Security of Online Examinations

Yousef W. Sabbah

Abstract Online-examination modeling has been advancing at a slow, thus steady pace. Such an endeavor is embedded in many of today's fast-paced educational institutions. So, the online examination (i.e. e-Examination) model demonstrated in this chapter proposes two major schemes that utilize the most up-to-date features of information and communication technology (ICT). We have integrated authentication methods into this model in the form of simulated and controlled, thus measurable enhancements. The new model complies with international examination standards and have been proved to be equally, if not more, immuned to its predecessor models, including classroom-based examination sessions. Therefore, it can be selected as a new model of examination to cut-down on the cost of exam administration and proctoring.

e-Examination systems are vulnerable to cyberattacks, leading to denial-of-service and/or unauthorized access to sensitive information. In order to prevent such attacks and impersonation threats, we have employed smart techniques of continuous authentication. Therefore, we propose two schemes; Interactive and Secure E-Examination Unit (ISEEU) which is based on video monitoring, and Smart Approach for Bimodal Biometrics Authentication in Home-exams (SABBAH) which implements bimodal biometrics and video-matching algorithms. Still, the model is scalable and upgradable to keep it open to smarter integration of state-of-the-art in the field of continuous authentication. For validation purposes, we have conducted a comprehensive risk analysis, and results show that our proposed model achieved higher scores than the previous ones.

1 Introduction

e-Learning utilizes Information and Communication Technology (ICT) to enhance the educational process. It is a modern model that provides an interactive-learning environment, which consists of tutors, students, contents, classrooms and the

Y.W. Sabbah (✉)
Faculty of Technology and Applied Sciences, Quality Assurance Department, Al-Quds Open University, Ramallah, Palestine
e-mail: ysabbah@qou.edu

I. Palomares et al. (eds.), *Data Analytics and Decision Support for Cybersecurity*, Data Analytics, DOI 10.1007/978-3-319-59439-2_6

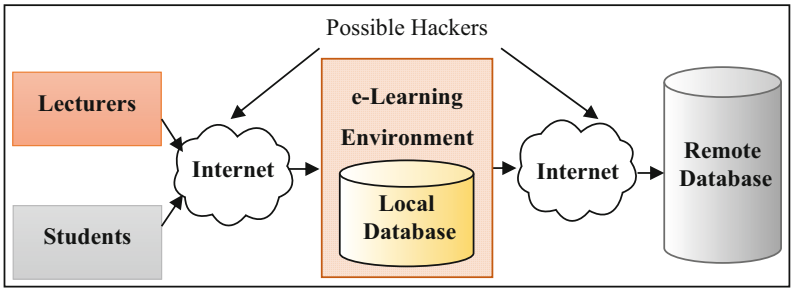

Fig. 1 Possible hackers in e-Learning environment [1] (Adapted)

educational process itself [1–8]. As depicted in Fig. 1, the Internet connects a learner with his lecturer and content regardless of place and time. Above and beyond, many academic institutions consider e-Learning a vital element of their information systems [1].

An e-Learning platform has different names, such as Learning and Course Management System (LCMS), Virtual Learning Environment (VLE), e-Learning Portal, etc. For instance, Moodle is a LCMS that supports social constructive pedagogy with interactive style. Interactive material includes Assignments, Choices, Journals, Lessons, Quizzes and Surveys [9]. Accordingly, we have implemented our proposed model based on Quiz module in Moodle.

For better performance, an e-Learning platform should be integrated withuniversity management information system (UMIS). This integrated solution combines all relevant technologies in a single educational environment (i.e. an e-University) that provides students, instructors and faculties with all required services [10].

In this chapter, we propose an integrated e-learning solution that consists of main and complementary components, as shown in Fig. 2. The academic portal (AP), with single sign-on (SSO), represents the core of this solution, and the authoring tools are used to build its Content. The middle annulus represents the main components, which are classified, in the inner annulus, into three groups; e-Content, delivery and assessment. The outer annulus illustrates the complementary components that represent together a University Management Information System (UMIS). All components are interconnected and can exchange data through the AP.

At the beginning, e-Learning systems were treated as research projects that concentrate on functionalities and management tools rather than security [11]. Nowadays, these systems are operational and heavily used worldwide. In addition, possible hackers may be located in the connections between either users and the system or the system and remote database [1], as shown in Fig. 1. Therefore, e-Learning systems should be provided with sufficient security to ensure confidentiality, integrity, availability and high performance.

Moreover, e-Examination security occupies the highest priority in e-Learning solutions, since this module contains the most sensitive data. In addition, an

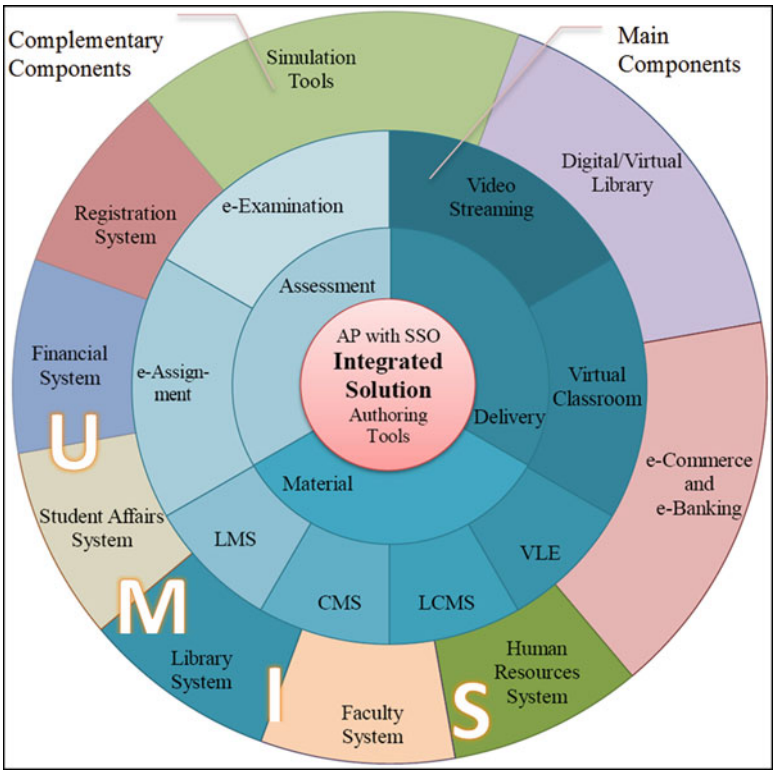

Fig. 2 A proposed integrated e-Learning solution; main and complementary components

efficient authentication method is required to make sure that the right student (e.g. examinee) is conducting an exam throughout the exam's period. The absence of trusted techniques for examinees' authentication is a vital obstacle facing e-Learning developers [12]. This is why opponents claim that e-Learning cannot provide a comprehensive learning environment, especially cheating-free online exams. Our contribution is to find a solution for this problem through a novel model for continuous authentication. This chapter introduces our proposed model in two schemes called ISEEU and SABBAH.

The chapter consists of four sections. The current section provides an overview of the main concepts of e-Learning and e-Examination systems and possible attacks that should be considered. The second section discusses the main security issues and authentication methods in e-Examination systems, as well as classification of the main existing authentication schemes. The third section describes our proposed continuous-authentication schemes. It provides a proposed implementation environment and settings and a comprehensive analysis, design and implementation of the schemes. Finally, the fourth section provides a comprehensive risk-analysis and evaluation to compare the suggested schemes with their predecessors, a full discussion of the results and conclusion, as well as challenges and future work.

2 e-Examination Security

Computer security is defined, in the NIST Handbook, as [13]:

> The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of its resources.

Computer and network security is a collection of tools and measures, which protect data that is stored in or exchanged among computers within a network [14]. Despite the major advancement introduced in system security in the last decade, many information systems fall victims to various cyberattacks worldwide [15, 16]. Information security is a serious issue and a fundamental requirement in e-Examination systems, since they add new threats and risks compared to other web-applications [7, 17–20]. In this context, security is discussed from two viewpoints; end-users (e.g. authors, teachers and students) and security functions (e.g. protecting content, personal security, access control, authentication and cryptography) [11]. Moreover, privacy issues should be investigated [19].

This section consists of three subsections. The first discusses the main e-Examination-security concepts that can assist in understanding the new features of our proposed authentication schemes. The second introduces the authentication methods that can be used in e-Examination. The last subsection describes the five existing authentication schemes that have been proposed in the previous studies.

2.1 e-Examination Security Concepts

This subsection aims at introducing the main e-Examination security concepts. We present security countermeasures and controls, C-I-A vs. P-I-A security goals, the need for continuous authentication and the impersonation threat types.

2.1.1 Security Countermeasures

Technical countermeasures and procedural requirements should be applied in e-Examination to ensure that lecturers, students and data are well-protected against possible risks [1, 21].

