International Journal of Electrical and Computer Engineering (IJECE)
Vol. 13, No. 5, October 2023, pp. 5333~5341
ISSN: 2088-8708, DOI: 10.11591/ijece.v13i5.pp5333-5341

Intelligent solution for automatic online exam monitoring

Ghizlane Moukhliss, Reda Filali Hilali, Hicham Belhadaoui
Computer Science and Smart Systems Laboratory, EST Casablanca, Hassan II University of Casablanca, Casablanca, Morocco

Article Info

Article history:

Received Sep 26, 2022
Revised Jan 17, 2023
Accepted Feb 4, 2023

Keywords:

Cheating detection
Continuous authentication
Face recognition
Machine learning
Online exam

ABSTRACT

E-learning has shown significant growth in recent years due to its unavoidable benefits in unexpected situations such as the coronavirus disease 2019 (COVID-19) pandemic. Indeed, online exam is a very important component of an online learning program. It allows higher education institutions to assess student learning outcomes. However, cheating in exams is a widespread phenomenon worldwide, which creates several challenges in terms of integrity, reliability and security of online examinations. In this study, we propose a continuous authentication system for online exam. Our intelligent inference system based on machine learning algorithms and rules, detects continuously any inappropriate behavior in order to limit and prevent fraud. The proposed model includes several modules to enhance security, namely the registration module, the continuous students' identity verification and control module, the live video stream and the end-to-end sessions recording.

Corresponding Author:

Ghizlane Moukhliss
Computer Science and Smart Systems Laboratory, EST Casablanca, Hassan II University of Casablanca
Km 7 El Jadida Road-r.p.8, B.P. 20000, Casablanca, Morocco
Email: ghizlane.moukhliss@gmail.com

1. INTRODUCTION

Generally significant learning outcomes can be categorized into three learning domains: cognitive, affective, and psychomotor [1]. All are important to student learning. The cognitive domain involves the recognition of knowledge and the development of intellectual skills. It is composed of six levels classified from the simplest to the most complex: knowledge, comprehension, application, analysis, synthesis and evaluation. The highest level is evaluation. It consists of examining learning outcomes and can be used for both measurement and improvement purposes. On the one hand, assessment measures the performance of students and whether they have achieved the intended learning outcomes. On the other hand, it is about monitoring students' progress through the learning process and providing guidance and feedback to help them move forward. However, the exam has a significant influence on students' learning behaviors. Since most students care about their grades, they cheat for different psychological or social reasons [2]. Such as fear of failure, pressure from parents, lack of time, low probability of being caught, feeling incompetent, desire to get a better grade. Furthermore, fraud is common in all countries regardless of their level of development. It represents a problem of educational inefficiency in all levels from primary to higher education [3]. In this sense, a recent study [4] proposes an academic dishonesty mitigation plan that encompasses strategies from prevention and detection approaches for effective security and integrity of online assessments. Generally, students can be assessed in many ways depending on the type of exam. Thus, exams can be divided into two types: the traditional exam (paper-based) and the online exam. Nevertheless, online tests raise additional concerns [5]. First, they take place on online learning platforms without students and instructors being present in the same location [6]. In addition, in an online assessment students can use computer technology to cheat. This is called "digital cheating" [7]. Therefore, strong and continuous security is needed to eliminate cheating [8]. In addition, it is difficult for the proctor to keep an eye on all students at once. Thus, this type of assessment presents a great challenge to the teacher [9]. On the one hand, the most difficult aspect is to verify the authenticity of the participants. On the other hand, how can we prove that the students in an online exam are who they say they are? In addition, how to detect, limit and prevent fraud in an online exam?

In this study, we address these issues by proposing a continuous authentication system that can verify the identity of candidates in real time during an online exam. Our strategy is based on machine learning algorithms using closed-circuit television (CCTV) cameras in the assessment room in addition to cameras installed on the candidates' personal computers (PCs). Throughout the online assessment process, our intelligent rule-based inference system continuously detects any inappropriate behavior. After this introduction, the rest of the paper is structured as follows: section 2 presents the literature review. Section 3 describes the proposed approach. The results and implementation are presented in section 4. Finally, the manuscript is concluded in section 5.

2. LITERATURE REVIEW

In the age of dematerialization, continuous authentication is applied in many fields. In relation to the academic world, during an online exam, educational institutions use continuous authentication systems to continuously verify the identity of students. In this sense, several academic researches [10] have been conducted in which the authors propose models using different identification methods and techniques, described below.

Many research studies have used a variety of methods based on biological characteristics [11]. For example, in their work, Shdaifat *et al.* [12] proposed a model using the iris biometric recognition technique in mobile examinations. Similarly, in [13] authors used fingerprint reader and eye tribe tracker to propose a system for monitoring online reviews. In their study [14], authors proposed a method to improve the robustness to pose and lighting variations in facial recognition. Hu *et al.* [15] proposed a new model to monitor students' abnormal behavior in an online exam, which determines the relationship between the candidate's head and mouth through a webcam.

