A New Model of Automatic and Continuous Online Exam Monitoring

Moukhliss Ghizlane
RITM Lab.; CED Engineering Sciences, ENSEM
ESTC, Hassan II University
Casablanca, Morocco
ghizlane.moukhliss@gmail.com

Belhadaoui Hicham
RITM Lab.; Computer Engineering Department
ESTC, Hassan II University
Casablanca, Morocco
belhadaoui_hicham@yahoo.fr

Filali Hilali Reda
RITM Lab.; Computer Engineering Department
ESTC, Hassan II University
Casablanca, Morocco
filalihilalireda@gmail.com

***Abstract*— Student cheating during exams is a widespread phenomenon around the world, regardless of the country's development level. With the expansion of e-learning, exam monitoring becomes more difficult to control. Therefore, real-time monitoring is necessary to secure the student's identity continuously throughout the evaluation period. As a result, we present in this article an online exam management system that provides automatic and continuous monitoring. The implemented solution uses face recognition for a strong student authentication. In order to increase the proposed system's performance, we have defined several parameters to detect any fraud behavior during the whole time that the candidate is using the exam management system.**

Keywords—Online exam, continuous authentication, machine learning, automatic monitoring

I. INTRODUCTION

In recent decades, information and communication technologies have become increasingly important in human life, especially in education.

Evaluation is a crucial part of education process. It allows evaluating knowledge and learning acquired during classes.

With the exponential growth of e-Learning, exam monitoring is one of the biggest challenges.

Cheating involves breaking the rules. Yet, around the world, many students cheat on an exam. Cheating techniques are not lacking[1], next to traditional methods of cheating(namely writing on a pencil case, hiding notes, writing on arms or hands, notes on the ruler, leaving the room, exchanging information between students), we find technological tools and devices (Including, the use of mobile phones, programmable calculator, MP3 players, wireless receivers, Pocket PCs, invisible Ink Pens and storage watches). Many studies have been conducted on students cheating activities and means by which a university can attempt to combat the problem [2]. Students may choose to cheat for several psychological or social reasons [3], such as time constraint, little chance of being caught, fear of failure, incompetence feeling , the parents pressure , wanting a better grade ...

978-1-7281-4216-6/19/$31.00 ©2019 IEEE

Exam is the most used way to evaluate students learning. However, exams can be divided into two types: traditional exam and online exam.

Traditional exam is paper-based and requires the presence of supervisor on the institution's premises and forces him to walk around tables and keep an eye on any cheating.

The online exam or e-exam, consists of evaluating students online[4], on computers, and requires the students presence in a classroom. It has several advantages[5], including: save printing and paperwork, reduce costs and time, and protect environment. Nevertheless, online exams are more subject to cheating than paper tests. Due to the absence of the physical supervisor, strong and continuous security is necessary to eliminate fraud [6]. In addition, this type of evaluation presents a great challenge for the teacher; first, how do we prove that online students are what they claim to be during an exam? Moreover, how to prevent students from cheating?

To resolve this problem, we propose an identification service platform that can verify in real time candidates identities during an online exam, whose technology is machine learning algorithms.

To explain our approach, this article is organized as follows: Section II describes authentication, Section III presents biometric authentication, Section IV depicts facial recognition, Section V introduces online monitoring, and Section VI presents the proposed solution. Finally a conclusion of our work is presented in Section VII.

II. AUTHENTICATION

In a traditional exam, a supervisor must be present at the evaluation center to identify students before the assessment. However, for an e-exam the student's authentication to the system is necessary[7].

Authentication is the cornerstone of digital identity's security.It allows to check if the user is the one he claims to be [8]. Therefore, candidate's authentication is the key element in online exam management systems security [9].

Authentication factors can be classified into three groups [10] : possession factors (something we have such as a smart

card), knowledge factors (something we know for example a PIN code) or biometrics (something we are like a biometric data)[11]. Single factor authentication is based on only one category. However, there are several ways of authentication [12] that can be combined. What is called multi-factor authentication (for example using a smart card in conjunction with a PIN code).