In general, *four technical security-countermeasures are used to measure security of e-Examination systems* or any computer system; confidentiality, integrity, availability and authenticity [1, 5, 14, 19, 22]. Regarding *procedural security-countermeasures, four essential requirements should be enforced*; security governance, security policy, security risk-management plan, and security-measures monitoring [1].

2.1.2 Security Controls

The following security controls are essential to protect e-Learning, thus e-Examination systems [1, 2, 14, 20, 23]:

- Access Control: Only the authorized entities can access a system.
- Encryption: Protection of private data against disclosure using cryptography.
- Firewalls: Filtering data exchanged between internal and external networks.
- Intrusion Detection: detection of attack attempts and alarm generation.
- Protection against Viruses and Spyware.
- Digital Signature: Ensuring that the received content is from a specific user.
- Digital Certificate: Verifying whether the transmitted digital content is genuine.
- Content Filter: Prevention of authorized entities from posting undesired content.

2.1.3 The Need for Continuous Authentication

More caution should be taken in online examination, where e-Examination systems should verify an examinee is the actual student [3, 21, 24–28]. Therefore, continuous and/or random authentication is required [21, 24, 25, 27, 28]. Confidentiality, integrity and availability (C-I-A) security goals can protect any system's hardware, software and data-assets against potential threats such as interception, modification, interruption and fabrication [25]. If the C-I-A goals are compromised, the critical assets will be compromised.

Apampa [25, 29] proposed that C-I-A security goals are unsuitable to protect all e-Examination assets, especially human assets (e.g. students, teachers and system administrators), since they have unpredictable attributes. For instance, the people who maintain the e-Examination system (i.e. system administrators) are valuable assets that do not depend on C-I-A goals; instead they should satisfy other goals. Students represent another example of such assets. To overcome this issue, Apampa [25, 29] proposed three new goals; Presence-Identity-Authentication (P-I-A), as indicated in Fig. 3 and defined below [25, 28]:

- *Presence* and continuously *authenticated presence*, which specifies a student's place.
- *Identity*, which differentiates a student from another.
- *Authentication*, which proves student's claimed identity.

2.1.4 Impersonation Threats

One reason for unsuccessful e-Learning is the lack of completely trustable, secured, protected and cheating-free e-Examination [3, 21, 24–28]. Many studies report that cheating is common in education [30–32]. Others report that around 70% of American high-school students conduct cheating in at least one exam, where 95% are never caught [33]. In addition, twelve studies report an average of 75% of

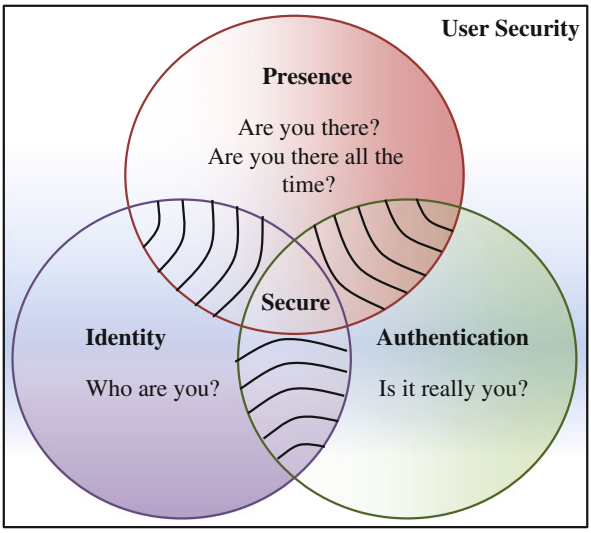

Fig. 3 Presence-Identity-Authentication (P-I-A) goals [25]

college students cheat [12, 30, 32]. The situation is worse in online exams, where 73.6% of examinees say that cheating is easier and can never be detected [25]. Impersonation is one of cheating-actions that should be prevented or at least detected in e-Examination systems.

Impersonation threats in e-Examination are categorized into three types [25]; Type A, Type B and Type C. Unfortunately, these types alone cannot assure cheating-free e-Exam sessions. Therefore, we proposed a Type D impersonation threat. These types are defined as follows:

1. *Type A* (Connived impersonation threat) supposes that a proctor is necessary. Impersonation might occur in two cases: the proctor could not detect it, or he allowed impersonation by force, sympathy, or for monetary purposes.
2. *Type B* occurs when a student passes his security information to a fraudulent who answers the exam. Username-Password pairs, fall in this type. However, strength of authentication method and existence of a proctor reduce this threat.
3. *Type C* occurs when the real student just login, letting a fraudulent to continue the exam on his behalf. Non-shareable attributes using biometrics approaches, such as fingerprint authentication fall in this greater security-challenging threat.
4. *Type D* might occur such that the real examinee is taking the exam, but another person assists him for correct answers.

2.2 Authentication Methods in e-Examination

Several authentication methods are proposed in e-Examination and similar web applications. These methods can be classified into three factors [24].

2.2.1 Knowledge Factors

These factors require a user to know something unique (e.g. a password) that others do not know. With a strong password policy, unauthorized parties cannot access users' information.

2.2.2 Ownership Factors

A user should possess some token that others do not have, such as keys or cards. Unauthorized parties cannot access users' information unless they obtain the required tokens.

2.2.3 Inherence Factors

Referred to as biometrics authentication approaches. They are categorized into two main methods [24]:

- Something a user is: This method utilizes image processing and pattern recognition, e.g. fingerprint, voiceprint, face recognition and retinal pattern.
- Something a user does: the most efficient for continuous user authentication in e-Examination, such as handwriting, keystroke dynamics and mouse dynamics.

Although some of the mentioned authentication methods are highly reliable, they have some drawbacks when used in e-Examination, as summarized in Table 1.

Inherence factors (e.g. biometrics authentication approaches) represent the most powerful approaches of authentication, since they are very hard to be fabricated. Therefore, these approaches are used in e-Examination schemes, as will be discussed in Sect. 2.3. We focus on three approaches, since they are used in our e-Examination model.

Table 1 Drawbacks of user authentication methods in e-Assessment (Extracted from [24])

Authentication method	Drawbacks
Knowledge factors	1. If the password is given away, the security policy will be cancelled 2. A password is requested once at login. They are never trusted for continuous authentication
Ownership factors	1. If the token is passed to others, the scheme is circumvented 2. A token is requested once at login. They cannot be trusted for continuous authentication
Inherence factors	1. They are more reliable, but require special hardware 2. They are unreasonably intrusive, expensive and difficult to implement 3. Some approaches repeat authentication continuously, but they are not fully trusted 4. They are never trusted in case of getting assistance from others

2.2.4 Fingerprint Authentication (FPA)

Fingerprint authentication (FPA) is implemented in many web applications. For instance, it is implemented for user authentication in e-Examination [12, 24, 34]. Nowadays, fingerprint is commonly used for user login, and manufacturers produced a fingerprint mouse, such that a finger scanner is compacted under the thumb for continuous authentication. In addition, reliable fingerprint servers are available with false reject rate (FRR) of 0.01% [5]. The main steps of fingerprint biometrics authentication proceed as follows [34]:

- Creating user-ID, scanning each user's thumb and storing it in a secure server.
- Log in using user-ID and fingerprint via a scanner device when prompted.
- The device will be disabled and the user will be able to access sensitive data.

Two metrics of security level are defined for fingerprint, as shown in Eqs. (1) and (2) [35]:

$$FAR = \frac{IFA}{TNIT} \tag{1}$$

$$FRR = \frac{CFR}{TNCT} \tag{2}$$

Where, *FAR* is the false acceptance rate, *IFA* is the ratio of impostors that were falsely accepted, *TNIT* is the total number of tested impostors, *FRR* is the false rejection rate, *CFR* is the ratio of clients that are falsely rejected, and *TNCT* is the total number of tested clients. *FAR* measures the probability that an impostor is falsely accepted, whereas *FRR* measures the probability that a valid user is rejected.

2.2.5 Keystroke Dynamics Authentication (KDA)

KDA proposes that typing rhythm is different from a user to another. It was proposed with five metrics of user identity verification [24]:

- Typing speed, measured in characters per minute.
- Flight-time between two keys up, including the time a user holds on a key.
- Keystroke seek-time that is required to seek for a key before pressing it.
- Characteristic sequences of keystrokes, i.e. frequently typed sequences of keys.
- Characteristic errors, i.e. the common errors made by a user to be identified.

Correlation is used to measure similarity among the features of the saved templates and the stroked keys, as shown in Eq. (3) [24].

$$r = \sum\nolimits_{i=1}^{n} (k_i * t_i) \Big/ \sqrt{\sum_{i=1}^{n} k_i^2 * \sum\nolimits_{i=1}^{n} t_i^2} \tag{3}$$

Where, r is the correlation, k is a vector of length n which stores flight-time of the template, t is a vector of length n which stores flight-time of the captured keys, and $i \in k$, t is the flight-time between two keystrokes.

