9_8

Emerging Technology and the Future of Online Proctoring. (2020).

Furby, L. (2020). Are You Implementing a Remote Proctor Solution This Fall? Recommendations from NLN Testing Services. *Nursing Education Perspectives, 41*(4), 269–270. https://doi.org/10.1097/01.NEP.0000000000000703

Ghizlane, M., Hicham, B., & Reda, F. H. (2019, December). A New Model of Automatic and Continuous Online Exam Monitoring. *Proceedings - 2019 4th International Conference on Systems of Collaboration, Big Data, Internet of Things and Security, SysCoBIoTS 2019*. https://doi.org/10.1109/SysCoBIoTS48768.2019.9028027

Golden, J., & Kohlbeck, M. (2020). Addressing cheating when using test bank questions in online Classes. *Journal of Accounting Education*, *52*. https://doi.org/10.1016/j.jaccedu.2020.100671

Hussein, M. J., Yusuf, J., Deb, A. S., Fong, L., & Naidu, S. (2020). An Evaluation of Online Proctoring Tools. *Open Praxis, 12*(4), 509. https://doi.org/10.5944/openpraxis.12.4.1113

Hylton, K., Levy, Y., & Dringus, L. P. (2016). Utilizing webcam-based proctoring to deter misconduct in online exams. *Computers and Education, 92–93*, 53–63. https://doi.org/10.1016/j.compedu.2015.10.002

Ilgaz, H., & Afacan Adanır, G. (2020). Providing online exams for online learners: Does it really matter for them? *Education and Information Technologies, 25*(2), 1255–1269. https://doi.org/10.1007/s10639-019-10020-6

Joshy, N., Ganesh Kumar, M., Mukhilan, P., Manoj Prasad, V., & Ramasamy, T. (2018). *Multi-factor authentication scheme for online examination*.

Karim, N. A., & Shukur, Z. (2016). Using preferences as user identification in the online examination. *International Journal on Advanced Science, Engineering and Information Technology*, *6*(6), 1026–1032. https://doi.org/10.18517/ijaseit.6.6.1412

Langenfeld, T. (2020). *Internet-Based Proctored Assessment: Security and Fairness Issues* (Vol. 39, Issue 3).

Li, X., Chang, K. M., Yuan, Y., & Hauptmann, A. (2015). Massive open online proctor: Protecting the credibility of MOOCs Certificates. *CSCW 2015 - Proceedings of the 2015 ACM International Conference on Computer-Supported Cooperative Work and Social Computing*, 1129–1137. https://doi.org/10.1145/2675133.2675245

Metzger, R., & Maudoodi, R. (2020). *Using Access Reports and API Logs as Additional Tools to Identify Exam Cheating*.

Milone, A. S., Cortese, A. M., Balestrieri, R. L., & Pittenger, A. L. (2017). The impact of proctored online exams on the educational experience. *Currents in Pharmacy Teaching and Learning, 9*(1), 108–114. https://doi.org/10.1016/j.cptl.2016.08.037

Moreno-Guerrero, A. J., Rodríguez-Jiménez, C., Gómez-García, G., & Ramos Navas-Parejo, M. (2020). Educational Innovation in Higher Education: Use of Role Playing and Educational Video in Future Teachers' Training. In *Sustainability* (Vol. 12, Issue 6). https://doi.org/10.3390/su12062558

Norris, M. (2019). *University online cheating-how to mitigate the damage*.

O'reilly, G., & Creagh, J. (2016). *A Categorization of Online Proctoring*.

Pandey, A. K., Kumar, S., Rajendran, B., & Bindhumadhava, S. B. (2020). E-parakh: Unsupervised online examination system. *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, *2020-Novem*, 667–671. https://doi.org/10.1109/TENCON50793.2020.9293792

Peterson, J. (2019). An Analysis of Academic Dishonesty in Online Classes. In *ACADEMIC DISHONESTY IN ONLINE CLASSES Mid-Western Educational Researcher ·* (Vol. 31).