In other studies, multiple biometric data are combined, such as facial recognition with fingerprint [16] or fingerprints and mouse patterns [17]. In [18] it was proposed a system combining different biometric features based on the type of interaction and the type of device used at a specific time. Indeed, the system captures raw data on facial features, voice, touch behavior, mouse dynamics and typing patterns during the use of the e-learning platform. Ryu *et al.* [19] proposed a continuous multi-biometric authentication system for student identification in an online exam using two modalities, facial recognition and keyboarding.

In addition, the study [20] from Michigan State University (MSU) in the United States proposed an automated monitoring solution for cheating prevention in online exams based on several biometric features with real-time tracking. About user behaviors, Morales and Fierrez [21] proposed a continuous authentication system based on keystroke dynamics. Other authors [13] have measured students' emotions during assessment and developed a multimodal emotion model for online exams. Another study suggested by Ullah *et al.* [22] used a series of personal and academic questions as challenge questions. They developed a dynamic model of student authentication in online exams based on the profile (PBAF). Kossingou *et al.* [23] proposed a platform to organize online exams while minimizing the possibility of cheating by students of the Central School of Free Software and Telecommunications of Dakar using various tools.

Other authors have developed monitoring solutions using machine learning and artificial intelligence techniques [24]. Radwan *et al.* [25] presented an intelligent approach using deep learning to efficiently detect suspicious behavior in real-time examination. Similarly, Malhotra and Chhabra [26] suggested a model for exam invigilation using deep learning and computer vision. Cheating detection was done based on the students' neck and head movement. In addition, the study implemented by Garg *et al.* [27] proposed a system to track students' faces in the exam based on deep learning techniques. Tiong and Lee [28] addressed the concerns of online cheating and proposes mechanisms for monitoring and reducing dishonest academic behavior using AI technology. Ashwinkumar *et al.* [29] developed an algorithm to facilitate online exam monitoring using deep learning. Duhaim *et al.* [30] suggested a model to reduce fraud in online assessments during the coronavirus disease 2019 (COVID-19) pandemic by extracting a set of reliable features from the Moodle platform while using data mining techniques.

3. METHOD

This section describes our continuous authentication model for verifying the identity of candidates in an online exam in real time. We start with a presenting the security policy. Then we detail the architecture of the proposed system. Finally, we list the monitoring rules and the risk classification.

3.1. Security policy

Our security policy is based on strong three-factor authentication. First, the student needs to authenticate himself with his multiservice smart card [31] and insert the personal identification number (PIN) code (first authentication phase) to request a session. Since the identification of a person from facial images is essential for security applications [32], the second phase is identity verification using facial recognition. After that, continuous identity verification throughout the examination is ensured. Following the same principle of functional process safety for risk reduction, based on the "separate monitoring from control" approach, our proposed model consists of two physically separate systems [2]. An online exam management system (EMS), operative part, and an automatic monitoring system (AMS) command part. The online exam server starts an exam session only after receiving an agreement from the automatic monitoring server. In the same way, in case of fraud, the monitoring system gives a session closure order to the examination platform. This separation has the advantage of ensuring availability, reliability and security. Thus, we have defined a set of techniques and rules to eliminate fraud cases. Figure 1 illustrates the different components of this policy.

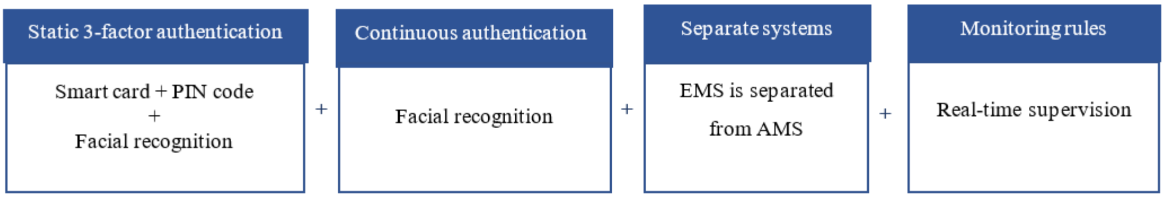


Figure 1. Security policy

3.2. Proposed system architecture

When conducting an online exam, educational institutions face the following challenges: i) verify student identity online at all times during the assessment period, ii) ensure that students pass exams without cheating, iii) report cases of fraud, and iv) evaluate students' skills appropriately. To address these challenges, two questions naturally emerge. First, on what basis does an automatic monitoring system define fraud. Then, how can fraud be prevented. To answer these questions, the main objective of our model is to make a decision about student action without disrupting their concentration based on a set of rules. These rules differ according to three main modules of the proposed system as shown in Figure 2.