2.2.6 Video Matching Algorithm

This algorithm is proposed originally for video search [36–38], but it can be used for continuous authentication and auto-detection of cheating actions. The examinee's video is matched against his stored template using tree-matching, as shown in Fig. 4. A video is divided into a number of scenes in a structured-tree; each consists of groups of relevant shots. The matching process moves level-by-level in a top-down manner, where similarity is calculated using color histogram and shot style. The algorithm uses a maximum order sum function to compute similarity in four steps [36]:

- Initialize a matrix D with zeros for all elements.
- Fill the matrix according to Eq. (4).

$$D(i+1, j+1) = \max\left(D(i,j), childSim(i,j), D(i,j+1)\right) \tag{4}$$

Where, D is the matrix, *max()* is the maximum function, and *childSim()* is the child similarity function.

- Locate the sum of child similarity for the optimal match by Eq. (5).

$$sum = D(numRow + 1, numCol + 1) \tag{5}$$

Where, *sum* is the sum of child similarity, *numRow* is the number of rows, and *numCol* is the number of columns.

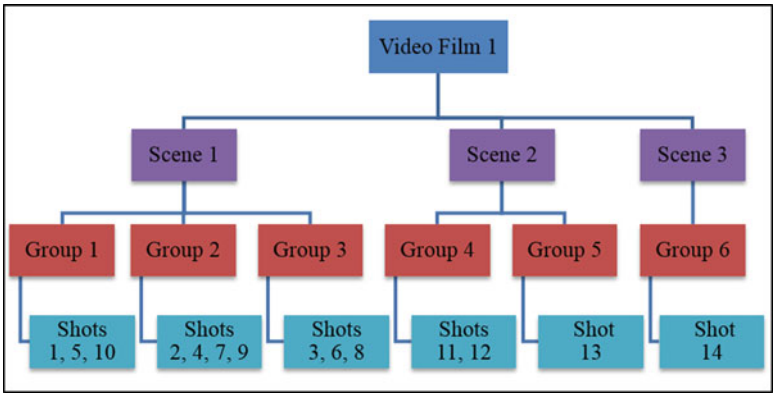

Fig. 4 Structured video tree [36]

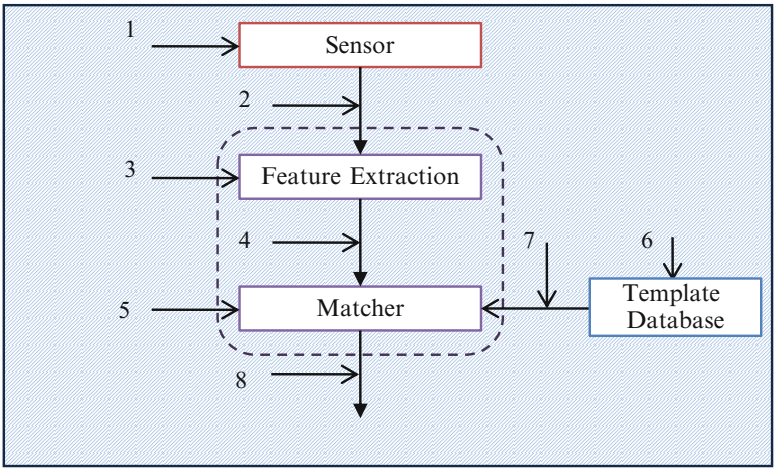

Fig. 5 Attack points in biometrics authentication systems [28]

- Normalize the sum, as shown in Eq. (6).

$$FeatureSimilarity = \left(\frac{sum}{numRow} + \frac{sum}{numCol}\right)/2 \tag{6}$$

Where, *FeatureSimilarity* is the feature similarity of the current level, *sum* is the sum of child similarity, *numRow* is the number of rows, and *numCol* is the number of columns.

Although biometrics authentication methods are the most efficient ones, still they are vulnerable to cyberattacks. Figure 5 depicts eight points of possible attacks as a result of one or more of the following four risks [28]:

- *Fake input* using either artificial or dummy fingers on the sensor.
- *Low-quality input/imprint* that makes it difficult to extract the minutiae points accurately.
- *Biometric-database modification* including features of fingerprint templates stored on enrollment for the first time.
- *Feature-extractor modification* that might result from attacks leading to incorrect rejection/acceptance of fingerprints.

2.3 Existing e-Examination Authentication Schemes

Existing solutions for e-Examination authentication are categorized into five main categories [25]. The same categorization will be adopted in Sect. 4 to conduct a comparison between these schemes and ours.

2.3.1 Proctored-Only Scheme

This approach requires a proctor or a testing administrator to monitor the exam-takers during their examinations. A case study was conducted in which 200 students set for e-Exam in a computer laboratory using WebCT [39]. Three adjacent laboratories were dedicated with three proctors concurrently. A WebCT expert circulated between labs for technical support. Authentication was easy since the proctors were the tutors of the course who knew their students very well. Login ID and password were kept with proctors who distributed them during each session.

Another supporter to this scheme raised three serious problems in e-Assessment [30]; taking assessment answers in advance, unfair retaking of assessments, and unauthorized help. One important caution to reduce the first problem is random selection of the questions for each student out of a large pool, as in Eq. (7) [30].

$$P = \frac{M^2}{N^2} \tag{7}$$

Where, P is the expected overlap between questions in two random exam sets, M is the exam size (i.e. number of questions), and N is the pool size (i.e. number of questions in the pool). In other words, to raise the probability of choosing a distinct set of questions for each student, at least, Eq. (8) should be satisfied [30].

$$N = S * M \tag{8}$$

Where, N is the pool size, S is the number of students to set for the exam, and M is the exam size. Proponents of this scheme consider proctor-based e-Assessment suitable, since it promotes identity and academic honesty [18, 30, 39].

2.3.2 Unimodal Biometrics Scheme

This scheme employs a single biometrics approach for authentication. For example, web authentication, based on face recognition, is used for the verification of student identity with BioTracker that can track students while doing their exams at home. BioTracker can be integrated with LMS, where three concepts are investigated; non-collaborative verification, collaborative verification and biometrics traces [40].

Handwriting approach is another example of this scheme, where a pen tablet is used for writing the most used characters in multiple-choice questions [41]. The written characters are compared with templates that have been taken before the exam [41]. Figure 6 depicts the structure of another similar approach that employs Localized Arc Pattern (LAP) method [41]. It identifies a writer based on one letter written on a piece of paper. It is adapted for multiple-choice e-Exams to recognize an examinee by his handwritten letters [41].

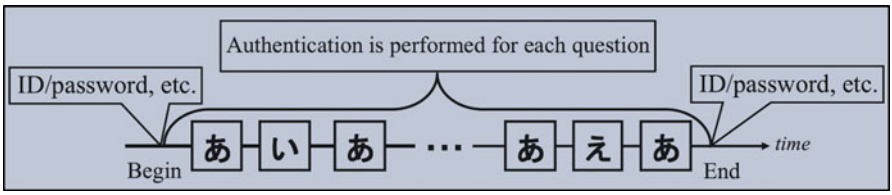

Fig. 6 Handwriting authentication using LAP [41]

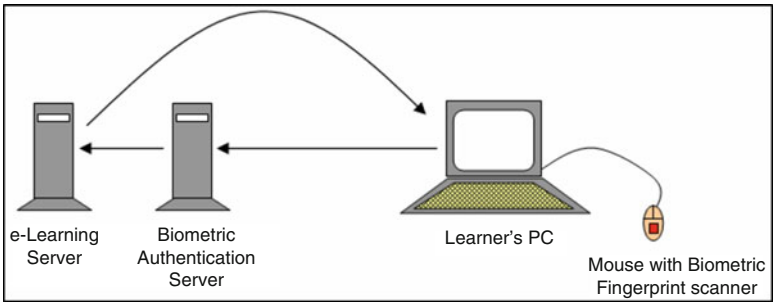

Fig. 7 Fingerprint for e-Exam user's authentication [12]

Another example takes multiple random fingerprints of the examinee throughout the e-Examination period, as shown in Fig. 7. It prevents plagiarism (i.e. pretending to be another examinee) [12, 28].

2.3.3 Bimodal Biometrics Schemes

In order to achieve better security in e-Examination, multiple biometrics approaches can provide reliable user authentication during the exam rather than instantaneous login. For instance, fingerprint is combined with mouse dynamics, where fingerprint is used for login, while mouse dynamics is used for continuous authentication during the exam, as shown in Fig. 8 [42]. Mouse dynamics approach extracts some features from mouse actions that vary from a user to another. This includes motion, click and double-click speed [42].

Fingerprint with head-geometry detection represents another combination, where a webcam captures the pictures of examinees during an e-Exam, and feature extraction and matching with the stored templates are performed [25, 43]. Its structure consists of three modules, as depicted in Fig. 9; (re)authentication ensures the examinee correctness, tracking determines an examinee's position and location, and classifier utilizes the information generated by the tracker to provide risk levels.