Pimple, O. (2021, January). *Digital Education For All - Is Mobile Learning The Way Ahead?* The Media Bulletin.

Pozo Sánchez, S., López-Belmonte, J., Moreno-Guerrero, A. J., Sola Reche, J. M., & Fuentes Cabrera, A. (2020). Effect of Bring-Your-Own-Device Program on Flipped Learning in Higher Education Students. In *Sustainability* (Vol. 12, Issue 9). https://doi.org/10.3390/su12093729

Prathish S, Narayanan S A, & Bijlani K. (2016). *An Intelligent System For Online Exam Monitoring*.

Raj, R. S. V., Narayanan, S. A., & Bijlani, K. (2015). Heuristic-based automatic online proctoring system. *Proceedings - IEEE 15th International Conference on Advanced Learning Technologies: Advanced Technologies for Supporting Open Access to Formal and Informal Learning, ICALT 2015*, 458–459. https://doi.org/10.1109/ICALT.2015.127

Remote Proctoring. (2020).

Rios, J. A., & Liu, O. L. (2017). Online Proctored Versus Unproctored Low-Stakes Internet Test Administration: Is There Differential Test-Taking Behavior and Performance? *American Journal of Distance Education, 31*(4), 226–241. https://doi.org/10.1080/08923647.2017.1258628

Singh, R., Timbadia, D., Kapoor, V., Reddy, R., Churi, P., & Pimple, O. (2021). Question paper generation through progressive model and difficulty calculation on the Promexa Mobile Application. *Education and Information Technologies*. https://doi.org/10.1007/s10639-021-10461-y

Sinha, P., Dileshwari, & Yadav, A. (2020). Remote Proctored Theory And Objective Online Examination. *International Journal of Advanced Networking and Applications*, *11*(06). /https://doi.org/10.35444/ijana.2020.11068

Slusky, L. (2020). Cybersecurity of Online Proctoring Systems. In *Journal of International Technology and Information Management* (Vol. 29).

Ullah, A., Barker, T., & Xiao, H. (2017). *A Focus Group Study: Usability and Security of Challenge Question Authentication in Online Examinations*.

Ullah, A., Xiao, H., & Barker, T. (2019). A Multi-factor Authentication Method for Security of Online Examinations. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and*

Telecommunications Engineering, LNICST, 256, 131–138. https://doi.org/10.1007/978-3-030-05928-6_13

Vincent-Lancrin, S., & van der Vlies, R. (2020). Trustworthy artificial intelligence (AI) in education. *OECD Education Working Papers*, *218*. https://doi.org/10.1787/a6c90fa9-en

Weiner, J. A., & Hurtz, G. M. (2017). A Comparative Study of Online Remote Proctored versus Onsite Proctored High-Stakes Exams. *Journal of Applied Testing Technology, 18*(1), 13–20.

Woldeab D, & Brothen T. (2019). OnlineProctoring, TestAnxiety, and Student Performance. *International Journal of E-Learning & Distance Education*, *34*(1).

Zhang, M. Z., Zhang, M. M., Chang, Y., Esche, D. S. K., & Chassapis, D. C. (2016). *A Virtual Laboratory System with Biometric Authentication and Remote Proctoring Based on Facial Recognition*.

Authors and Affiliations

Aditya Nigam[1] · Rhitvik Pasricha[1] · Tarishi Singh[1] · Prathamesh Churi[2]

✉ Prathamesh Churi
Prathamesh.churi@ieee.org; Prathamesh.churi@gmail.com

Aditya Nigam
adityanigam002@gmail.com

Rhitvik Pasricha
pasricharhitvik@gmail.com

Tarishi Singh
tarishi1109@gmail.com

[1] Computer Engineering Department, Mukesh Patel School of Technology Management & Engineering, NMIMS University, Mumbai, India

[2] Assistant Professor, Computer Engineering Department Mukesh Patel School of Technology Management & Engineering, NMIMS University, Mumbai, India