SURVEILLANCE OR SUPPORT? A SYSTEMATIC LITERATURE REVIEW OF ARTIFICIAL INTELLIGENCE SUPPORTED PROCTORED ONLINE EXAMS

Dr. Aysin Gaye USTUN

ORCID: 0000-0001-9564-0761
Department of Computer Technology
Sinop University
Sinop, TURKIYE

Dr. Bunyami KAYALI

ORCID: 0000-0001-6419-9088
Department of Computer Technology
Bayburt University
Bayburt, TURKIYE

Dr. Mehmet YAVUZ

ORCID: 0000-0001-6218-232X
Management Information Systems
Bingol University
Bingol, TURKIYE

Dr. Aras BOZKURT

ORCID: 0000-0002-4520-642X
Department of Open and Distance Learning
Anadolu University
Eskisehir, TURKIYE

Received: 11/04/2025 **Accepted:** 17/06/2025

ABSTRACT

Proctored online exams have become widespread, especially after COVID-19, increasing exam security and efficiency. In recent years, artificial intelligence developments have increased these systems' importance by expanding their use. Accordingly, this study aims to provide an in-depth understanding of the conceptual structure of artificial intelligence-supported proctored online examination (AI-SPOE) research. Systematic literature review and text mining were used as methods. Thirty-two studies in Scopus and Web of Science databases were analyzed according to the PRISMA technique. While all the studies were examined in the context of content analysis, abstracts and keywords of the relevant studies were analyzed by text mining. The current study found it effective in increasing academic integrity and exam security, but problems such as privacy violations, exam anxiety, and algorithmic biases were encountered. Although methods such as biometric verification and behaviour analysis successfully detect cheating, technical difficulties, and false positives negatively affect the user experience. In the future, more inclusive designs, transparent algorithms, and alternative evaluation methods are suggested. In conclusion, the study emphasizes the potential of AI-SPOE systems and highlights the importance of ethical and technical improvements.

Keywords: Artificial intelligence, ai, online exam, proctored exam, higher education.

INTRODUCTION

With the rapid transformation in education during the pandemic, online proctored exam technologies within the scope of assessment and evaluation activities have also become widespread (Lee & Fanguy, 2022). Online exams are considered an integral part of online distance education programs, and their reliability, accuracy, and equitable nature are intensely debated among educators and researchers (Hussein et al., 2020). In recent years, with the increasing use of artificial intelligence (AI)-supported solutions in educational environments, the potential role of AI in this field has come to the fore (Rahman, 2022) and brought a different dimension to the discussions.

It is known that AI has important potential in terms of assessment and evaluation processes as well as its contributions such as personalization of teaching processes and learning analytics (Holmes et al., 2019). It can be said that AI-SPOE is frequently preferred especially in ensuring academic honesty in online exams (Nigam et al., 2021). Techniques such as facial recognition, voice analysis, eye movement tracking, and behavioural analysis allow the detection of potential violations by monitoring students' behaviour during exam processes (Priyanka & Shravani, 2023). However, while these technologies hold promise for improving exam security, they also bring challenges such as privacy violations, algorithmic biases, and ethical issues (Aydemir et al., 2024; Bozkurt et al., 2026a, 2026b). There are questions about the ability of algorithms to ensure fairness, especially in terms of equity and impartiality (Berti et al., 2010), which directly affects students' sense of participation and psychological well-being (Jui & Rivas, 2024). These recent studies comprehensively examine the impact of these technologies by addressing the advantages and disadvantages of AI-SPOEs.

LITERATURE REVIEW

The widespread use of online exams during the COVID-19 pandemic has increased research focus addressing multiple aspects of these assessment methods in terms of academic integrity, student preferences, authentication, and technological innovations (Butler-Henderson & Crawford, 2020; Dayananda et al., 2021; Kaddoura et al., 2022; Muzaffar et al., 2021; Newton & Essex, 2024; Noorbehbahani et al., 2022; Topuz & Kinshuk, 2024). The reviewed studies reveal that cheating rates in online exams increased during the pandemic and this increase was associated with factors such as opportunity availability, exam difficulty, time management problems, and technical inadequacies (Newton & Essex, 2024; Noorbehbahani et al., 2022). In addition, ease of use, perceived usefulness, and security methods stand out among the factors affecting students' acceptance of online exams, and it is seen that students prioritize feedback mechanisms and the possibility of home exams (Topuz & Kinshuk, 2024; Dayananda et al., 2021). Studies emphasize that AI and machine learning-based technologies are particularly effective in areas such as authentication, anomaly detection, fraud detection, and automatic grading (Butler-Henderson & Crawford, 2020; Kaddoura et al., 2022; Muzaffar et al., 2021). However, it has been noted that these technologies bring challenges such as privacy violations, algorithmic biases, and ethical issues. While online exams offer the advantages of accessibility and flexibility, they struggle with issues such as digital inequality and vulnerabilities, and innovative methods such as biometric verification and dynamic question banks have been found to provide partial solutions to these problems (Butler-Henderson & Crawford, 2020; Dayananda et al., 2021; Noorbehbahani et al., 2022).

It was found that there are relatively few studies that systematically examine proctored online exams (Fatima et al., 2022; Kuleva & Miladinov, 2024; Mendez-Ortega, 2021; Najar & Ahmad, 2024; Oncul, 2021). While studies have emphasized that proctored online exams increase security in areas such as facial recognition, motion tracking, and fraud detection, these systems encounter problems such as privacy concerns, algorithmic biases, and digital literacy deficiencies (Fatima et al., 2022; Kuleva & Miladinov, 2024; Mendez-Ortega et al., 2021). It has been observed that proctored exams are effective in protecting academic integrity, but increase cost and student anxiety, while unproctored exams, although easy to administer, can encourage ethical violations (Oncul, 2021; Najar & Ahmad, 2024). It was concluded that low-cost, accessible, and student-friendly systems need to be developed, while larger data sets and adaptive algorithms are needed (Fatima et al., 2022; Mendez-Ortega et al., 2021).

Only one systematic review study was found in the literature analyzing research in the AI-SPOE application area (Nigam et al., 2021). Nigam et al. (2021) stated that AI-SPOEs are effective in improving cheating detection, authentication, and exam security and that these systems increase exam reliability with techniques such as biometric verification, facial recognition, motion detection, and continuous authentication. In the same study, it was emphasized that privacy concerns data security issues, high cost, and network infrastructure requirements limit the large-scale application of these technologies. In addition, the risk of AI algorithms producing false positives and causing ethical concerns among students stands out as important factors affecting the acceptability of these systems.

This study, which examines the articles on AI-SPOEs in Scopus and Web of Science databases, differs from other studies in the field in that it covers current research published in 2024. As one of the few literature reviews on AI-SPOEs, the study identifies the gap in the literature and serves as a guide for both educators and policy makers. In addition, the study makes inferences about the future of AI-SPOEs in education in the context of ethical dimensions, student experiences and technological developments. In this direction, the study aims to understand the conceptual structure of existing research on AI-SPOEs in depth. In line with this purpose, the study will seek answers to the following research questions:

- What is the distribution of the most used words in AI-SPOE studies?
- What are the tools and algorithms used in AI-SPOE?
- What are the methods of ensuring exam integrity in AI-SPOE?
- What are the problems/challenges in AI-SPOE?
- What are the recommendations for the future of AI-SPOE?

METHOD

A systematic literature review was used in the study. According to Moher et al. (2015), a systematic review's main purpose is to answer a specific research question by bringing together all relevant evidence that meets predetermined criteria. Systematic reviews adopt a systematic search process to identify studies that meet these eligibility criteria and allow for an explicit synthesis of the characteristics and findings of the included studies.

As an alternative to such traditionally conducted literature reviews, the use of semi-automated methods is recommended (Audrin & Audrin, 2022). Due to the large amount of relevant data available in the early stages of the literature review process (Ananiadou et al., 2009; Fabbri et al., 2013), researchers need to utilize text analysis and automatic data extraction techniques (Thomas et al., 2011). In such studies, when the number of classes used in article evaluation increases, valuable results can be obtained by integrating tools such as text mining into the systematic structure at the coding stage (Karami et al., 2020). Text mining is an effective method that helps to reveal new insights by facilitating large-scale information analysis and is increasingly used in educational research (Ferreira-Mello et al., 2019). However, these methods seem to be underutilized in scientific articles in the field of education and systematic literature reviews on AI-SPOE. Text mining is a highly effective tool for understanding the literature on AI-SPOE, especially given its ability to perform analyses on large datasets. This method is designed to fulfill three main functions. These are (1) facilitating information retrieval, (2) making meaningful inferences from existing information, and (3) conducting in-depth analyses by highlighting direct and indirect relationships between various pieces of information (Thomas et al., 2011). These processes are critical for conducting the systematic literature review.

Data Screening Process of the Study

The databases used for literature review include Scopus and Web of Science. In this process, the two databases were searched several times separately by two researchers and all studies that fall within the scope of the inclusion/exclusion criteria were tried to be reached. The articles in this study were accessed between October and November 2024. Accordingly, the inclusion and exclusion criteria are given in Table 1.