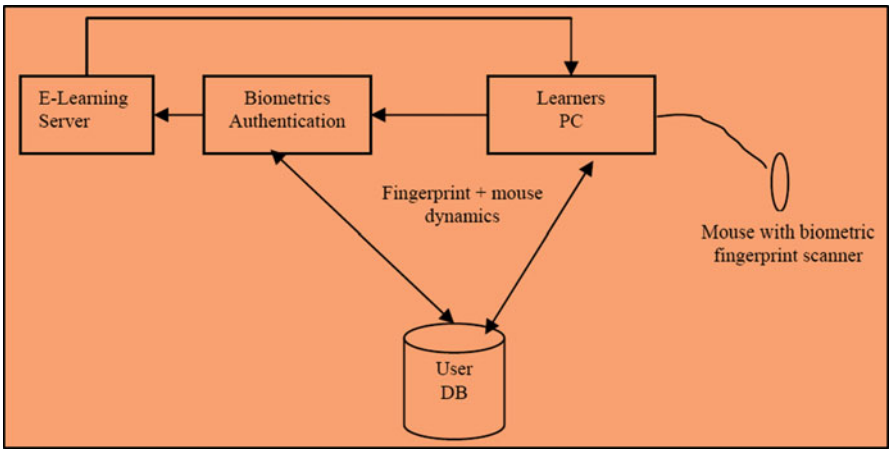

Fig. 8 Bimodal biometrics approach using fingerprint and mouse dynamics [42]

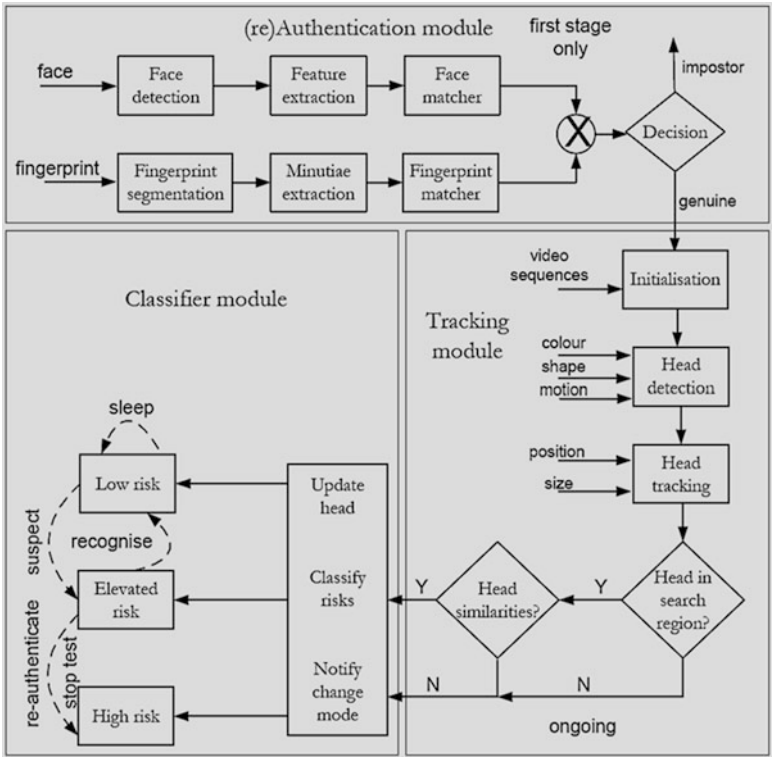

Fig. 9 A bimodal biometrics scheme (e-Assessment security architecture) [25]

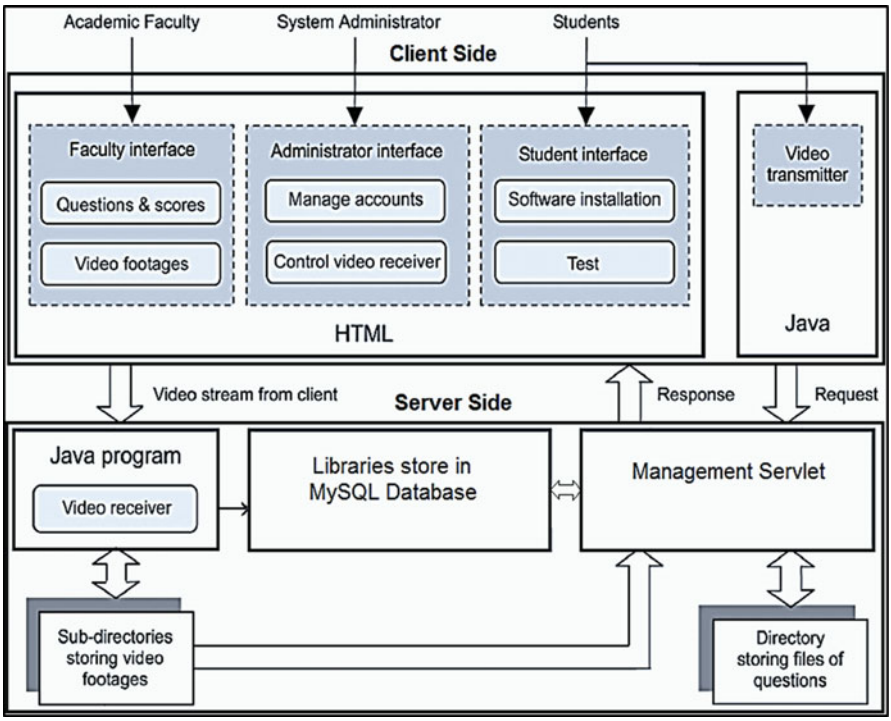

Fig. 10 Structure of e-Test scheme [44] (Adapted)

2.3.4 Video Monitoring

Video monitoring of student activities during examination are also applied in e-Examination using a webcam [44]. Figure 10 shows e-Test scheme's structure, which requires a password for login, and random or periodic video footages are captured during the exam to be revised by the proctor after finishing. It provides three main interfaces: administrator interface (manages user accounts and video receiver), faculty interface (uploads exams, shows results and views the captured footages) and student interface [44]. Unfortunately, this scheme needs extra efforts to watch video footages.

2.3.5 Biometrics Authentication and Webcam Monitoring

This scheme combines fingerprint and real-time video-monitoring, as illustrated in Fig. 11 [35]. When connection to the server is established, the examinee is asked to scan his fingerprint. If it matches the stored one, he can continue. When an exam starts, the webcam streams video to the server to monitor the exam-taker. On mismatch, the exam is interrupted and processed as it is.

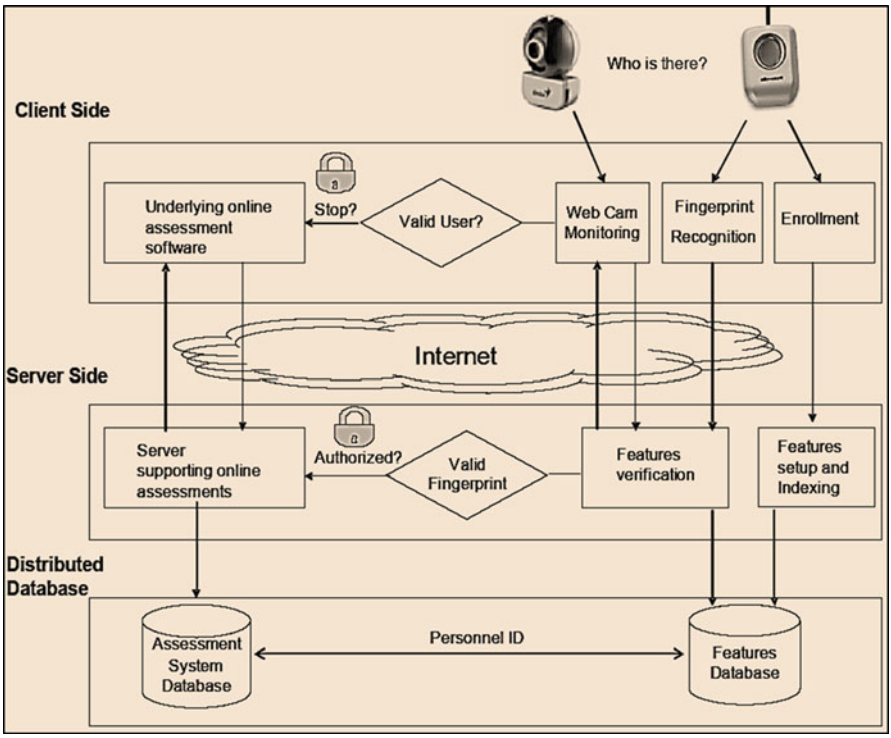

Fig. 11 Structure of combined fingerprint and video-monitoring in e-Examination [35]

3 The Proposed e-Examination Model

Our proposed e-Examination schemes are implemented as modules within a LCMS (i.e. Moodle). In order to achieve the desired security level, the whole environment should be secured. For instance, hardware, software, network infrastructure, operating system, e-Learning system, e-Examination system and other valuable assets in educational institutions should be protected against possible attacks.

