# Synchronous Authentication with Bimodal Biometrics for e-Assessment

## A Theoretical Model

Yousef Sabbah
Open Learning Center (OLC)
Al-Quds Open University (QOU)
Ramallah, Palestine
ysabbah@qou.edu

Imane Saroit and Amira Kotb
Information Technology Department
Faculty of Computers and Information, Cairo University
Giza, Egypt

***Abstract*—This paper presents a theoretical model for summative e-assessment in distance learning for the future, where exams can be conducted distantly, e.g. at home. This model aims to provide e-learning systems with an authentication approach that guarantees cheating-free summative e-assessment. It utilizes a combination of live video monitoring and a bimodal biometrics approach. Together they form a robust and highly secure model to ensure that the examinee is the correct person throughout the e-assessment period without a need for a proctor. Advanced techniques of image and video processing and feature extraction are required to implement this model.**

***Keywords- Authentication; Biometrics; e-Assessment; e-Learning***

## I. INTRODUCTION

It has been claimed that the lack of trusted, secure and cheating-free e-assessment is the main reason of unsuccessful e-learning [1-7]. In a survey conducted to evaluate this issue, 73.6% said that cheating is easier in an e-examination than in its traditional counterpart [7]. This paper provides a theoretical approach that contributes in resolving this issue using video monitoring, keystroke dynamics and fingerprint for synchronous authentication. The proposed model automates the process, and a proctor is no longer required. It employs advanced techniques of image/video/action processing and feature extraction as well as pattern recognition. A media server is also required to broadcast examination sessions to a special purpose server that handles these processing tasks. This provides a highly secure e-examination model, taking into account that it is a part of a secure e-learning system where essential security controls are provided.

The rest of this paper is divided into five sections. Section II discusses e-learning security, and focuses on user authentication and continuous authentication requirements. Section III, on the other hand, presents the different schemes of e-assessment authentication and defines their security threats. In section IV, the proposed model is presented. Section V evaluates the proposed model against various security issues including impersonation threats. Finally, the conclusion is presented in section VI.

## II. E-LEARNING SECURITY

The main objective of e-learning is to enhance teaching and learning by utilizing Information and Communication Technology (ICT) applications and modern tools [8]. Such technologies include Web-based portals, Learning Management Systems (LMS), Course Management System (CMS), Virtual Classrooms (VC) and Video Streaming (VS) [1, 8-12].

Security is very important in e-learning as a Web-based application, which is ICT dependent. This makes it vulnerable to various types of possible cyber-attacks and security risks. Higher security reduces the probability of system failures and ensures higher availability. The following security controls are essential in order to protect e-learning systems [8-10, 13-15]: (1) Access Control, (2) Encryption, (3) Firewalls, (4) Intrusion Detection, (5) Protection against Viruses and Spywares, (6) Digital Signature, (7) Digital Certificate, and (8) Content Filter.

Unlike the past decade, when security has often been neglected in e-learning systems, nowadays, security is a fundamental requirement. It has been considered relevant because of the following [12, 14, 16, 17]:

- e-Learning systems are risky projects.
- e-Learning systems are productive systems that need to be secured.
- New electronic systems add new threats.
- User acceptance to an e-learning system is related to system trust.
- Feeling secure in online e-learning is a social aspect of users.

### *A. Security Requirements*

In general, four security requirements have been used to measure security of any computer system [8, 12-13, 17-18]:

- **Confidentiality**: ensure that data are private, and accessible only by authorized entities.

- **Integrity**: ensure that data are original and have not been modified by unauthorized parties, either accidentally or intentionally.
- **Availability**: ensures that system resources are up and available for authorized parties at any given time.
- **Authenticity**: or user authentication verifies a user's identity whilst trying to access system resources by ensuring who is granted access to which resources.

### *B. Authentication Factors*

User authentication to e-learning systems is one of the most important issues. Authentication has been implemented with something a user knows, a user owns, a user is, or a user does. Biometric authentication such as fingerprint, keystroke dynamics, head-geometry detection, and iris are promising examples of something a user is. In general, authentication methods can be divided into three categories called factors. They are [4]:

*1) Knowledge Factors:* require a user to know something unique (e.g. a password) that others do not know. A password may consist of a combination of characters, numbers and/or symbols. With a strong password policy, an institute can provide authentication security for users, where unauthorized parties cannot access their accounts.

