Online-Journals.org

iJET International Journal of Emerging Technologies in Learning

iJET | eISSN: 1863-0383 | Vol. 18 No. 14 (2023) | OPEN ACCESS

https://doi.org/10.3991/ijet.v18i14.40423

PAPER

Continuous and Transparent E-Invigilation of E-Assessments

Salam S. Ketab[1], Abdulwahid Al Abdulwahid[2](✉)

[1]Centre for Security, Communications and Network Research at Plymouth University, Plymouth, United Kingdom

[2]Computer and Information Technology Department, Jubail Industrial College, Royal Commission for Jubail and Yanbu, Jubail, Saudi Arabia

abdulwahida@rcjy.edu.sa

ABSTRACT

A massive number of users are currently utilizing e-learning. Despite the flexibility provided, the traditional methods of course delivery are still used, including e-examinations. There is significant concern about the potential for cheating. The current solutions in this respect fundamentally fail to offer the required level of security. This paper seeks to develop an e-invigilator that will provide continuous and transparent invigilation of examinees. The study involves a detailed presentation of the proposed architecture and a complete design to be the core of the system, which captures, processes, and monitors students in a controlled and convenient fashion. The proposed framework prototype was developed, presented, and utilized, involving 51 participants to conduct an experiment to explore the viability of the proposed framework. For all 51 participants in this experiment, the false rejection rate was 0 in 2D facial recognition mode, while in 3D facial recognition mode it was 0.04827. Moreover, in order to evaluate the robustness of the approach against targeted misuse, three participants were tasked with a series of nine threat scenarios. The false acceptance rate was 0.038 in the 2D mode and 0 in the 3D mode.

KEYWORDS

biometrics, e-learning, electronic invigilation, electronic assessment, face recognition

1 INTRODUCTION

Before what is now called "the digital age," the first emergence of distance- or remount-based learning for the past 100 years was via correspondence and broadcast courses [1], [2]. However, the last decade saw significant growth (more than 70 million students and 1.2 million teachers across 7.5 million courses played an evolutionary role in education development) [3], [4]. Although flexibility has been offered, cheating, misuse, or unauthorized or illegal help during the e-examinations still raise serious concerns [5]. In spite of the fact that many researchers have explored solutions for this issue, they could not offer the integrity required [6], [7], the transparency [8], and/or universality and experimental validation [9]. The number of suggested solutions to minimize cheating behaviors during the online test has varied and can be

Ketab, S.S., Al Abdulwahid, A. (2023). Continuous and Transparent E-Invigilation of E-Assessments. *International Journal of Emerging Technologies in Learning (iJET)*, 18(14), pp. 78–104. https://doi.org/10.3991/ijet.v18i14.40423

Article submitted 2023-04-13. Resubmitted 2023-05-06. Final acceptance 2023-05-07. Final version published as submitted by the authors.

categorized as the following: human proctoring systems, biometric-based solutions, commercial solutions, and system-level security solutions. However, there is still a gap in the current online examination regarding sensitive information and user authenticity, and it is a vital research area to seek solutions. Therefore, this paper explores the feasibility of developing a robust online monitoring environment that can provide the same or better levels of security than what current physical centers provide. Furthermore, it seeks to research and develop an e-invigilator that will provide continuous but non-intrusive monitoring; this should be achieved utilizing the most transparent and robust biometric modalities.

The rest of this paper is organized as follows: An analysis of the current state of the art in the use of biometrics in e-assessment, which goes on to describe the domain of active authentication, is presented in Section 2. Section 3 presents the proposed system requirements and the development of an overall and complete architecture, with Section 4 describing the prototype of the system. Section 5 reflects on the experimental methodology and results before Section 6 presents a discussion. Finally, the concluding remarks are presented in Section 7.

2 LITERATURE REVIEW

The idea of utilizing a human invigilator and avoiding the technical challenges involved in electronic monitoring of the e-assessments is supported by researchers [10]. Yet studies have reported that this method could face many obstacles. The problem of student similarity has been highlighted by Apampa et al. [11], as they said the inspector would not be able to differentiate between them. Moreover, there could be cooperation between the invigilator and the imposter candidate or a high possibility of cheating due to the very close seat distribution [12].

Many other studies have involved the candidate's biometrics to provide the required security; some have adopted a single biometric approach, such as iris recognition [13] or keystroke recognition [14]. Nevertheless, due to the many limitations of this method, other researchers supported the idea of more robust multimodal biometrics, such as Asha and Chellappan [15] and Ross and Jain [16]. A user identification system in the login process along with a continuous authentication strategy have been proposed by [17], utilizing fingerprint and head geometry scanning. However, this particular study focused on the learner's acceptance of multimodal biometric systems for verification throughout the online test, and neglected the practicality, security, applicability, and performance of the proposed method. Asha and Chellappan [15] combined physiological (fingerprint recognition) and behavioral (mouse dynamics) biometrics in one mouse device. Despite the fact that the mouse dynamics method offers secondary authentication, suspicious activities can be done due to the very long time required for data collection [18].

The security of online assessments is also enhanced by the approach of real-time video proctoring of students [19]. A well-evaluated arbitrary video-based monitoring of e-assessment has been proposed by Ko and Cheng [20]. In order to ensure secure examination conditions, relying on audio and video monitoring of the environment surrounding the student, the system authenticates the examinee's identity and hence detects or prevents cheating. Weaknesses, however, can be combined with this approach, such as the massive storage required to store the recorded videos, the long time for reviewing these videos or audios, the potential academic dishonesty, the effect of human emotions or bias, and the lack of concentration of the inspector during the real-time exam time. In addition to video monitoring, Sabbah [21] has suggested a multimodal biometric method employing fingerprint recognition and keystroke analysis. However, the study does not explain how the approaches overcame the issue of cheating, and there is no experimental validation to examine the performance of the biometrics. A prototype proposed by Hernández et al. [22] offers student identification (at the beginning of the e-test) using fingerprint recognition and synchronized continuous observation of students using a web camera until the end of the assessment. Although the study is well evaluated, it does not demonstrate how the video monitoring mechanism (during and after the exam) would work. Moreover, the role of the fingerprint is limited to merely one-time identification rather than continuous verification. Software and hardware solutions have been offered in other studies.

Ullah et al. [23] have defined a scheme to secure the online exam relying on a profile-based authentication framework, employing the actions of enrollment and building the required profile depending on challenging questions. This method could be more feasible than biometric authentication; it is, however, intrusive due to the number of questions that the candidate should answer. There is also a lack of a clear explanation of how to prevent potential illegal help from the surrounding environment. Pan et al. [24] focused their efforts on developing a secure atmosphere for e-examination, avoiding utilizing special network topologies and hardware devices. Onyesolu et al. [25] recommended a combination between a distributed firewall to control network packets from all devices and a fingerprint biometric system for student identification.

A method called RAPTOR has been suggested by Carlisle and Baird [26] as a convenient and cost effective approach that requires the students to use a bootable CD on their own machine in order to run the e-assessment. Furthermore, instead of a CD, Ko and Cheng [27] used a flexible, easy-to-use, and secure Iomega Zip bootable disk that contains the essential files for conducting the e-assessment. All these aforementioned systems, however, are dedicated to a very narrow scope of e-tests. [28], [29], [30], and [31] are among the most famous commercial companies that offer controlled e-examination environments. Yet, all the commercial solutions currently fail to reach the necessary level of security and integrity; they are restricted to particular versions of operating systems (e.g., Windows and Mac); furthermore, none of them has completely overcome the problem of widely deployed virtual machines, which can be used to run unauthorized actions during the online assessment.

In 2016, many universities across Europe collaborated to create a secure e-assessment environment called the TeSLA project [32]. Relying on the combination of new technologies in the fields of authentication (e.g., 2D facial recognition, speech recognition, and keyboard analysis) and authorship, they are trying to develop a system that facilitates e-assessment in such a way that it guarantees that the legitimate student has logged in (authentication) and personally takes the exam (authorship). Despite the fact that TeSLA is merely “a developing project” and very far from the final version to fully judge it, the system gives more weight to many educational and ethical aspects than the robustness and transparency of the approach.

All in all, none of the suggested systems, prototypes, projects, or schemes described in the literature can play the role of a robust, transparent, secure, feasible, applicable, and continuous authentication system and be a satisfactory alternative.

3 PROPOSED SYSTEM ARCHITECTURE

The proposed system is not an e-assessment system but rather an overarching system that provides the monitoring and tracking of participants during an e-assessment. The idea of developing a system that takes on the role of a physical proctor (human) can face lots of challenges, barriers, and requirements, including:

- The system should have the ability to continuously monitor, by biometric means, a user in the most convenient fashion possible.
- The system should be secure against external and internal threats.
- The system needs to use effective mechanisms to mitigate cheating.
- The system needs to be scalable to manage the storage, retrieval, and processing of biometric samples.
- A system that is flexible to enable it to adapt to new monitoring and biometric technologies.
- A system that is user-centric (through the application of HCI principles).
- The system should be platform-independent.
- The system needs to minimize specialized hardware.

All these system requirements have been met by utilizing the combination of processes within the novel multi-modal biometric framework. The framework employs a combination of system-level monitoring and multiple transparent authentication techniques.

3.1 The overall architecture

The following proposed architecture can be considered an intensive development of a robust online monitoring environment that can provide the same or better levels of security than what current physical centers provide. To increase the level of security, various monitoring approaches will be utilized. Furthermore, the system also tries to prevent cheating behavior. This novel e-invigilation system is designed in a modular fashion to incorporate a range of behavioral and physiological biometrics (the most user-friendly and robust techniques). This range of techniques provides an opportunity to capture biometric samples under a range of different examination scenarios (e.g., essay writing, multiple choice test). The overall architecture of the proposed E-Invigilation of E-Assessments (EIEA) system is depicted in Figure 1.