Table 1. Inclusion and exclusion criteria

Criteria for Acceptance	Written as an article Written in English Being open access Systematic reviews
Criteria for Non-Acceptance	Publications such as papers, technical reports, preprints, withdrawn, etc. Not relevant to the research topic

Selection of Articles

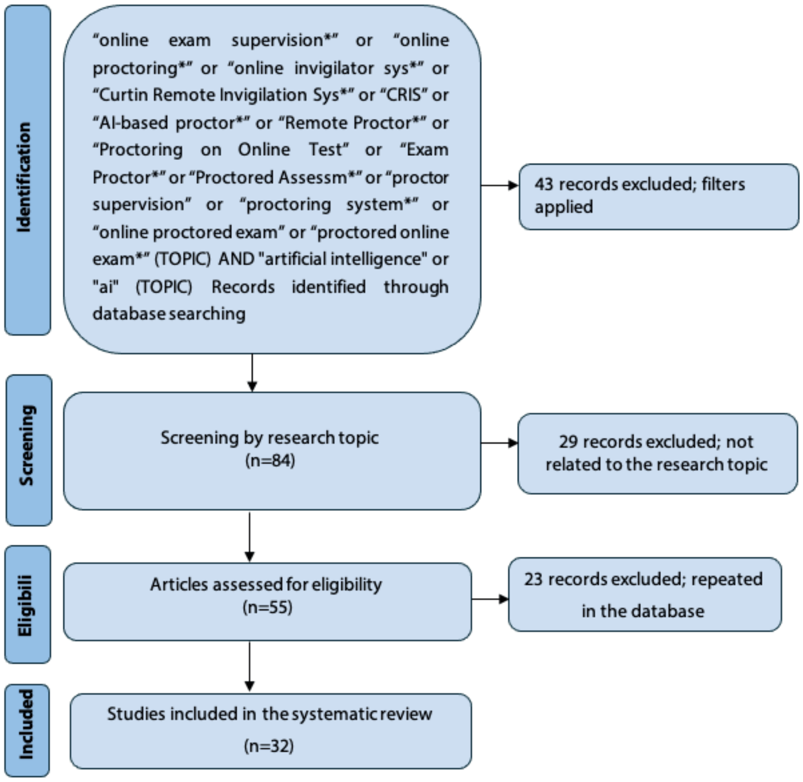

Figure 1. Prisma of article selection

As a result of the unfiltered search with the keyword group in Figure 1, a total of 127 articles were found in Web of Science (n=70) and Scopus (n=57) databases. For each search, the filters of "Article" type, "written in English" and "Open Access" were applied in the databases. According to the relevant criteria, 43 articles were excluded from the study, leaving a total of 84 articles from Web of Science (n=41) and Scopus (n=43) and databases. When 29 articles "not related to the research topic" were excluded from the study in the two databases, a total of 55 articles remained. It was determined that 23 of these articles were repeated in the databases. Finally, 32 articles remained (See Table 1).

Table 2. Literature review: Related studies examined within the scope of the study

ID	Authors	Article Title	Source Title	Country	Type of Proctored
[1]	Woldeab & Brothen (2019)	Online proctoring, test anxiety, and student performance	International Journal of E-Learning & Distance Education	USA	Synchronous
[2]	Daftary et al. (2020)	Case study: Innovation in experiential learning or assessment implementing virtual experiences and remote assessments during the covid-19 pandemic: A college experience	Pharmacy Education	USA	Automatic
[3]	Slusky (2020)	Cybersecurity of online proctoring systems	Journal of International Technology and Information Management	USA	Mixed
[4]	Sinha et al. (2020)	Remote proctored theory and objective online examination.	International Journal of Advanced Networking and Applications	India	Automatic
[5]	Langenfeld (2020)	Internet-based proctored assessment: Security and fairness issues	Educational Measurement: Issues and Practice	USA	Mixed
[6]	Labayen et al. (2021)	Online student authentication and proctoring system based on multimodal biometrics technology	IEEE Access	Spain	Automatic
[7]	Nigam et al. (2021)	A systematic review on AI-based proctoring systems: Past, present and future	Education and Information Technologies	India	Mixed
[8]	Paredes et al. (2021)	Remote proctored exams: Integrity assurance in online education?	Distance Education	Mexico	Automatic
[9]	Coghlan et al. (2021)	Good proctor or "big brother"? Ethics of online exam supervision technologies.	Philosophy and Technology	Australia	Mixed
[10]	Saba et al. (2021)	Categorizing the students' activities for automated exam proctoring using proposed deep l2-graftnet CNN network and ASO based feature selection approach	IEEE Access	Saudi Arabia	Automatic
[11]	Mutawa & Sruthi (2022)	Students' perspective towards online proctoring in exams during covid-19	Journal of Engineering Research (Kuwait)	Kuwait	Mixed
[12]	Yoder-Himes et al. (2022)	Racial, skin tone, and sex disparities in automated proctoring software	Frontiers in Education	USA	Automatic
[13]	Eaton (2022)	The academic integrity technological arms race and its impact on learning, teaching, and assessment	Canadian Journal of Learning and Technology	Canada	N/A
[14]	Surahman & Wang (2022)	Academic dishonesty and trustworthy assessment in online learning: A systematic literature review	Journal of Computer Assisted Learning	Taiwan	N/A
[15]	Henry & Oliver (2022)	Who will watch the watchmen? The ethico-political arrangements of algorithmic proctoring for academic integrity	Postdigital Science and Education	UK	N/A
[16]	Jia & He (2022)	The design, implementation and pilot application of an intelligent online proctoring system for online exams	Interactive Technology and Smart Education	China	Automatic
[17]	Nurpeisova et al. (2022)	The study of mathematical models and algorithms for face recognition in images using python in proctoring system	Computation	Kazakhstan	N/A
[18]	Renzella et al. (2022)	Verifying student identity in oral assessments with deep speaker	Computers and Education: Artificial Intelligence	Australia	N/A
[19]	Tweissi et al. (2022)	The accuracy of AI-based automatic proctoring in online exams	Electronic Journal of e-Learning	Jordan	Mixed
[20]	Nurpeisova et al. (2023)	Research on the development of a proctoring system for conducting online exams in Kazakhstan	Computation	Kazakhstan	Mixed

[21]	Mitra (2023)	Redesign of online proctored exams for stem learners in higher education institutions: Proposal for incorporating higher-order thinking skills and democratic pedagogy via Operhot platform	FEMS Microbiology Letters	India	Synchronous
[22]	Fidas et al. (2023)	Ensuring academic integrity and trust in online learning environments: A longitudinal study of an AI-centered proctoring system in tertiary educational institutions	Education Sciences	Greece	Automatic
[23]	Sattar et al. (2023)	An advanced and secure framework for conducting online examination using the blockchain method	Cyber Security and Applications	Bangladesh	Automatic
[24]	Tejaswi et al. (2023)	Proctor net: An AI framework for suspicious activity detection in online proctored examinations	Measurement	India	Automatic
[25]	Tejaswi (2023)	An automated online proctoring system using attentive net to assess student mischievous behaviour	Multimedia Tools and Applications	India	Automatic
[26]	Jacobs & Mncube (2023)	Proctoring as a human substitution for online summative assessments in a comprehensive open distance e-learning institution: Opportunities and obstacles	Independent Journal of Teaching and Learning	South Africa	Mixed
[27]	Close et al. (2024)	The ethical consequences, contestations, and possibilities of designs in educational systems	TechTrends	USA	N/A
[28]	Verma et al. (2024)	Automated smart artificial intelligence-based proctoring system using deep learning	Soft Computing	India	Automatic
[29]	Gopane et al. (2024)	Cheat detection in online examinations using artificial intelligence	ASEAN Engineering Journal	India	Automatic
[30]	Dang et al. (2024)	Auto-proctoring using computer vision in MOOCs system	Multimedia Tools and Applications	Vietnam	Automatic
[31]	Valkova (2024)	Remote proctoring in language assessment: Exploring the impact on test-takers' scores and perceptions	Studies in Language Assessment	UK	Automatic
[32]	Liu et al. (2024)	Multiple instances learning for cheating detection and localization in online examinations	IEEE Transactions on Cognitive and Developmental Systems	China	Automatic

Most of the reviewed studies (59%) dealt with automated proctoring systems, while 28% examined mixed methods and only 6% examined simultaneous surveillance systems. In addition, 9% did not specify any technical surveillance method, but rather adopted a conceptual or literature-based approach. In terms of methodology, a significant number of studies included qualitative case studies, systematic reviews, technology-oriented application development studies, and survey-based quantitative research.

Again, the vast majority of studies have focused on the contributions of online proctoring systems in increasing academic integrity, authentication, or reducing cheating behavior. Artificial intelligence-based models have been reported to achieve high accuracy rates. On the other hand, some studies have discussed the ethical issues that arise in the use of the systems, while others have found that they can increase test anxiety and create inequality, especially for students with low technical skills.

Finally, it is observed that most of the studies provide case studies limited to specific countries or institutions. This is a major methodological limitation that reduces the generalizability of the findings. For example, many implementation studies only covered trials at one university and did not test the long-term results of use or the functioning of the system in different cultural contexts. Furthermore, most of the studies that developed technical systems focused only on model accuracy in a laboratory setting and did not adequately consider the actual user experience and student-teacher interactions.

Data Analysis and Validity-Reliability

In this study, Leximancer, a text mining tool, was used to analyse the relationships between the most frequently used words within the scope of the first research question. Leximancer is a powerful analysis software that automatically identifies conceptual structures in the text and visualises the relationships between these structures through thematic concept maps. In this way, the main concepts of the study and the relationships between these concepts were analysed in a structured framework. In addition, 32 articles covering the other research questions were analysed in depth by the first and second authors of the study through content analysis method. The content analysis process was conducted systematically to ensure validity and reliability in qualitative research. Firstly, a standard content analysis form was developed in line with the research questions and the relevant theoretical framework. This form was structured to include categories such as tools and algorithms, methods, problems/challenges and recommendations. Finally, the form was finalised after being reviewed by a field expert.

Before proceeding to the analysis process, the first and second authors of the study independently coded five randomly selected co-authored articles within the scope of the pilot study. This practice aimed to test the functioning of the coding framework and to evaluate the inter-coder agreement before starting the content analysis. In addition, the number of articles examined in this pilot study conducted before the analysis was between 10% and 20% of the total sample, as recommended by Hazzi and Maldaon (2015), which is in line with the pilot study rates recommended in qualitative data analysis. Within the scope of validity and reliability, the internal consistency rate between these codings was calculated as 92%. This rate is above the minimum acceptability level of 80% suggested by Miles and Huberman (2010) and this shows that the inter-coder reliability in the study is high.

The first two authors each independently analysed 16 articles and completed the content analysis form. The coding process was carried out both based on predetermined themes (deductive approach) and by adding new codes derived from the data during the analysis process (inductive approach). The coded data were systematically entered into the content analysis form and the textual equivalent of each code was clearly stated. After the coding process was completed, the third author and the field expert reviewed all content analysis forms, checked possible errors in data entry and evaluated coding consistency. In the solution of the disagreements experienced during the control process, all researchers discussed the coding results and provided a common opinion.

Various strategies were applied to increase the validity and reliability of the study. Internal validity (accuracy) was ensured by presenting the systematic review process in detail and by involving more than one researcher in the analysis process. External validity (transferability) was secured by elaborating the data collection process. Internal reliability (consistency) was ensured through multiple control steps and common coding in the coding process, while external reliability (verifiability) was ensured by reporting the data collection and analysis processes in detail (Yalman & Uzunoz, 2021). All these practices support that the study is based on a solid methodological foundation and the reliability of the findings.