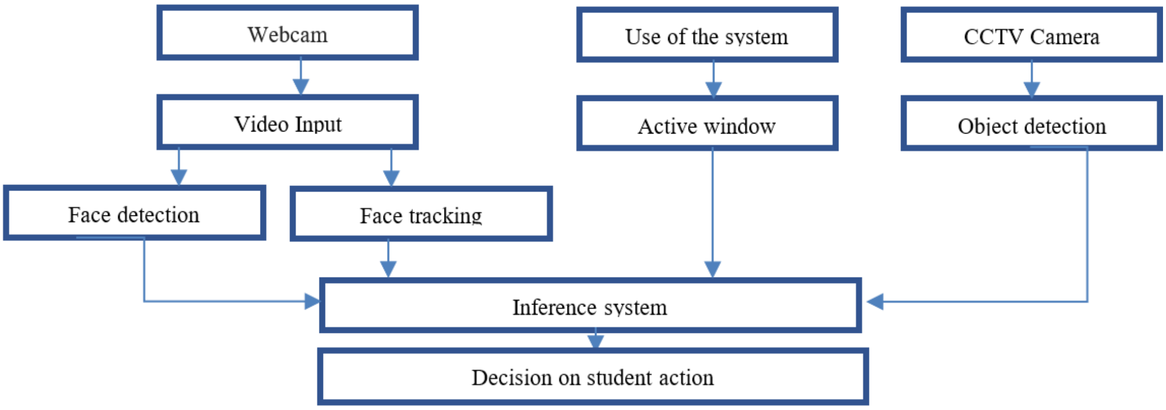


Figure 2. Online monitoring system's architecture

The three modules include video input processing, object detection and active window capture. The latter allows for automatic detection of all processes running in the system during the exam. With the video input, it is possible to monitor the student's face throughout the exam. While the student is taking the exam, it is possible that his or her head moves frequently or that he keeps his head turned for some time. All these elements are recorded. Thus, object detection is very useful in case the candidate tries to use the phone or search for text in a book, document, notepad.

3.2.1. Video analysis

Video input processing is the first module to be analyzed. Indeed, a webcam is used to capture the student's facial movements during the exam. These videos are the inputs to the automatic monitoring system. Thus, face detection as shown in Figure 3 allows to discover: several detected faces Figure 4 detected face looking forward; detected face looking to the right; detected face looking to the left or no detected face. After detection, face tracking ensures that the student is physically present during the evaluation. In addition, tracking the student's movements is very important. As in traditional surveillance, abnormal head direction can be an indicator of possible fraud. For example, if the student looks around a few times or when his eyes are not on the screen for an extended period of time.

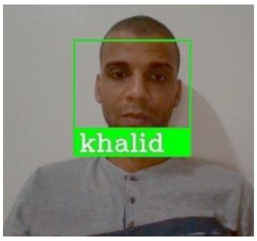


Figure 3. Detection of the student's face at the beginning of the exam

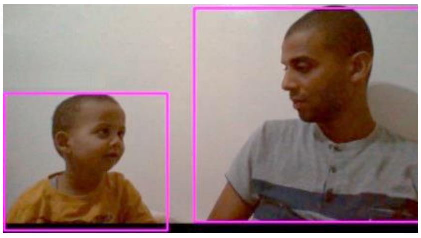


Figure 4. Multiple faces detected during the exam

3.2.2. System usage analysis

With the help of system usage analysis, window changes in the computer used by the student are detected. In case the candidate opens a web browser to search for answers or connects a device to the system or uses another software, this usage capture is detected. In fact, during an evaluation the output of the active window capture is a log with the start and end time of the processes [33]. For example, when the student tries to connect devices to the PC via the universal serial bus (USB) port, it is detected by the capture process.

3.2.3. Object detection

The third module is object detection. The student may make many mistakes that can be captured by object detection. For example, the presence of a cell phone next to the student can be a clue to potential fraud. This is also checked for text in an exam with unauthorized materials; reading from a text is a form of cheating. Lastly, these outputs (video input, system usage and object detection) form the inputs to the rule-based intelligent inference system. Then, the system classifies these rules to detect the possibilities of errors produced. In the following section, we present the different monitoring rules and their classification.

3.3. Monitoring rules: risk classification

The proposed automatic monitoring system consists of evaluating a set of important rules to ensure security and eliminate fraud. By analyzing the students' actions and movements, a classification module determines the risk level of the detected fault. Indeed, we have defined three levels of risk classification: low, medium and high. Each rule is assigned to a risk level Figure 5. Consequently, the inference system makes decisions following the result of the risk classification module. Obviously, when the system detects an attempt to cheat (non-compliance with the rules) an alert is generated and the student receives a warning indicating the fault committed.

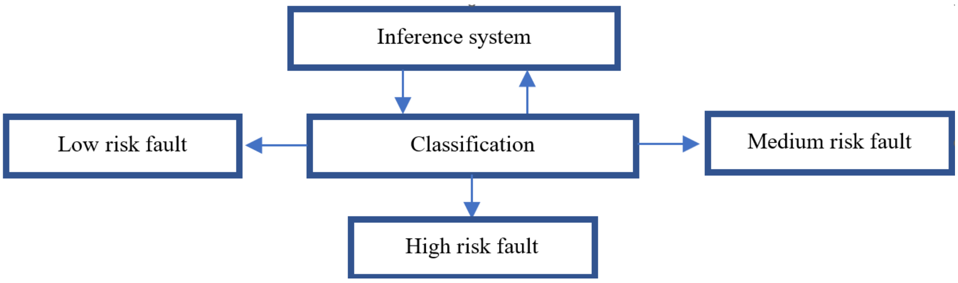


Figure 5. Risk classification diagram

3.3.1. Low risk fault

We define a low-risk fault when the authenticated student is always present in the camera's field of view. In addition, his movements do not pose a security risk to the electronic evaluation system. After three such alerts, the fault is reclassified as medium risk.