*2) Ownership Factors:* a user should possess some token that others do not have, such as dongles, keys or cards. Unauthorized parties cannot access users' information unless they obtain this token.

*3) Inherence Factors:* provide accurate means of authentication, but described to be expensive and difficult to implement. Two main methods have been implemented [4]:

*a) Something the user is:* a highly reliable method for user authentication. Biometric methods which utilize image processing and pattern recognition fall in this type. Examples of such method include fingerprint, voiceprint, retinal pattern and DNA sampling. Fingerprint is the most popular approach but requires special purpose hardware. Hence, it will be discussed with more details in subsection C.

*b) Something a user does:* this method is efficient for continuous user authentication in online examination. It includes handwriting, walking gait and typing rhythm (keystroke dynamics).

### *C. Fingerprint Authentication (FPA)*

Secure Web Access Module (SWAM) approach that uses fingerprint has been proposed essentially to perform sensitive transactions in e-banking [19]. For simplicity, FPA will be used along this paper as an acronym for fingerprint authentication. Fingerprint has also been implemented for user authentication in e-examination [4, 20]. A special hardware, which might be a portable fingerprint scanner with USB connector, is required to scan a user's imprint. The main steps of SWAM approach can be summarized as follows [19]:

- Creating user-Id and password for each user, scanning each user's thumb, and storing them in a secure server.
- Log in to the site using user-id and password.
- In case of access to sensitive data, the fingerprint scanner device will be enabled and the user is prompted to print his thumb.
- The device will be disabled and the user will be able to access sensitive data.

### *D. Keystroke Dynamics Authentication (KDA)*

Keystroke dynamics propose that typing rhythm is different from a user to another. For simplicity, KDA will be used along this paper as an acronym for keystroke dynamics authentication. The metrics used for user verification in this technique include: (1) typing speed, (2) flight-time, (3) keystroke seek-time, (4) characteristic sequences of keystrokes, and (5) characteristic errors [4].

## III. E-ASSESSMENT SECURITY

Because secure and cheating-free e-examination have not been yet achieved, it is still difficult to trust e-assessment within an e-learning model. Impersonation is the main threat that encounters e-assessment and requires synchronous/ continuous authentication. More cautious should be taken in online examination, where e-learning systems should verify an examinee is the actual student throughout an exam [1-7]. Multiple technologies and tools are supposed to provide cheating-free e-examination. An agent-based reference model might be used to deal with cheating scenarios as appealing obvious actions [1, 6]. Several schemes have been used to solve this issue; proctored-only, uni-modal/ bimodal biometrics, video monitoring, and biometric with webcam.

### *A. e-Assessment Authentication Schemes*

Current solutions for the major threats of e-assessment (i.e. impersonation threats) have been categorized into five main categories. These categories have been analyzed in terms of suitability to the three types of impersonation threats.

#### *1) Proctored-only Scheme*

This approach requires a proctor or a testing administrator to monitor the exam-takers during their examinations. Proponents of this approach consider human proctoring a suitable low-technology method for e-assessment authentication. This scheme promotes identity and academic honesty [7].

#### *2) Uni-modal Biometric Scheme*

This scheme employs a single biometric approach for authentication, such as fingerprint, typing rhythm, handwriting, or face recognition. Multiple random fingerprints of the examinee might be taken throughout the e-examination period to add more security [6, 7, 20].

#### *3) Bimodal Biometric Schemes*

In order to achieve better security in e-learning systems, multiple biometric approaches are required to be combined. This provides reliable user security for the duration of the exam rather than instantaneous login. For instance, fingerprint might be combined with mouse or keystroke dynamics [7].

Alternatively, fingerprint can be combined with head-geometry detection using a webcam [7].

*4) Video Monitoring*

A proven approach for high security has been monitoring of student activities during online examination using video. Random video monitoring has been proposed for secure internet examination. A password has been required for login and a proctor is supposed to watch the video either live or recorded [7].

*5) Biometrics and Webcam Monitoring*

This approach combines fingerprint and real-time video-monitoring until the exam ends [7].