FINDINGS

RQ1. Distribution of the Most Used Words in AI-SPOE Studies

The findings obtained under this heading will contribute to revealing the conceptual framework of the field in line with the aim of the study and which themes are emphasised in literature. It will also lead to a strategic insight that will guide similar studies in the future. In this regard, abstracts and keywords were subjected to concept map analysis with the help of Leximancer text mining tool and various themes were revealed. This analysis method is used to transform lexical association information from natural language into semantic and relational patterns in an unsupervised manner (Smith & Humphreys, 2006). The results of the analysis are given in Figure 2.

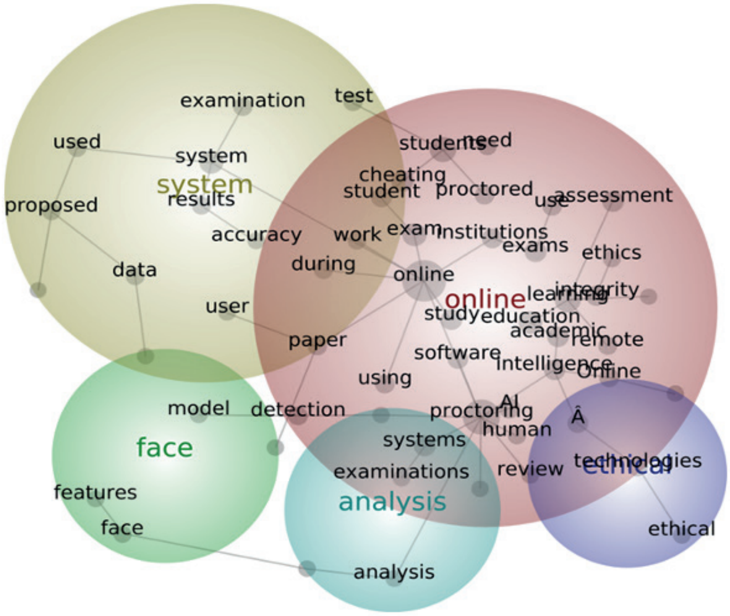

Figure 2. Concept map of abstracts and keywords visualized through text mining.

As a result of the analysis (See Figure 2), the theme "online" (Hits=147) was the most prominent. In this theme, the words learning, proctoring, students, exam, cheating, assessment, AI, systems, integrity, software, technology, detection, remote, ethics, and algorithms were related to each other. This theme shows that online proctored exams are closely related to AI-supported technological systems, ethical principles, algorithms, academic integrity, fraud detection, and remote exam practices. While AI systems play an active role in proctoring exams and fraud detection, ethical principles form a fundamental basis for issues such as student privacy and fair assessment. Algorithms are used to make exam processes meaningful and reliable. Remote exams, on the other hand, provide geographical flexibility but also bring challenges such as security and ethical concerns. This analysis emphasizes the importance of implementing online exams reliably and ethically, supported by technological solutions. Another theme obtained within the scope of the analysis is "system" (Hits=89). In this theme, the words examination, paper, test, results, proposed, accuracy, features, user, and time were related to each other. This theme provides important clues about the functioning of proctored exam systems and the basic elements of these systems. It also draws attention to the importance of considering elements such as accuracy, user-friendly features, time management, and result reliability as a whole in the design and implementation of proctored exam systems. Other prominent themes in the study were data (Hits=50), analysis (Hits=24), and ethical (Hits=21). Within the scope of these themes, it is seen that the words face, model, recognition, ethical, and academic dishonesty are related to each other. Data, analysis, and ethical themes focus on data use, analysis processes, and ethical dimensions in proctored exams. The Data theme emphasizes the role of facial recognition technologies in authentication and suspicious behaviour detection. The analysis theme addresses the processing of this data and fraud detection with AI models, while the ethical theme emphasizes the fair, ethical, and student privacy-friendly use of technology. These themes reveal that the effective use of technology as well as ethical principles and the protection of academic integrity are critical. The concept map for the themes obtained within the scope of this research question is given in Figure 2.

t-SNE, a nonlinear dimensionality reduction technique that aims to preserve the local structure of unsupervised data, is used to analyze and visualize high-dimensional data (Van der Maaten & Hinton, 2008). To identify the focal points of the articles, t-SNE analysis was performed using textual data collected from the abstract and keywords of the studies, and the findings are shown in Figure 3.

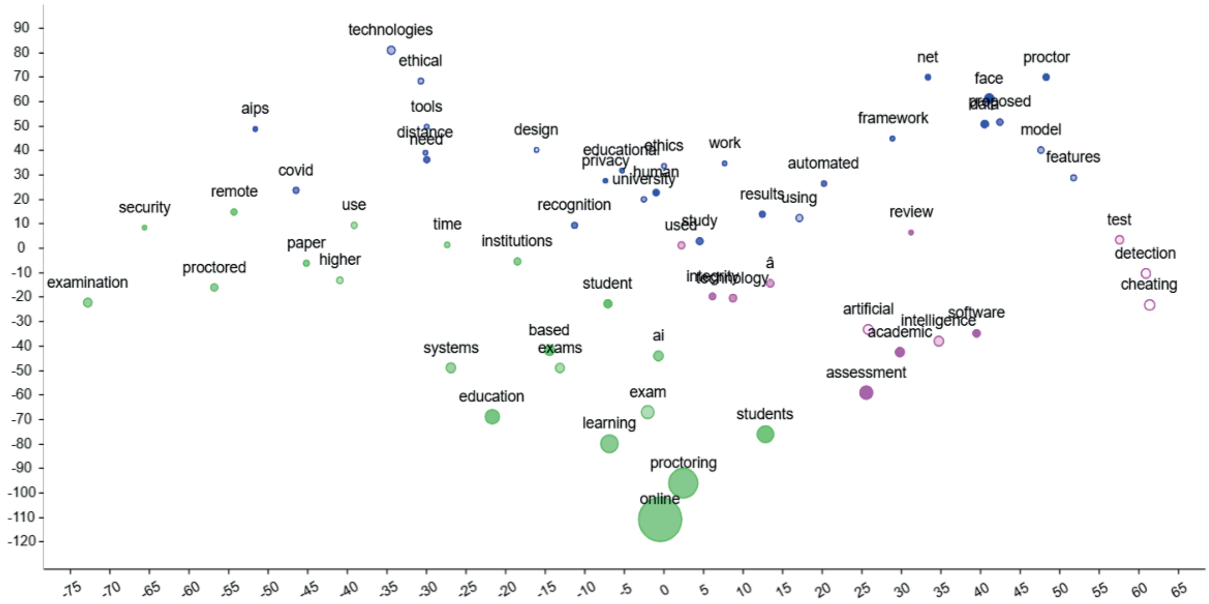

Figure 3. t-SNE analysis of abstracts and keywords of articles

According to Figure 3, there are three main clusters: green, pink, and blue. In the green cluster, which is the largest cluster, online, proctoring, learning, students, exams, systems, and AI stand out. In addition, security, higher education, and remote are other terms used in this cluster. It can be said that these words emphasize proctored systems and AI in assessment and evaluation exams in online learning. In the other cluster, pink, the concepts of assessment and evaluation, artificial intelligence, software, and technology were prominent. In addition to these concepts, the words test, detection, and cheating were also used. These concepts can be said that AI and software technologies are used to detect cheating in assessment and evaluation exams. Finally, in the blue cluster, the keywords face, data, model, proctor, recognition, ethical, privacy, and automated were prominent. It can be said that the words in this cluster can reveal the ethical and privacy violations that automatic face recognition models may create in online proctored exams.

RQ2. Tools and Algorithms Used in AI-SPOE Studies

Under this heading, the tools and algorithms used in the development of systems for ensuring exam integrity in studies on AI-SPOE are mentioned. These tools and algorithms are generally used for purposes such as authentication or image processing. These tools and algorithms are shown in Figure 4.

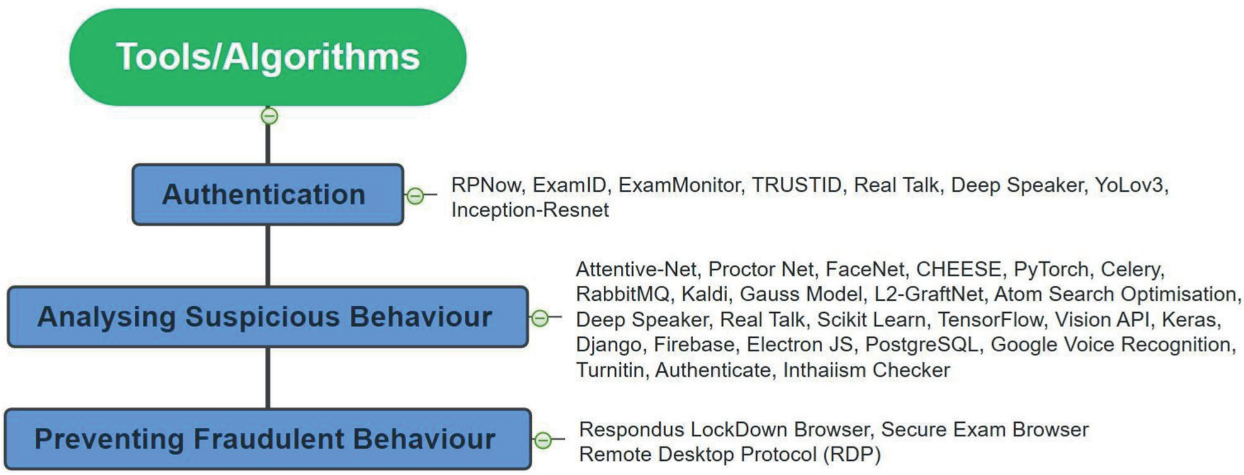

Figure 4. Tools and algorithms used in AI-SPOE

Figure 4 shows that the tools and algorithms used are grouped under three categories: authentication, analysing suspicious behaviour, and preventing fraudulent behaviour. Biometric verification methods such as face recognition, voice recognition, eye recognition, and fingerprint analysis are generally used to authenticate students in online exams and to prevent impersonation behaviour. RPNow [8], ExamID [2], and ExamMonitor [2] are the main tools used for authentication in online exams. Similarly, TRUSTID [22] application supported by technologies such as SpeechBrain [22], and PostgreSQL [20][22] is another application used for face and voice authentication. Real Talk [18] and Deep Speaker [18] systems contribute to the real-time authentication of students during exams. Finally, models such as YoLov3 [20] and Inception-Resnet [24] have been used to improve face recognition efficiency.

