Study of AI-based architectures for remote examination monitoring using Machine Learning

Moustapha DER[1, †], Ahmed D. KORA[2,*,†] and Samba NDIAYE[3,†]

[1] *Digital Sciences and Technologies (STN) - Doctoral School of Computer Mathematics (EDMI) University Cheikh Anta DIOP UCAD - Research Laboratory (E-INOV LAB) at the Multinational Higher School of Telecommunications (ESMT) - Dakar (SENEGAL),*

[2] *Digital Sciences and Technologies (STN) - Doctoral School of Computer Mathematics (EDMI) University Cheikh Anta DIOP UCAD - Research Laboratory (E-INOV LAB) at the Multinational Higher School of Telecommunications (ESMT) - Dakar (SENEGAL)*

[3] *Faculty of Science and Technology of Cheikh Anta DIOP University (UCAD) - DOCTORAL SCHOOL OF MATHEMATHIC COMPUTER (EDMI) - University Cheikh Anta DIOP (UCAD) - Dakar (SENEGAL)*

Abstract

Article reviews the challenges education administrators and teachers face when turning to online exam proctoring. However, we suggest a use case involving human monitoring with cutting-edge technology, paving the way for test administration for greater ease of administration while maintaining stability. Given the growing trend of distance learning in universities, training schools, distance learning platforms, it is necessary to put in place some sort of appropriate control to avoid cheating and to have a fair evaluation. Indeed, human monitors therefore play a vital role, i.e., they can watch live feeds and identify any potentially harmful activity that automated algorithms might miss. In conclusion, the results show that the human-surveillance-technology combination is more effective in detecting fraud than using an addition of one or the other type only.

Keywords

surveillance, proctoring, machine learning, supervisor, reliability, stability, examination, evaluation, score, confidence, fraud, cheating, remote monitoring

1. Introduction

Firstly, artificial intelligence (AI) and machine learning (ML) have revolutionized many sectors including education [1]. Indeed, traditional surveillance methods requiring the physical presence of supervisors are not adapted to the virtual environment, hence the need for advanced technological solutions. However, remote monitoring [2] of exams has emerged as an innovative solution to ensure the integrity of remote assessments. Remote proctoring, or proctoring, consists of supervising exams remotely to ensure their integrity and prevent cheating. However, remote monitoring of assessments poses considerable challenges in terms of detecting fraud [3], ensuring reliability, stability [4] of assessments to ensure integrity, fairness and credibility of assessments.

2. Online examination monitoring

Initially with the development of online learning [4], monitoring of online exams has become an essential aspect in the evaluation process. Indeed, many studies are being done to find innovative solutions to combat cheating during online exams. However, these solutions seek to cover all possible aspects, notably the authentication system, as indicated by the authors, Wang et al. have [4] proposed a

Cotonou '24 : Conférence Internationale des Technologies de l'Information et de la Communication de l'ANSALB, June 27–28, 2024, Cotonou, BENIN
You can use this document as the template for preparing your publication. We recommend using the latest version of the ceurart style. ∗ Corresponding author. These authors contributed equally. Envelope-Open
[1*] Corresponding author.
[†] These authors contributed equally.
moustapha.der@esmt.sn (M. DER); Ahmed.kora@esmt.sn (A.D. KORA); samba.ndiaye@ucad.edu.sn (S. NDIAYE)
0009-0007-7489-6363 (M.DER); 0000-0002-7636-2054 (A. D. KORA); 0000-0003-0559-9908 (S. NDIAYE)

continuous authentication system for online exams based on machine learning algorithms and rules [2]. Obviously, this detects any inappropriate behavior to limit and prevent fraud.

Therefore, this continuous approach uses machine learning algorithms to multivariate sequential monitoring procedures to detect questionable behavior during testing, to automated online monitoring systems using audio and visual tracking components, to the implementation of 'a microservices architecture [5] for fault-tolerant online exam proctoring systems. Additionally, behavioral biometrics and smart exam proctoring tools help analyze student interactions during exams. These machine learning techniques detect cheating behavior [6] with high accuracy. Indeed, the advancements aim to improve the integrity, reliability and security [7] of online exams by effectively monitoring candidates and preventing fraudulent activities [8].