There are two types of authentication [8] : static authentication and continuous authentication.

A. *Static Authentication*

In case of an online exam, static authentication is performed at the beginning to access the exam, and will remain valid throughout the session until the user closes this session.

In our approach, for the first level of security, we use a smart card for access to the evaluation room [13], and also for authentication to the exam management system [14].

Our solution includes two authentication factors, namely a smart card and a password.

B. *Continuous Authentification*

Continuous or dynamic authentication provides an additional security measure next to the initial authentication. It applies after starting an exam session and continuously checks the student's identity (if the current student is the same as the one who started the exam) during the exam period.

In such a high-risk environment (online monitoring platform), student's continuous authentication is very important.

As possession and knowledge authentication factors can be stolen, loaned or transferred to a third party. He will have the same access without the system detects it. For this reason, these techniques are not enough to verify the student's online identity. This is a potential threat for an online exam [15]. These factors are therefore vulnerable.

Biometrics remains a potential solution for continuous authentication [16]. Because it is based on the natural person's verification and it cannot be borrowed or modified.

III. BIOMETRICS

Biometrics is the science of using digital technology to identify individuals based on the unique physical and biological characteristics of each individual [16].

Using a human characteristics is the best way to authenticate a user[17]. In other words, an authentication factor based on biometrics cannot be forgotten or lost contrary to the possession and knowledge factors[18].

An online biometric authentication system is a system for verifying a person's identity in real time by measuring their particular characteristics or their body's behavior [19].

Biometric devices such as fingerprint readers or iris scanners collect a person's biometric data and transform it into digital forms.

A biometric authentication system, identifies a person by comparing their actual data to those already stored in a database using algorithms [20].

Several biometric authentication's models [21] are proposed some rely on physiological characteristics such as fingerprints [22], facial recognition [23] and iris scan [24] or voice. And others are based on person 's behavioral side as the signature, the keyboard dynamics [25] or mouse dynamics[26]. Or a combination of several features in multimodal biometrics form.

In general, regardless of biometric means used, the principle of the authentication system is the same: to certify the person's identity by comparing data presented with prerecorded ones of the person it claims to be.

Given diversity of academic disciplines, our model relies on facial recognition for continuous authentication of students during an online exam regardless of the discipline.

IV. FACIAL RECOGNITION

Traditionally, to identify a person we rely on his photo or an official document containing his portrait, such as his identity card, passport or driver's license.

Faces are the most commonly used biometric elements for humans to recognize each other [27].

In the age of Artificial Intelligence (AI), facial recognition becomes a major challenge for all organizations.

In case of face recognition authentication, the camera captures a face, then transforms it into digital data using an automatic learning algorithm, and compares it to a database. It is in some ways a faithful and increased replica of the process in the human brain.

Facial recognition works in two separate modules [28]: shown in the figure 1.

First, the registration module (or learning): it is a program that we use at student's registration in the system. And can capture multiple photos in a few seconds. In addition, it checks the quality of the image to ensure that a good digitized quality of photo is captured. Finally, it records all the photos taken in a database.

The verification module (or recognition): is a program that verifies the user's identity. Using the computer's camera, the program extracts the photo and details. And compares them with data stored in database.