3.3.2. Medium risk fault

An error is classified as medium risk, if the user tries to cheat by opening another system window for example (he will be blocked by the system). Also, if the system detects the same login from two different places. If the student repeats the same error three times, the error is reclassified as high risk.

3.3.3. High risk fault

Detecting the faces of students being examined throughout the assessment is very important. It ensures the face tracking process. Thus, a fault is defined as high risk when the student's presence becomes suspicious. For example, when the student goes out of the camera's field of view or when the system detects several faces in the same frame. After three high-risk faults, the session will be automatically closed.

4. RESULTS AND DISCUSSION

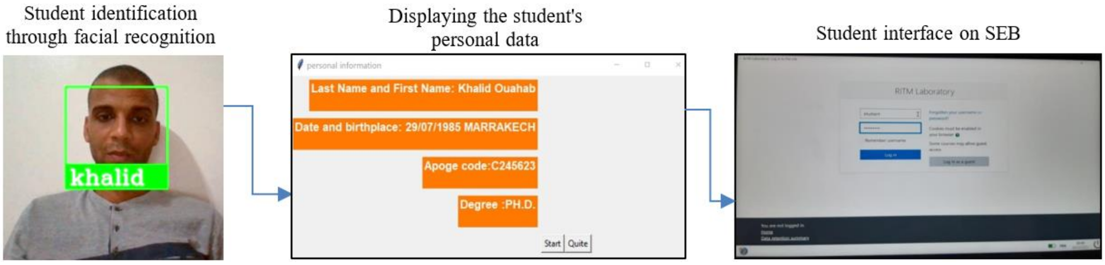
In this section we first introduce the techniques used. Then we discuss the results obtained. Finally, we present the possible performance tests of the proposed model.

4.1. Techniques used

To implement our approach, we used Python as the programming language due to its cross-platform aspect and rich library in the artificial intelligence domain. We used the relational database management system SQLlite as the database server to store the data. For object detection we used the yolo v3 library. In addition, we used the deep face library for the emotion algorithms. Finally, we used the open source computer vision library (OpenCV) library [34] library and the face recognition library in the process of detecting and recognizing students faces for continuous authentication. Thus, to meet the challenges of biometric face authentication, we set up two new techniques to handle face tracking. The first one is based on a motion detection algorithm that calculates the difference between two consecutive video frames. Based on a previously defined threshold, it determines the movements in the video stream. The second one is based on the use of OpenCV face detection algorithms with face recognition association. After the initial detection, a pattern matching is performed to detect the face pattern in the new video frames. To control any fraud attempt we have developed several features. Certainly, several e-learning applications exist [35], [36] but to implement our automatic monitoring system, we used the Moodle 3.9 learning management system (LMS). The purpose of such a choice is twofold; First, Moodle is the e-learning platform used by the Hassan II University of Casablanca via the digital workspace. In addition, as of this version, Moodle is fully compatible with the safe exam browser (SEB) which locks the Moodle platform and ensures that no student accesses an other program. As a result, this improves the security of online exams.

4.2. Authentication phase

Authentication is the first step in the process by which users can access university services [37]. First, the student accesses the examination room with his or her multi-service smart card [38]. Then, he/she must authenticate with the same card to open a new session by inserting it in the card reader connected to the computer and typing his/her PIN code. After that, our program verifies the identity of the student using facial recognition Figure 6 and displays a summary of the personal data. Finally, by clicking on 'start' the examination platform is automatically launched and the student can start the evaluation.


Student identification through facial recognition
khalid
Displaying the student's personal data
personal information
Start
Quite
Student interface on SEB
RITM Laboratory
Log in

Last Name and First Name: Khalid Ouahab

Date and birthplace: 29/07/1985 MARRAKECH

Apoge code:C245623

Degree :PH.D.

Figure 6. Authentication phase

4.3. Monitoring (back-end)

During the exam, the student only has access to the Moodle platform and specifically to the exam. However, our automatic monitoring system runs on the back-end. The fraud attempt counter is initially set to 0 Figure 7. Our program processes, calculates, and reports all fraud attempts Figure 8. For example, if the student uses a cell phone during the exam Figure 9. In addition, if the student reaches three warnings, the session will be closed automatically. In addition, the teacher or administrator can see the candidate's activity from the school's workstations via the local network. In this regard, we developed a script sending the live video images over the network socket. We used the python language and OpenCV for the image processing. Thus, this session is recorded from start to finish in case of need for a later review. A video will be recorded with the student's national code.