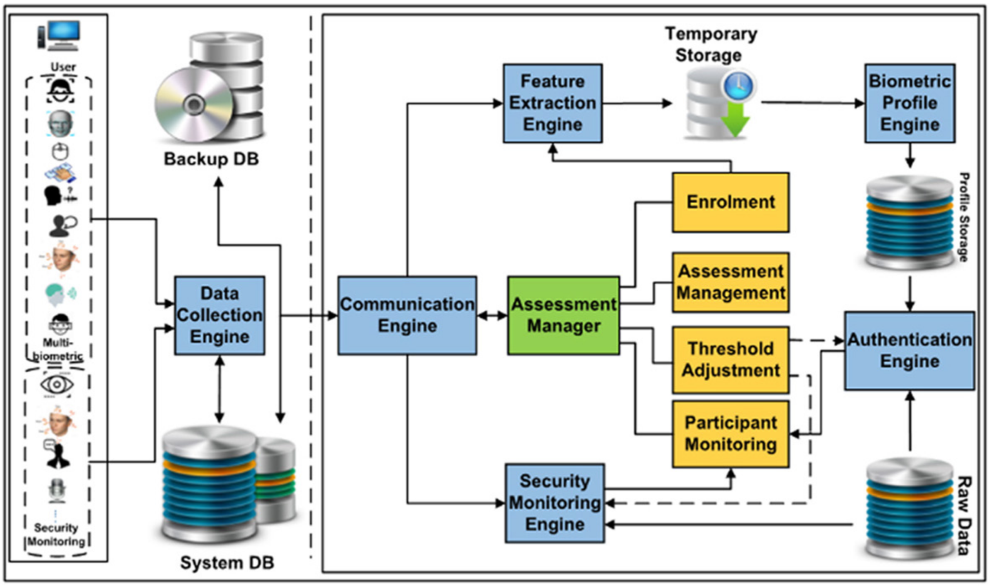


Fig. 1. Overall e-invigilation of e-assessment (EIEA) system

The architecture has been designed around two operational objectives: continuous biometric-based monitoring of the participant and system-level monitoring to prevent cheating. On top of this, there is a variety of management-level functionality that provides the basis for creating and managing assessments. This can be identified within the architectural diagram as the Data Collection Engine, Feature Extraction Engine, Biometric Profile Engine, Authentication Engine, Security Monitoring Engine, Communication Engine, and Assessment Manager, respectively. The architecture permits a degree of client-side pre-processing of biometric samples in order to reduce the volume of data to be transmitted and provide an increased level of privacy (as template generation is typically a one-way process). The following sections will describe the components and processes of the above architecture.

Robust and transparent multi-biometric monitoring. It is obligatory to rely on more than one biometric trait to achieve the idea of providing a secure online assessment, given the range of assessment types and hardware availability. Therefore, this research proposes the use of multi-biometrics as a robust, reliable, secure, and convenient process of continuous, non-intrusive verification beyond the initial identification or login process. Therefore, the study seeks to combine many biometric techniques, including but not limited to: 2D and 3D face recognition, mouse dynamics, keystroke analysis, voice verification, linguistic analysis, eye movements, head movements, and iris recognition, in order to achieve and guarantee a secure online assessment environment.

Data Collection Engine. The primary role of the Data Collection Engine is to capture a user's input interaction (for both biometric authentication and security monitoring). Although platform independency is a feature, the actual samples to be captured by this engine will be dependent upon the hardware contained within or connected to the machine being used during the e-test. However, the system allows the users to decide the level of security during the selection of biometric modalities or the security mechanisms to be involved. The Data Collection Engine, as shown in Figure 2, contains a number of interfaces that will be utilized in order to capture the input data; each of these interfaces captures samples from their respective input devices.

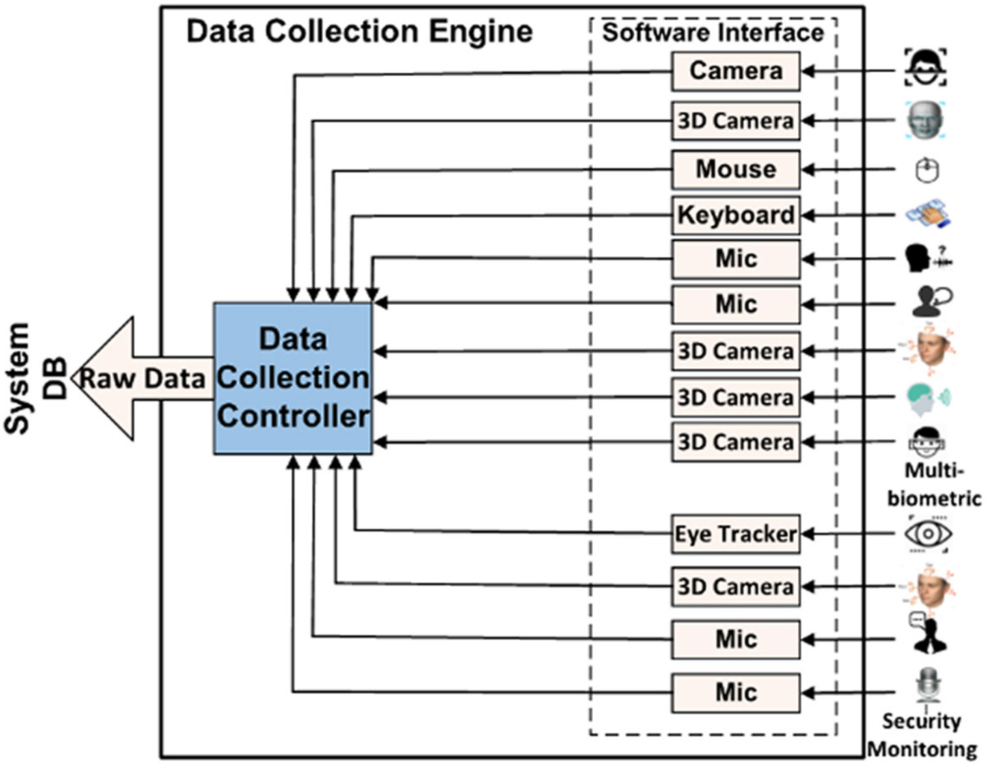


Fig. 2. Data Collection Engine

To provide continuous identity verification, as depicted in the above figure, the data collection engine would basically be able to collect samples from different biometric modalities (multi-biometrics model). Furthermore, in order to maintain security, several mechanisms have been developed to enable continuous monitoring of the system. These include, for instance, the use of a microphone to record and store the entire section and the use of that recording to be pre-processed for voice recognition. It is also possible to collect the student's eye movements from the 3D Camera or Eye Tracker device whilst the student is reading or interacting with the machine during the exam (for detecting the eye positions whether they are within the screen boundaries or not). With the same former sensors, a student's head movements can be detected while he or she is interacting with the machine, specifying whether they are looking at the screen or elsewhere. Once this stage is completed for all the e-assessments, the system (Communication Engine) will send an email to the relevant academic that created this assessment, telling them that the data collection and processing have finished and the data is ready to be rewired. The academic could then log in to the system and send a command to the system (via the Assessment Manager) in order to establish the individual reviewing to take the final decision (deny or confirm cheating). There is no need for academic or student registration as the authentication is managed by a plug-in process to the centralized system; there is no need for a username or password as the user's ID is enough to identify the profile against that staff member or student.

Feature Extraction Engine. After capturing and storing students' biometric data, the Feature Extraction Engine will extract all necessary biometric features and remove any erroneous ones. As long as a variety of biometric modalities have been captured by different devices, the further processing phases for each one will be accomplished in a different way. As illustrated in Figure 3, there is a separate feature extractor agent for each biometric modality that has been captured and stored within the system's database by the Data Collection Engine.

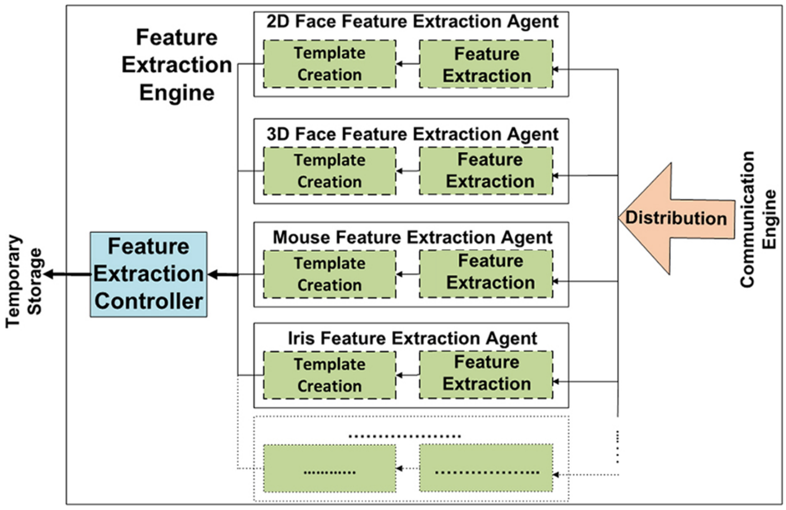


Fig. 3. Feature Extraction Engine

Therefore, the main responsibility of this engine is to extract all potential features from the processed data and transform this data into a feature vector that encloses the concentrated biometric characteristics to be used effectively for student multi-biometric authentication systems. These feature vectors will be consecutively transformed into sample templates in a standard format to be stored in the Temporary Storage by the Feature Extraction Controller.

Biometric Profile Engine. The key role of the Biometric Profile Engine is to generate a variety of biometric profile templates to be utilized by the Authentication Engine for classification. In order to accomplish this, many template generation algorithms have been employed to take the sample template from the Temporary Storage and produce a unique biometric template (Figure 4). As discussed in the previous section, the content of each of these biometric templates is different from one biometric modality to another. For instance, the template that is generated for the 2D facial recognition technique could involve a number of distance measurements between key features of a face, while the template generated for the keystroke analysis technique could involve a number of weight values corresponding to a trained neural network for the authorized user. Both the sample template and biometric template will be stored within the Profile Storage element by the Biometric Profile Controller.