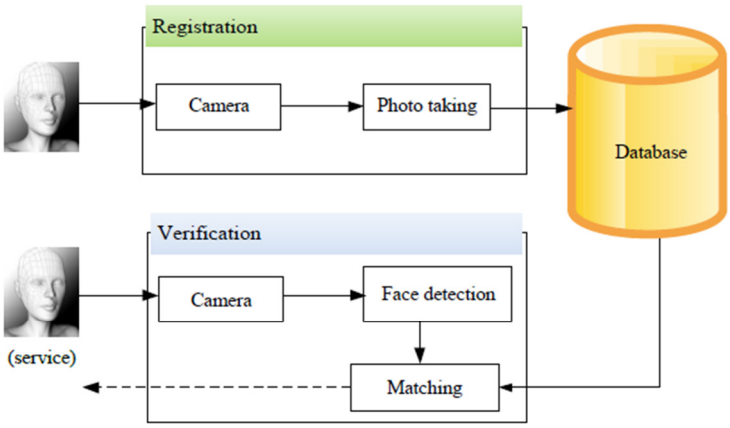

Fig.1.Facial Recognition

V. ONLINE MONITORING

Contrary to physical proctors in a traditional exam, we propose an automated process for monitoring online exams without any need of physical proctors invigilate and control the exam. This solution allows both monitoring students during the exam, detecting, preventing and reporting any cheating activity during a session. In addition, it allows teachers and admins to view the candidate's screen – live.

It is an integrated program using machine learning technology. It is based on the CCTV cameras installed in the examination room as well as on the computers cameras.

Online monitoring is a process of authentication, authorization and control students during an online exam continuously. As shown in Figure 2.

To take an online exam, a student must first identify himself with his smart card [29], and then succeed through the authentication algorithm of staying in front of the screen and comparing his face with information gathered during the initial registration process. After a verification of access rights the student is allowed to take the exam. During the examination, the automatic monitoring program tracks, controls and records the student's movements.

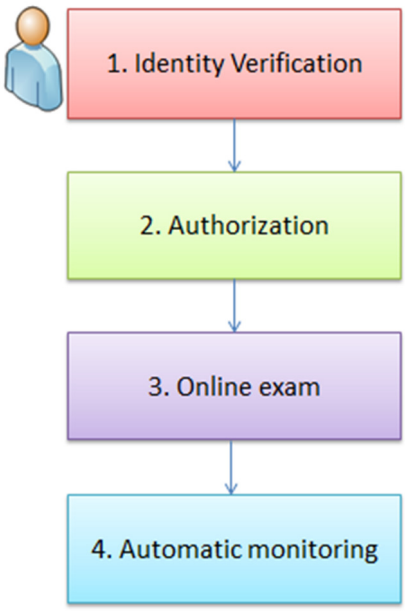

Fig.2. Online monitoring process

The automatic monitoring solution we have proposed in this paper consists of several modules to increase the system's performance. Figure 3 illustrates the online exam management system algorithm.

First, the online exam management system verifies the candidate's registration. A candidate can take an exam only after completing the registration process.

Since the solution includes two authentication layers, initially a valid smart card with correct pin code and facial recognition must be used to authenticate the candidate. During the examination session, facial recognition is used to permanently guarantee that the candidate is the one who claims to be.