In addition to authentication, it is important to analysing suspicious behaviours of students during the exam to ensure online exam security. In this context, video and image processing tools are generally utilized. Tools such as Attentive-Net [24], Proctor Net [26], and FaceNet [29] are among the tools used to detect suspicious behaviour of students thanks to their eye gaze tracking, mouth movement tracking, and head pose estimation features. Furthermore, systems such as CHEESE [32] provide contextual analysis for cheating detection by extracting multimodal features. For video and audio processing, tools such as PyTorch [16], Celery [22] and RabbitMQ [22] have been used. High-performance deep learning inference optimizers such as TensorRT [16] are also integrated to process and optimize video data. Machine learning algorithms and deep neural networks were also used to analyze student activities during the exam and detect cheating. Models such as L2-GraftNet [10] and Atom Search Optimization (ASO) [10] have achieved effective results in identifying and classifying exam behaviours. Machine learning frameworks such as Scikit Learn [29], TensorFlow [16], Vision API [20], and Keras [24][25] have facilitated the creation and implementation of neural network models. For the development of these systems, technologies such as Django [20][22], Firebase [4], Electron JS [6], and PostgreSQL [20] [22] were utilized.

In online exams, voice and text detection technologies are other tools used to identify suspicious behaviours of students. These technologies have been used to detect unauthorized communication between students during exams. Kaldi [6] and Gaussian Mixture Models (GMM) [6] have been used to detect voice activity in online exams. The Google voice recognition API [19] was used to convert voice inputs into text. Software such as Turnitin, Authenticate, and Inthaiism Checker [14] have been used to detect plagiarism, especially copy-and-paste texts, within the scope of text detection technologies [23][24]. The methods used in plagiarism detection include semantic-based and grammar-based methods.

Another method used to ensure online exam security is to impose some restrictions to prevent students from resorting to cheating behaviour. In this direction, lockdown browsers and network restriction tools appear as system components used in AI-supported systems. Respondus LockDown Browser [3] and Secure Exam Browser (SEB) [19] are tools that allow students to access only the exam tab during the exam and restrict other applications. Remote Desktop Protocol (RDP) [23] was used to monitor network interactions and prevent non-exam access [24].

RQ3. Methods of Ensuring Exam Integrity in AI-SPOE Studies

Under this heading, the cheating detection methods used to ensure exam integrity in the studies conducted on AI-SPOE are included. These methods mentioned in the related studies are shown in Figure 5.

Figure 5. Methods for ensuring exam integrity within AI-SPOE

According to Figure 5, cheating detection methods used to ensure exam security are categorized under four categories. These categories are named as authentication mechanisms, real-time monitoring, denial of access to devices, and ensuring exam security. One of the first methods that exam systems proctored use to increase the security of online exams and ensure academic integrity is authentication mechanisms. In this context, methods such as face recognition [2][5][6][22][23][27], voice authentication [5][6][23], writing style recognition [7][23], and biometric analysis such as fingerprint reading, eye/iris scanning [4][6][30][32][33] are used. These systems provide functions such as face spoofing detection and authentication. Continuous verification mechanisms focus on detecting attempts by students to take exams with fake identities or pre-recorded images. For example, systems provide authentication by comparing live images with recorded photos [28] and analyzing mouth movements [25][29] to detect facial forgery.

Another way to ensure exam security within AI-SPOE is to monitor student behaviour during the exam in real time to detect abnormal behaviour and cheating attempts. Detections are based on recording video and audio streams [19] and using advanced algorithms to detect cheating attempts [4]. In cheating detection, AI analyzes students' behavioural indicators such as eye movements [20][25][26][30][33], head positions

[33], emotion detection [29] and body posture [30][31]. For example, eye gaze tracking [33] monitors the degree to which students focus on the exam, while head position analysis evaluates students' attention to the environment. By extracting multimodal features such as facial and behavioural analysis, the systems identify abnormal events to flag suspicious situations. For example, micro-expressions and gesture analysis are used to detect abnormal movements. The system flags unusual sounds and light changes as suspicious activities.

Another method used by AI-powered proctored systems to identify abnormal and fraudulent behaviour is environmental monitoring to detect other people in the environment or unauthorized device use. 360-degree camera images [18][20][23][26][27][28], microphone and desktop screen recordings are used to monitor students' exam environment. By analyzing the captured video footage and ambient sounds, the system can identify situations where another person can help the student off-screen. Speech analysis, phone usage detection [29], and active window tracking are used to detect violations such as the use of unauthorized devices or materials. Furthermore, lockdown scanners and network connection limitations increase the security of the exam process by preventing students from accessing external resources during the exam. Again, AI-powered software monitors the student's keyboard input, screen activities, and voice communications. Keyboard sniffer programs [4][8][21] can detect unauthorized access attempts during the exam.

Finally, another method used to ensure online exam integrity is to increase exam security. In general, advanced technologies such as blockchain-based systems [3] are used for data security. At the same time, institutions adopt a multi-layered approach to minimize cheating attempts by implementing high-quality exam design [14], randomized question ordering [24], and adaptive examination methods [14]. Moreover, plagiarism prevention software [24] and automated AI-based proctored systems are deployed to protect academic integrity

RQ4. Problems/Challenges in AI-SPOE Studies

The problems encountered in the studies examined within the scope of AI-SPOE were analyzed. The findings are given in Figure 6.

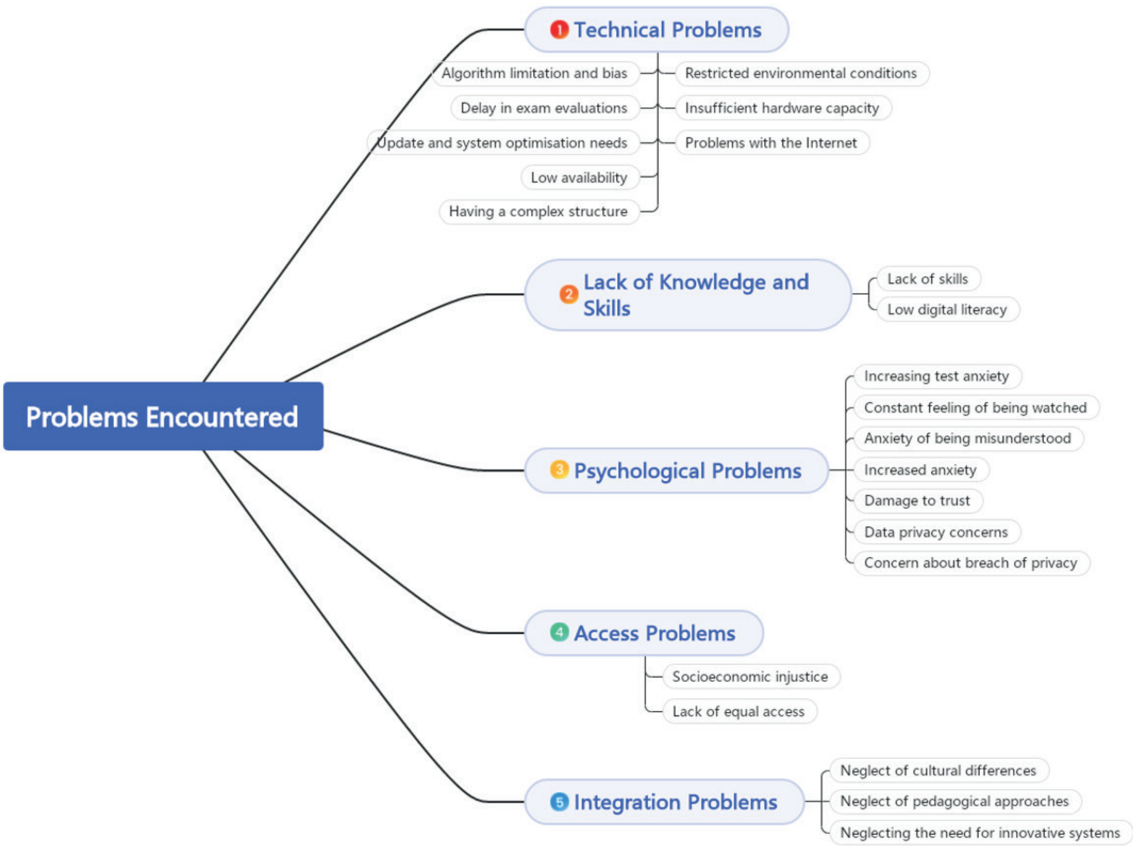

Figure 6. Issues/challenges in AI-SPOE implementations

Figure 6 shows that the problems encountered are grouped under five categories: technical problems, lack of knowledge and skills, psychological problems, access problems, and integration problems. Technical problems experienced by both students and faculty members are the first of the major criticisms expressed against these systems. Face recognition errors [3] in these systems cause students to experience difficulties in the authentication process and this raises concerns about digital proctored. Similarly, limited environmental conditions such as low light and loud noise [2][17][23][30][32] and insufficient hardware capacity for the devices used in online exams [3][4][5][23][26][30] increase the error rates of the systems [4][6]. Internet-related interruptions or quota problems are among other technical problems [4][5][6][19][23][26]. In addition, while the use of much hardware together creates a complex structure [3][7][17][19][23][26], this situation brings the perception of low usability [19] to the forefront. Another consequence of this situation is the need for updates and system improvements [21]. Again, because of the technical limitations mentioned above [11][19][21][28][31], it can be mentioned that image quality decreases and exam evaluations are delayed. The significant delay in reporting times [2] negatively affects the grading and feedback process.

Other technical problems include concerns about algorithm limitation and biases. These limitations reduce the cheating resilience of the systems [2][7]. This can lead to false cheating detections, resulting in questioning of students who do not engage in cheating behaviour [19][21][28][29]. AI-based proctored systems can disproportionately affect certain groups, such as students of color and women, especially due to biases in facial recognition algorithms [30]. The false flagging of students with darker skin tones has demonstrated the discriminatory potential of such software. This highlights the need to consider both socioeconomic differences and the diversity of the datasets used in training the systems.

Within the second category, lack of skills and low digital literacy levels are expressed as the problems encountered [9][16][24][26]. This situation may cause individuals not to use digital technologies effectively and not to analyze the information they may encounter in the online environment correctly. In addition, lack of skills and low digital literacy levels may increase student anxiety during the use of these complex systems [9][16][24][26].