3. Assessing confidence in surveillance

Meaning of Notations Used in the Following

Code	Mean
$TE^{c}_{i,j}$	Evaluation of the confidence of the surveillance of candidate i by supervisor j in a context c
BM^{c}_{i}	Memory of the supervisor in a context c
$bh^{c}_{i,k}$	Behavior of a candidate i during an interaction k in a context c
$lg_{i,c}$	The interactions between candidate i and the supervisor in a context c
u_i	User i i.e. candidate i
c	Context c
$acc_{i,k}$	The degree of anomaly of candidate i in an interaction k
$delay_{i,k}$	The gap in an interaction k between a supervisor and a candidate i
R^{c}_{i}	Reliability of candidate i in context c
S^{c}_{i}	Stability of candidate i in a context c
$L\_TP^{c}_{i}$	Local profile of user i in context c
$r^{i}_{c,k}$	The degree of confidence of candidate i during an interaction k in a context c
$c^{i}_{df,k}$	The waiting time factor
$-c^{i}_{af,k}$	The anomaly factor
t_q	Time to the interaction q
Δtq	Time difference between the times of an interaction k and an interaction q
θ	The forgetting factor

$$TE^{c}_{i,j} =< BM^{c}_{i},\ L\_TP^{c}_{i} > \quad (1)$$

Assessing the trustworthiness of online exams [6] is crucial to ensuring honesty [3], fairness, reliability and even quality of learning in assessment processes. The level of confidence in exam success varies according to the measures used in our model. The aim of advanced monitoring is to guarantee the integrity of the exam and prevent any fraud or cheating. Having an experienced invigilator when invigilating an exam is essential to guarantee the integrity [9] and smooth running of the tests.

So that an experienced supervisor [10] can quickly identify suspicious behavior and effectively manage unforeseen situations. Thanks to their knowledge [11] of the regulations, they can intervene appropriately to prevent cheating while maintaining a calm environment conducive to the concentration of candidates. Additionally, their experience [10] allows them to reassure students by answering their questions with confidence and clarity, helping to reduce exam-related stress and anxiety. In short, their expertise is a major asset in ensuring the justice and fairness of the evaluation. Since this monitor's confidence can be strengthened by using reliable and effective monitoring tools [9] that reduce uncertainty and errors in judgment.

4. Trust Model

For example, the evaluation of confidence [12] to follow up on the surveillance of a candidate i by a supervisor j in a context c is expressed in the form of a tuple in (1) composed of the abilities of the supervisor formulated by BM^{c}_{i} in (2), which is a register or memory which stores all the information of the entire session and the attitudes of the candidates denoted by their local trust [13] profile $L\_TP^{c}_{i}$ in (4) to emerge the reliability and stability of candidates.

$$BM^{c}_{i} =< bh^{c}_{i,k} > \text{i ε } [1, \text{M}] \text{ k ε } [1, lg_{i,c}] \quad (2)$$

In other words, the candidate's behavior is monitored throughout the exam phase as well as the various interactions made during the session [14]. In short, everything saved in the memory BM^{c}_{i} of the supervisor which records all interactions with the candidate u_i in context c.

$$bh^{c}_{i,k} =< u_i, c, acc_{i,k}, delay_{i,k} > \quad (3)$$

$bh^{c}_{i,k}$ denotes the behavior of the candidate materialized by a quadruplet in (3) involving the users, the context, the degree of anomaly noted during the session [14], and the deviation noted in an interaction between the proctor and the candidate. The memory size symbolizes lgi,c through the interactions of the recorded BM^{c}_{i} session.