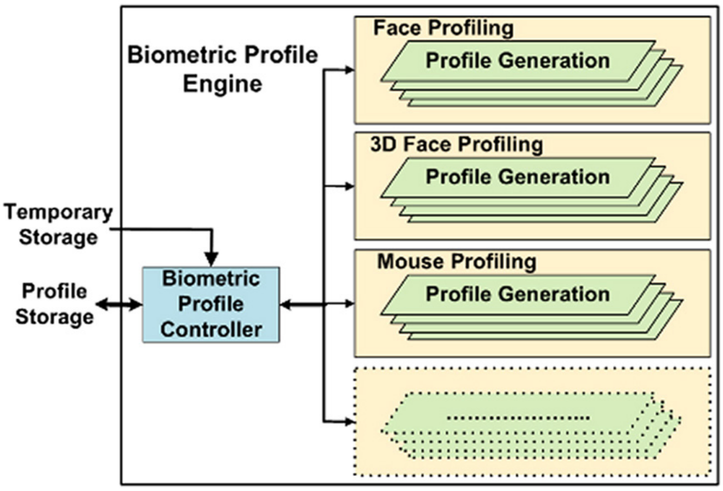


Fig. 4. Biometric Profile Engine

Authentication Engine. The main functionality of the Authentication Engine is to implement the student authentication process. It is this component that has the ability to perform authentication for every permutation of the user's input data separately. Figure 5 shows that the Authentication Engine consists of an Authentication Controller and a number of Authentication Agents (a variable number equal to the number of the chosen biometric modalities). The authentication process will be achieved by fetching the required user's input data (a sample template) and the corresponding biometric template from the Profile Storage. Basically, the Authentication Agent calculates a matching value by comparing the similarity between the sample and the biometric profile template, resulting in a matching score. The result of biometric authentication for each individual technique will be sent to the Authentication Controller to be compared with a predefined threshold; if the result is less than the threshold, the sample(s) will be supposed to be valid, and the authentication process then continues without any further action. Nonetheless, if the result exceeds the threshold, the sample(s) will be classified as invalid, and the Authentication Controller will send the result of biometric authentication of that individual technique to the Participant Monitoring (in order to make the final decision by the academic). The raw data in this stage is also necessary, as the Authentication Controller brings a copy of these data to send them along with the authentication result (in case of authentication failure, to present the related instances of misuse).

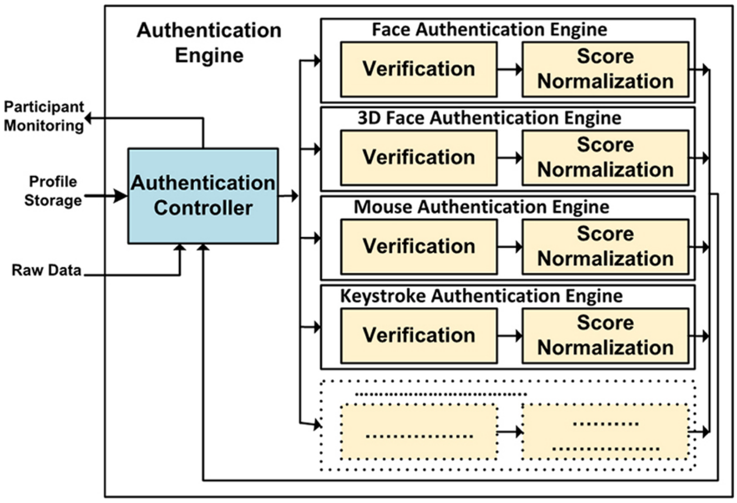


Fig. 5. Authentication Engine

Security Monitoring Engine. While the biometric-based approaches provide a basis for continuously verifying the authenticity of the participant, the system has also been hardened to detect misuse (e.g., head or eye movements, speech recognition, and etc.) and prevent or minimize the opportunity for cheating. Figure 6 illustrates there are many system security considerations that have been taken in account during the development of EIEA system by preventing test takers from: reaching computer resources, ports, or even the network including the internet facilities; accessing unauthorized applications prior to and during the e-test; the ability to minimize, close, and resize the online assessment window; the ability to print, print screen, screen-sharing, desktop capture, or remote access; implementing any capturing functions including: hot keys, copy, cut and paste; reaching any computer-based information such as notes, websites, or instant messaging; the right-click; function keys; browser menu; running virtual machine programs.

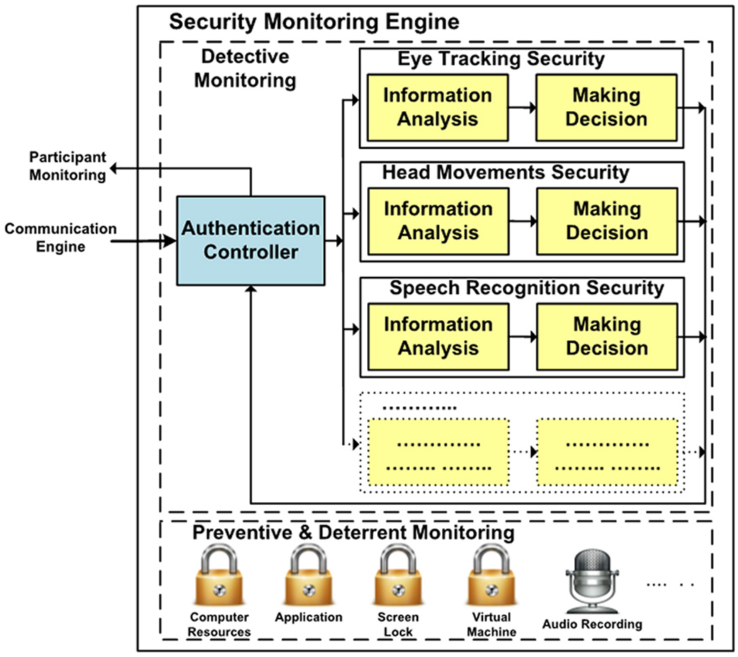


Fig. 6. Security Monitoring Engine

Communication Engine. The Communication Engine provides a communication interface between the stored data and the online system framework. The device that is used for conducting the e-assessment is responsible for capturing biometric and security input data (using the available devices) of the student and storing it in the system database (e.g., servers). The role of the Communication Engine is to transfer information based on four categories, as demonstrated in Figure 7.

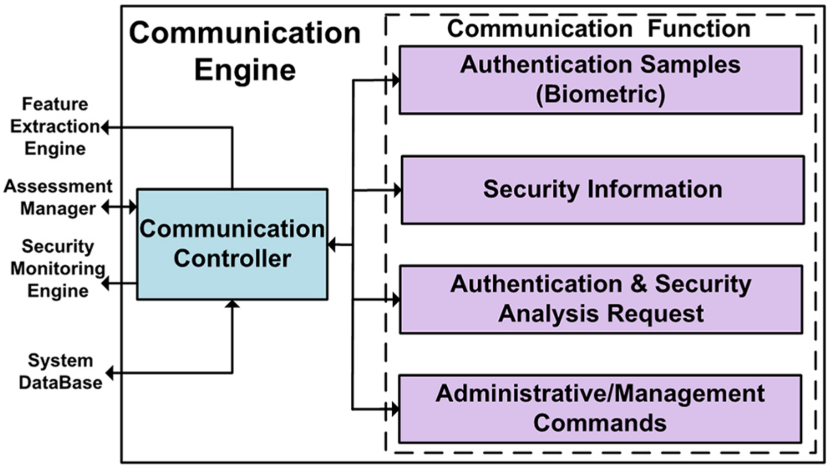

Communication Engine
Feature Extraction Engine
Assessment Manager
Security Monitoring Engine
System DataBase
Communication Controller
Communication Function
Authentication Samples (Biometric)
Security Information
Authentication & Security Analysis Request
Administrative/Management Commands

Fig. 7. Communication Engine

Once the authentication input data is collected, it will be retrieved by the Communication Engine to be submitted to the Feature Extraction Engine, and the stored continuous security detection input data will also be retrieved by the Communication Engine to be submitted to the Security Engine. The communication engine works as a bridge between the captured biometric and security input and the framework. The Communications Engine also enables the Assessment Manager to send some high-level commands to the student (e.g. orders for performing re-enrolment), the academic (e.g., the need for archiving the entire system database), or implement the periodical predefined operations (e.g., implementing automatic partial or complete (hot or cold) backup operations to the entire system database periodically in order to improve the system performance).

Assessment Manager. The primary role of the Assessment Manager is to enable the user to achieve a variety of management-level functionalities that provide the basis for creating and managing assessments. There are different views provided to the users (i.e., academics and students), a higher administrative authority and grants are given to the academic over the student. As illustrated in Figure 8, further to the high-level administrative abilities, utilizing these user-friendly interfaces, the academic can create and define an exam, view, or even edit existing exams, in addition to reviewing the authentication and security results to make the final decision. The student, on the other hand, can schedule, review, and take available exams, in addition to enrolling or reenrolling in the biometric modalities. The system could automatically send emails, information, requests, or alarming actions to academics and students (if necessary) and also implement periodic functions such as partial or complete system database backups.