This section describes the proposed e-Examination model in three subsections. The first presents the proposed model's requirements, while the second and the third provide full description of the proposed model (i.e. ISEEU and SABBAH schemes respectively and their system-development life-cycle including analysis, design, and implementation).

3.1 The Proposed-Model's Requirements

In this subsection we provide the main requirements of our proposed e-Examination model, which includes a proposed implementation environment, hardware and software requirements, a state diagram and a cheating-action list.

3.1.1 A Proposed Implementation-Environment

We propose a perfect implementation environment which meets our proposed e-examination model requirements, as shown in Fig. 12.

The workflow of the proposed environment can be summarized in seven main steps; *Admission, Registration* (enrollment), *Tuition payment* through a secure banking link to the financial system (FS), *Employment of staff members* through the HR system (HRS), *Scheduling and distribution of courses* on faculty members

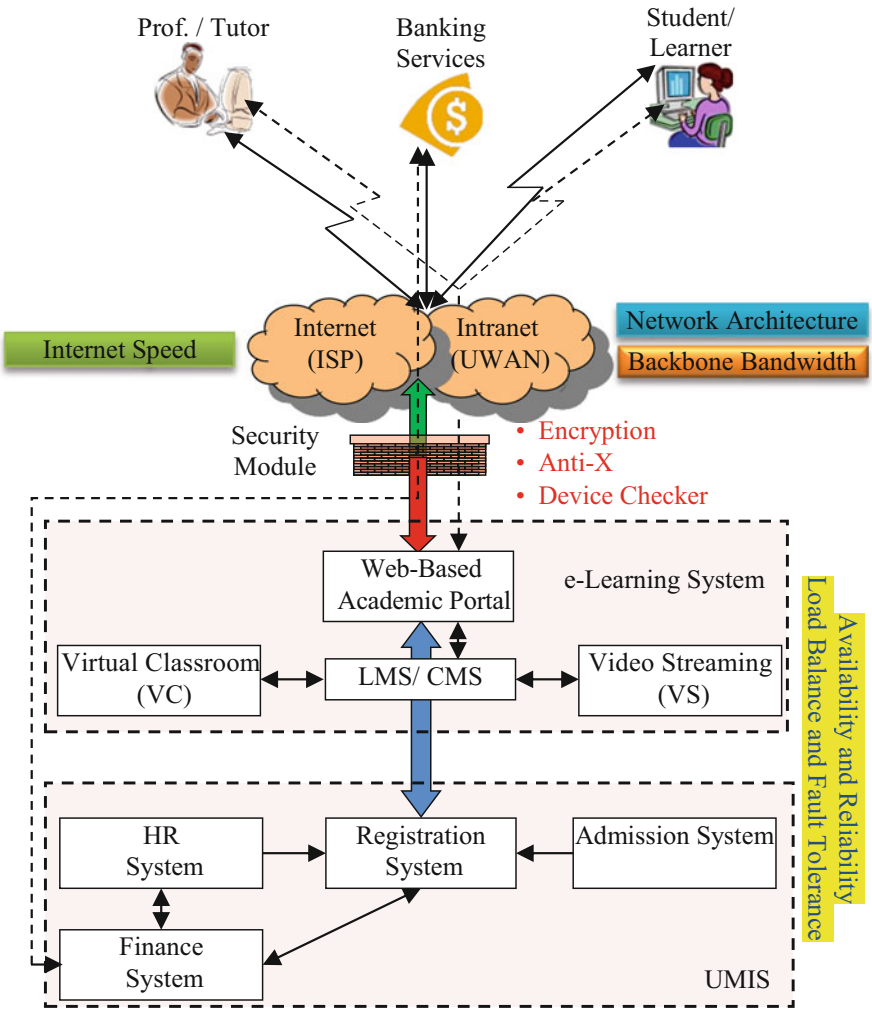

Fig. 12 Structure of the proposed implementation environment

and student access to e-Learning services, *Examination* where e-Exams are auto-corrected and scores are transferred to the registration system, and finally *Salary payment* through a payroll module of the FS and slip delivery.

3.1.2 A Proposed Security Module

The AP and other web applications can be reached via the Internet or the Intranet through a security module shown in Fig. 13. It protects the proposed e-Examination schemes against several vulnerabilities:

1. *Encryption:* Secure Socket Layer/Transport Layer Security (SSL/TLS) protocol is employed to encrypt the data stream between the web-server and the browser.
2. *Firewall/Access Control Lists (ACL):* It blocks unauthorized parties from access to the e-Examination system and prevents any possible connection to assistants.
3. *Cross-Site Scripting (XSS) Detector:* A web vulnerability scanner that indicates vulnerable URLs/scripts and suggests remediation techniques to be fixed easily.
4. *SQL injection Detector:* A web vulnerability scanner that detects SQL injection.
5. *Anti-X (X = Virus, Worm, Spyware, Spam, Malware and bad content):* A reliable firewall/anti-X is installed, and black lists of incoming/outgoing traffic are defined. These lists and definitions of viruses and spyware are kept up-to-date.
6. *Device checker and data collector:* Checks that the authentication devices are functioning properly, and ensures that only one of each is installed, by testing interrupt requests (IRQ) and address space. It collects data about current user and detects violations and exceptions and issues alerts to the e-Examination system.

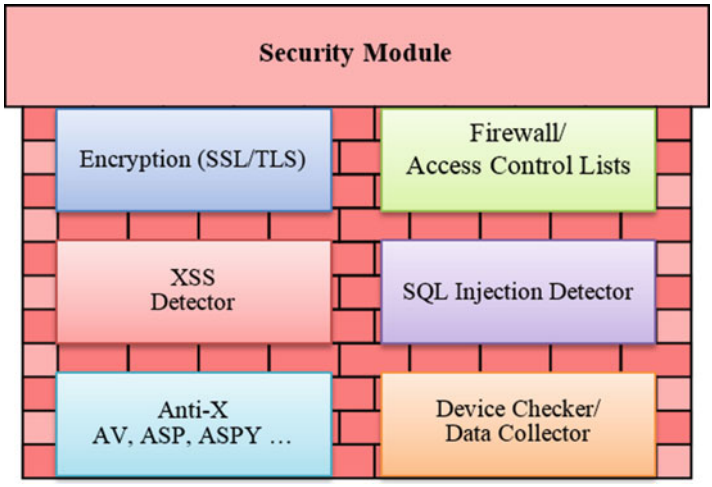

Fig. 13 A proposed security-module

3.1.3 Hardware and Software Requirements

The hardware and software required by the entire integrated e-Learning solution (i.e. the implementation environment) refer specifically to those required to develop the e-Examination scheme. Tables 2 and 3 illustrate hardware and software requirements in both server and client sides

Table 2 Recommended hardware requirements of the proposed schemes

Side	Hardware requirement	Proposed scheme	
		ISEEU	SABBAH
Server-side	1. Media server (MS) with moderate specs	☒	☐
	2. e-Learning server (ELS) with ordinary specifications	☐	☒
	3. Mobile phone module (MPM), e.g. video modem	☒	☐
	4. A video/ fingerprint/ keystroke processing server (VFKPS)	☒	☒
Client-side	1. A personal computer (PC) or a laptop with ordinary specs	☒	☐
	2. 1 Mbps internet connection	☒	☒
	3. A webcam with reasonable resolution	☒	☒
	4. A microphone and a speaker or headphones	☒	☒
	5. A mobile unit (MU) with a camera attached	☐	☐
	6. A biometrics authentication fingerprint-mouse	☐	☒

Table 3 Recommended software requirements for the proposed schemes

Side	Software requirement	Proposed scheme	
		ISEEU	SABBAH
Server-side	1. Windows Server 2008 or RedHat Linux Enterprise RHLE 5.6 or later	☒	☒
	2. Wowza server version 3.0 or later	☒	☒
	3. Moodle server 2.0 or later	☒	☒
	4. PHP 5.3.2 or later, MySQL 5.0.25 or later and Apache web server	☒	☒
	5. The corresponding e-Examination model and security modules	☒	☒
	6. Continuous video matching and fingerprint and keystroke APIs	☐	☒
Client-side	1. Microsoft Windows XP or later	☒	☒
	2. Web browser (e.g. Google Chrome or Internet Explorer 6.0 or later)	☒	☒
	3. Adobe flash media live encoder 3.2 and flash player 10 or later	☒	☒
	4. Continuous fingerprint, keystroke dynamics and video matching APIs	☐	☒

Server Side

Regarding hardware, our proposed e-Examination scheme requires an *e-Learning server (ELS)* and *a media server (MS)* with *sufficient specs* based on the number of expected users. Note that SABBAH scheme requires a *VFKPS server with high storage, memory and processing power*.

Regarding software, a *server operating system*, and *a streaming server* are required. Also, the e-Examination schemes are installed as modules over *Moodle 2.0 server* with suitable *application programming interfaces (APIs)*.