In (3) $acc_{i,k}$ reveals the degree of anomaly noted following an interaction [15] "k" so that $acc_{i,k}$ tends towards zero (0) [$acc_{i,k}$→0] if the behavior is too questionable and one (1) [acc →1] if the behavior is normal. $acc_{i,k}$ ε [O,1], $delay_{i,k}$ determines the gap in an interaction between the invigilator and the candidate

5. Trust Evaluation Method

As this waiting time can significantly affect the effectiveness and efficiency of online proctoring [16]. Therefore the register used is the memory of the monitor which memorizes the past responses or behavior of the user to adjust the monitoring strategy to respond to new threats [10] or tactics used by fraudsters. Based on BM_i^c, the monitor v_t can determine the user's local profile in terms of reliability (R_i^c) and stability (S_i^c). The local profile $L\_TP_i^c$ can be written in the form:

$LTP_i^c = (u_i, c, R_c^i, S_c^i)$ (Eq 4)

$R_c^i = \{r_{c,k}^i | k \,\varepsilon\, [1, lg_{i,c}]\}$ (Eq 5)

Reliability is a crucial aspect that ensures that the results obtained are accurate, fair and representative of the skills and knowledge of the candidates. So, the monitor's memory, that is, their ability to remember past incidents and detect suspicious patterns [17] of behavior, can improve the reliability of online monitoring.

or $r_{c,k}^i = \frac{1}{1+e^{-c_{af,k}^i}} c_{df,k}^i$ (Eq 6)

In addition, the degree of confidence of candidate i during an interaction k in a context c in online monitoring considers the measure of credibility and reliability that the online monitoring system grants to candidates. However, this degree of confidence [12] will be determined by the following factors: the candidate's past behavior, the consistency of their responses, the authenticity of their actions and compliance with predefined rules.

But the anomalous element of surveillance is essential for detecting suspicious activity, identifying potential threats, preventing fraud, improving accountability [11] and analyzing emerging trends. By integrating anomaly detection mechanisms into our model, we strengthen security and effectively protect our digital assets and their users against surveillance threats. For the abnormal factor refers to the ability of our model to detect and report behavior or activity that deviates from the norm or he is considered unusual or suspicious. Indeed, a calm and organized atmosphere builds confidence, while a chaotic or stressful environment can undermine confidence [11]. The abnormal factor $c_{af,k}^i$ is given in (7).

$c_{af,k}^i = 1 - e^{-\sum_{q=1}^{k}(acc_{i,q} x \theta^{\Delta tq})}$ (Eq 7)

θ is a factor of forgetting. The forgetfulness factor refers to the ability of the monitoring system to consider the time elapsed since the collection of a certain piece of data took place. As a result, it is essential to understand that not all information maintains the same relevance or value over time. Thus, the forgetting factor comes into play to determine when and how data should be forgotten, updated or archived in our monitoring system.

$\Delta tq = t_k - t_q$ (Eq 8) where t_q is the time of the $q^{ième}$ interaction.

Let's mention the latency factor in online monitoring refers to the period between the detection of a suspicious event or activity and the intervention or decision-making of the monitor or automated system. Thus, this waiting time can have a significant impact on the effectiveness and efficiency of online proctoring. The latency [18] factor in online monitoring refers to the amount of time between the detection of a suspicious event or activity and the intervention or decision-making of the monitor or automated system [15]. Adequate wait time allows the supervisor to make informed and accurate decisions with sufficient information to assess the situation. Therefore, a hasty reaction [19] due to too short a waiting time can lead to hasty decisions or errors in judgment. The waiting time factor is evaluated using the following formula in (9).

$c_{df,k}^i = 1 - e^{-\sum_{q=1}^{k}(delay_{i,q} x \theta^{\Delta tq})}$ (Eq 9)

In other words, stability in (10) refers to the ability of a monitoring system to maintain consistent and reliable performance [19] under varying and changing conditions. Thus, it is crucial to ensure consistent, reliable and secure system performance, as well as to ensure the accuracy and reliability of monitoring measurements over time.