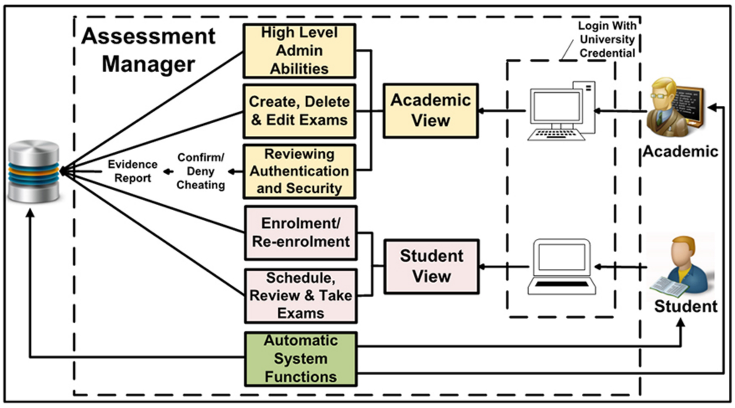

Assessment Manager
High Level Admin Abilities
Create, Delete & Edit Exams
Reviewing Authentication and Security
Enrolment/ Re-enrolment
Schedule, Review & Take Exams
Automatic System Functions
Academic View
Student View
Login With University Credential
Academic
Student
Evidence Report
Confirm/ Deny Cheating

Fig. 8. Assessment Manager

4 PROTOTYPE

Given the flexibility of the aforementioned architecture, a number of decisions had to be made concerning the most transparent and robust biometric modality to be used in order to provide sufficient continuous identity verification [33], what effective security approaches were to be applied or developed, and how to employ the most efficient software or hardware to achieve the targeted level of secure e-examination and controlled monitoring. Essentially, the intention of the prototype is to validate the concept of the model. The prototype was developed not to be a complete operational prototype or to implement a full commercial operational system, but to provide sufficient functionality in order to address the research questions that will be identified in the validation stage. Therefore, in order to monitor the exam taker and ensure that only a legitimate student is taking the exam, the system offers continuous user identity verification employing 2D and 3D facial recognition biometrics. In order to achieve better performance, the depth information was utilized to provide a kind of 3D facial recognition technology, as the actual 3D algorithm was not available. A security layer including an eye tracker to follow or record the student's eye movement, speech recognition to detect inappropriate communication, continuous head movement tracking to check whether they were focusing on the computer screen, and multiple face detection. In order to accomplish the e-invigilated e-test, there are seven steps (as illustrated in Figure 9) that the student needs to follow, including:

- The student needs to go to the university to take the exam on a lab computer (or install the system on their personal computer, laptop, or tablet).
- Login with their University credential.
- The student should achieve all the required biometric enrollments (if they have not enrolled previously or the re-enrolment process is required as there is an order from the academic or administrator to achieve this).
- The system will show student's exams.
- The student will select the exam to start.
- The invigilation processes will run during the exam time.
- The invigilation (authentication and security) results will be saved on the server for later processing.

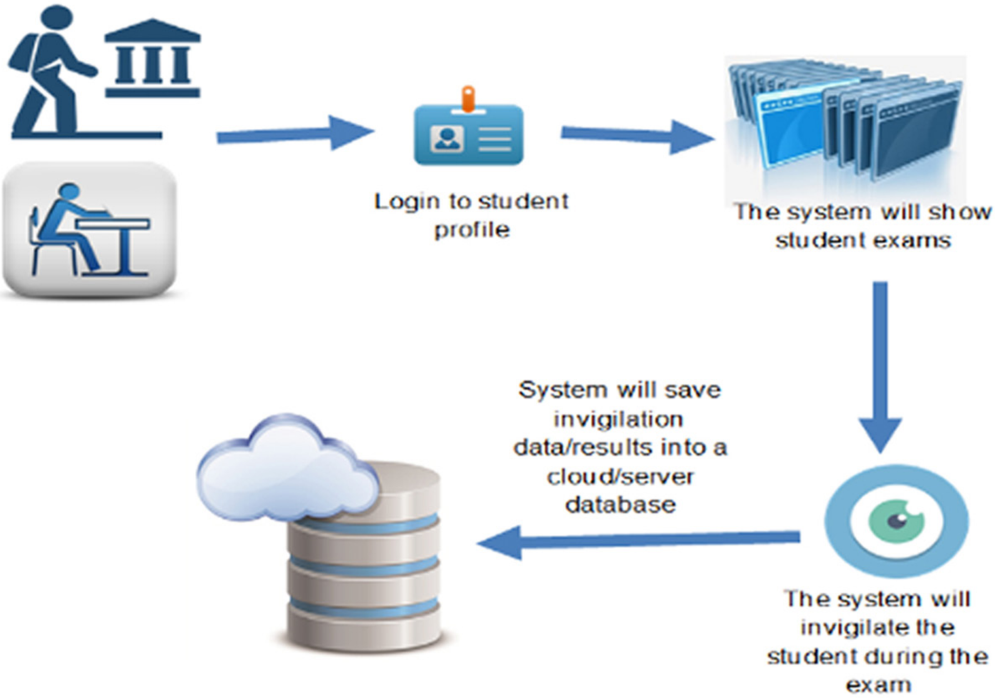
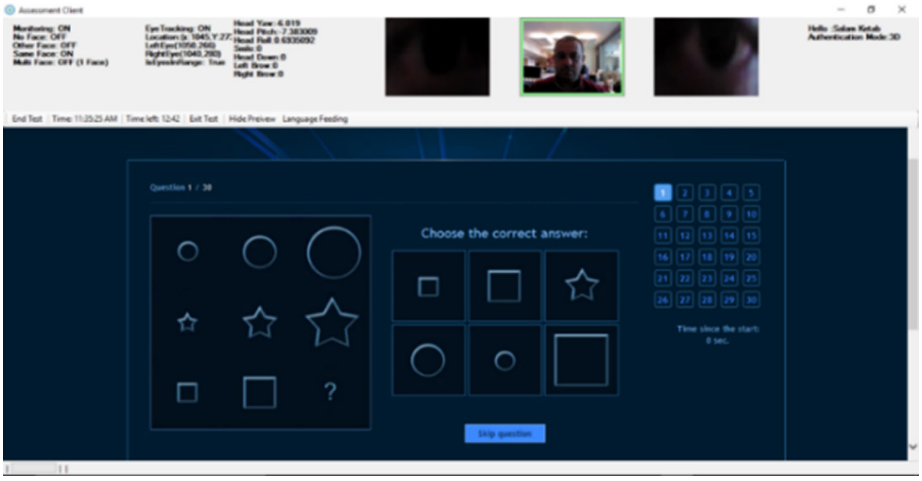

Login to student profile
The system will show student exams
System will save invigilation data/results into a cloud/server database
The system will invigilate the student during the exam

Fig. 9. Student subsystem flow diagram

The principle of ease of use has been given a high priority in this part of the system; the system provides many simple windows with clear instructions. All the student need is to do is to enter their domain username and password, and the system will recognize them and lead them to an appropriate page that enables them to: Biometric enrolment or re-enrolment, security calibration, review available tests, schedule available tests, and take available tests [34]. Once the enrolment process is completed, the student can login to the test, and the system will direct them to an automated and controlled invigilation environment as shown in Figure 10.



Monitoring: ON
No Face: OFF
Other Face: OFF
Same Face: ON
Multi Face: OFF (1 Face)

EyeTracking: ON
Location:(x: 1045,Y:27
LeftEye(1050,260)
RightEye(1040,280)
IsEyesInRange: True

Head Yaw: 6.019
Head Pitch: -7.383009
Head Roll 0.6335092
Smile: 0
Head Down: 0
Left Brow: 0
Right Brow: 0

Hello :Salam Ketab
Authentication Mode: 3D

Time since the start:
0 sec.

Fig. 10. Student view when taking an e-assessment

From an e-invigilation viewpoint, three small windows on the upper side of the e-assessment window present a video stream that the camera is taking for facial recognition and student eyes, in addition to other icons that represent other sensors that are in operation (represented by a group of numeric and logical parameters). The purpose of these is to provide feedback to the candidate that the e-invigilation software is in operation.

5 SYSTEM EXPERIMENTAL VALIDATION

This section presents the validation of the developed system to provide secure, flexible, transparent, and continuous identity verification and security level techniques for monitoring users and identifying cheating in e-assessments. Given the requirements identified in Section 3, there are core research questions need to be answered:

- The ability to capture, process, and identify users through the use of biometrics
- The ability for the system to identify, track, and monitor users with a view to identifying misuse
- The operational nature of the whole architecture

5.1 Methodology

The scenario for the experimental exercise sought to create a real dataset of a reasonable number of real participants over a reasonable period of time of real online assessment employing the previously developed prototype. Methodologically, it is common to have studies that involve fewer than 20 participants as a targeted baseline [5], [35]. However, this study sorted to collect that number and managed, during the period of collection, to collect 51 participants. The subjects were recruited via e-mail or directly. The experiment has been achieved, involving:

- Participants were asked to take a controlled or monitored online assessment for a maximum duration of 15 minutes as part of their regular participation.
- Calibration: the participants calibrate the basic eye movement around the screen in order to ensure the right positioning.
- Registration: samples of participants' faces are received and stored in the Intel RealSense databases for later 2D and 3D facial recognition.
- Biometric student verification in the log-in phase: in each log-in, the verification process is done by facial recognition algorithms (2D and 3D facial recognition, respectively).
- Participants sat for a virtual assessment that contained 30 simple multiple-choice questions. It was determined that the test questions would take longer than the period required for the capture.
- Continuous participant identity verification via the face recognition algorithms, as the camera cannot take concurrently 2D and 3D, therefore, a decision was taken to take 2D facial recognition mode for 5 minutes and 3D facial recognition mode for 10 minutes.
- During the experiment, the participants' biometrics/data (2D, 3D, and depth information) and eye movement or focus on the screen will be collected using custom software for that purpose via a 3D web camera and Eye Tracker sensor then saved anonymously in a secure database.
- The security subsystems are continuously running, including: Eye tracking (in 2D and 3D modes), head movements (in 3D mode only), speech recognition

(in 2D and 3D modes), multiple faces detection (in 2D and 3D modes), and the entire session sounds recording (in 2D and 3D modes).

The experiment diagram depicted in the Figure 11 shows the flow of all of the above biometric identity verification and security restrictions.