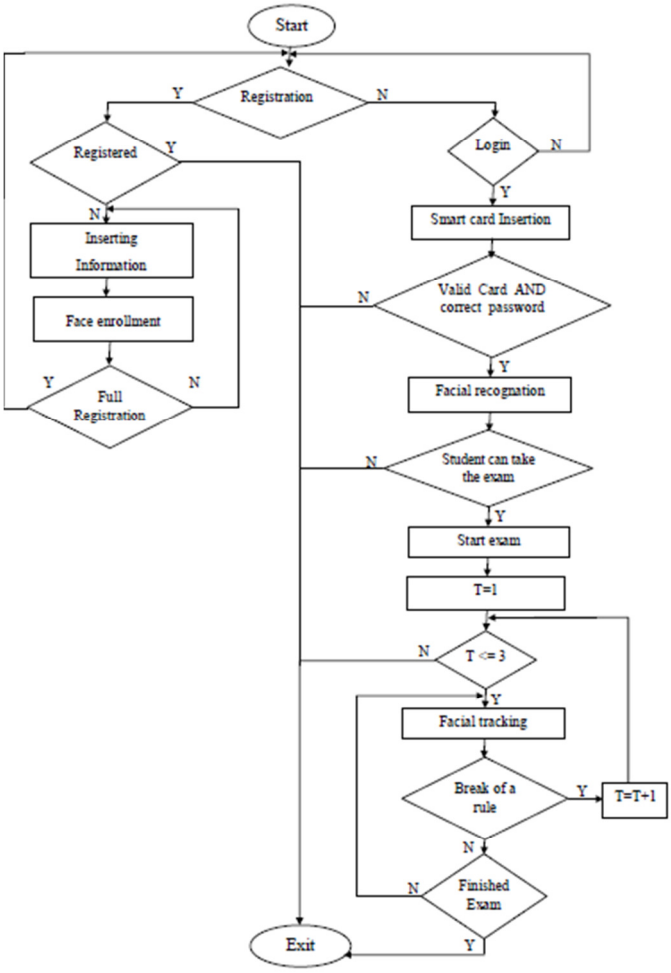

Fig.3. Online Exam Management Algorithm

VI. PROPOSED SOLUTION

Security is an important aspect of an online exam. To ensure digital identity security during an online examination, we proposed the model in Figure 4.

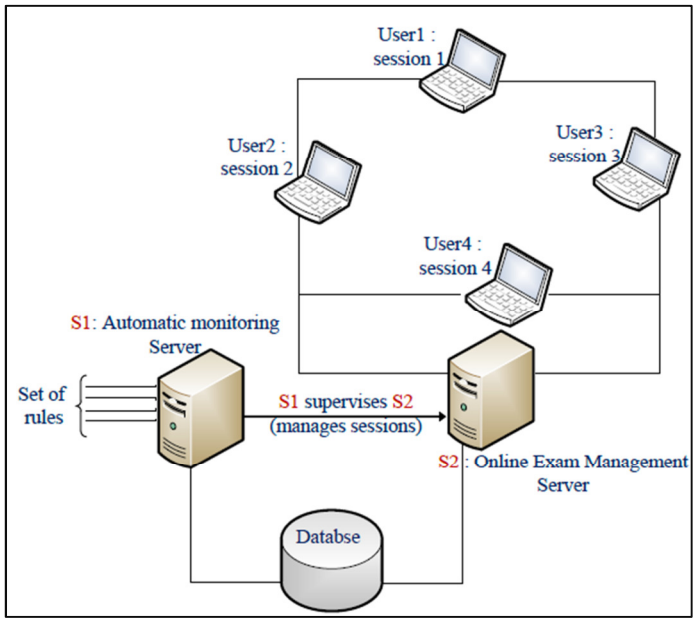

Fig.4. Proposed Architecture

To ensure a high level of security, we have defined two distinct systems: an online exam management system and an automatic monitoring system.

The users' computers are connected to the online examination management server S2. They only have access to the exam platform; they do not have access to the monitoring server.

Server S2 manages the electronic examination sessions. First of all, the user must authenticate with his smart card (the first authentication phase) in order to request a session. The second phase is the student's identity verification using S1 server, face detection and verification of match between database and the person in front of camera.

The monitoring server (S1) supervises online examination management system hosted on the server (S2).

If S2 server receives an OK from S1 server, it starts a session for the student concerned, otherwise the request is rejected.

S2 works under S1's supervision, if a logoff command is received. S2 immediately closes the session.

The model containing learning rules (using artificial intelligence) is hosted on S1 server.

First, deep learning allows us to create biometric recognition software that can uniquely identify or verify a person.

In-depth learning methods can exploit very large sets of face data and learn rich and compact representations of faces, allowing modern models to function properly and then surpass human face recognition capabilities.

In addition, Deep Learning is based on human brain concept and the neurons interaction.

As a result, the proposed program learns and recognizes set of rules that have been defined, as shown in Table I.

Table I. Rules to be respected

Number	Rule
1	Candidate can’t use his mobile phone.
2	Candidate should not speak.
3	Candidate should not leave the camera’s frame.
4	Candidate should not leave the classroom during the exam.
5	Candidate should not turn left or right more than time period.
6	Candidate should not lower his head more than time period.
7	No documents should be placed next to the student.
8	The candidate must not open another browser window.
9	Only one face per session should be detected during the exam.