### *B. e-Assessment Impersonation Threats*

Impersonation threats in e-assessment are the most vital risks (i.e. cheating scenarios) that might be encountered during an e-exam. They occur when an examinee pretends to be another. They have been divided into three types [7]:

*1) Type A impersonation,* which might occur in two cases, either the proctor could not detect it, or he allowed impersonation by force, sympathy or bribery.

*2) Type B,* which occurs when a student passes his security information to another, who uses them to answer the exam on his behalf. Username-password pairs fall in this type.

*3) Type C,* which occurs when a student just login to an exam, letting another to continue on his behalf. Non-shareable attributes such as biometrics fall in this type.

*4) Type D,* a new threat defined in this paper, where a student logins and answer the exam but with an assistant giving him the answers.

### *C. Emerging e-Assessment Authentication Models*

Although some of the authentication methods (factors), which have been discussed in section II, are highly reliable, they all have some drawbacks when used in e-examination, as illustrated in table I.

In fact, even the most accurate schemes are still vulnerable to several risks. For instance, four risks have been identified in biometrics authentication approaches [6]: (1) fake input, (2) low-quality input, (3) biometric-database modification, and (4) feature-extractor modification. Several methods have been proposed to protect different systems against these risks. Even though Fig. 1 depicts eight attack points in biometrics authentication systems [6].

On the other hand, the five e-assessment authentication schemes have been evaluated by [7] in terms of vulnerability to the different types of impersonation threats. This evaluation has shown that the first scheme is only vulnerable to Type A threats, knowing that this scheme is not suitable for e-examinations. The second prevents cheating scenarios of pretending to be the real examinee, hence, solves Type B. It will be suitable for Type C if continuous authentication is performed throughout the e-examination period [7]. In the third, when fingerprint is combined with mouse dynamics, it solves Type B, but unclearly solves Type C due to delay incurred in data-capturing.

TABLE I. DRAWBACKS OF USER AUTHENTICATION METHODS WHEN USED IN E-EXAMINATION

| Methods or Factors | Drawbacks |
|---|---|
| ***Knowledge factors*** | • If the password is disclosed, even if strong enough, the password security policy will be cancelled [4].<br>• Requested once at login, saved and repeated by cookies; never trusted for authentication throughout e-examination. |
| ***Ownership factors*** | • If the token is passed to others, the authentication scheme will be circumvented [4].<br>• Requested once at login and repeats by cookies; cannot be trusted for authentication throughout e-examination. |
| ***Inherence factors*** | • Accurate means of authentication but requires special-purpose hardware.<br>• Difficult to implement and unreasonably intrusive and expensive [4].<br>• Not fully trusted, although some approaches proposed repeated and random authentication throughout e-examination [4, 20].<br>• Never trusted in case of Type D threat. |

Alternatively, fingerprint with face-geometry detection offer a promising combination that solves Type B and Type C threats. In the fourth scheme, live video monitoring might fail if the proctor overlooked or unfocussed, while recorded needs extra administrative efforts. It is vulnerable to Type A, B and C threats. Fingerprint of the fifth scheme solves Type B threats, while video monitoring was unclear. Moreover, security will be broken if the view of the webcam is changed [7].

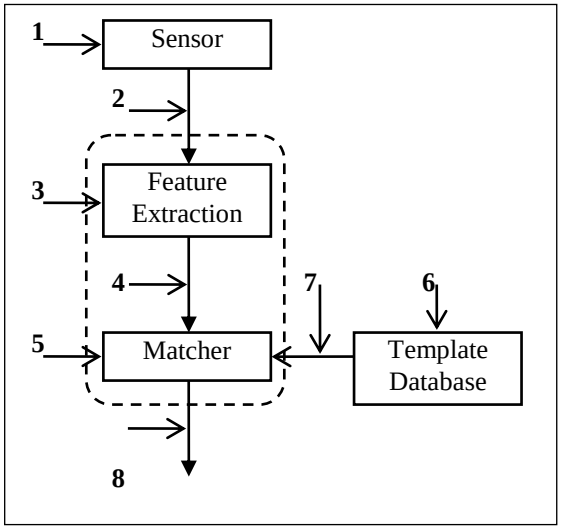


Figure 1. Attack Points in Biometric Authentication Systems [6]

Moreover, Confidentiality, integrity, and availability (C-I-A) security requirements or goals are not suitable for e-assessment content but not process security. Hence, different

goals are required, in order to ensure continuous protection. For example, continuous random authentication is required in e-examination over time, to ensure that the examinee is the correct one [3-7]. Three goals have been proposed for this purpose [6-7]:

- Presence and continuously authenticated presence (specify student's place).
- Identity (differentiate a student from another).
- Authentication (prove student's claimed identity).