Another problem encountered in studies on AI-SPOE is the negative psychological impact of proctored systems on students. Proctored systems can increase students' test anxiety and cause a decrease in their performance [1][5][15][21][31]. Students may have difficulty focusing on the test due to the feeling of being constantly monitored [5][7][11][27]. Again, the anxiety of not being misunderstood restricts students' movements [4]. This situation reflects negatively on exam results [5][7][8][11]. In addition, perceptions about the reliability of technology directly affect students' trust and overall satisfaction with these systems. In particular, the lack of transparency about the reliability and fair functioning of these systems can undermine trust between educational institutions and students [9][27]. Other negative pragmatic effects include concerns about data confidentiality and privacy [2][9][13][15][17][21][23]. In addition, the implementation of technologies such as biometric recognition and behaviour analysis has strengthened the perception of privacy violations among students.

In the implementation of proctored technologies, issues of equal access and socioeconomic justice have been frequently raised. Internet connectivity problems, low hardware capacity, and high costs have created significant barriers, especially for disadvantaged groups [4][5][14][23].

The last category under this heading is integration problems. The integration of technology into educational processes involves neglecting cultural differences, pedagogical approaches and innovative systems [7][19]. This can damage student-teacher relationships in the long run and lead to mistrust in the educational environment. Most importantly, a focus on preventing cheating through AI detection can lead to a narrow view of assessment, neglecting the need for innovative processes and systems that measure learning more effectively. There is a risk that the use of detection tools can reinforce entrenched power dynamics and decision-making norms in educational systems [27].

RQ5. Recommendations for the Future of AI-SPOE Systems

The recommendations in the studies examined within the scope of AI-SPOE were analyzed. The results of the analysis are given as categories and codes in Figure 7.

Figure 7. Recommendations for AI-SPOE

When Figure 7 is analyzed, four categories were formed under the recommendations heading: recommendations for educational environments, recommendations for developers, recommendations for researchers, and recommendations for decision-makers. Firstly, it is suggested that AI-supported systems can be used to ensure online exam security for educational environments [4][14][15][16][18][20][23][24][25][28]. However, educators should work on alternative assessment methods to complement the limitations of proctored technologies [11][15][27]. Methods such as project-based assessments, oral exams, and grading student participation can reduce cheating while providing more meaningful learning opportunities [5][6]. Giving students the freedom to choose different assessment tools instead of exams can reduce anxiety and increase motivation.

In these studies, three main recommendations for system developers were mentioned. The first one is to improve the user experience. To use proctored exam systems effectively, it is recommended to organize comprehensive training programs for faculty members and students [2][4][13][18][20][21][26]. To improve the user experience, systems should aim to include non-intrusive authentication methods and reduce privacy concerns related to the use of biometric technologies. In addition, collecting regular feedback from students and faculty members is important for both technical improvements and increasing satisfaction [8][20][25][26][27][29]. Other suggestions for system developers are the need for technical improvement of algorithms and existing systems. Continuous improvements to increase the accuracy of AI and machine learning algorithms in proctored technologies are recommended in this context [2][5][17][19][22][25]. It has been stated that algorithms used in face recognition, behaviour analysis, and fraud detection should be trained with larger and more diverse datasets [28][29][30][32]. In addition, solutions that can adapt to low hardware capacities should be developed to increase the accessibility of examination platforms. It is also recommended to develop and implement hybrid models that combine AI and human supervision in proctoring systems [6][7][13][19][25][28]. These models can reduce false positive markings and address ethical concerns about students. Hybrid systems can provide higher accuracy in cheating detection through human and machine collaboration. Finally, the integration of new technologies such as blockchain can help improve data security and the integrity of exams [3].

In the studies conducted for AI-SPOEs, it is recommended that clear guidelines regarding the ethics and confidentiality of online proctored technologies should be set for decision-makers [3][5][6][7][11][15][26]. Within the scope of collaboration between stakeholders, transparent management processes should be established to increase trust, especially between students and educators, and stakeholders' perspectives should be considered [9][13][23][27]. In addition to online proctored technologies, human-centered approaches should be prioritized in learning and assessment processes. Policies should be developed to use technology not only to prevent cheating but also as a tool to promote student achievement [7][8][13]. Finally, the use of proctored systems should be made accessible to all [4][5][6][16][21][29]. Steps should be taken to address the disadvantages of students with limited access to basic resources such as hardware and internet access.

Recommendations for researchers include conducting more large-scale and long-term research to measure the effects of proctored systems and improve future practices. Issues such as academic integrity, pedagogical effects [15], student satisfaction, and reliability of systems should be comprehensively examined in different educational contexts [2][3][5][10][19][27][31].

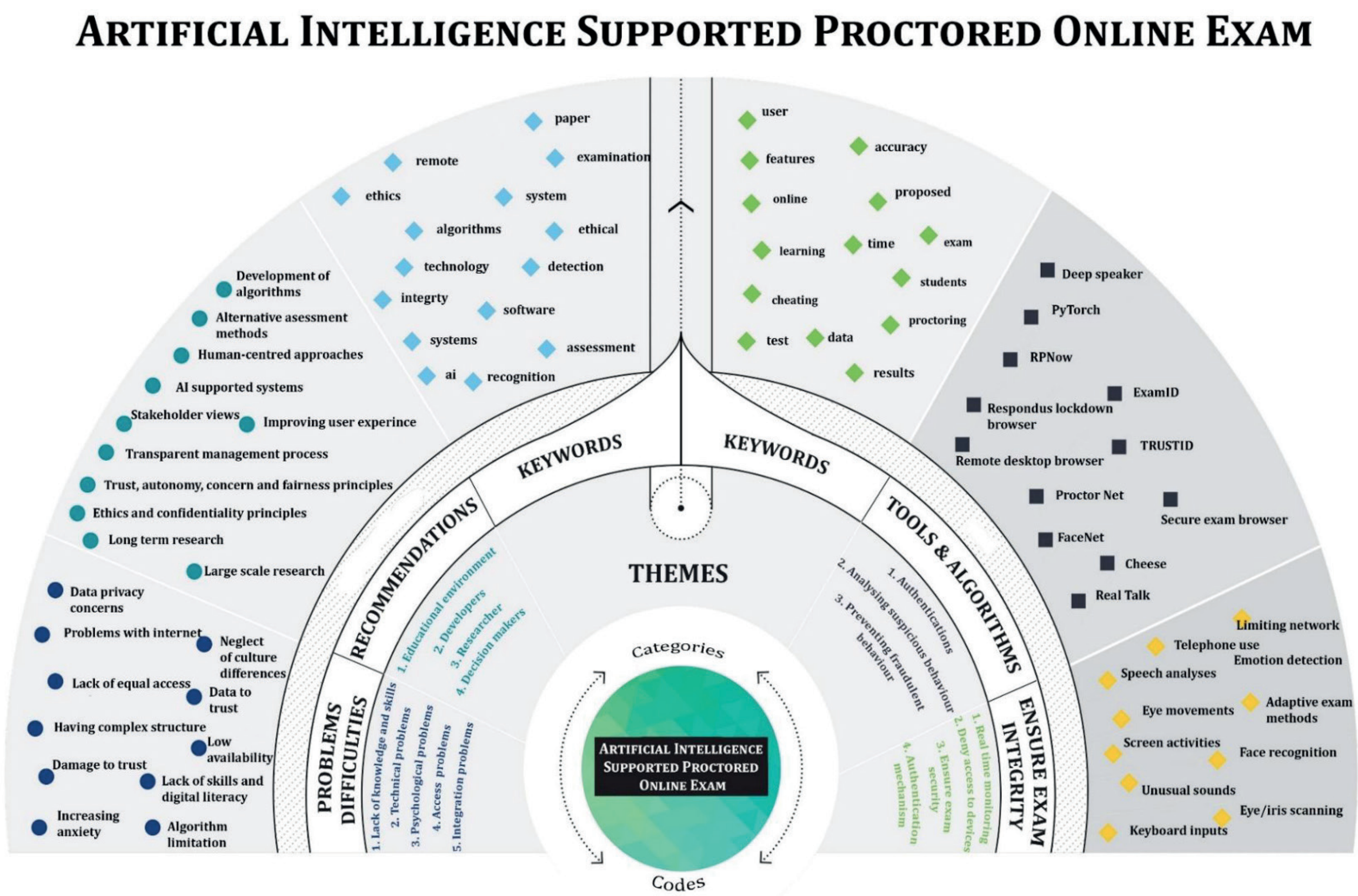

Figure 8. Summary of findings

DISCUSSION

The study aims to provide an in-depth understanding of the conceptual structure of research on AI-SPOEs. For this purpose, 32 related studies in Web of Science and Scopus databases were analyzed with Systematic Literature Review. Within the scope of the analysis, keywords used, tools and algorithms used, problems encountered, methods of ensuring exam integrity, and recommendations were examined.

AI-SPOE authentication uses different tools and algorithms to detect suspicious behaviour and prevent fraudulent behaviour. Tools such as TRUSTID, Proctorlock, ProctorU, ExamID/ExamMonitor can authenticate students by analyzing their unique biometric characteristics (face, voice, eye, fingerprint, etc.) to increase exam security. It is known that such low-cost and fast response (Zimik & Keishing, 2021) authentication methods, especially face recognition algorithms (Abu-Ein & Masadeh, 2023; Haliassos et al., 2021; Mazaheri & Roy-Chowdhury, 2022), are effectively used in educational environments (Tanwar et al., 2019). Tools and algorithms such as CHEESE, Atentive Net, PyTorch face recognition model, RetinaFace, and Proctor Net can monitor student behaviour during exams and identify suspicious behaviour. Camera-based tracking and posture analysis is another widely used method for detecting cheating behaviours, especially during exam processes (Dilini et al., 2021; Samir et al., 2021). Multimodal analysis of different indicators such as head position, object detection, and eye movements together provide high accuracy rates in cheating detection (Abozaid & Atia, 2022). Finally, applications such as Respendus Lock Down Browser and Remote Desktop Protocol (RDP) restrict networks and browsers, preventing students from unauthorized access to devices and resources.

In AI-SPOEs, exam integrity is ensured through authentication, real-time monitoring, blocking access to devices and resources, and strategies to enhance exam security. It is noteworthy that these strategies are in line with the tools used and their intended use. As mentioned before, these systems can authenticate students by analyzing their unique biometric characteristics (face, voice, eyes, fingerprints, etc.). In this way, impersonation behaviour can be prevented, and exam integrity can be ensured. In addition, AI-supported software that analyzes keyboard input can examine behavioural data such as typing speed, editing habits, and writing style of students and use these analyses in authentication processes (Juola et al., 2013). Studies emphasize that biometric verification improves exam integrity, reduces reliance on passwords, and provides a reliable solution to authentication problems (Al Rousan & Intrigila, 2020; Sudar et al., 2019).