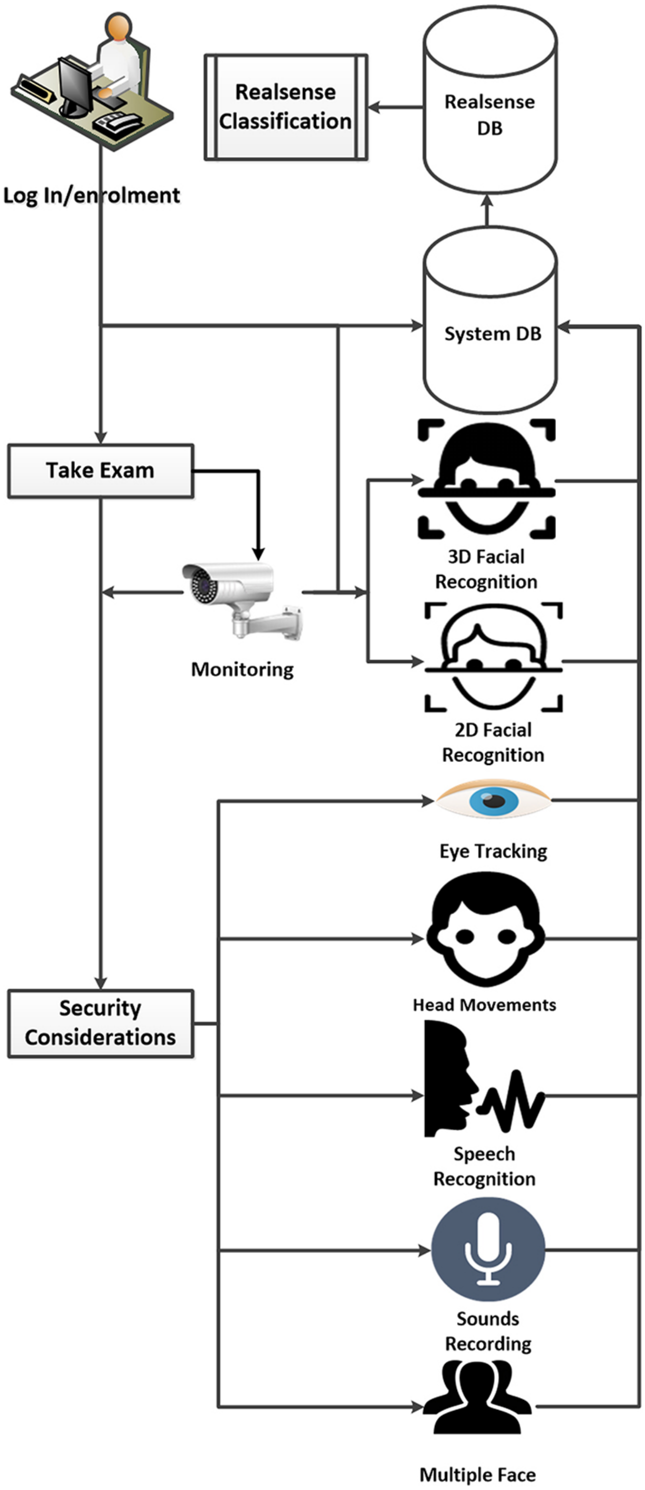


Fig. 11. Experiment process diagram

Threat scenarios. In order to evaluate the robustness of the approach against targeted misuse, in addition to the previous 51 regular participations, three participants were tasked with a series of scenarios that map to typical misuse. A comprehensive analysis of the system design has come up with the following nine threat scenarios that could represent the typical threats during the e-assessment:

1. The exam taker leaves the location or the chair (no one in front of the camera) for a period of time
2. Using the keyboard, mouse, or laptop mouse pad by somebody else, in which the other person (the impostor) should be very close to the legitimate participant in order to achieve this (two faces in front of the camera)
3. Providing unauthorized help to the participant by answering the questions orally by another individual
4. Fixing the camera and the eye tracker in front of the genuine exam taker and moving the computer to another illegitimate individual to give unauthorized help (e.g., answering the questions for the rest of the test)
5. Turning the head of the participant to the left, right, up, or down (looking for unauthorized help from somebody else)
6. Using a photo of a legitimate or genuine exam taker in front of the camera by another illegitimate individual (e.g., full-color 2D photo from a tablet or smartphone device) try to bypass the 2D and 3D facial recognition continuous verification of the student.
7. An impostor uses a 2D photograph of the legitimate or genuine exam taker as a mask to bypass the 2D and 3D facial recognition continuous identity verification with eye holes and to bypass the eye tracker security via these holes.
8. Another individual pretends to be a genuine exam taker and sits in front of the camera for a period of time.
9. Asking the participant to wear relatively dark glasses in order to examine the ability of the eye tracker's infrared to penetrate the glasses and to explore whether the glasses have any direct impact on the facial recognition performance.

Devices installation. As illustrated in Figure 12, the capturing devices have been attached to the computer in front of the participant (the front-facing peripheral F200 3D camera and The Eye Tribe eye tracker).

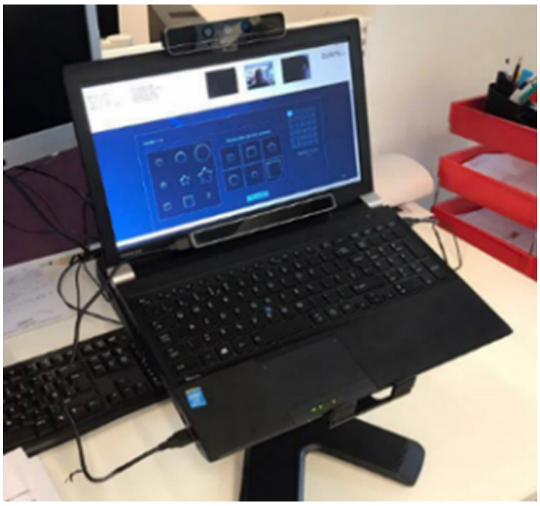


Fig. 12. The capturing devices attached to the laptop computer in front of the participant

5.2 Results

The experiment results can be divided into:

- All regular participations
- Threat scenarios results
- Operational considerations

All regular participation. The FRR was 0 for every participant in the 2D mode and also 0 for 45 of them and less than 0.0965 for the rest 6 in the 3D mode; consequently, for all 51 participants who participated in this experiment, the FRR was 0 in the 2D facial recognition mode for the best, worst, and average. While in 3D facial recognition mode, the best FRR result was 0, and the worst was 0.09655, and hence, the average was 0.04827. As a consequence, participants' results contain 1 to 14 of the 146 rejected samples; this more likely means that the participant's face, at that point in time, was not stable, which made the recognition system straggled. All these actions and FRR results are summarized in Table 1.

Table 1. FRR results of the 51 legitimate participants

Mode	The FRR of the 51 Regular Legitimate Participants		
	Best	Worst	Average
2D Results	0	0	0
3D Results	0	0.09655	0.04827

Based on the above FRR results, the biometric recognition performance was very good. The nature of the methodology meant the quality of the samples would likely be consistent (i.e., in the same room, with the same illumination, and typically at the same physical distance within acceptable parameters); therefore, face recognition algorithms have proven to work very well when given a steady front facial image, and consequently, the experiment has proven that the image capturing was very easy, and hence the recognition system performed properly in the classification of that. However, if this system were deployed on more varied bases, for instance, on some kind of mobile base platform or at home, where it could be dark or the lights off, then the quality and nature of the samples might be different. Therefore, care will still need to be taken in poorly illuminated rooms or environments where the camera is positioned, where the quality or angle of the capture may prove problematic. However, the nature of the eye tracking is to ensure that the eyes are in the view of the screen, which is exactly where the face recognition camera needs them to be in order to get both eyes; thus, the orientation is essentially fixed automatically as a product of the design of the system [34]. Additionally, the system basically needs appropriate illumination in order to allow the user to access the test, so these should help ensure providing the required level of illumination during the rest of the test. Furthermore, illumination issues will be mitigated with the complete architecture when involving, for instance, advanced 3D facial recognition or iris recognition technologies that rely on infrared beams scanning more than face images and even in completely dark rooms. In general, the previous results have shown that the performance of the FRR in the 2D mode with regular participation was better than the performance of the FRR in the 3D mode. However, to enhance the overall system performance, a flipping strategy between 2D and 3D facial recognition can be employed; for instance, every 3 seconds the mode flips from 2D to 3D, and thus every 6 seconds the system implements 2D facial recognition.

Threat scenarios results. This particular phase of the experiment has proven the system's ability to identify, track, and monitor users with a view to identifying unauthorized help that could be provided by somebody else during the e-assessment. In the 2D mode, when participants left the location or chair, the camera captured no face in front of it; in addition, the eye tracker lost the eye movement information. While in 3D mode, the camera captured no face, no head movements, no depth information, and no face expiration information; in addition, the eye tracker lost the eye movement information. In real e-assessment, with this particular threat, in order to avoid recording a massive number of unnecessary misused information (as there is no need to record any more information to provide evidence of cheating), the system can implement a time threshold (e.g., 20 seconds, as the academic could see this time is more than enough to get unauthorized help), which represents the maximum period that the participant's face is allowed to be absent from the camera shot before logging the system out automatically and considering the case as an absolute cheating. This strategy can help save system resources and consequently enhance the operational nature of the whole system.

In the case of somebody else using the keyboard, mouse, or laptop mouse pad, as presented in Figure 13, the person should be close enough to the legitimate user to do this; the camera captured more than one face in both 2D and 3D modes.

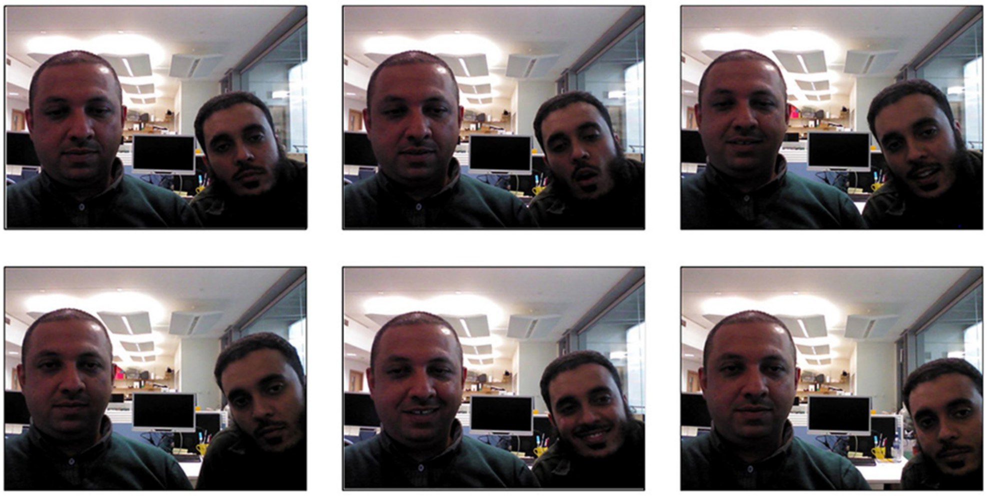


Fig. 13. Multiple face capture

During the real test, the chance to capture two or more faces can occur from time to time depending on the surrounding environment; for instance, in a university lab where there are many people, they could overlap in the background of the captured image. Therefore, a minimum period of time (e.g., a 3 second threshold) can be used to decide whether the case of more than one face in the captured image is a potential cheating attempt, in order to avoid recording and sending ordinary actions and consider them misuse cases that might distract the academic in the reviewing and judging phase. Furthermore, it is also possible to append additional policy when multiple face cases occur multiple times with the same strange face; the system could then potentially consider them as misuse cases even though they last less than the predefined threshold. Moreover, as the e-assessment could be taken within the institutional examination centers, it could be worth defining a list of exceptional or trusted faces (e.g., inspectors' faces) just in case they would be captured in the background during the test. The system should not consider this misuse.