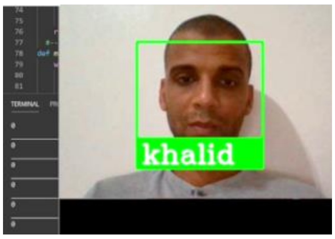


Figure 7. Fraud attempt counter set to 0

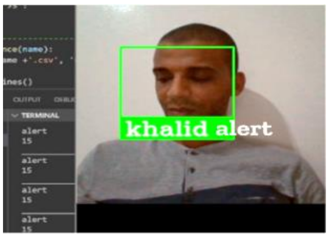


Figure 8. Alert message (fraud)

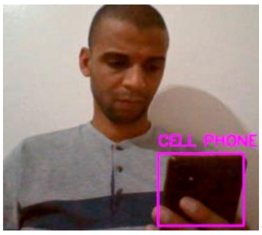


Figure 9. Phone detection

4.4. Real-time performance testing

The automatic surveillance system proposed in this research requires real-time processing, including face detection, facial recognition, decision making, alert reporting, live streaming, and end-to-end recording as illustrated in Figure 10. The specification of these modules appears in the processing and response time constraints. In this regard, it is necessary to verify that the operating system is capable of operating under real-time conditions. For this purpose, we used the real-time (RT) Linux system to run our proposed model.

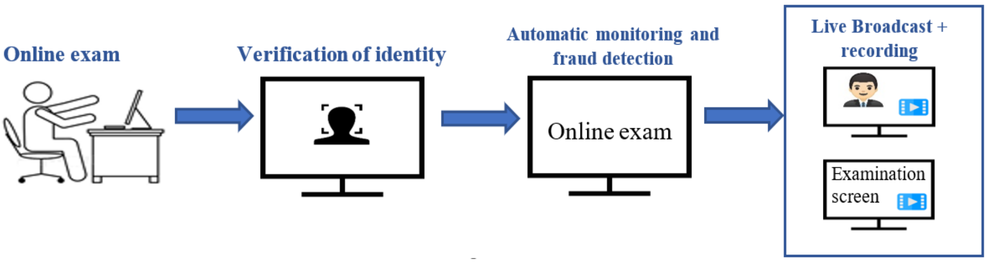
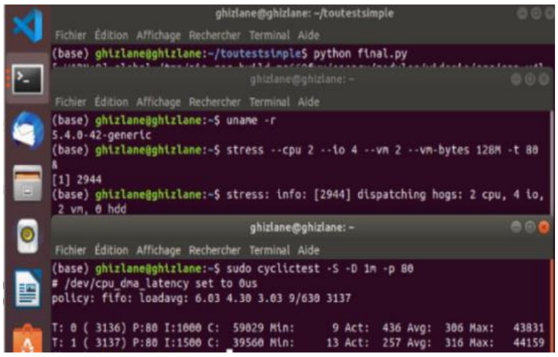

Online exam
Verification of identity
Automatic monitoring and fraud detection
Online exam
Live Broadcast + recording
Examination screen

Figure 10. Services requiring real-time processing

Finally, to test the performance of the operating system on which our solution runs in real time, we put the resources under stress in order to load the system, both the processor and the memory. Thanks to the cyclictest tool we have deduced that the system meets the requirements even when overloaded. Figure 11 shows the execution of our global program 'final.py' on a standard Linux kernel Kernel 5.4.0-42-generic (not modified with PREEMPT_RT patch). While Figure 12 shows the execution of the same program 'final.py' on the PREEMPT_RT patched Kernel 5.4.43-rt25.


ghizlane@ghizlane: ~/toutestsimple
Fichier Édition Affichage Rechercher Terminal Aide
ghizlane@ghizlane: ~
Fichier Édition Affichage Rechercher Terminal Aide
ghizlane@ghizlane: ~
Fichier Édition Affichage Rechercher Terminal Aide

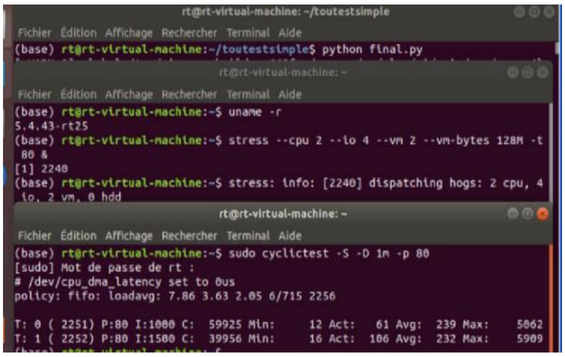
```
(base) ghizlane@ghizlane:~/toutestsimple$ python final.py
```

```
(base) ghizlane@ghizlane:~$ uname -r
5.4.0-42-generic
(base) ghizlane@ghizlane:~$ stress --cpu 2 --io 4 --vm 2 --vm-bytes 128M -t 80
&
[1] 2944
(base) ghizlane@ghizlane:~$ stress: info: [2944] dispatching hogs: 2 cpu, 4 io,
 2 vm, 0 hdd
```

```
(base) ghizlane@ghizlane:~$ sudo cyclictest -S -D 1m -p 80
# /dev/cpu_dma_latency set to 0us
policy: fifo: loadavg: 6.03 4.30 3.03 9/630 3137

T: 0 ( 3136) P:80 I:1000 C:  59029 Min:      9 Act:  436 Avg:  306 Max:   43831
T: 1 ( 3137) P:80 I:1500 C:  39560 Min:     13 Act:  257 Avg:  316 Max:   44159
```