Client Side

Hardware requirements for both ISEEU and SABBAH schemes are; *a personal computer* connected to *1 Mbps or more Internet speed*, a *webcam* with reasonable resolution and *headphones*. Also, software requirements include; *an operating system, a web browser, a media encoder* and *a flash player* plugins. Additionally, SABBAH requires *a biometrics mouse* with continuous fingerprint-scanner and its *suitable APIs*.

3.1.4 A Proposed State Diagram

In traditional exams, proctors control and manage exam sessions. They distribute exam papers, announce the start and termination times, monitor and terminate exams or report cheating actions and violations. Similarly, in our proposed schemes, a proctor or the system itself should manage the exam sessions using a state diagram with four possible states (2-bits) with an initial Null state, as shown in Fig. 14.

Transition of the states goes into eight steps throughout an e-Exam for both of our proposed schemes, except that SABBAH replaces *Proctor* with *VFKPS*, as follows:

1. *Null-Ready*: before starting an e-Exam, its state is *Null*, where all records, including number of attempts, are null. When the examinee opens quiz block in Moodle, he is asked to submit his ID, while the "Attempt now" button is dimmed. At this point, the exam state changes to *Ready '00'* and the proctor is notified.
2. *Ready-Start*: if the proctor validates the examinee's identity, he clicks "Accept" in his control toolbox to cause a transition from *Ready* to *Start '01'*. At this point, the "Attempt now" button is enabled, and the examinee is notified to start.
3. *Ready-Null*: if the proctor suspects an examinee is not the correct one, he clicks "Reject", causing a transition from *Ready* to *Null*. So, the examinee should retry.
4. *Start-Pause*: on exceptions, such as webcam removal, the exam is paused for exception handling, and its state is changed from *Start '01'* to *Pause '10'*.

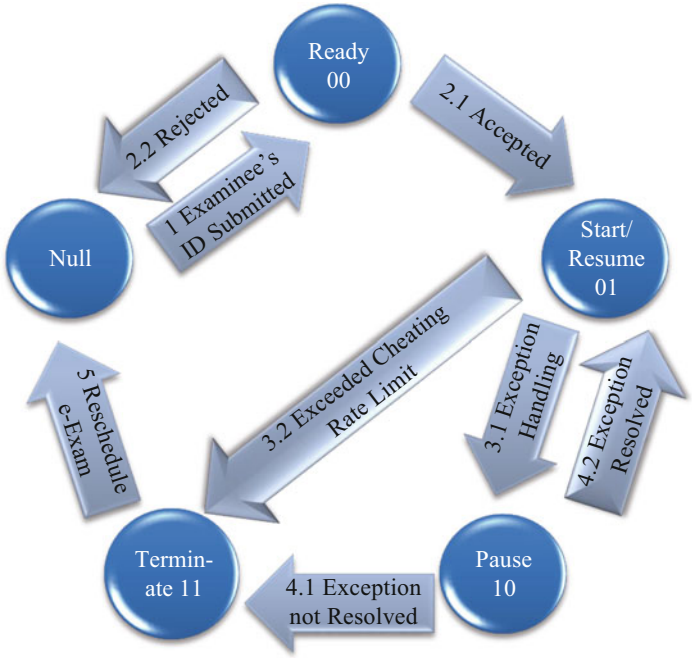

Fig. 14 State diagram of the proposed e-Examination models (ISEEU and SABBAH)

5. *Start-Terminate*: if a violation limit is exceeded, the exam terminates abnormally with a total score of 0, causing a transition from *Start '01'* to *Terminate '11'*. Termination also occurs if an examinee submits his exam or the time is over.
6. *Pause-Resume*: if an exception is handled, the state transits from *Pause '10'* back to *Resume '01'*, and an examinee can continue his e-Exam.
7. *Pause-Terminate:* if exception handling fails for a number of tries, a transition from *Pause '10'* to *Terminate '11'* terminates and reschedules the e-Exam.
8. *Terminate-Null*: if an e-Exam is rescheduled for any reason, its state transits from *Terminate '11'* to *Null*. This deletes all the records of that examinee as if he has not yet conducted his exam. He can re-attempt the exam accordingly.

3.1.5 A Proposed Cheating Action List

In our schemes, we propose a list of cheating actions to measure violation rate and decide penalties, such as deduction from the total score, as illustrated in Table 4.

We conducted a survey with a sample of 50 experts of security, proctoring and education. Each expert was asked to assign a weight of 1–5 to each violation, where violations with higher risks are assigned higher weights. Then, the weights are averaged, approximated and normalized to obtain the final weights of risks.

Table 4 The most popular cheating actions with average risks

No.	Violation/cheating action	Average risk (des. order)
1	Someone else replaced him	0.40
2	Someone else (assistant) is sitting beside him	0.35
3	Redirecting the webcam or disabling it	0.30
4	Incoming/Outgoing calls (Mobile or Telephone)	0.25
5	Send/Receive messages (SMS, MMS, etc.)	0.20
6	Using PDAs (Calculator, iPhone, Android, etc.)	0.20
7	Looking at a textbook or a cheat sheet	0.20
8	Talking with someone	0.10
9	Looking around	0.10
10	Hiding face with hand or another object, or by sleeping on desk	0.10

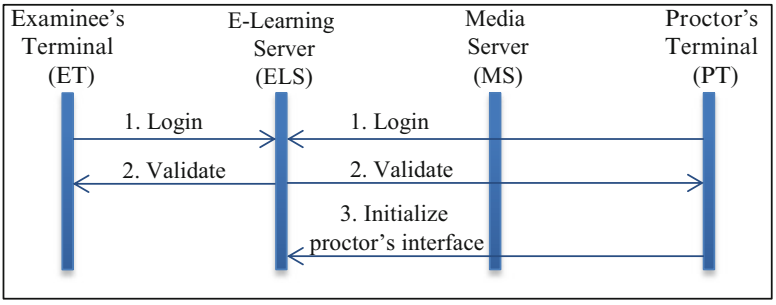

Fig. 15 Pre-operation of ISEEU

3.2 Interactive and Secure e-Examination Unit (ISEEU)

Interactive and Secure e-Examination Unit (ISEEU) is implemented on Moodle using PHP, MySQL, HTML, AJAX, and other scripting languages. A media server is also used for streaming exam sessions to the corresponding proctor and for recording. ISEEU provides online e-Exams with new features such as interaction between proctors and examinees, and minimizing cheating including access to resources and impersonation threats. ISEEU is one of the simplest and the most efficient approaches of e-Exam authentication. An examinee himself, rather than one or part of his organs, is identified continuously throughout his e-Exam. Security and reliability wise, it can be more efficient than in-classroom sessions.

Pre-Operation of ISEEU starts with a few steps that prepare for e-Examination, as shown in Fig. 15. The main steps of pre-operation are:

1. *Login*: Clients (e.g. examinees or proctors) start with login to the e-Learning portal (e.g. Moodle), using username and password.
2. *Validate examinee/proctor*: if an examinee's or a proctor's identity is initially validated by the e-Learning server (ELS), he is granted access to the system.

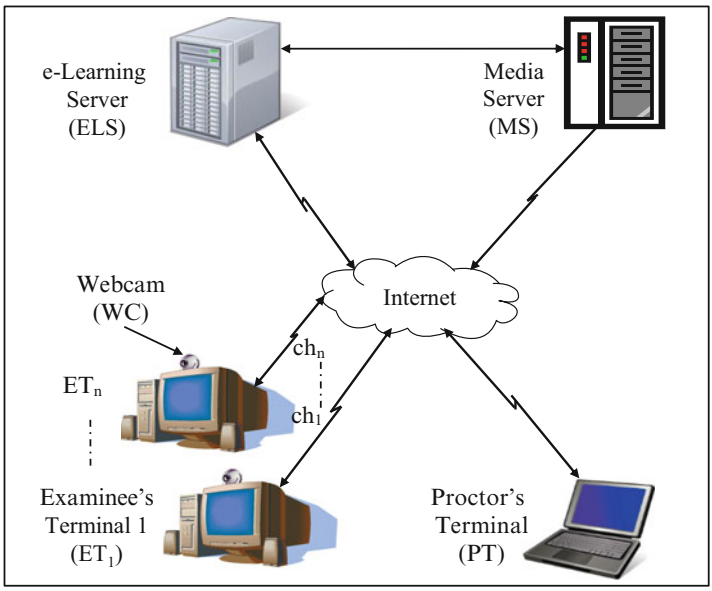

Fig. 16 Structure of ISEEU model

3. *Initialize proctor's interface*: On the main interface of the e-Course, users with proctor role clicks a link to a monitoring interface, which consists of multiple video screens; one per examinee. It can be zoomed in/out when a violation action is suspected. Also, it contains a control toolbox and a dropdown violation-list.

3.2.1 ISEEU Structure

ISEEU employs a webcam attached to an examinee's terminal (ET) that streams his exam session to a media server (MS) through the Internet, as shown in Fig. 16.