A strong proctor memory can also help detect anomalies or unusual behavior that could indicate malicious or fraudulent activity by questioning the proctor's experience. Based on these, the monitor can more quickly identify alarm signals and take preventive measures to maintain the stability of the system affiliated with reliability by impacting the confidence level factor [11]. The stability in (10) is calculated based on the following formula:

$S_c^i = 1 - \frac{\sum_{k=1}^{lg_{i,c}}(|r_{c,k+1}^i - r_{c,k}^i|)}{lg_{i,c}-1}$ (Eq 10)

This is why the evaluation of the local confidence of the supervisor is evaluated in (11) which requires the histories concerning the expertise of the stakeholders (monitoring and supervisor) combined with current and historical [20] factors to assess the level of confidence. A confident supervisor will intervene appropriately and proportionately if suspicious behavior occurs.

$local\_T_c^j(i) = \omega_{curr,i} . curr\_T_c^j(i) + \omega_{hist,i} . hist\_T_c^j(i)$ (Eq 11)

$hist\_T_c^j(i) = \sum_{k=1}^{lg_{i,c}}(r_{c,v}^i \frac{\varphi_v}{\sum_{r=1}^{lg_{i,c}} \varphi_r})$ (Eq 12)

The history is evaluated against a series of data relating the reliability standardized to the factor of waiting time or forgetting throughout the session. In our context [21] the defined time interval is 0.5.

$\varphi_v = 2^{-(t-t_{i,v})}$ (Eq 13)

$curr\_T_c^j(i) = \left(0.5 + g(h_{i,j}^c).\left(r_{c,lg_{i,c}}^i - 0.5\right)\right).\varepsilon$ (Eq 14)

Although the invigilator may detect abnormal or suspicious behavior [22] and intervene or monitor candidates more closely. Therefore, the behavior of a supervisor, fluid and respectful communication with candidates indicate mutual trust, while a tense or conflicting conversation can be a sign of a lack of trust. So, the latter can lead to increased anxiety [15] or suspicion and create tense dynamics between stakeholders.

The latter can become nervous, which can paradoxically lead to even more suspicious behavior [2] or to involuntary errors, reinforcing the impression of abnormality. Since many detected deviations may force the monitor to apply more severe corrective or disciplinary measures, thereby increasing the difference in stakeholder behavior. Although this may include more interrogations, identity checks or trips to the examination room, or even sanctions [2].

$$g(h_{i,j}^{c}) = \begin{cases} \leftthreetimes h^2, & si\ 0 \le h \le \frac{1}{\sqrt[2]{2\leftthreetimes}} \\ 1, & sinon \end{cases} \quad \text{(Eq 15)}$$

$$\epsilon = \begin{cases} 1, & si\ r_{c,lg_{i,c}}^{i} > 0.5 \\ 0, & sinon \end{cases} \quad \text{(Eq 16)}$$

That is why the memory [5] of the supervisor plays a key role in the reliability and stability of the monitoring control work, which facilitates the detection of deviations [20], the ability to adapt to changes, consistency decisions and the development of supervisor skills. Strong memory can improve the overall performance of the system and increase its ability to meet the ever-changing challenges [23] of surveillance. The memory will allow:

- Recognize the faces and voices of students authorized to take the exam. Because this can help detect any unauthorized presence or identify suspicious behavior.
- Detect unusual behaviors in students, such as constant head movements, frequent glances at another screen, or suspicious [24] facial expressions, which could indicate an attempt at cheating.
- Know the exam instructions such as rules on the use of allowed resources, deadlines for completing each section, etc. This can help them quickly identify any violations of the exam rules [2].
- Monitor the communications of students who communicate with each other during the exam, whether by chat, video conference [14] or other means. This memory can facilitate the detection of unauthorized collaborations.

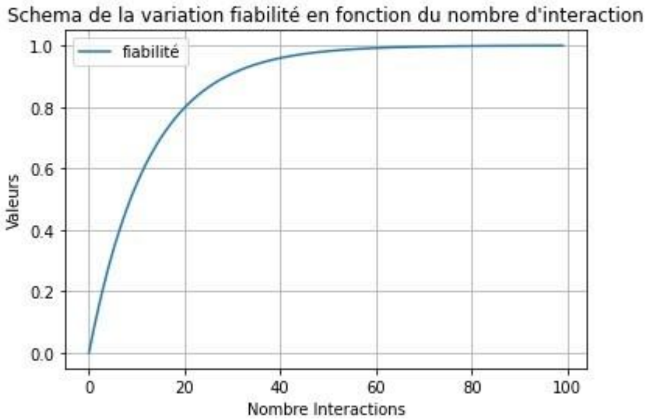
6. Numerical experiments

Experimental Result

Scenario 1: Variation in reliability as a function of the number of interactions.