In the third threat scenario, further to the entire session recording process, once another individual answered the questions orally, the speech recognition algorithm captured the spoken sentence in both 2D and 3D modes (as the recognition system is continuously active during the assessment) relying on an English dictionary of the most 10,000 words used in the English language, and if there is any spoken word or sentence by any person that is picked up with the microphone, then it will be recorded and characterized by this recognition system as a potential attack. The system could also improve its ability to more effectively detect users with a view to identifying misuse by using a different strategy; for instance, if the captured human speech was accompanied by more than one face in front of the camera concurrently, the system would more likely consider this a cheating attempt.

The result of the fourth scenario has shown that it was very difficult for the participant to hold and handle both the camera and the eye tracker and mimic their original locations. Therefore, the system captured misuse photos via both eye tracker (eye movements) and 3D camera head movement security subsystems. Yet, this particular scenario would not be able to be achieved easily in the future planned development of the system, due to the fact that the 3D camera (Intel RealSense technology) itself will be built into most types of current computers. Furthermore, the eye tracking security process can be accomplished utilizing the same 3D camera; thus, the current camera has the ability to provide this, but the researcher has preferred to employ a separate eye tracker to achieve the highest level of accuracy.

In the case of turning the head to the left, right, up, or down (e.g., looking for unauthorized help from somebody else or reading a book or a text on a mobile phone), they have completely been captured by Eye Tracker in the 2D mode, and by Eye Tracker in addition to the 3D camera, relying on the head movements security strategy that were running together in the 3D mode only. Generally, throughout the actual test, it is normal for the student to move their head in different orientations from time to time. Therefore, it is advisable to define a minimum period of time (e.g., a 2 second threshold, as this would be enough time to get unauthorized help by looking outside the computer screen) that can be used to decide whether the head motion in the captured image is a potential cheating attempt, in order to avoid recording and sending ordinary actions and consider them misuse cases that might distract the academic in the reviewing and judging phase. Furthermore, the position of the face in front of the screen in these four different orientations could also be flexible, and appropriate angles could be chosen among a range of maximum and minimum parameters. This could provide the system with more flexibility in terms of considering whether the student's head is in an acceptable position or not and avoiding sending a massive number of normal or legal face images for review. It is also possible to apply additional policy when this type of misuse occurs multiple times successively; the system could then potentially consider them as misuse cases even though they last less than the predefined threshold. Moreover, in order to avoid recording a number of unnecessary misused information, the system can implement a threshold time (e.g., 20 seconds, as this would be the maximum period of time to get definitely unauthorized help by looking outside the computer screen) in which the participant's face is allowed to look outside the screen before logging the system out automatically and considering the case as definitive cheating. Additionally, with all the previous head movement potential security policies, if the student's eyes (according to the eye tracker monitoring) were looking continuously inside the screen boundaries, then the head orientation can be given wider movement angles than the predefined limitations.

When participants have been asked to put a photo of a genuine exam taker in front of the camera (e.g., A full-color 2D photo from a mobile device), the recognition has succeeded for the majority of the samples that have been captured by the 2D facial recognition algorithm. However, they have been captured by Eye Tracker anyway because there is no eye movement in the photos. In 3D mode, the photos have been captured by Eye Tracker in addition to the 3D camera via the 3D facial recognition sub-algorithm because there is no depth or head movement information in this mobile 2D image. The absence of eye movements in this specific attack was 0 for all eye tracking parameters, which means no human was in front of the computer screen and suggests considering this as definitive cheating. Therefore, to avoid recording a huge number of dispensable misused information, the system can also implement a time threshold that represents the maximum period that the participant's eye tracking information is allowed to be 0 before logging the system out automatically and considering the case as absolute cheating.

The same can be said for the seventh scenario, which asked the participant to behave as an intruder by using a photograph of the legitimate user as a mask with eye holes to bypass the eye tracker challenge. The experiment results have shown that the holes should be much bigger than the original eyes in order to enable the eye tracker to reach the intruder's eyes. Nevertheless, because there is no depth or head movement information in these photographs, this particular attack has completely failed in 3D mode. As the head movement security represents one of the system parameters that could be utilized to identify for sure the presence of the student in front of the computer or exam screen, the system could also implement a time threshold that represents the maximum period that the head movement information is allowed to be 0 (as no head movement is recorded) before logging the system out automatically and considering the case as a definite cheating.

In the eighth threat scenario, during both 2D and 3D modes, the system easily highlighted that there was another person in front of the camera. With this attack, a strict rule could be applied, as whenever an illegitimate person sits the exam in complete absence of the genuine exam taker, the system should treat this as definitive cheating without any indulgence; therefore, the system could log out automatically after a short time.

Finally, in order to examine the ability of the eye tracker infrared to penetrate the glasses and to explore whether the glasses have any direct impact on the facial recognition performance, the experimental results have proven that the eye tracker infrared beams were penetrating the glasses and achieved the same performance without wearing glasses; furthermore, it has also been proven that there is no direct correlation between wearing glasses and the performance of the facial recognition system. Essentially, when conducting the main experiment, some of the 51 participants have been wearing different glasses; however, the system has also proven the same results in this threat scenario. Table 2 summarizes the results.

Table 2. Results of the 9 threat scenarios repeated with 3 participants

Threat	Continuous 2D and 3D Facial Recognition Identity Verification and System Security					
	2D	3D	Head	Eye	Speech	MultiFace
1	✓	✓	✓	✓	–	–
2	✓	✓	✓	✓	–	✓
3	✓	✓	✓	✓	✓	–
4	✓	✓	✓	✓	–	–
5	✓	✓	✓	✓	–	–
6	✓	✓	✓	✓	–	–
7	✓	✓	✓	✓	–	–
8	✓	✓	✓	✓	–	–
9	✓	✓	✓	✓	–	–

Table 3 demonstrates the results of the 2D and 3D facial recognition FAR of the 2nd, 6th, 7th, and 8th threat scenarios per participant.

Table 3. The 2D and 3D facial recognition FAR of all the threat scenarios per participant

Threat	FAR Results					
	2D Mode			3D Mode		
	User1	User2	User3	User1	User2	User3
2	0	0	0	0	0	0
6	0.076	0.076	0	0	0	0
7	0.038	0.076	0	0	0	0
8	0	0	0	0	0	0

The results were 0 for all cases in both 2D and 3D facial recognition authentication, except the FAR of participants 1 and 2 of the 6th and 7th scenarios were 0.076, 0.076, 0.038, and 0.076, respectively, in the 2D facial recognition mode. Therefore, the best, worst, and average FAR are summarized in Table 4.

Table 4. The best, worst and average FAR of the three participants in the threat scenarios

Mode	Best	Worst	Average
2D Facial Recognition Results	0	0.076	0.038
3D Facial Recognition Results	0	0	0

In general, the FAR in this phase is just for identification of how reliable the facial recognition system is; therefore, one of the reasons why it was not important to test with lots of people (more than 3 participants) is because the purpose was not essentially to test the FAR or FRR. The FRR has previously been included in the usability analysis simply because if the legitimate person gets flagged up as illegitimate a lot of the time, then the academic will spend a very long time reviewing images that are perfectly legal, and that will represent a problem in the convenience and usability of the system from the academic perspective.

Operational considerations. In some discussions with the participants and conference audience, some people and experts were wondering whether the volume of the collected data, including the database and the samples, was feasible or not. In terms of the operational aspects and the required space on the disk, the database size, including all photos and Intel RealSense DB, was 978.1 MB, which, while not a small volume of data, is operationally within limits and demonstrates the ability to be scalable (into the order of hundreds (rather than thousands) of simultaneous assessments). Detailed data sizes are shown in Table 5.

Table 5. Complete data sizes

Categorizations	Participants	
	Per User	All the 51 Users
2D Samples	1 Every 4 Seconds (about 73), 2 MB	3723 Samples, 102 MB
3D Samples	1 Every 4 Seconds (about 146), 4 MB	7446 Samples, 204 MB
Audio Recording	12 MB	612 MB
Eye Tracking	0.6 MB	30.6 MB
Head Movements	0.5 MB	25.5 MB
Total Size	19.1 MB	974.1 MB + 4 MB For DB

In the 2D mode, 73 facial recognition samples per user are captured on average, as no more than 2MB on disk is required for these samples per participant. A total of 102 MB of storage is used to store 3723 photos across all 51 participants. On average, 3D facial recognition captures 146 samples per user. Less than 4MB on disk is required for these samples per user (the sizes of the 2D and 3D facial recognition samples could be reduced if the academic decides to increase the period of taking the samples (e.g., > 5 seconds)). A total of 204 MB is used to store 7446 photos across all 51 participants. The recorded session (audio) was less than 12 MB per user and 612 MB for all participants. 30.6 MB is the total size of eye-tracking security data in the whole experiment and about half a MB for each user. The required space for the data on head movements' security per participant is 500 KB and 25.5 MB for all of them. However, in order to use the available space effectively, compression techniques can be implemented on the stored data, which could reduce the size of the stored data, particularly the sound files.

In general, from a processing perspective, it is less time sensitive because the system follows a batch processing mechanism; therefore, it can take a long time to complete (it could take a day to come back, which will be perfectly fine). What is required is that the system be able to capture and store the information in real-time but the actual process of the biometric sample is not very important because the nature of the proposed processing itself solves or mitigates the problem as discussed previously.