In addition, several security threats and issues have neither been resolved nor even mentioned by any of the previous authentication schemes. Firstly, an examinee might look around at the available resources, such as his textbooks, worksheets, local computer, the Internet and/or got assistance from others besides him. So, continuous video monitoring and lock functions on resources are required. Secondly, Biometrics schemes, such as keystroke/ mouse dynamics or on-mouse continuous fingerprints, each depends on a specific device that might never or rarely been used while using another device. For instance, an examinee never requires typing in multiple-choice or matching questions and rarely requires a mouse in essay questions. Hence, emerging techniques are required to resolve this issue.

Finally, the previously-mentioned video monitoring schemes are insufficiently efficient, where cheating cannot be stopped when detected, since they lack to interaction and cheating indicators. Moreover, the camera might be removed or turned to another object leading to failure. Therefore, a new scheme that provides interaction and cheating indicators as well as dealing with camera failures is vital.

## IV. THE PROPOSED MODEL

### A. *A Basic Model (ISEEU)*

The basic model behind the idea of the proposed model is a previously proposed model; Interactive and Secure E-Examination Unit (ISEEU) [21]. In other words, the new model comes as an upgrade to ISEEU, which is a proctor-based model for e-assessment authentication. In ISEEU, an examinee should be connected to a media server (MS) via a webcam that is attached to his terminal (ET), as shown in Fig. 2. The MS, in turn, creates a channel ($ch_n$) for each examinee to broadcast the exam session to his proctor through an e-learning server (ELS). Each examinee's session will be streamed through his channel, and all the videos appear on the proctor's terminal (PT).

The major challenges of ISEEU are: (1) It requires manual intrusion, i.e. it is not fully automated. (2) If the web camera stopped working, or intentionally removed by the examinee, the exam will be paused for a predefined period of time and waits for an action by the proctor or the examinee to be resumed. Otherwise, the exam will be saved on that point, or simply terminated, to be rescheduled. (3) If an examinee managed to broadcast his live video to the media server on behalf of another, there is no means to ensure that he is the correct examinee.

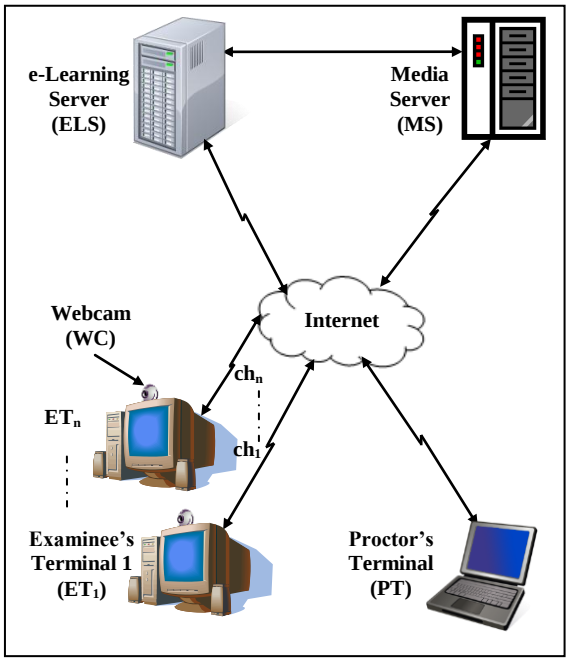


Figure 2. Structure of ISEEU model using a Web camera.

### B. *An Emerging Model*

In this paper, one of the emerging models of continuous/ synchronous authentication for summative e-assessment, or alternatively e-examination, is introduced. The structure of this model is depicted in Fig. 3.