The MS, in turn, forwards exam sessions to proctors through the e-Learning server (ELS). Each examinee's session is streamed through his channel, and all the video streams appear on the proctor's terminal (PT). Both examinee and proctor are connected to the ELS and the MS through a security module that protects them against possible attacks.

3.2.2 ISEEU Procedure

The flowchart of ISEEU is shown in Fig. 17. It describes its operation and the procedure of conducting e-Exams. Moreover, the sequence diagram of Fig. 18 interactively clarifies its operation in 18 steps:

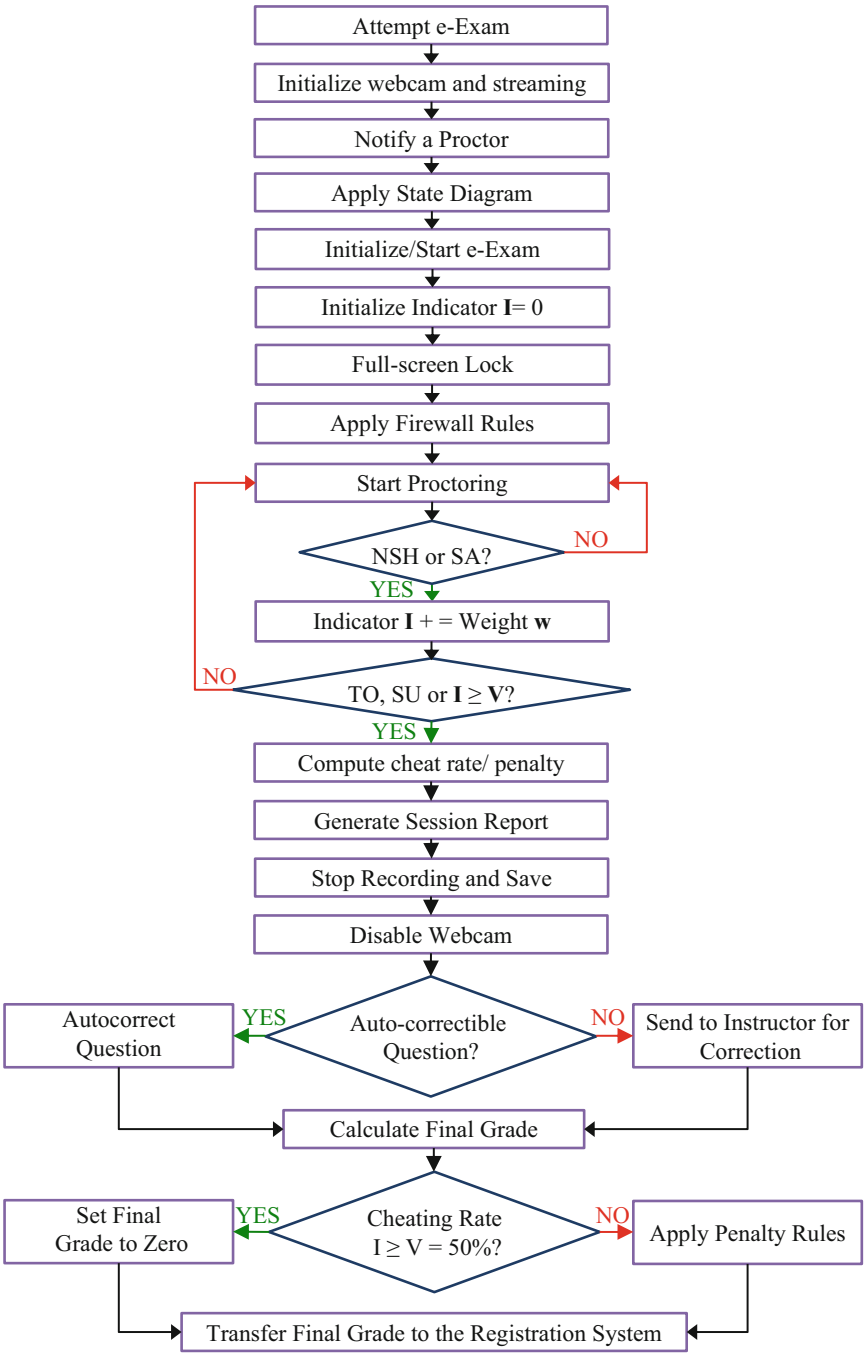

Fig. 17 ISEEU-operation procedure

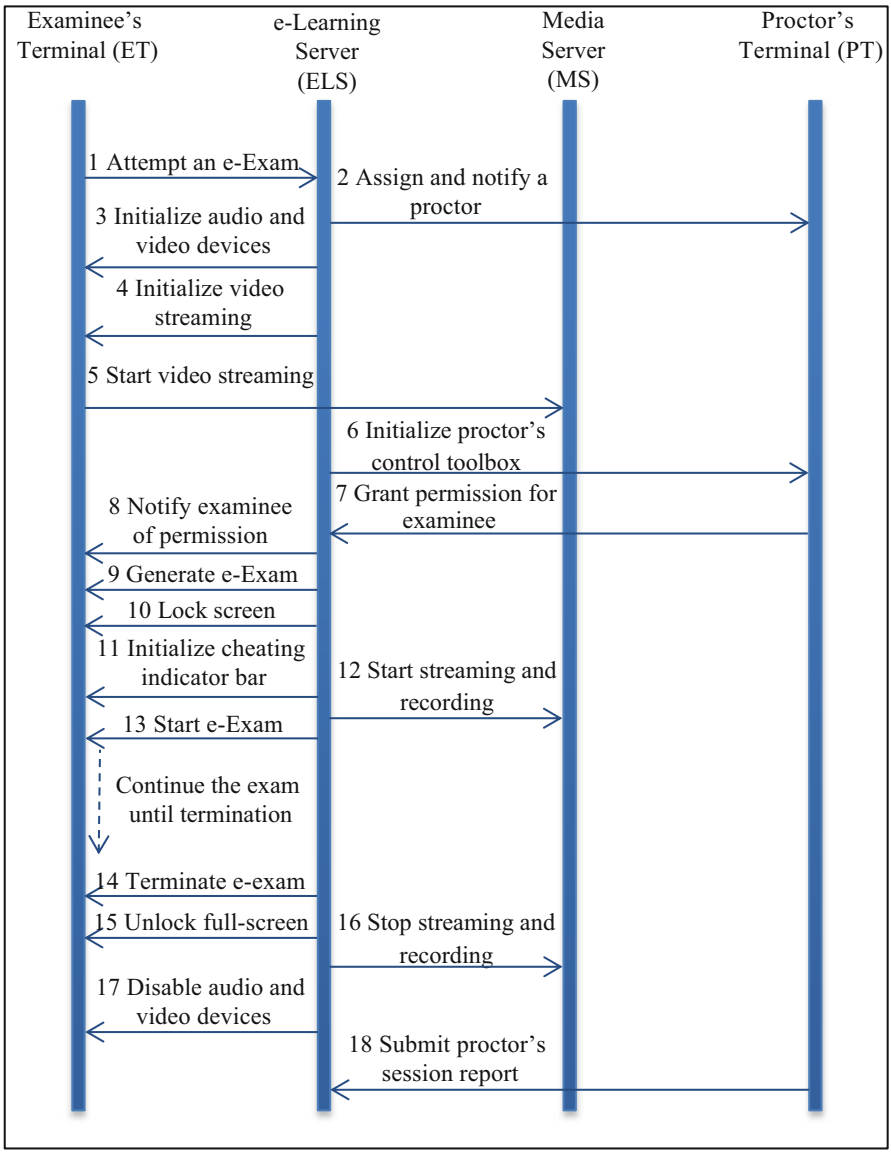

Fig. 18 ISEEU Sequence Diagram

1. *Attempt an e-Exam*: the "Attempt now" button on the exam's interface it disabled. At this point forward, *the state-diagram* controls the transition between different states based on specific events.
2. *Assign and notify a proctor*: the system generates a query to the database on the ELS to determine the corresponding proctor. If he is online, it notifies him.