When a rule is not respected, the system considers it as a potential cheat attempt. The candidate will then have a warning and the counter will be incremented.

After 3 warnings or alerts, the online test is automatically stopped.

Automatic monitoring program locks the information system only to exam requests while simultaneously barring access to any other pre-existing applications or information that appear to be used to cheat during exam.

Candidate is entitled to only one session and he can take the exam from a browser window.

If the candidate tries to connect with the same credentials in two places or in two different browsers, then the system will display warning.

A student is allowed to access only the exam window.

In addition, during the online exam process an option prevents opening of another browser window or tab.When a candidate tries to open a new window, an alert forces him to return to the exam window.

Moreover, access to keyboard shortcuts for copying and pasting is completely prevented.

Finally, we have included in our solution, other security techniques:

- Exam sessions can be viewed in real-time by administrators.

- A detailed audit log of the exam is established, an analysis of the candidate movements appears to detect a fault or a fraud. All of this is recorded end-to-end for later review.

VII. CONCLUSION

In this article, we presented a continuous online authentication system using an automatic face recognition algorithm to verify the user's identity and detect incorrect behaviors continuously throughout the online evaluation process.

The proposed solution consists of several modules. First, the registration module; consists in creating a biometric model of the student's face during his first registration at the university by taking several photos.

Than the identity verification module confirms that the student presented is what he claims to be. Two verification steps are used: smart card authentication as well as facial recognition.

Once the student's identity is confirmed, the monitoring module takes over to authenticate the student continuously, from the beginning to the end of the online exam, by detecting incorrect behavior and any cheating attempt.This is verified continuously by taking pictures from the user's

webcam. As a result, continuous monitoring is based on a set of machine learning algorithms to detect fraud cases.

The last module provides logging, where exam sessions can be viewed by real-time test administrators and are recorded end-to-end for later review.

REFERENCE

[1] E. M. Anderman et T. B. Murdock, « The Psychology of Academic Cheating », in *Psychology of Academic Cheating*, Elsevier, 2007, p. 1‑5.

[2] K. Curran, G. Middleton, et C. Doherty, « Cheating in Exams with Technology »:, *International Journal of Cyber Ethics in Education*, vol. 1, n° 2, p. 54‑62, avr. 2011.

[3] B. Keresztury et L. Cser, « New Cheating Methods in the Electronic Teaching Era », *Procedia - Social and Behavioral Sciences*, vol. 93, p. 1516‑1520, oct. 2013.

[4] « Authenticating student work in an e-learning programme via speaker recognition - IEEE Conference Publication ». [En ligne]. Disponible sur: https://ieeexplore.ieee.org/document/5412484/.

[5] R. Bawarith, D. A. Basuhail, D. A. Fattouh, et P. D. S. Gamalel-Din, « E-exam Cheating Detection System », *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 8, n° 4, 2017.

[6] « e-cheating: Combating a 21st Century Challenge -- THE Journal ».Disponible sur: https://thejournal.com/articles/2001/11/01/echeating-combating-a-21st-century-challenge.aspx.

[7] A. Ullah, H. Xiao, M. Lilley, et T. Barker, « Using Challenge Questions for Student Authentication in Online Examination », 2012.

[8] P. Bours et H. Barghouthi, « Continuous Authentication using Biometric Keystroke Dynamics », p. 12, 2009.

[9] A. Moini et A. M. Madni, « Leveraging Biometrics for User Authentication in Online Learning: A Systems Perspective », *IEEE Systems Journal*, vol. 3, n° 4, p. 469‑476, déc. 2009.

[10] H. Al-Assam, H. Sellahewa, et S. Jassim, « On security of multi-factor biometric authentication », in *2010 International Conference for Internet Technology and Secured Transactions*, 2010, p. 1‑6.

[11] I. Velásquez, A. Caro, et A. Rodríguez, « Authentication schemes and methods: A systematic literature review », *Information and Software Technology*, vol. 94, p. 30‑37, févr. 2018.