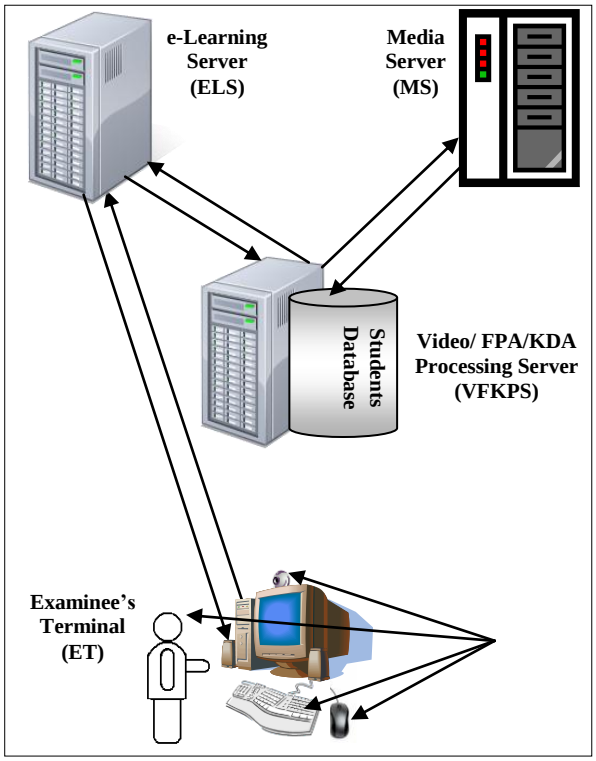


Figure 3. Structure of the proposed model for e-assessment authentication

The proposed model adds a bimodal biometrics scheme to ISEEU, which consists of continuous random fingerprint and keystroke dynamics. The first employs an on-mouse fingerprint scanner, whereas the latter depends on the keyboard as discussed in section II. Another important advantage is automation, where the proctor's terminal (PT) is substituted by a Video/FPA/KDA Processing Server (VFKPS).

High specifications are required for VFKPS server to ensure high performance and fast response. Multiprocessors with a huge capacity of storage are preferable to be able to manipulate images and videos as well as the keystrokes.

Moreover, advanced techniques of image processing, pattern recognition, image/video feature extraction and action/time processing are required to detect who is the exam-taker. The proposed model operates in three phases; before, during, and after conducting the e-exam, as follows:

*1) Before e-Examination*

When a student registers for an e-learning course, the following are requested:

- His fingerprint is taken by the registrar using a scanner attached to his computer.
- A still photo is captured by a high resolution camera attached to the registrar's computer, and as short video (around 1 min) is recorded using an arc-moving video camera.
- A training set of keystrokes is captured for each student by typing a passage using a computer dedicated for this purpose.

All the above data are then transferred to the VFKPS; processed, their features are extracted, and saved in each student's profile.

*2) During e-Examination*

*a) Initialization:* this phase enables, checks, configures and calibrates the hardware of the required devices. Login to the e-learning and the e-examination systems takes place in this phase.

- FPA initialization: when a student opens the login screen of his e-learning system, (1) the fingerprint scanner is enabled, (2) he is asked to enter his imprint by placing his finger on the on-mouse scanner, (3) the VFKPS server performs a matching process with the saved imprint, and (4) the scanner remains on. If matched, login succeeds; otherwise, it fails with an error message to retry.
- KDA initialization: when a student (examinee) tries to start an e-examination, (1) a welcoming screen appears with a multimedia demo of instructions, (2) a training screen appears and asks him to type some specific paragraphs as a training set to the KDA, (3) keystrokes data is captured and transferred to the VFKPS, (4) the server, in turn, performs intensive analysis and the keystrokes' features are extracted using appropriate applications, and (5) these features are compared with the data in his profile. If matches, he is moved to the next step, otherwise, he is asked to try again.
- Video initialization: after KDA initialization completes, the examinee is moved to a blank video screen. Then, (1) the web camera is enabled and his video appears on the screen, (2) he is asked to calibrate his audio and video devices using some smart tools, (3) he is reminded of a chat service with a technical support agent online 24/7, to help in case of technical issues, (4) if the audio/video test passes, his video is matched with the one in his profile, and finally, (5) if matched and the examinee is identified, he is moved to the next phase, otherwise he just continues trying.