Case 1: Number of attempts = 100, memory length = 50, number of interactions = 10

Trust Evaluation 0.999999999033467



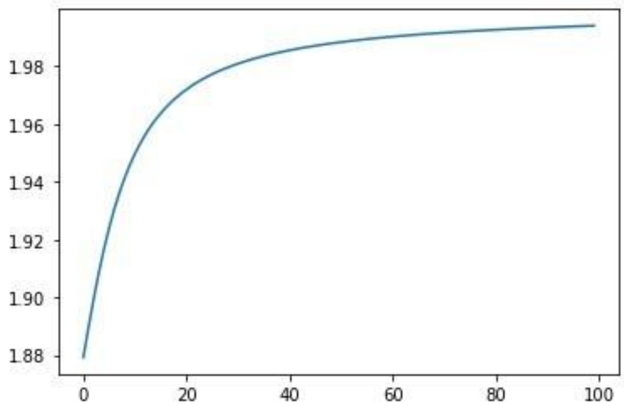
7. **Note 1**: Following the simulation carried out after scenario 1, we note that the reliability tends towards 100% when the number of interactions increases. From 50, we are already 100% confident. Which means that the cheating rate is almost zero when supervision is more rigorous.

The point is that reliability stabilizes as a function of the number of iterations. As a result, it tends towards 99.99999%. The error rate has become too low: 0.000000008.

Scenario 2: Variation in reliability as a function of the number of interactions.

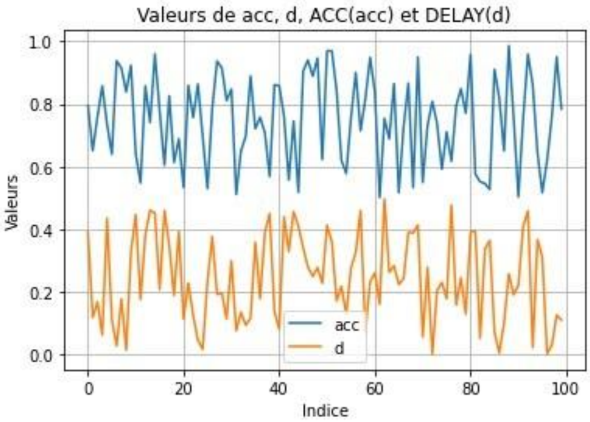
Case 2: Number of attempts = 100,
memory length = 250, number of interactions = 100

Variation in stability as a function of memory size



Scenario 3: Variation in reliability as a function of the number of interactions.

Case 2: Number of attempts = 100, memory length = 50, number of interactions = 10



8. Conclusion and future work

Ultimately, the delicacy [22] of exam monitoring no longer needs to be demonstrated, especially since it strongly influences the future of learners [9]. In other words, the scourge of cheating partly innates to human beings in a tendency to seek ease leads to a poor reflection of competence [15]. Thus, it introduces a biased assessment of the results of the candidates' performances. In addition, it is important to succeed in formalizing the level of confidence or reliability [25] of exam monitoring.

First, online consultation of exams has multiple benefits, such as increased flexibility and accessibility for students. However, it also raises major challenges regarding data privacy, fairness and security. In addition, it is essential to put in place clear protocols to ensure the integrity [26] of exams while preserving the rights of candidates, to use reliable technologies and to raise participants' awareness of ethical [27] issues. To conclude, by taking these elements into account, online monitoring [16] can be transformed into an effective and fair tool for remote assessment [1].