Basically, the infrastructure of the proposed architecture of the system would then need to include three types of servers:

- A web application server
- A backend processing server
- A database server

In a worst-case-scenario, the web application and database servers could be duplicated for the purpose of providing mirror servers for data redundancy. Both the backend processing and the web application servers would be quite small compared with the database server, as all the collected data would be stored on the latter. About 19 MB of data per student, however, can be considered feasible to store this volume of data (the required space on the database server). For example, in Plymouth University, which is one of the largest universities in the UK, there are about 25000 students [36]. If they took that test for 1 hour (Four-fold the conducted online assessment time during the experiment), this could require 19 MB (data size for 15 minutes) × 4 = 76 MB per student for 1 hour, which means 76 MB × 25 K = 1,900,000 MB (1.9 TB) for all the 25000 students. Therefore, this would cost the value of a local server with hard drive(s) < 2 TB, and the cost would be about $750 [37]. However, if the system in a cloud-based environment (Cloud Server), for the same volume of data, the cost would be about $187.00 per month [38]. Therefore, these estimated costs can be considered far less than employing hundreds of human inspectors (who might be untrusted or inexperienced) to achieve the monitoring process on this number of online examinations that should be taken inside the university using its resources, including the electricity, computers, equipment, and all other infrastructure that would be required to accomplish every test.

6 DISCUSSION

Generally, in the online assessment environment, the system can face many challenges; some of them are general and can be controlled in the same way traditional examinations would deal with such things as people's health, cultural, religious, or even technological problems. Some people might suffer from health problems such as eyesight permanent vision problems (e.g., blindness or being cross-eyed). These particular cases, as with the traditional examinations, should be managed by providing special cases that the institution can specify to make the online examination possible and secure at the same time. The solution could involve the exclusion of some biometric modalities and security restrictions (e.g., iris recognition, eye movements, or eye tracking security). Furthermore, as the online examinations are supposed to be implemented on a global basis, there are numerus cultures, so the system should be fixable and could adapt to deal with them. For instance, some cultures insist that women must wear face veils; in this case, the exclusion may include the essential biometric modality (i.e., face recognition) rather than the secondary; the alternative here should be a range or combination of solid biometric modalities (e.g., iris recognition) in addition to other behavioral biometrics (e.g., mouse dynamics, keystroke analysis, eye movements, or head movements).

Other challenges might be related to the student's ability to always invent new ways of cheating, for instance, using a small earphone to hear the answers of somebody else outside the room. Basically, it is very difficult to read the question in front of anyone else but the participant without catching him by the camera. Even though they could access the question somehow, the problem can be solved by asking the student to show their ears to the camera before the exam starts to take photos of them to ensure there are no earphones in there. Fortunately, these photos might also be utilized for ear recognition of the student identification in the log-in process, providing an additional robust and transparent biometric method.

Furthermore, a typical problem would be connected to the nature of the exam itself, for example, some exams might include particular questions that might need relatively long time and/or calculations to be solved, this would require using pen and paper apart of the computer/machine being used to achieve the e-assessment, or accessing some resources on or out the computer, in this case, when defining the exam questions, there is an ability to highlight a specific question and turn off the eye tracking security while answering this sort of highlighted questions as might be additional work is required, therefore there is expectation for user's eyes to probably move from the screen, and in this case this strategy does not allow the system to flag misuse. Moreover, another expectation could be applied for open book assessments; in these cases, there is essentially no need for eye tracking, as it is no problem if the exam taker looks at the resource or reads text books during the exam.

Due to its transparency and reliability, Intel RealSense face recognition technology has been chosen to be the main authentication approach in this e-invigilation system. Beyond the former modality, many of the other proposed biometric modalities can be utilized to enhance performance. For instance, low-cost mouse movements and keystroke recognition could provide a high level of transparency and usability, in addition to their encouraging implementation, especially in the case of combining them with other biometric techniques such as linguistic analysis. However, more work is required on those modalities to get them to the point of being reliable and implementable within this system.

Both eye tracking (left eye, right eye, and the center point of 30 samples every second) and head movement information (Roll, Yaw, and Pitch of 3 × 25 samples every second) are continuously measured and recorded in every test during the experiment. This could give the opportunity to explore the possibility of proposing that these collected data be employed to produce novel and new behavioral biometric modalities (namely, eye and head movement biometric modalities), which can be utilized as additional non-intrusive and feasible modalities to improve authentication performance. These eye and head movements are unconscious human behavior, which means people cannot feel anything when they occur. This fact puts these techniques at the top of the list of the most transparent biometric modalities list and means they can be collected even without the user's knowledge.

During the experiment, participants' left and right eye images are collected by the custom software, as demonstrated in Figure 14. This occurs in the registration stage using the 3D camera, which opens the door for utilizing these images (perhaps after enhancement processes) for iris recognition as an additional strong biometric modality to the system. Iris recognition offers an interesting opportunity as it is generally considered to be a highly reliable modality with robust performance. However, research has not thoroughly investigated to what extent a partial iris image is useful in providing identity verification and to what degree of performance; therefore, further research needs to be done looking at the use of iris recognition and also the iris recognition of partial iris.

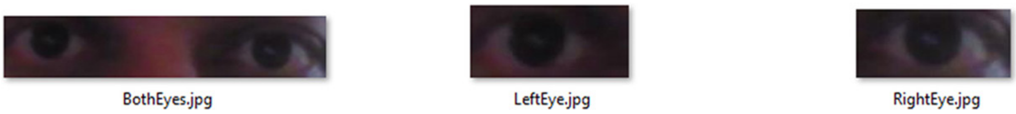


Fig. 14. Example of left and right eyes captured photos

The use of an eye tracker in the experiment was interesting as it is an effective, efficient, and reliable technique. However, current implementations still require sensitive near-infrared cameras or sensors in order to achieve the eye tracking process. Though, the 3D camera has further functionality that could also enable eye tracking, which can be considered promising as this type of technology, and particularly the 3D camera, it will be integrated widely into consumer hardware devices. Therefore, it is more likely that all the hardware and software that the proposed system needs will be included or installed by default within the devices in the future. In order to enhance the overall performance of the continuous identity verification system, the collected and saved eye movement information (using the eye tracking security system) can be utilized to produce a promising new and very transparent biometric modality, as it is one of the biometrics that can be collected from the face area without any direct connection or even without the student's knowledge (passively).

In both 2D and 3D modes, the speech recognition algorithm captures every spoken sentence, relying on an English dictionary. As part of the aforementioned prototype (section 4), a subroutine called "Language Selection" has been developed and can be fetched, enabling the system administrator to easily change the size or type of dictionary according to their needs. Since the recognition algorithm can be applied on any language and the dictionary language is not restricted to English, system users can choose any language they would like (e.g., French, Arabic, or Chinese). As long as it captures the start and end of the speech, then the duration of each spoken sentence can be calculated. Therefore, in the event of any unauthorized talks that happen during the e-assessment, this will give the academic a chance to listen to those particular short periods rather than the whole session. Furthermore, these captured sentences can be used to facilitate linguistic analysis or even be utilized for voice verification purposes as further transparent biometric modalities. Moreover, in such a recognition system, the academic can predefine a particular set of words to be included in the security subsystem in order to match them with the words of the captured sentences; this would help to normalize priorities and consequently enhance the captured and reported cases of speech recognition misuse. For example, if the test is database systems, then the academic can predefine a group of words (e.g., SQL, Attribute, or DBMS) that could be considered more commonly used when talking about database system examination, and then the system could prioritize presenting these particular sentences as misuse actions over the other sentences.

The inclusion of additional biometric modalities (e.g., iris recognition, scar and mole identification, or mouse movement) in the theoretical architecture would deal with some threat (e.g., identical twins or even the face veil that some people would wear) that the 2D and 3D facial recognition algorithms in the current developed and utilized prototype would not be able to recognize. However, the results of the implemented threat scenarios have evidently shown the suggested approach's ability to identify, track, and monitor users with a view to identifying unauthorized assistance that could be provided by somebody else during the e-assessment. The resultant FAR has proven that the participant biometric modality could not be forged by illegitimate users.

7 CONCLUSION

To solve a key issue in e-learning (the cheating problem), detailed planning and concentration are essential for designing a more secure, transparent, and continuous authentication mechanism for e-assessments. In order to reach an acceptable level that enables this system to be appropriate, various system authentication and security requirements were addressed. Hence, the architecture has been designed around two operational objectives: continuous biometric-based monitoring of the participant and system-level monitoring to prevent cheating. On top of this, there is a variety of management-level functionality that provides the basis for creating and managing e-assessments.

The paper has experimentally explored the viability of a more secure, transparent, and continuous authentication mechanism for e-assessments employing the developed prototype. The focus was on face recognition as the most transparent multimodal (2D and 3D) biometric and novel security features through eye tracking, head movements, multiple face detection, and speech recognition. A multiple-scenario experiment was conducted, involving 51 participants. For all these participants, the FRR was 0 in 2D facial recognition mode, while in 3D facial recognition mode it was 0.04827. Moreover, in order to evaluate the robustness of the approach against targeted misuse, three participants were tasked with a series of nine threat scenarios. The FAR was 0.038 in the 2D mode and 0 in the 3D mode.

The experiment results have also shown the ability of the proposed system to capture, process, and identify users through the use of biometrics. The achieved FRR has validated to a great extent the usability of the system and its ability to correctly recognize a legitimate user utilizing facial recognition in 2D and 3D modes under normal use. The results in this context have also demonstrated that the participant's face expressions (e.g., smile or eyebrow down) play no role in the recognition performance. Furthermore, the other factors have no effect on the facial biometric recognition performance, such as wearing glasses or a head veil during the regular experiment test time. The capturing mechanism has been accomplished transparently during the entire 51 controlled e-assessments with a reliable biometric sampling process.

Furthermore, experimentally, the employed security restrictions have evidently identified all the misuses that have been carried out as predefined threats by the three participant groups.