*b) Operation:* in this phase, the exam actually starts, and so the timer's countdown. Also, a full screen locks the examinee's desktop to prevent access to related resources from local disks, by the network or the Internet.

- FPA operation: the fingerprint scanner captures the imprint in two modes that can be configured by the administrator; randomly or periodically, and the imprints are transferred continuously for processing and matching in the VFKPS.
- KDA operation: the examinee's activities on the keyboard are continuously captured and sent to the VFKPS for processing and matching.
- Video operation: takes video shots randomly or periodically and sends them for continuous processing and matching.

*c) Violation:* occurs when some rules are violated (i.e. not followed), either by the system or the examinee. This case, the exam saves its status, pauses and a procedure is followed for troubleshooting to be resolve before the exam resumes.

- System violation: occurs when the keyboard, the mouse or the camera, for any reason, stops responding, is turned off or removed. Also, power off, internet disconnection and application and operating system errors are considered system violations. All these violations should be manipulated by the examination system. Considering that the examinee did not cause any of them, this will not be treated as cheating; hence, no penalty will be applied. Just the exam saves its state, pauses and notifies the technical support agent. When the violation reason is detected and resolved, the exam resumes. Restart and shutdown of either hardware or software are applicable and allowed to fix the problem. One point should be emphasized here that the previously answered questions cannot be reviewed after the system is back operational.
- Examinee violation: occurs when the examinee violates the exam instructions and directions and cheats or tries to cheat. Examples of cheating might be impersonation, getting assistance from others, access to exam resources or material, etc. The violations should be categorized and weighted, and the system will be programmed to calculate the cheating rate of an examinee based on these weights.

1. FPA violations: include (a) unmatched fingerprint with the stored one, and (b) the imprint has not been captured for a predefined period in questions that require a mouse.
2. KDA violations: such as (a) unmatched features of keystrokes with the stored ones, and (b) keystrokes absence for a predefined period in essay questions that require a keyboard.
3. Video violations: are not limited to (a) unmatched face and/or head, (b) specific parts of the body do not show for a predetermined number of tries, (c) suspicious actions and moves, such as looking around, sleeping, bending and focusing on out-of-site objects, and (d) producing noise, speech or voice, etc.

Finally, on each violation, the system generates a relevant warning message that appears on the examinee's screen, and the cheating indicator increases based on each violation's weight. A specific rate, if exceeded, terminates the exam with a zero total grade.

*d) Termination:* in this phase, the examination session actually terminates, either normally or abnormally.

- Normal termination: this occurs either when the exam's time is over, or when an examinee submits all questions and finishes. In both cases, the system saves the session status report and recording. This report includes all violations and the cheating rate. Finally, the system unlocks the full screen and turns off all hardware devices used for authentication.
- Abnormal (cheating) termination: as discussed previously, each time a student commits a violation, it is evaluated and its rate appears to the examinee on his cheating indicator bar. When this rate exceeds a specific limit, say 50%, the exam automatically terminates with a zero total grade. In fact, this rate or action depends on the institution's rules. Some institutions might allow him to complete the exam, and the cheating indicator still tracks his violations. After it is finished, a suitable penalty is applied. However, after this abnormal termination, the same procedure as in (a) is followed.

*3) After e-Examination*

After an exam terminates, a session report is generated. Also, session recording is stopped and saved. Then the exam is corrected, where auto-correctable questions (e.g. multiple-choice and matching) are corrected, otherwise, they are sent to the instructor to be corrected manually. The total grade is then recalculated by adding the grades of all questions. Then, a penalty is applied on the total based on the cheating indicator's rate extracted from the generated session report. For instance, the penalty of cheating rate 50% and more can be a total of zero in the exam. Otherwise, an equation can be set according to each institution's rules and standards.

Finally, in case of uncertainty, a monitoring specialist is notified and given access to the recorded session of that examinee and relevant data. He revises the session, evaluates cheating rate and submits his report, which is taken into account in recalculating the examinee's final grade.