References

[1] C. de La Higuera and M. Pauly Harquevaux, “GTnum LS2N ”The impact of Artificial Intelligence through Open Education” #IA_EO – Methodology of the digital thematic group #IA_EO - Digital thematic groups of the Directorate digital technology for education (Ministry of National Education and Youth) 2020-2022”. February 2023. Available at: https://hal.science/hal-04002890.

[2] Y. S. Baso et al., « Reducing Cheating in Online Exams Through the Proctor Test Model », Int. J. Adv. Comput. Sci. Appl., vol. 14, no 1, 2023, doi: 10.14569/IJACSA.2023.0140139.

[3] F. Chabi, F. Schmidt, and J.-F. Bercher, “Analysis and prediction of multivariate time series for monitoring the health of engineering structures”, in GRETSI 2023, XXIX Francophone Treatment Conference du Signal et des Images, Grenoble, France, August 2023. Available at: https://hal.science/hal-04174436.

[4] I. E. Allen et J. Seaman, « Grade Change: Tracking Online Education in the United States », Babson Survey Research Group, janv. 2014.

[5] M. Romero, H. Aloui, L. Heiser, L. Galindo, and A. Lepage, “A brief overview of resources, practices and actors in AI and education”, Université Côte d’Azur, Research Report, Apr. 2021. Available at: https://hal.science/hal-03190014 [

[6] S. G. Rabiha, I. H. Kartowisastro, R. Setiawan, et W. Budiharto, « Survey of Online Exam Proctoring Model to Detect Cheating Behavior based on Face Recognition », in 2022 8th International Conference on Systems and Informatics (ICSAI), déc. 2022, p. 1-7. doi: 10.1109/ICSAI57119.2022.10005488.

[7] I. Y. Jung et H. Y. Yeom, « Enhanced Security for Online Exams Using Group Cryptography », IEEE Trans. Educ., vol. 52, no 3, p. 340-349, août 2009, doi: 10.1109/TE.2008.928909.

[8] Y. K. Aini, A. Saleh, et H. A. Darwito, « Implementation of Background Subtraction Method to Detect Movement of Examination Participants », in 2020 International Electronics Symposium (IES), sept. 2020, p. 494-500. doi: 10.1109/IES50839.2020.9231922.

[9] S. Abdulrahman, H. Tout, H. Ould-Slimane, A. Mourad, C. Talhi, et M. Guizani, « A Survey on Federated Learning: The Journey From Centralized to Distributed On-Site Learning and Beyond », IEEE Internet Things J., vol. 8, no 7, p. 5476-5497, avr. 2021, doi: 10.1109/JIOT.2020.3030072.

[10] Associate Professor of Counselor Education, St. John’s University, Utopia Parkway, Queens, New York. et G. Cicco, « Building Effective Supervisory Relationships in the Online Counseling Course: Faculty And Student Responsibilities », -Manag. J. Sch. Educ. Technol., vol. 10, no 2, p. 1-8, nov. 2014, doi: 10.26634/jsch.10.2.2968.

[11] A. Shata, Z. N. Haitaamar, et A. Benkrid, « Baseline Estimation in Face Detection for AI Proctored Examinations through Convoluted Neural Networks », in 2023 International Conference on IT Innovation and Knowledge Discovery (ITIKD), mars 2023, p. 1-5. doi: 10.1109/ITIKD56332.2023.10100328.

[12] E. Hadjipavlou, « Big data, surveillance et confiance : la question de la traçabilité dans le milieu aéroportuaire », phdthesis, Université Côte d’Azur, 2016. Consulté le: 14 mai 2024. [En ligne]. Disponible sur: https://theses.hal.science/tel-01592865

[13] « Qu’est-ce que l’examen en ligne : une vue d’ensemble | Constructor ». Consulté le: 14 mai 2024. [En ligne]. Disponible sur: https://constructor.tech/fr/blog/what-is-ai-proctoring

[14] D. P. D. Dayananda, S. Vasanthapriyan, K. G. L. Chathumini, et M. A. C. S. S. Fernando, « A Systematic Literature Review on Online Exams in COVID-19 Pandemic: Assessment Methods, Students’ Preferences, Dishonest Behaviors and Challenges in Online Exams », in 2021 From Innovation To Impact

(FITI), déc. 2021, p. 1-6. doi: 10.1109/FITI54902.2021.9833059.