[12] I. Velásquez, A. Caro, et A. Rodríguez, « Kontun: A Framework for recommendation of authentication schemes and methods », *Information and Software Technology*, vol. 96, p. 27‑37, 2018.

[13] M. Ghizlane, F. H. Reda, et B. Hicham, « A Smart Card Digital Identity Check Model for University Services Access », in *Proceedings of the 2Nd International Conference on Networking, Information Systems & Security*, New York, NY, USA, 2019, p. 67:1–67:4.

[14] G. Moukhliss, R. F. Hilali, H. Belhadaoui, et M. Rifi, « A New Smart Cards Based Model for Securing Services », vol. 17, n° 1, p. 15, 2019.

[15] K. M. Apampa, G. Wills, et D. Argles, « An approach to presence verification in summative e-assessment security », in *2010 International Conference on Information Society*, 2010, p. 647‑651.

[16] N. A. Mahadi, M. A. Mohamed, A. IhsanMohamad, M. Makhtar, et M. F. A. K. and M. Mamat, « A Survey of Machine Learning Techniques for Behavioral-Based Biometric User Authentication », *Recent Advances in Cryptography and Network Security*, oct. 2018.

[17] R. Saifan, A. Salem, D. Zaidan, et A. Swidan, « A Survey of behavioral authentication using keystroke dynamics: Touch screens and mobile devices », *Journal of Social Sciences (COES&RJ-JSS)*, vol. 5, n° 1, p. 29‑41, 2016.

[18] P. V. Lakshmi et V. S. Susan, *Biometric Authentication Using ElGamal Cryptosystem And DNA Sequence*. .

[19] S. Prabhakar, S. Pankanti, et A. K. Jain, « Biometric recognition: security and privacy concerns », *IEEE Security Privacy*, vol. 1, n° 2, p. 33‑42, mars 2003.

[20] O. Enström, *Authentication Using Deep Learning on User Generated Mouse Movement Images*. 2019.

[21] A. C. Weaver, « Biometric authentication », *Computer*, vol. 39, n° 2, p. 96‑97, févr. 2006.

[22] « A New Fingerprint Authentication Scheme Based on Secret-Splitting for Enhanced Cloud Security - Semantic Scholar ». [En ligne]. Disponible sur: https://www.semanticscholar.org/paper/A-New-Fingerprint-Authentication-Scheme-Based-on-Wang-Ku/57f12f64a2a73cbebfc5f51014fc60075490d632.

[23] « A face recognition scheme using wavelet-based local features - IEEE Conference Publication ». Disponible sur: https://ieeexplore.ieee.org/document/5958933.

[24] « An Iris Biometric System for Public and Personal Use ». Disponible sur: https://dl.acm.org/citation.cfm?id=621411.

[25] P. Bours et S. Mondal, « Continuous Authentication with Keystroke Dynamics », in *Gate to Computer Science and Research*, 1st éd., vol. 2, Y. Zhong et Y. Deng, Éd. Science Gate Publishing P.C., 2015, p. 41‑58.

[26] C. Shen, Z. Cai, X. Guan, Y. Du, et R. A. Maxion, « User Authentication Through Mouse Dynamics », *IEEE Transactions on Information Forensics and Security*, vol. 8, p. 16‑30, 2013.

[27] K. Sundararajan et D. L. Woodard, « Deep Learning for Biometrics: A Survey », *ACM Comput. Surv.*, vol. 51, n° 3, p. 1‑34, mai 2018.

[28] Y. Atoum, L. Chen, A. X. Liu, S. D. H. Hsu, et X. Liu, « Automated Online Exam Proctoring », *IEEE Transactions on Multimedia*, vol. 19, n° 7, p. 1609‑1624, juill. 2017.

[29] M. Ghizlane, F. H. Reda, et B. Hicham, « A Security Policy for Access Control to Academic Services Based on Public Key Infrastructures and Smart Cards », in *2018 6th International Conference on Multimedia Computing and Systems (ICMCS)*, 2018, p. 1‑6.