Another strategy AI-enabled systems use to ensure exam integrity is real-time monitoring. By monitoring eye movements and head positions during the exam, they can detect behavioural anomalies and potential cheating attempts. These technologies, which also detect the presence of other people in the room, make it possible to detect potential violations and intervene immediately (Irfan et al., 2021). With the help of 360-degree camera images, microphones, and screen recordings, fraudulent behaviour in online exams can be detected and prevented (Satre et al., 2023). In the literature, Nabil et al. (2022) and Kamalov et al. (2021) demonstrated the potential of deep learning models to increase exam integrity by monitoring students' movements and focus of attention. These studies emphasize the importance of innovative technology-supported approaches in ensuring exam integrity. For example, studies on speech analytics have shown that this technology is an effective tool for identifying people's emotional states from their speech or analyzing their behaviour (Bekmanova et al., 2022).

In online exams, another strategy used to increase exam integrity is the restriction of access to devices and resources. Locking scanners and network connection limitation tools aim to reduce the likelihood of cheating by restricting students' access to external resources during the exam. Monitoring screen activity also detects actions that may be intended for cheating (Tweissi et al., 2022). Research shows that these measures contribute to exam integrity (Slusky, 2020). However, some negative effects of the implementation of these technologies are also mentioned. It is known that the use of these tools can increase students' stress levels and cause more technical problems (Ruzgar & Chua-Chow, 2023).

Five main problems arise in AI-SPOE implementations. These problems are technical, lack of skills, negative psychological effects, equal access problems, and integration problems. Within the scope of technical problems, face recognition errors come first. This affects both the reliability and acceptability of the system (Yusuf et al., 2022). Problems such as low light conditions and ambient sounds are among the main factors that reduce the effectiveness of authentication algorithms (Zarkasyi et al., 2020). Connection interruptions and limited hardware capacities are also cited as other reasons for this situation (Green et al., 2021; Kharb & Chahal, 2023). Algorithmic biases and discrimination appear as another technical problem. Biases in face recognition algorithms disproportionately affect certain demographic groups, resulting in higher error rates for individuals with darker skin tones (Ntoutsi et al., 2020). The main reason for this situation, which has the potential to increase discrimination risks, is the lack of diversity in the data sets used (Jain & Menon, 2023). The fact that data sets predominantly include only certain demographic groups limits the generalization capacity of models and prevents them from producing egalitarian results (Roselli et al., 2019).

One of the major problems encountered in the implementation of AI-SPOEs is the negative psychological effects of the system on students. There are criticisms that the systems increase students' anxiety and worry while decreasing student performance (Wecks et al., 2024). One of the main reasons for this is that students feel that they are constantly being watched and cannot move too much to avoid being misunderstood (Langenfeld, 2020; Sinha et al., 2020). In addition, the constant monitoring situation increases the anxiety level in students and negatively affects exam performance, while it can damage student-teacher relationships and the trust environment (Birnhack & Perry-Hazan, 2020). These systems used in education not only provide security but also create a "sense of constant proctored" that aims to control student behaviour. This leads students to change the way they write and speak (Dawson, 2002). Moreover, lack of skills and low levels of digital literacy are other problems encountered in the implementation of AI-SPOEs. This situation causes individuals to be unable to use digital technologies effectively and analyze the information they may encounter in the online environment correctly. Apart from these, lack of skills and low digital literacy levels are other factors that increase student anxiety during the use of these complex systems (Jacobs & Mncube, 2023; Tejaswi et al., 2023).

Another problem encountered in the implementation of AI-SPOEs is the issue of equal access. While effective use of these technologies often requires costly hardware and strong internet connections, these requirements can create significant barriers for disadvantaged groups (Cecchini & Scott, 2003; Mossberger et al., 2012). For example, low-income households have difficulty accessing the necessary technological infrastructure, limiting participation in education and other digital services (Van Dijk, 2020). Lack of internet connectivity is a major problem, especially for individuals living in rural areas (Yaacoub & Alouini, 2020). Moreover, the high costs of proctored technologies create a financial burden for organizations with limited resources, such as schools and public institutions, which further limits the opportunities for disadvantaged groups to benefit from digital equality and deepens socioeconomic injustices (White & Black, 2022). In this context, policies should be developed both to overcome infrastructure deficiencies and to reduce the costs of these technologies in the dissemination of proctored technologies.

As a result, the problems experienced in AI-SPOE applications can be summarized as technical glitches, psychological effects, equal access difficulties and digital skills deficiencies. In solving technical problems, it is important to train algorithms with inclusive data sets and develop technologies that are sensitive to environmental conditions. To reduce psychological impacts, user-friendly, less intrusive designs and practices that foster an environment of trust should be adopted. Equal access problems can be addressed through low-cost technological solutions and investments in internet access in rural areas. In addition, training programs and information activities should be carried out to increase digital literacy levels. Overcoming these challenges requires addressing both technical and social dimensions through multifaceted strategies. In this context, ensuring a user-friendly interface and supporting learner autonomy—as emphasized in distance education textbook criteria—can enhance the pedagogical quality of such systems (Yavuz et al., 2020). Moreover, integrating designs that foster social presence can mitigate the 'cold' surveillance effect of AI, reducing transactional distance and creating a more humanized learning environment (Yavuz et al., 2025).

The AI-SPOEs recommend that policies on student privacy and ethical values should be clearly articulated for decision-makers. In particular, the proliferation of video proctored systems raises serious concerns that threaten students' privacy rights. Studies emphasize that proctored technologies lead to violations of children's data privacy and therefore human rights should be protected (Karagianni & Papakonstantinou, 2022). Moreover, the implementation of current practices without considering ethical and legal frameworks leads to a disruption of the balance between privacy and security. This is particularly evident in the use of video-proctored systems (Nagpal & Chaturvedi, 2016). These findings suggest that privacy and ethical principles must be considered in the implementation of proctored technologies in education. It has also been reported that online exam environments affect students' exam experiences and satisfaction (Henderson et al., 2022). Therefore, for the effective use of these technologies, it is important not only to focus on exam security but also to take supportive measures to improve students' experiences.

For AI-SPOE developers, algorithmic discrimination can impede social progress by reinforcing social inequalities and emphasizing the need for a wider diversity in data sets to create a fair system (Introna & Wood, 2004). In this context, ethical and legal principles should play a central role in the design and implementation of AI-SPOEs, and transparency and oversight mechanisms should be developed to identify and address biases (Varona & Suarez, 2022). All these elements are critical for AI-SPOEs to function in a fair, impartial, and credible manner.

For educational environments, hybrid proctored models are proposed to evaluate suspicious behaviour with the collaboration of AI and human observers. There is a growing interest in the effectiveness of this method in online exam security (Tweissi et al., 2022). While AI can quickly and systematically analyze large amounts of data such as keyboard input, facial expressions, voice communication, and screen activity (Juola et al., 2013), human observers are involved in assessing more complex or contextual situations. This is especially critical for AI-enabled systems to improve the accuracy and reliability of the assessment by weeding out false positives and negatives (Potluri & Sistla, 2022).

Finally, the future of AI-SPOE may be reshaped by innovative technologies such as explainable artificial intelligence (XAI), adaptive testing systems and learning analytics. Explainable AI can provide trust and accountability by increasing the transparency of system decisions (Gunning & Aha, 2019). Adaptive tests can offer more accurate and individualized measurement by dynamically adjusting the question level based on student performance (van der Linden & Glas, 2000). Learning analytics integration makes it possible to monitor not only achievement but also the learning process (Ifenthaler & Yau, 2020). Moreover, monitoring emotional states during an exam can support the assessment process from a cognitive and affective perspective (Picard, 1997). The use of these technologies in line with ethical principles will increase the social acceptance of these systems (Floridi & Cowls, 2019).

LIMITATIONS

Although this review adheres to a systematic process and incorporates text mining techniques to enhance the breadth of findings, several limitations should be noted. First, the search was confined to English-language and open-access publications within two databases (Scopus and Web of Science), potentially excluding relevant studies published in other languages or housed in other databases. Second, while text mining tools provided a robust overview of prevailing themes, these methods may inadvertently overlook context-specific nuances not captured by keyword frequency. Third, despite efforts to ensure reliability through multiple coders, the subjective nature of content analysis may still introduce interpretive bias. Finally, given the pace of AI development, it is possible that rapidly emerging technologies and newly published articles were not captured in the study's time frame. Future research could expand the search across additional databases, include non-English sources, and employ longitudinal approaches to assess how AI-supported proctored exam technologies evolve over time.

CONCLUSION AND IMPLICATIONS

This study comprehensively examined the use and impact of AI-SPOE in educational processes. The findings obtained through a systematic literature review show that AI-SPOE systems offer significant opportunities in terms of exam security and academic integrity. Technologies such as facial recognition, voice analysis, and behaviour tracking have been shown to provide high accuracy in authentication and cheating detection processes. However, the technical challenges, ethical issues, and algorithmic biases encountered in the implementation of these systems stand out as important issues that need to be resolved.

While students and lecturers appreciated the security and accessibility advantages of such systems, they also emphasized negative aspects such as privacy concerns and psychological effects. Privacy violations during the monitoring of exam environments and the possibility of systems producing false results hurt the acceptability of these technologies. Furthermore, socioeconomic inequalities and technological access issues make it difficult to implement AI-SPOE systems equitably.

The findings suggest that transparency in technology design, use of diverse data sets, and ethical guidance should be prioritized to make AI-SPOE systems more inclusive and fairer. Alternative assessment methods are recommended to be considered as a complementary approach to the limitations of proctored exams. Finally, the development of guidance programs for students and instructors in the integration of AI-SPOE into educational processes is critical to improve the user experience and increase trust. Finally, this study provides important insights on the role and impact of AI-SPOE technologies in educational settings and constitutes a valuable resource to guide policymakers, educators, and technology developers.