[15] S. Maniar, K. Sukhani, K. Shah, et S. Dhage, « Automated Proctoring System using Computer Vision Techniques », in 2021 International Conference on System, Computation, Automation and Networking (ICSCAN), juill. 2021, p. 1-6. doi: 10.1109/ICSCAN53069.2021.9526411.

[16] S. Coghlan, T. Miller, et J. Paterson, « Good proctor or “Big Brother”? AI Ethics and Online Exam Supervision Technologies », 15 novembre 2020, arXiv: arXiv:2011.07647. Disponible sur: http://arxiv.org/abs/2011.07647

[17] M. A. Qureshi, T. S. Chaudhery, R. Patil, et S. Correia, « Honest Grade - An Online Education Platform », in 2021 Smart Technologies, Communication and Robotics (STCR), oct. 2021, p. 1-4. doi: 10.1109/STCR51658.2021.9589013.

[18] M. Aziz et F. Meyer, « Étude de l’impact de l’usage de l’intelligence artificielle dans une plateforme de formation en ligne », Solidar. Numér. En Éducation Une Cult. En Émerg., vol. 31. Disponible sur: https://www.academia.edu/download/89653706/Actes_du_Colloque_ROC2021.pdf#page=42

[19] M. A. Nugroho, M. Abdurohman, et B. Erfianto, « Increasing Automatic Proctoring System Performance using Distributed Round-Robin Load Balancer », in 2023 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT), juill. 2023, p. 377-382. doi: 10.1109/IAICT59002.2023.10205750.

[20] A. M. Tripathi, R. Kasana, R. Bhandari, et N. Vashishtha, « Online Examination System », in Smart Trends in Computing and Communications, vol. 286, Y.-D. Zhang, T. Senjyu, C. So-In, et A. Joshi, Éd., in Lecture Notes in Networks and Systems, vol. 286. , Singapore: Springer Singapore, 2022, p. 709-717. doi: 10.1007/978-981-16-4016-2_67.

[21] A. M. Al-Nuimi et G. J. Mohammed, « Face Direction Estimation based on Mediapipe Landmarks », in 2021 7th International Conference on Contemporary Information Technology and Mathematics (ICCITM), août 2021, p. 185-190. doi: 10.1109/ICCITM53167.2021.9677878.

[22] X. Li, K. Chang, Y. Yuan, et A. Hauptmann, « Massive Open Online Proctor: Protecting the Credibility of MOOCs certificates », in Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing, in CSCW ’15. New York, NY, USA: Association for Computing Machinery, févr. 2015, p. 1129-1137. doi: 10.1145/2675133.2675245.

[23] J. Londoño-Cardozo, « The evolution of accounting practice in the age of artificial intelligence: challenges and opportunities for higher education in public accounting », avr. 2024.

[24] M. T. Gumbo, « Online or offline supervision? Postgraduate supervisors state their position at University of South Africa », South Afr. J. High. Educ., vol. 33, no 1, avr. 2019, doi: 10.20853/33-1-2673.

[25] Q. Zhang, Q. Ding, J. Zhu, et D. Li, « Blockchain Empowered Reliable Federated Learning by Worker Selection: A Trustworthy Reputation Evaluation Method », in 2021 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), mars 2021, p. 1-6. doi: 10.1109/WCNCW49093.2021.9420026.

[26] F. Castagnino, « Critique des surveillances studie s. Éléments pour une sociologie de la surveillance »:, Déviance Société, vol. Vol. 42, no 1, p. 9-40, mars 2018, doi: 10.3917/ds.421.0009.

[27] S. Coghlan, T. Miller, et J. Paterson, « Good Proctor or “Big Brother”? Ethics of Online Exam Supervision Technologies », Philos. Technol., vol. 34, no 4, p. 1581-1606, déc. 2021, doi: 10.1007/s13347-021-00476-1.