Figure 11. Test on the unmodified linux kernel


rt@rt-virtual-machine: ~/toutestsimple
Fichier Édition Affichage Rechercher Terminal Aide
rt@rt-virtual-machine: ~
Fichier Édition Affichage Rechercher Terminal Aide
rt@rt-virtual-machine: ~
Fichier Édition Affichage Rechercher Terminal Aide

```
(base) rt@rt-virtual-machine:~/toutestsimple$ python final.py
```

```
(base) rt@rt-virtual-machine:~$ uname -r
5.4.43-rt25
(base) rt@rt-virtual-machine:~$ stress --cpu 2 --io 4 --vm 2 --vm-bytes 128M -t
 80 &
[1] 2240
(base) rt@rt-virtual-machine:~$ stress: info: [2240] dispatching hogs: 2 cpu, 4
 io, 2 vm, 0 hdd
```

```
(base) rt@rt-virtual-machine:~$ sudo cyclictest -S -D 1m -p 80
[sudo] Mot de passe de rt :
# /dev/cpu_dma_latency set to 0us
policy: fifo: loadavg: 7.86 3.63 2.05 6/715 2256

T: 0 ( 2251) P:80 I:1000 C:  59925 Min:     12 Act:   61 Avg:  239 Max:    5062
T: 1 ( 2252) P:80 I:1500 C:  39956 Min:     16 Act:  106 Avg:  232 Max:    5909
```

Figure 12. Kernel 5.4.43-rt25 patched PREEMPT_RT

In the first case, Figure 11 allows us to conclude that for an unpatched Linux system, the average 2-thread delay is distributed at 306-316 (us) deviation from the desired trigger. Thus, the right column represents the most important result, i.e., the worst-case latency where the maximum delay is distributed at 43831-44159 (us). In the second case Figure 12, 2 threads with the same priority running in the system with a PREEMPT_RT patched core, the average is very slightly degraded to 232-239 (us). However, the main observation is that the maximum deviation is distributed at 5062-5909 (us) which is significantly better than before. We can conclude for a two central processing unit (CPU) core system running one thread (SCHED_FIFO) per core at priority 80 and which is also under high load due to stress execution in a separate terminal: the maximum detected processing latency, in the real-time system is much lower compared to an unpatched RT system. Therefore, an rt-patched kernel has a more deterministic behavior with respect to latency jitter.

5. CONCLUSION

In this study, an automatic online and continuous monitoring system has been proposed. Our specific purpose is to detect, limit and prevent fraud during an online exam based on automatic face recognition technology using artificial intelligence. The proposed model is divided into several modules. First, to take an exam, the student must authenticate himself. The first one requires multi-service smart card authentication while the second one relies on facial recognition. After confirming the student's identity, the control module takes over to continuously authenticate the student throughout the online assessment process.

The monitoring module is used to detect incorrect behavior and attempted fraud based on a set of rules. It includes system usage analysis, CCTV and computer video streams. The last module provides a logging system, in which exam sessions can be viewed by administrators or teachers in real time. Thus, these sessions are recorded from end to end in case they need to be reviewed later. Next, we tested the performance of the operating system on which our solution runs in real time. Using the stress' tool preparing a stressed environment for cyclic test we concluded from the experimental results that the maximum latencies are much lower in a real-time kernel compared to non-RT Linux.

The proposed model will be implemented and enhanced using the recent evolutionary operators and hybrid recommender systems. This article opens perspectives for improvement and refinement of existing work such as the enhancement of the automated proctoring system to include remote online exams. Thus, students residing in different geographical areas and cities can take the exam from any location. Therefore, continuous automatic proctoring will eliminate the constraints of the institution's location in this case.

REFERENCES

[1] B. S. Bloom, *Taxonomy of educational objectives: the classification of educational goals. Book 1, cognitive domain*. Longmans, Green, 1956.

[2] M. Ghizlane, B. Hicham, and F. H. Reda, "A new model of automatic and continuous online exam monitoring," in *2019 International Conference on Systems of Collaboration Big Data, Internet of Things & Security (SysCoBIoTS)*, Dec. 2019, pp. 1–5, doi: 10.1109/SysCoBIoTS48768.2019.9028027.

[3] T. M. Radwan, S. Al Abachy, and A. S. Al-Araji, "A one-decade survey of detection methods of student cheating in exams (features and solutions)," *Journal Of Optoelectronics Laser*, vol. 41, no. 4, pp. 355–367, 2022.

[4] M. Garg and A. Goel, “A systematic literature review on online assessment security: current challenges and integrity strategies,” *Computers & Security*, vol. 113, Feb. 2022, doi: 10.1016/j.cose.2021.102544.

[5] A. Y. H. Liao, Y.-Y. Hsieh, C.-Y. Yang, and M.-S. Hwang, “Research on the trusted online examination systems,” *International Journal of Network Security*, vol. 24, no. 3, pp. 541–550, 2022.

[6] S. Kaddoura, D. E. Popescu, and J. D. Hemanth, “A systematic review on machine learning models for online learning and examination systems,” *PeerJ Computer Science*, vol. 8, May 2022, doi: 10.7717/peerj-cs.986.