BIODATA and CONTACT ADDRESSES of AUTHORS

Aysin Gaye USTUN is an assistant professor at Sinop University Vocational School in Turkiye. She received her Ph.D. from Ataturk University's Department of Computer Education and Instructional Technology in Turkiye. Her academic interests include open and distance learning environments, educational technologies, artificial intelligence, and coding education at the K-12 level. She has worked in various departments, including as the Head of the Department of Computer Technology at Sinop University and at the Distance Education Center. She has authored book chapters, academic articles, and papers indexed in national and international databases.

Aysin Gaye USTUN
Department of Computer Technology, Vocational School
Address: Sinop University, 57000, Sinop, Turkiye
Phone: +90 368 271 57 57/6623
E-mail: austun@sinop.edu.tr

Bunyami KAYALI graduated from Erzincan University, Faculty of Education, Department of Mathematics Education in 2008. Between 2018 and 2022, he completed his doctorate at Ataturk University in Computer and Instructional Technologies Education. From 2008 to 2021, he taught at various institutions affiliated with the Ministry of National Education. Currently, he is employed as an Assistant Professor at Bayburt University, Department of Computer Technologies. His areas of research interest are distance education, instructional technology, and artificial intelligence.

Bunyami KAYALI
Department of Computer Technology, Technical Sciences Vocational School
Address: Bayburt University, 69000, Bayburt, Turkiye
Phone: +90 458 211 11 53
E-mail: bunyamikayali@bayburt.edu.tr

Mehmet YAVUZ graduated from the Department of Computer Education, Faculty of Technical Education, Firat University in 2009. Between 2018 and 2022, he pursued his doctoral studies in the Department of Computer Education and Instructional Technologies at Ataturk University. From 2011 to 2021, he served as a teacher in various institutions affiliated with the Ministry of National Education. He is currently an Assistant Professor at Bingol University, where he serves at both the Distance Education Application and Research Center and the Department of Management Information Systems. His research interests include digital transformation, distance education, instructional design, instructional technologies, and artificial intelligence.

Mehmet YAVUZ
Management Information Systems, Faculty of Economics and Administrative Sciences
Address: Bingol University, 12000, Bingol, Turkiye
Phone: +90 426 216 00 12
E-mail: myavuz@bingol.edu.tr

Aras BOZKURT is a researcher and faculty member at Anadolu University, Turkiye. With MA and PhD degrees in distance education, Dr. Bozkurt's work focuses on empirical studies in areas such as distance education, online learning, networked learning, and educational technology. He applies critical theories like connectivism, rhizomatic learning, and heutagogy to his research. Dr. Bozkurt is also interested in emerging research paradigms, including social network analysis, sentiment analysis, and data mining. Dr. Bozkurt's studies also cover the integration of artificial intelligence technologies into educational processes in the axis of human-machine interaction. His dedication to advancing the field is reflected in his editorial roles as the Editor-in-Chief of Open Praxis and Asian Journal of Distance Education, as well as his roles as an associate editor for prestigious journals like Higher Education Research and Development, Online Learning, eLearn Magazine, and Computer Applications in Engineering Education.

Aras BOZKURT
Open and Distance Learning Department, Open Education Faculty
Address: Anadolu University, 26470, Eskisehir, Turkiye
Phone: +90 222 335 05 80
E-mail: arasbozkurt@gmail.com

REFERENCES

Abozaid, A., & Atia, A. (2022, July). Multi-modal online exam cheating detection. In *2022 International Conference on Electrical, Computer and Energy Technologies (ICECET)* (pp. 1-6). IEEE.

Abu-Ein, A. A., & Masadeh, A. E. (2023, July). Face recognition method for online exams. In *2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)* (pp. 1-4). IEEE.

Al Rousan, M., & Intrigila, B. (2020). A comparative analysis of biometrics types: Literature review. *Journal of Computer Science*, *16*(12), 1778-1788. https://doi.org/10.3844/jcssp.2020.217.224

Ananiadou, S., Rea, B., Okazaki, N., Procter, R., & Thomas, J. (2009). Supporting systematic reviews using text mining. *Social Science Computer Review, 27*(4), 509–523. https://doi.org/10.1177/0894439309332293

Audrin, C., & Audrin, B. (2022). Key factors in digital literacy in learning and education: A systematic literature review using text mining. *Education and Information Technologies*, *27*(6), 7395-7419. https://doi.org/10.1007/s10639-021-10832-5

Aydemir, M., Erdogdu, E., & Ucar, H. (2024). Exploring online learners' perspectives in relation to proctored exams. *Turkish Online Journal of Distance Education*, *25*(4), 33-50. https://doi.org/10.17718/tojde.1459600

Bekmanova, G., Yergesh, B., Sharipbay, A., & Mukanova, A. (2022). Emotional speech recognition method based on word transcription. *Sensors*, *22*(5), 1937. https://doi.org/10.3390/s22051937

Berti, C., Molinari, L., & Speltini, G. (2010). Classroom justice and psychological engagement: Students' and teachers' representations. *Social Psychology of Education*, *13*(4), 541-556. https://doi.org./10.1007/s11218-010-9128-9

Birnhack, M., & Perry-Hazan, L. (2020). School proctored in context: High school students' perspectives on CCTV, privacy, and security. *Youth & Society*, *52*(7), 1312-1330. https://doi.org/10.1177/0044118X20916617

Butler-Henderson, K., & Crawford, J. (2020). A systematic review of online examinations: A pedagogical innovation for scalable authentication and integrity. *Computers & Education*, *159*, 104024. https://doi.org/10.1016/j.compedu.2020.104024

Bozkurt, A., Crompton, H., & Fell Kurban, C. (2026a). The Devil is in the Det[ai]ls: AI Agents, Ghost Students, and the Crisis of Verified Presence in an Agentic AI World. *Open Praxis*, *18*(1), 1–12. https://doi.org/10.55982/openpraxis.18.1.1145

Bozkurt, A. (2026b). *Reimagining curriculum and assessment in the age of generative AI.* IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-7579-3

Cecchini, S., & Scott, C. (2003). Can information and communications technology applications contribute to poverty reduction? Lessons from rural India. *Information Technology for Development*, *10*(2), 73-84. https://doi.org/10.1002/itdj.1590100203

Dawson, S. (2002). The impact of institutional proctored technologies on student behaviour. *Proctored & Society*, *4*(1/2), 69-84.

Dayananda, D. P. D., Vasanthapriyan, S., Chathumini, K. G. L., & Fernando, M. A. C. S. S. (2021). A systematic literature review on online exams in covid-19 pandemic: Assessment methods, students' preferences, dishonest behaviours and challenges in online exams. *2021 From Innovation to Impact (FITI)*, *1*, 1-6. https://doi.org/10.1109/FITI54902.2021.9833059

Dilini, N., Senaratne, A., Yasarathna, T., Warnajith, N., & Seneviratne, L. (2021, December). Cheating detection in browser-based online exams through eye gaze tracking. In *2021 6th International Conference on Information Technology Research (ICITR)* (pp. 1-8). IEEE.

Fabbri, S., Hernandes, E., Di Thommazo, A., Belgamo, A., Zamboni, A., & Silva, C. (2013). Using information visualization and text mining to facilitate the conduction of systematic literature reviews. In J. Cordeiro, L. a. Maciaszek, & J. Filipe (Eds.), Enterprise information systems (Vol. 141, pp. 243–256). Springer. https://doi.org/10.1007/978-3-642-40654-6_15

Fatima, T., Azam, F., & Muzaffar, A. W. (2022, October). A systematic review on fully automated online exam proctoring approaches. In *2022 24th International Multitopic Conference (INMIC)* (pp. 1-5). IEEE.

Ferreira-Mello, R., Andre, M., Pinheiro, A., Costa, E., & Romero, C. (2019). Text mining in education. *WIREs Data Mining and Knowledge Discovery, 9*(6), e1332 https://doi.org/10.1002/widm.1332

Floridi, L., & Cowls, J. (2019). A unified framework of five principles for AI in society. *Harvard Data Science Review*, *1*(1). https://doi.org/10.1162/99608f92.8cd550d1

Gunning, D., & Aha, D. (2019). DARPA's explainable artificial intelligence (XAI) program. *AI Magazine*, *40*(2), 44–58. https://doi.org/10.1609/aimag.v40i2.2850

Haliassos, A., Vougioukas, K., Petridis, S., & Pantic, M. (2021). Lips don't lie: A generalisable and robust approach to face forgery detection. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 5039-5049).

Hazzi, O., & Maldaon, I. (2015). A pilot study: Vital methodological issues. *Business: Theory and Practice, 16*(1), 53-62.

Holmes, W., Bialik, M., & Fadel, C. (2019). *Artificial intelligence in education promises and implications for teaching and learning*. Center for Curriculum Redesign.

Hussein, M. J., Yusuf, J., Deb, A. S., Fong, L., & Naidu, S. (2020). An evaluation of online proctoring tools. *Open Praxis*, *12*(4), 509-525.

Ifenthaler, D., & Yau, J. Y. K. (2020). Utilising learning analytics to support study success in higher education: A systematic review. *Educational Technology Research and Development*, *68*(4), 1961–1990. https://doi.org/10.1007/s11423-020-09788-z

Introna, L., & Wood, D. (2004). Picturing algorithmic proctored: The politics of facial recognition systems. *Proctored & Society*, *2*(2/3), 177-198.

Irfan, M., Aslam, M., Maraikar, Z., Jayasinghe, U., & Fawzan, M. (2021, December). Ensuring academic integrity of online examinations. In *2021 IEEE 16th International Conference on Industrial and Information Systems (ICIIS)* (pp. 295-300). IEEE.

Jain, L. R., & Menon, V. (2023, November). AI algorithmic bias: Understanding its causes, ethical and social implications. In *2023 IEEE 35th International Conference on Tools with Artificial Intelligence (ICTAI)* (pp. 460-467). IEEE.

Jui, T. D., & Rivas, P. (2024). Fairness issues, current approaches, and challenges in machine learning models. *International Journal of Machine Learning and Cybernetics*, 1-31. https://doi.org/10.1007/s13042-023-02083-2

Kaddoura, S., Popescu, D. E., & Hemanth, J. D. (2022). A systematic review on machine learning models for online learning and examination systems. *PeerJ Computer Science*, *8*, e986. https://doi.org/10.7717/peerj-cs.986

Kamalov, F., Sulieman, H., & Santandreu Calonge, D. (2021). Machine learning based approach to exam cheating detection. *Plos One*, *16*(8), e0254340.