## V. Evaluation of the Proposed Model

The proposed model is an emerging theoretical one that could be implemented in the near future. Its evaluation criteria will be based on comparison with the previous schemes of e-assessment authentication in terms of security, efficiency and applicability. Compared with the mentioned e-assessment authentication schemes and the ISEEU model, the proposed model solves all types of impersonation threats A, B and C. Moreover, it supports the C-I-A goals and satisfies the P-I-A goals of continuous authentication i.e. presence, identity and authentication.

Although it has many features and solutions to many security issues applicable in e-assessment, the proposed model has some limitations or challenges. But who keeps track with researches related to advancement and enhancement of information and communication technologies, discovers that this model could be implemented and developed very soon. Subsections A and B explore the features and challenges of the model respectively.

### *A. Features*

After the presented description of the proposed model, it has been shown that it provides many features and advantages that have not been shown in the previous models, or shown but not sufficiently efficient. These features include but not limited to:

*1) Fully automated:* a proctor is no longer needed, even the penalties of cheating are automatically applied.

*2) Fully secure:* it solves all impersonation threats, satisfies C-I-A goals, and compatible with P-I-A goals. Also, the cheating indicator gives implication of close monitoring, full screen lock prevents access to exam resources, and video monitoring prevents access to other resources; including getting assistance from others.

*3) Highly efficient:* a virtual session but efficient as a real one in conducting cheating-free e-exams.

*4) Reliable and redundant:* three schemes cooperate together, if one fails another passes. They fulfill the required objective of e-assessment authentication.

*5) Reasonable and relatively inexpensive:* especially, it substitutes proctors who are paid for monitoring.

### *B. Challenges*

With the above features, any system is faced with some obstacles or challenges that should be resolved technically or procedurally to obtain the optimal security and performance. Some of these challenges are listed below:

*1) Video processing and feature extraction:* still need to be enhanced for better accuracy in feature extraction and matching.

*2) Internet speed and robustness:* this model requires high-speed and stable internet connection, especially at the peak times. This challenge is going to be solved day by day.

*3) Performance and capacity:* it requires high specification for the VFKPS server in terms of processor speed and disk space.

*4) Implementation complexity:* automatic video processing and feature extraction still complex to be implemented, and researches are thoroughly conducted to overcome this issue. Moreover, its users require special-purpose hardware. Hence, it is hard to be implemented nowadays.

*5) Failure penalties:* in failures such as internet disconnection or power failures which are highly probable in many countries, the answered questions cannot be reviewed for security purposes.

## VI. CONCLUSION

An emerging theoretical model has been presented for future implementation. It benefits from the strengths of three schemes of e-assessment security management and excludes the weaknesses. The result is a robust, reliable and secure model for continuous and random authentication. Although proposed for e-assessment authentication in this paper, the proposed model can be implemented in many systems to access sensitive data, such as e-banking, e-commerce, e-government, etc.

This model extremely depends on a psychological factor that assists in preventing an examinee from cheating. It provides an interactive virtual examination environment that keeps track with examinees in any action, motion, or even a whisper. Throughout the exam period, he feels of a close monitoring system, which indicates any violation on his screen and deducts from his grade for each cheating trial. Hence, he never tries to cheat even when he is alone at home.

Automation is an important feature offered by the model, which resolves type A impersonation threats whatever the reason is. Moreover, this feature cancels the need for tens of paid proctors, which means a cost-effective model. Full security and redundancy appear when the three schemes support each other, especially if one fails. Although, each scheme alone is still vulnerable to attacks, they form together a reliable scheme. On the other hand, the main challenge is to provide efficient and accurate techniques for image/video processing and feature extraction, which are still under enhancement. These techniques also require high performance and a huge storage, which degrade at peak times. Another challenge is the penalty of device failure, which is still possible.

Finally, if the video processing part is alternatively replaced with image processing, in which random screen shots are captured randomly and matched with a still photo, the model will be simpler and more applicable to be implemented. But the compromise will be less accuracy and less reliability.

## REFERENCES


[1] M. Hentea, M. J. Shea, and L. Pennington, *A perspective on fulfilling the expectations of distance education*, Proceedings of the 4th Conf. on Info. Tech. Curriculum (CITC4), Indiana, USA, pp. 160–167, October 2003.