[7] T. Saba, A. Rehman, N. S. M. Jamail, S. L. Marie-Sainte, M. Raza, and M. Sharif, “Categorizing the students’ activities for automated exam proctoring using proposed deep L2-graftNet CNN network and ASO based feature selection approach,” *IEEE Access*, vol. 9, pp. 47639–47656, 2021, doi: 10.1109/ACCESS.2021.3068223.

[8] M. Ghizlane, F. H. Reda, and 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 - NISS19*, 2019, pp. 1–4, doi: 10.1145/3320326.3320401.

[9] D. R. Mdaka and T. E. Mathonsi, “An algorithm to identify and authenticate students writing electronic exams in supervised environment,” in *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, Dec. 2021, pp. 1–4, doi: 10.1109/ICECET52533.2021.9698772.

[10] A. W. Muzaffar, M. Tahir, M. W. Anwar, Q. Chaudry, S. R. Mir, and Y. Rasheed, “A systematic review of online exams solutions in e-learning: techniques, tools, and global adoption,” *IEEE Access*, vol. 9, pp. 32689–32712, 2021, doi: 10.1109/ACCESS.2021.3060192.

[11] S. Hosgurmath, V. V. Mallappa, N. B. Patil, and V. Petli, “A face recognition system using convolutional feature extraction with linear collaborative discriminant regression classification,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 2, p. 1468, Apr. 2022, doi: 10.11591/ijece.v12i2.pp1468-1476.

[12] A. M. Shdaifat, R. A. Obeidallah, G. Ghazal, A. Abu Sarhan, and N. R. Abu Spetan, “A proposed iris recognition model for authentication in mobile exams,” *International Journal of Emerging Technologies in Learning (iJET)*, vol. 15, no. 12, p. 205, Jun. 2020, doi: 10.3991/ijet.v15i12.13741.

[13] R. Bawarith, A. Basuhail, A. Fattouh, and S. Gamalel-Din, “E-exam cheating detection system,” *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 4, 2017, doi: 10.14569/IJACSA.2017.080425.

[14] H. S. G. Asep and Y. Bandung, “A design of continuous user verification for online exam proctoring on m-learning,” in *2019 International Conference on Electrical Engineering and Informatics (ICEEI)*, Jul. 2019, pp. 284–289, doi: 10.1109/ICEEI47359.2019.8988786.

[15] S. Hu, X. Jia, and Y. Fu, “Research on abnormal behavior detection of online examination based on image information,” in *2018 10th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC)*, Aug. 2018, pp. 88–91, doi: 10.1109/IHMSC.2018.10127.

[16] A. Moini and A. M. Madni, “Leveraging biometrics for user authentication in online learning: a systems perspective,” *IEEE Systems Journal*, vol. 3, no. 4, pp. 469–476, Dec. 2009, doi: 10.1109/JSYST.2009.2038957.

[17] S. Asha and C. Chellappan, “Authentication of e-learners using multimodal biometric technology,” in *2008 International Symposium on Biometrics and Security Technologies*, Apr. 2008, pp. 1–6, doi: 10.1109/ISBAST.2008.4547640.

[18] G. Fenu, M. Marras, and L. Boratto, “A multi-biometric system for continuous student authentication in e-learning platforms,” *Pattern Recognition Letters*, vol. 113, pp. 83–92, Oct. 2018, doi: 10.1016/j.patrec.2017.03.027.

[19] R. Ryu, S. Yeom, and S. H. Kim, “Continuous multibiometric authentication for online exam with machine learning,” in *ACIS 2020 PROCEEDINGS*, 2020, pp. 1–8.

[20] Y. Atoum, L. Chen, A. X. Liu, S. D. H. Hsu, and X. Liu, “Automated online exam proctoring,” *IEEE Transactions on Multimedia*, vol. 19, no. 7, pp. 1609–1624, Jul. 2017, doi: 10.1109/TMM.2017.2656064.

[21] A. Morales and J. Fierrez, “Keystroke biometrics for student authentication,” *Proceedings of the 2015 ACM Conference on Innovation and Technology in Computer Science Education*, Jun. 2015, doi: 10.1145/2729094.2754847.

[22] A. Ullah, H. Xiao, M. Lilley, and T. Barker, “Using challenge questions for student authentication in online examination,” *International Journal for Infonomics*, vol. 5, no. 3/4, pp. 631–639, Sep. 2012, doi: 10.20533/iji.1742.4712.2012.0072.

[23] G. M. S.-J. Kossingou, B. M. Degboe, K. Gaglo, S. Ouya, and G. Mendy, “Sharing of experience in the organization of distance exams within African universities in the context of covid-19: case of the central School of free software and telecommunications of dakar,” in *2021 IEEE Global Engineering Education Conference (EDUCON)*, Apr. 2021, pp. 732–737, doi: 10.1109/EDUCON46332.2021.9453847.

[24] A. Nigam, R. Pasricha, T. Singh, and P. Churi, “A systematic review on AI-based proctoring systems: past, present and future,” *Education and Information Technologies*, vol. 26, no. 5, pp. 6421–6445, Sep. 2021, doi: 10.1007/s10639-021-10597-x.