8 ACKNOWLEDGMENT

The authors wish to gratefully acknowledge the voluntary participants in the experimental phases of this study.

9 REFERENCES

[1] J. Bailie and M. Jortberg, "Online learner authentication: Verifying the identity of online users," *Journal of Online Learning and Teaching,* vol. 5, no. 2, p. 25, 2009.

[2] A. Rovai, "Online and traditional assessments: What is the difference?" *Internet and Higher Education*, vol. 3, no. 3, pp. 141–151, 2000. https://doi.org/10.1016/S1096-7516(01)00028-8

[3] IT Parks Update, "ICFOSS, IIITM-K 3-day Programme for Academic & Research Institutions | IT Parks Update," 2014. [Online]. Available: http://itparksupdate.in/icfoss-iiitm-k-3-day-programme-for-academic-research-institutions/ [Accessed: 25-Nov-2014].

[4] M. AL-Smadi, M. Hofler, and C. Guetl, "Integrated and Enhanced E-Assessment Forms for Learning: Scenarios from Alice Project," In *14th International Conference on Interactive Collaborative Learning (ICL),* pp. 626–631, 2011. https://doi.org/10.1109/ICL.2011.6059662

[5] U. Mothukuri, "Invigilated Online Assessment: Various Ways to Minimize Unauthorized Help," In *2012 IEEE Symposium on E-Learning, E-Management and E-Services (IS3e)*, pp. 1–4, 2012. https://doi.org/10.1109/IS3e.2012.6414961

[6] N. L. Clarke, P. Dowland, and S. M. Furnell, "E-Invigilator: A Biometric-Based Supervision System for e-Assessments," In *International Conference on nformation Society (i-Society),* p. 5, 2013.

[7] Y. Khlifi, "An advanced authentication scheme for e-evaluation using students behaviors over e-learning platform," *International Journal of Emerging Technologies in Learning (iJET)*, vol. 15, no. 4, pp. 90–111, 2020. https://doi.org/10.3991/ijet.v15i04.11571

[8] A. A. Alghamdi, M. A. Alanezi, and F. Khan, "Design and implementation of a computer aided intelligent examination system," *International Journal of Emerging Technologies in Learning (iJET)*, vol. 15, no. 1, pp. 30–44, 2020. https://doi.org/10.3991/ijet.v15i01.11102

[9] 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, pp. 205–216, 2020. https://doi.org/10.3991/ijet.v15i12.13741

[10] N. Rowe, "Cheating in online student assessment: Beyond plagiarism," *Online Journal of Distance Learning Administration*, 2004.

[11] K. Apampa, G. Wills, and D. Argles, "Towards Security Goals in Summative E-assessment Security," In *International Conference for Internet Technology and Secured Transactions, (ICITST)*, pp. 1–5, 2009. https://doi.org/10.1109/ICITST.2009.5402505

[12] L. Gilbert, V. Gale, B. Warburton, and G. Wills, "Report on Summative E-Assessment Quality (REAQ)," pp. 1–96, 2009.

[13] A. Bal and A. Acharya, "Biometric Authentication and Tracking System for Online Examination System," In *2011 International Conference on Recent Trends in Information Systems*, pp. 209–213, 2011. https://doi.org/10.1109/ReTIS.2011.6146869

[14] E. Flior and K. Kowalski, "Continuous Biometric User Authentication in Online Examinations," In *2010 Seventh International Conference on Information Technology: New Generations*, pp. 488–492, 2010. https://doi.org/10.1109/ITNG.2010.250

[15] S. Asha and C. Chellappan, "Authentication of E-learners Using Multimodal Biometric Technology," In *2008 International Symposium on Biometrics and Security Technologies*, pp. 1–6, 2008. https://doi.org/10.1109/ISBAST.2008.4547640

[16] A. Ross and A. Jain, "Information fusion in biometrics," *Pattern Recognition Letters*, vol. 24, no. 13, pp. 2115–2125, 2003. https://doi.org/10.1016/S0167-8655(03)00079-5

[17] Y. Levy and M. Ramim, "Initial development of a learners' ratified acceptance of multibiometrics intentions model (RAMIM)," *Interdisciplinary Journal of E-Learning and Learning Objects*, vol. 5, p. 19, 2009. https://doi.org/10.28945/84

[18] Z. Jorgensen and T. Yu, "On Mouse Dynamics as a Behavioral Biometric for Authen tication," *Proc. 6th ACM Symp. Information, Comput. Commun. Secur. – ASIACCS '11*, p. 476, 2011. https://doi.org/10.1145/1966913.1966983

[19] N. H. Lin, L. Korba, G. Yee, T. K. Shih, and H. W. Lin, "Security and Privacy Technologies for Distance Education Applications," *18th Int. Conf. Adv. Inf. Netw. Appl. 2004. AINA 2004.*, vol. 1, pp. 580–585, 2004.

[20] C. C. Ko and C. D. Cheng, "Secure internet examination system based on video monitoring," *Internet Res.*, vol. 14, no. 1, pp. 48–61, 2004. https://doi.org/10.1108/10662240410516318

[21] Y. W. S. Sabbah, "Proposed Models for Secure E-Examination System," Cairo University, 2012.

[22] J. A. Hernández, A. O. Ortiz, J. Andaverde, and G. Burlak, "Biometrics in Online Assessments: A Study Case in High School Students," In *18th International Conference on Electronics, Communications and Computers (conielecomp 2008)*, pp. 111–116, 2008. https://doi.org/10.1109/CONIELECOMP.2008.36

[23] A. Ullah, H. Xiao, and M. Lilley, "Profile Based Student Authentication in Online Examination," In *Information Society (i-Society)*, pp. 109–113, 2012.

[24] C. Pan, K. Yang, and T. Lee, "Secure Online Examination Architecture Based on Distributed Firewall," In *IEEE International Conference on e-Technology, e-Commerce and e-Service*, pp. 533–536, 2004.

[25] M. Onyesolu, V. Ejiofor, M. Onyeizu, and D. Ugoh, "Enhancing security in a distributed examination using biometrics and distributed firewall system," *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 9, p. 6, 2013.

[26] M. Carlisle and L. Baird, "Design and Use of a Secure Testing Environment on Untrusted Hardware," In *Information Assurance and Security Workshop*, pp. 349–354, 2007. https://doi.org/10.1109/IAW.2007.381953

[27] C. C. Ko and C. D. Cheng, "Flexible and secure computer-based assessment using a single zip disk," *Computers & Education*, vol. 50, no. 3, pp. 915–926, 2008. https://doi.org/10.1016/j.compedu.2006.09.010

[28] Software Secure, "Remote-Proctor-Now for Educational Institutions," 2008.

[29] Respondus, "Real People. Real Proctoring. – Online Proctoring – ProctorU," 2014. [Online]. Available: http://www.proctoru.com/. [Accessed: 21-Oct-2014].

[30] Coursera, "Coursera," 2014. [Online]. Available: https://www.coursera.org/. [Accessed: 29-Sep-2014].

[31] Kryterion, "Testing Platform | Kryterion," 2014. [Online]. Available: http://kryteriononline.com/testing-platform/. [Accessed: 29-Sep-2014].

[32] The Open University, "TeSLA Project," 2016. [Online]. Available: http://tesla-project.eu/tesla-technical-architecture/. [Accessed: 01-Jan-2016].

[33] S. S. Ketab, N. L. Clarke, and P. S. Dowland, "E-Invigilation of E-Assessments," In *Proceedings of INTED2015 Conference*, pp. 1582–1591, 2015.

[34] S. S. Ketab, N. L. Clarke, and P. S. Dowland, "A robust e-invigilation system employing multimodal biometric authentication," *International Journal of Information and Education Technology*, vol. 7, no. 11, pp. 796–802, 2017. https://doi.org/10.18178/ijiet.2017.7.11.975

[35] M. Al-Smadi, M. Hoefler, and C. Guetl, "An Integrated Model for E-Assessment of Learning Experiences Enriched with Complex Learning Resources," In *Proceedings 3rd IEEE International Conference on Intelligent Networking and Collaborative Systems INCoS*, pp. 824–829, 2011. https://doi.org/10.1109/INCoS.2011.52

[36] HESA UK, "Higher Education Statistics Agency," 2017. [Online]. Available: https://m.hesa.ac.uk/uk-he-stats/?p=institution&y=15/16&l=P&g=&s=&n=1. [Accessed: 16-Apr-2017].

[37] Dell, "Dell Online Server Prices," 2017. [Online]. Available: http://www.dell.com/uk/business/p/enterprise-deals#poweredge-tower-server-deals?lnktrgt=parent. [Accessed: 23-Apr-2017].

[38] Amazon, "Amazon Web Services Simple Monthly Calculator," 2017. [Online]. Available: https://calculator.s3.amazonaws.com/index.html. [Accessed: 23-Apr-2017].

10 AUTHORS

Salam S. Ketab, PhD received a bachelor's degree in computer science from Baghdad University, Iraq, in 2001. He was awarded his MSc with distinction in computer science from Baghdad University, Iraq, in 2005. He then obtained his PhD from the Centre for Security, Communications and Network Research at Plymouth University, United Kingdom. His research interests include information security, biometrics, and e-learning (E-mail: salam.ketab@plymouth.ac.uk).

Abdulwahid Al Abdulwahid, PhD is an Assistant Professor of Cybersecurity with the Computer and Information Technology Department, Jubail Industrial College at Royal Commission for Jubail and Yanbu, KSA. He also served as the department chairperson, the College Dean of student affairs, and the Deputy Managing Director at Jubail University College. He was awarded his B.Sc. in computer information systems from KFU, KSA, in 2003, M.Sc. in management of information technology from UoN, U.K., in 2010, and Ph.D. in Cyber security from the Centre for Security, Communications and Network Research, UoP, U.K. He is the General Secretary of the Board of Directors of the Scientific Saudi Society for Cyber Security, a Professional Member of the ACM and the Association of Information Security and has published and presented a number of papers in credible journals and conferences. His research interests include cyber security, user authentication, biometrics, and artificial intelligence (E-mail: abdulwahida@rcjy.edu.sa).