[2] K. Abouchedid, and G. M. Eid, *eLearning challenges in the Arab world: revelations from a case study profile*, Quality Assurance in Education, vol.12, no.1, pp.15-27, 2004.

[3] N. H. Mohd Alwi, and I.-S. Fan, M. D. Lytras et al. (Eds.), *Information security threats analysis for e-learning*, Tech. Enhanced Learning, Quality of Teaching and Edu. Reform, Proc. the 1st Int. Conf. TECH-EDUCATION, CCIS, vol. 73, Athens, Greece, pp. 285-291, May 2010.

[4] E. Flior, and K. Kowalski, *Continuous biometric user authentication in online examinations*, Seventh Int. Conf. on Information Technology: New Generations (ITNG), Las Vegas, NV, pp .488-492, April 2010.

[5] A. Marcus, J. Raul, R. Ramirez-Velarde, and J. Nolazco-Flores, *Addressing secure assessments for Internet based distance learning still an irresolvable issue*, 9th Latin-American Conf. of Educational Computing, Caracas, March 2008.

[6] S. Alotaibi, *Using biometrics authentication via fingerprint recognition in e-exams in e-learning environment*, The 4th Saudi International Conference, The University of Manchester, UK, July 2010.

[7] K. M. Apampa, Gary Wills, and David Argles, *User security issues in summative e-assessment security*, IJDS, vol. 1, no. 2, June 2010.

[8] E. Kritzinger, (Eds.) D. Kumar, and J. Turner, *Education for the 21st Century- Impact of ICT and Digital Resources*, Proc. of International Federation for Information, vol.210, pp.345-349, Springer 2006.

[9] Y. Sabbah, *An Interactive and Secure E-Examination Unit: A proposed model for proctoring online exams*, the 2011 RoEduNet Int. Conf.-Networking in Education and Research, Romania, Iasi, 23-25 June 2011.

[10] Y. Sabbah, Comprehensive Evaluation of e-learning at Al-Quds Open University, Internal Report, Al-Quds Open University, OL Center, May 2010.

[11] H. A. El-Ghareeb, *E-Learning and Management Information Systems, Universities Need Both*, E-learning Magazine, Sep 2009.

[12] R. Raitman, L. Ngo, and N. Augar, *Security in the Online eLearning Environment*, Proceedings of the 5th IEEE International Conf. on Advanced Learning Technologies (ICALT'05), Kaohsiung, Taiwan, pp.702-706, Jul 2005.

[13] W. Stallings, *Data and Computer Communications*, 8th Edition, Prentice Hall 2007.

[14] S. Banerjee, *Designing a Secure Model of an eLearning System- A UML-Based Approach*, IEEE Potentials Mag., vol.29, no.5, pp.22-27, Sep-Oct 2010.

[15] V. Ciriani, S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, *Combining Fragmentation and Encryption to Protect Privacy in Data Storage*, ACM TISSEC, vol.13, no.3, article 22, 33 pages, Jul 2010.

[16] E. R. Weippl, *In-depth tutorials: Security in e-Learning*, eLearn Magazine, vol.2005, no.3, Mar 2005.

[17] K. El-Khatib, L. Korba, Y. Xu, and G. Yee, *Privacy and Security in eLearning*, International Journal of Distance Education, vol.1, no.4, pp.1-19, 2003.

[18] J. F. Gonzalez, M. C. Rodriguez, M. L. Nistal, and L. A. Rifon, *Reverse OAuth: A Solution to Achieve Delegated Authorizations in Single Sign-On eLearning Systems*, Computers & Security, vol.28, no.8, pp.843-856, Nov 2009.

[19] A. Kapil and A. Garg, *Secure Web Access Model for Sensitive Data*, International Journal of Computer Science & Communication (IJCSC), vol.1, no.1, pp.13-16, Jan-Jun 2010.

[20] Y. Levy and M. Ramim, *A theoretical approach for biometrics authentication of e-exams*, Chais Conf. on Instructional Technologies Research, The Open University of Israel, Raanana, Israel, pp. 93-101, 2007.

[21] Y. Sabbah, *E-learning at Al-Quds Open University, Current Situation: A Case Study*, Journal of Excellence in e-Learning (IJEEL), vol.3, no.2, pp.1-16, Jun 2010.