[25] T. M. Radwan, S. Alabachi, and A. S. Al-Araji, “In-class exams auto proctoring by using deep learning on students’ behaviors,” *Journal Of Optoelectronics Laser*, vol. 41, no. 5, 2022.

[26] M. Malhotra and I. Chhabra, “Automatic invigilation using computer vision,” *Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)*, 2021, doi: 10.2991/ahis.k.210913.017.

[27] K. Garg, K. Verma, K. Patidar, N. Tejra, and K. Patidar, “Convolutional neural network based virtual exam controller,” in *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, May 2020, pp. 895–899, doi: 10.1109/ICICCS48265.2020.9120966.

[28] L. C. O. Tiong and H. J. Lee, “E-cheating prevention measures: detection of cheating at online examinations using deep learning approach-a case study,” *arXiv preprint arXiv:2101.09841*, vol. 20, no. 20, Jan. 2021.

[29] A. J. S, H. S. Kumaran, S. U, K. P. B. V. Rajesh, and L. R, “Deep learning based approach for facilitating online proctoring using transfer learning,” in *2021 5th International Conference on Computer, Communication and Signal Processing (ICCCSP)*, May 2021, pp. 306–312, doi: 10.1109/ICCCSP52374.2021.9465530.

[30] A. M. Duhaim, S. O. Al-mamory, and M. S. Mahdi, “Cheating detection in online exams during covid-19 pandemic using data mining techniques,” *Webology*, vol. 19, no. 1, pp. 341–366, Jan. 2022, doi: 10.14704/WEB/V19I1/WEB19026.

[31] G. Moukhliss, R. F. Hilali, H. Belhadaoui, and M. Rifi, “A new smart cards based model for securing services,” *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 17, no. 1, pp. 41–55, 2019.

[32] A. A. Moustafa, A. Elnakib, and N. F. F. Areed, “Optimization of deep learning features for age-invariant face recognition,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 2, pp. 1833–1841, Apr. 2020, doi: 10.11591/ijece.v10i2.pp1833-1841.

[33] S. Prathish, A. N. S., and K. Bijlani, “An intelligent system for online exam monitoring,” in *2016 International Conference on Information Science (ICIS)*, Aug. 2016, pp. 138–143, doi: 10.1109/INFOSCI.2016.7845315.

[34] G. Bradski and A. Kaehler, *Learning openCV: Computer vision with the openCV library*. O’Reilly Media, 2008.

[35] S. Bhaskaran, R. Marappan, and B. Santhi, “Design and analysis of a cluster-based intelligent hybrid recommendation system for e-learning applications,” *Mathematics*, vol. 9, no. 2, Jan. 2021, doi: 10.3390/math9020197.
[36] S. Bhaskaran and R. Marappan, “Design and analysis of an efficient machine learning based hybrid recommendation system with enhanced density-based spatial clustering for digital e-learning applications,” *Complex & Intelligent Systems*, Sep. 2021, doi: 10.1007/s40747-021-00509-4.
[37] G. Moukhliss, O. Malasse, R. Hilali, and H. Belhadaoui, “A digital identity security model with smart card and public key infrastructure,” *Compusoft*, vol. 8, no. 11, pp. 3477–3484, 2019, doi: 10.6084/ijact.v8i11.1038.
[38] M. Ghizlane, F. H. Reda, and 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)*, May 2018, pp. 1–6, doi: 10.1109/ICMCS.2018.8525978.

BIOGRAPHIES OF AUTHORS

Ghizlane Moukhliss received her Ph.D. degree in Computer Science from Hassan II University, Casablanca, Morocco in 2021. Currently, she is a Professor at the Department of Computer Science and Mathematics, EST Sidi Bennour, Chouaib Doukkali University, Morocco. Her research interests include information system security, software engineering, Machine Learning and performance of higher education. She can be contacted at email: ghizlane.moukhliss@gmail.com.

Reda Filali Hilali was in 2006, founding member of the Computer Engineering Department, at the Higher School of Technology, Casablanca Morocco. Since this date, he is full-time Professor at this department. In 2013, he co-authored of a book on algorithmic with the support of Hassan II University Casablanca, Morocco. He was also in 2022, founding member of the Computer Science & Smart Systems laboratory domiciled at the same school. Its research axes are divided into three parts: Data Warehouse and Decision Systems, Information Systems Security, cloud computing security and big data. During the last ten years, he has co-authored many journals indexed articles and international indexed conferences papers. He has also participated in the organization of international scientific events (Cideev’19, Syscobiots'19) and has been reviewer for international and national conferences. He can be contacted at email: filalihilalireda@gmail.com.

Hicham Belhadaoui received his Ph.D. degree at the National Polytechnic Institute of Lorraine, France. He is currently a Professor at the Computer Engineering Department, Higher School of Technology, Hassan II University of Casablanca, Morocco. His research interests include the Reliability, Automatic Signal Processing and Computer Engineering. He can be contacted at email: belhadaoui_hicham@yahoo.fr.