Karagianni, A., & Papakonstantinou, V. (2022). Proctored in schools across Europe: A new phenomenon in light of the COVID-19 pandemic? The cases of Greece and France. *European Journal of Educational Research, 11*(2), 1219-1229. https://doi.org/10.12973/eu-jer.11.2.1219

Karami, A., Lundy, M., Webb, F., & Dwivedi, Y. K. (2020). Twitter and research: A systematic literature review through text mining. *IEEE access*, *8*, 67698-67717. https://doi.org/10.1109/ACCESS.2020.2983656

Karasar, N. (2008). *Bilimsel arastirma yontemi kavram-ilke-teknikler* [*Concept-Policy-Techniques for Scientific Research Method]* (18th Edition). Ankara: Nobel Yayinevi.

Kharb, L., & Chahal, D. (2023). Privacy Threats in facial recognition-based identity verification. *International Journal of Advanced Research in Science, Communication and Technology, 3*(5), 569-572. https://doi.org/10.48175/ijarsct-11686.

Kuleva, M., & Miladinov, O. (2024, June). Exploring the efficacy of online proctoring in online examinations: A comprehensive review. In *Environment, Technologies, Resources. Proceedings of the International Scientific and Practical Conference* (Vol. 2, pp. 192-196).

Lee, K., & Fanguy, M. (2022). Online exam proctoring technologies: Educational innovation or deterioration?. *British Journal of Educational Technology*, *53*(3), 475-490. https://doi.org/10.1111/bjet.13182

Mazaheri, G., & Roy-Chowdhury, A. K. (2022). Detection and localization of facial expression manipulations. In *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision* (pp. 1035-1045).

Mendez-Ortega, M. G., Herrera-Granda, E. P., Malte, A. E., & Enriquez, R. B. (2021). Supervision and control of students during online assessments applying computer vision techniques: A systematic literature review. *Universal Journal of Educational Research*, *9*(5), 1000-1013. https://doi.org/10.13189/UJER.2021.090513

Miles, M, B., & Huberman, A. M. (2010). *Qualitative data analysis: An expanded Sourcebook*. Sage.

Moher, D., Shamseer, L., Clarke, M., Ghersi, D., Liberati, A., Petticrew, M., Shekelle, P., & Stewart, L. A. (2015). Preferred reporting items for systematic review and meta-analysis protocols (PRISMAP) 2015 statement. *Systematic Reviews, 4*(1), 1. https://doi.org/10.1186/2046-4053-4-1

Mossberger, K., Tolbert, C. J., Bowen, D., & Jimenez, B. (2012). Unraveling different barriers to internet use: Urban residents and neighborhood effects. *Urban Affairs Review*, *48*(6), 771-810. https://doi.org/10.1177/1078087412453713

Muzaffar, A. W., Tahir, M., Anwar, M. W., Chaudry, Q., Mir, S. R., & Rasheed, Y. (2021). A systematic review of online exams solutions in e-learning: Techniques, tools, and global adoption. *IEEE Access*, *9*, 32689-32712. https://doi.org/10.1109/ACCESS.2021.3060192

Nabil, R. H., Barid, M., Sami, A., & Hossain, M. N. (2022). An intelligent examination monitoring tool for online student evaluation. *Malaysian Journal of Science and Advanced Technology*, *2*(3), 122-130. https://doi.org/10.56532/mjsat.v2i3.62

Nagpal, S., & Chaturvedi, R. (2016). Protective or Panoptic? The role of video proctored in educational institutes. *Research Journal of Social Science & Management, 5*(9), 23-31.

Najar, G. Al., & Ahmad, M. N. (2024). A review on factors affecting the success of online proctoring system. *Journal of Information Systems Research and Practice*, *2*(2), 56-70.

Newton, P. M., & Essex, K. (2024). How common is cheating in online exams and did it increase during the COVID-19 pandemic? A systematic review. *Journal of Academic Ethics*, *22*(2), 323-343. https://doi.org/10.1007/s10805-023-09485-5

Nigam, A., Pasricha, R., Singh, T., & Churi, P. (2021). A systematic review on AI-based proctoring systems: Past, present and future. *Education and Information Technologies*, *26*(5), 6421-6445. https://doi.org/10.1007/s10639-021-10597-x

Noorbehbahani, F., Mohammadi, A., & Aminazadeh, M. (2022). A systematic review of research on cheating in online exams from 2010 to 2021. *Education and Information Technologies*, *27*(6), 8413-8460. https://doi.org/10.1007/s10639-022-10927-7

Oncul, B. (2021). Dealing with cheating in online exams: A systematic review of proctored and non-proctored exams. *International Technology and Education Journal*, *5*(2), 45-54.

Picard, R. W. (1997). *Affective computing*. MIT Press.

Potluri, T., & Sistla, V. P. K. (2022, December). A comprehensive survey on the AI based fully automated online proctoring systems to detect anomalous behaviour of the examinee. In *2022 International Conference on Recent Trends in Microelectronics, Automation, Computing and Communications Systems (ICMACC)* (pp. 407-411). IEEE.

Priyanka, L., & Shravani, K. (2023). An intelligent web-based tracking system powered by artificial intelligence. *Material Science*, *22*(03), 238-254.

Rahman, A. (2022). Mapping the efficacy of artificial intelligence-based online proctored examination (OPE) in higher education during COVID-19: Evidence from Assam, India. *International Journal of Learning, Teaching and Educational Research*, *21*(9), 76-94. https://doi.org/10.26803/ijlter.21.9.5

Roselli, D., Matthews, J., & Talagala, N. (2019, May). Managing bias in AI. In *Companion Proceedings of the 2019 World Wide Web Conference* (pp. 539-544).

Ruzgar, N. S., & Chua-Chow, C. (2023). Perception of students on online exams and how sequential exams and the lockdown browser affect student anxiety and performance. *WSEAS Transactions on Computer Research*, *11*, 92-110. https://doi.org/10.37394/232018.2023.11.9

Samir, M. A., Maged, Y., & Atia, A. (2021, November). Exam cheating detection system with multiple-human pose estimation. In *2021 IEEE International Conference on Computing (ICOCO)* (pp. 236-240). IEEE.

Satre, S., Patil, S., Mane, T., Molawade, V., Gawand, T., & Mishra, A. (2023, May). Online exam proctoring system based on artificial intelligence. In *2023 International Conference on Signal Processing, Computation, Electronics, Power and Telecommunication (IConSCEPT)* (pp. 1-6). IEEE.

Slusky, L. (2020). Cybersecurity of online proctoring systems. *Journal of International Technology and Information Management*, *29*(1), 56-83. https://doi.org/10.58729/1941-6679.1445

Smith, A. E., & Humphreys, M. S. (2006). Evaluation of unsupervised semantic mapping of natural language with Leximancer concept mapping. *Behaviour Research Methods*, *38*, 262-279.

Sudar, K. M., Deepalakshmi, P., Ponmozhi, K., & Nagaraj, P. (2019, December). Analysis of security threats and countermeasures for various biometric techniques. In *2019 IEEE International Conference on Clean Energy and Energy Efficient Electronics Circuit for Sustainable Development (INCCES)* (pp. 1-6). IEEE.

Tanwar, S., Obaidat, M.S., Tyagi, S., Kumar, N. (2019). Online signature-based biometric recognition. In: Obaidat, M., Traore, I., Woungang, I. (eds) *Biometric-based physical and cybersecurity systems.* Springer, Cham. https://doi.org/10.1007/978-3-319-98734-7_10

Topuz, A. C., & Kinshuk. (2024). Students' acceptance of and preferences regarding online exams: A systematic literature review. *Educational Technology Research and Development*, *72*(2), 1111-1151. https://doi.org/10.1007/s11423-023-10333-x

Tweissi, A., Al Etaiwi, W., & Al Eisawi, D. (2022). The accuracy of AI-based automatic proctoring in online exams. *Electronic Journal of e-Learning*, *20*(4), 419-435. https://doi.org/10.34190/ejel.20.4.2600

van der Linden, W. J., & Glas, C. A. W. (2000). *Computerized adaptive testing: Theory and practice*. Springer. https://doi.org/10.1007/978-1-4757-0270-6

Van der Maaten, L., & Hinton, G. (2008). Visualizing data using t-SNE. *Journal of Machine Learning Research*, *9*(11).

Van Dijk, J. (2020). *The digital divide.* John Wiley & Sons.

Varona, D., & Suarez, J. L. (2022). Discrimination, bias, fairness, and trustworthy AI. *Applied Sciences*, *12*(12), 5826. https://doi.org/10.3390/app12125826

Wecks, J. O., Voshaar, J., Plate, B. J., & Zimmermann, J. (2024). Generative AI usage and academic performance. *Social Science Research Network*. https://doi.org/10.2139/ssrn.4812513

Yaacoub, E., & Alouini, M. S. (2020). A key 6G challenge and opportunity—Connecting the base of the pyramid: A survey on rural connectivity. *Proceedings of the IEEE*, *108*(4), 533-582. https://doi.org/10.1109/JPROC.2020.2976703

Yalman, E., & Uzunoz, A. (2021). Validity and reliability in qualitative research *In* Scientific research skills and current patterns in research. Article reviews and sample article studies. Ed. A. Uzunoz. ss. 103-117.) Pegem.

Yavuz, M., Hasancebi, M., & Kursun, E. (2020). Acik ve uzaktan ogrenme ders kitaplarinda bulunmasi gereken ozellikler: sistematik literatur taramasi. *Pamukkale Universitesi Egitim Fakultesi Dergisi*, (50), 533-560. https://doi.org/10.9779/pauefd.728848

Yavuz, M., Kayali, B., Ustun, A. G., Ucar, H., Erdogdu, E., & Bozkurt, A. (2025). Investigating the relationship between social presence and transactional distance in online distance learning environments through structural equation modeling analysis. *Interactive Learning Environments*, 1-16. https://doi.org/10.1080/10494820.2025.2589408

Yusuf, A., Suciati, N., & Saikhu, A. (2022, August). Design of automated exam proctoring for user authentication through face augmentation and verification. In *2022 11th Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS)* (pp. 357-361). IEEE.

Zarkasyi, M. I., Hidayatullah, M. R., & Zamzami, E. M. (2020, June). Literature review: Implementation of facial recognition in society. In *Journal of Physics: Conference Series* (Vol. 1566, No. 1, p. 012069). IOP Publishing.

Zimik, S., & Keishing, C. (2021). A study on the performance of biometric devices with reference to employee interface. *Indian Journal of Management and Language (IJML), 2*(1), 8-12.