3. *Initialize audio and video devices*: initialize the examinee's audio and video devices (e.g. headphones and webcam) and asks him to calibrate them.
4. *Initialize video streaming*: both the media encoder on the examinee's terminal (ET) and the media server (MS) are initialized, and their connection is check.
5. *Start video streaming*: a channel is assigned and a connection is established between the ET and the MS. The examinee is asked to calibrate the webcam until his face is top-centered, before his video starts streaming.
6. *Initialize proctor's control toolbox and notify him*: initializes the control toolbox for both examinee and proctor and activates the required functions.
7. *Grant permission to examinee*: the examinee waits permission from his proctor to start. While waiting, an examinee can play a demo of instructions. At this step, all necessary functions are activated. Proctors interact with examinees via chat option in the toolbox and follow a predefined procedure to verify their identity.
8. *Notify examinee of permission*: if an examinee is identified, the proctor approves by clicking "Accept". This enables the "Attempt now" button, and an examinee is notified to start his e-Exam.
9. *Generate e-Exam*: this step randomly generates the questions from a question bank on the ELS that guarantees different questions for each examinee.
10. *Lock the examinee's screen*: immediately, the exam-interface is locked with a full screen, and all functions, that allow access to resources, are disabled.
11. *Initialize cheating indicator bar*: a graphical cheating indicator bar is initialized to 0% ($I = 0$) and appears on the exam's interface.
12. *Start streaming and recording*: the e-Exam session streaming and recording start. It is stored to the MS in order to be revised on uncertainty.
13. *Start e-Exam*: the timer is initialized, the exam session starts and continues until time is over (TO), exam is submitted (SU) or terminated when violation limit ($I \geq V$) is exceeded. On exceptions, such as device failure or disconnection, the device checker handles exceptions before the exam is being resumed.
14. *Terminate e-Exam*: If the exam terminates, it is closed with a relevant warning message. The questions are auto-scored and scores appear to the examinee.
15. *Unlock full-screen*: the examinee's interface is unlocked to its normal state.
16. *Stop streaming and recording*: streaming is stopped and the video is saved.
17. *Disable audio and video devices*: the webcam goes off.
18. *Submit session report*: It generates a session report that contains all violations. A proctor revises it and the recorded session, if necessary, and submits his report.

During an e-Exam, a proctor might pause/resume a session and can generate alerts and violations by choosing from a list. Cheating rate is calculated each time and appears on a cheating indicator bar (I) on the examinee's interface. This rate is accumulated on each issued violation ($I+ = w$), such as no show (NSH) or suspicious actions (SA). It is paused or terminated if a violation rate is exceeded ($I \geq V$).

3.3 *Smart Approach for Bimodal Biometrics Authentication in Home-exams (SABBAH)*

SABBAH scheme resolves the major challenges of ISEEU, especially that it does not require manual intrusion. The following subsections introduce the new features.

3.3.1 SABBAH Structure and Features

SABBAH scheme comes as an upgrade of ISEEU. We add a bimodal biometrics scheme, which consists of continuous fingerprint and keystroke dynamics. The first employs a mouse with a built-in fingerprint scanner, while the latter employs the keyboard, as depicted in Fig. 19. Another important difference is automation, where the PT is substituted by a Video/FPA/KDA Processing Server (VFKPS).

The new features of SABBAH over ISEEU can be summarized as follows:

- Fingerprint is used for login and for continuous verification. It guarantees the examinee's presence if the webcam fails, and continues while it is being fixed.
- Keystroke dynamics ensure that the actual examinee is typing in essay questions.

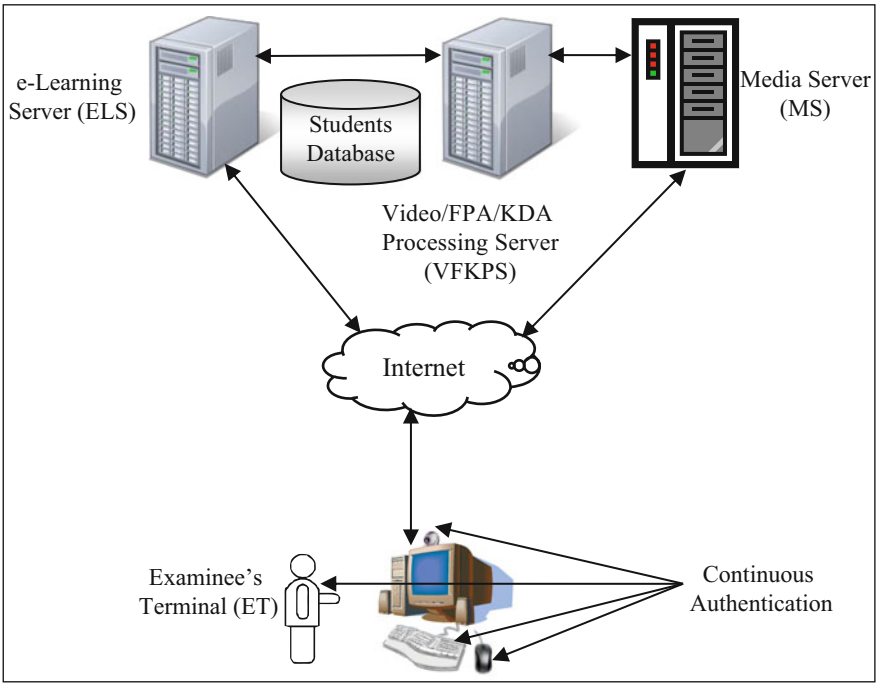

Fig. 19 Structure of SABBAH e-Examination Scheme

- The device checker ensures that authentication devices are the only functional ones, by investigating ports, interrupt requests (IRQ) and memory addresses.
- Firewall/access lists module rejects unknown in/out protocols by closing all ports except the required ones. This prevent communication with possible assistants.
- The VFKPS server automatically substitutes proctors using video comparison.

3.3.2 SABBAH Procedure

SABBAH operates in three phases; enrollment, exam session, and finalization. Again, Fig. 18 describes SABBAH sequence. Most steps are the same except authentication methods and the VFKPS, which replaces the proctor's terminal (PT).

Phase I: Enrollment

This phase starts when a student enrolls e-Learning courses, as shown in Fig. 20:

1. Student's fingerprint is scanned at the registrar's desk.
2. A still photo and a short video are captured by a high-resolution camera.
3. A training set of keystrokes is captured by typing a passage on a dedicated PC.
4. The VFKPS performs feature extraction and saves that on the ELS.

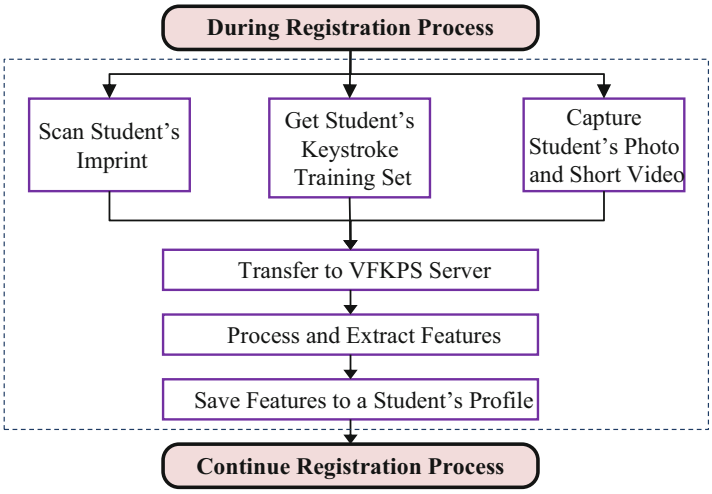

Fig. 20 Phase I (Enrollment)

Phase II: e-Examination Session

In this phase, an exam passes into four possible states in the VFKPS as illustrated in Fig. 21. When an examinee opens his video interface, he is asked to check video and audio settings. Then he submits his ID, while the "Attempt now" is dimmed.

Initialization

This phase enables, checks, configures calibrates devices, and login to the ELS and the e-Examination system takes place. It consists of three steps; FPA, KDA and video initialization, as shown in Fig. 21.

FPA Initialization When a student opens the login screen, the fingerprint scanner is enabled, and he is asked to enter his imprint on the on-mouse scanner. The VFKPS runs a matching algorithm with the saved imprint. If login succeeds, the examinee moves to the next step. Otherwise, he should just retry.

KDA Initialization This starts if the FPA succeeds, where a multimedia demo appears with instructions, and the examinee is asked to type a short paragraph. Keystrokes are transferred to the VFKPS for feature extraction and matching with the stored ones. If they match, he moves to the next step, otherwise, he should retry.

Video Initialization After KDA initialization completes, the examinee is moved to a blank video screen. Then, the webcam is enabled and his video appears, and the examinee is asked to calibrate video and audio devices. He is reminded of chat service with technical-support agents 24/7 online. The matching algorithm extracts the features and compares them with the stored ones. Finally, if matched, he moves to the next step, otherwise, he will just keep trying.

Operation

On exam initialization, the system chooses randomly from a large pool of questions to minimize the chance for examinees to get similar questions. The pool size should be at least equal to the number of examinees times the exam size. In this phase, the exam actually starts, and so the timer's countdown. Also, a full screen locks the examinee's desktop and the security module closes the ports to prevent access to related resources from local disks, internet, remote desktops or remote assistants. The cheating indicator is initialized to zero ($I = 0$).

FPA Operation The fingerprint scanner captures the imprint in two modes; randomly or periodically. The imprints are transferred to the VFKPS for continuous matching. If matched, a new imprint is captured. Otherwise, it continues trying and moves to KDA matching.

KDA Operation The examinee's activities on the keyboard are continuously captured and sent to the VFKPS for matching. If matched, a new keystroke set is captured. Otherwise, it continues trying and moves to video matching.

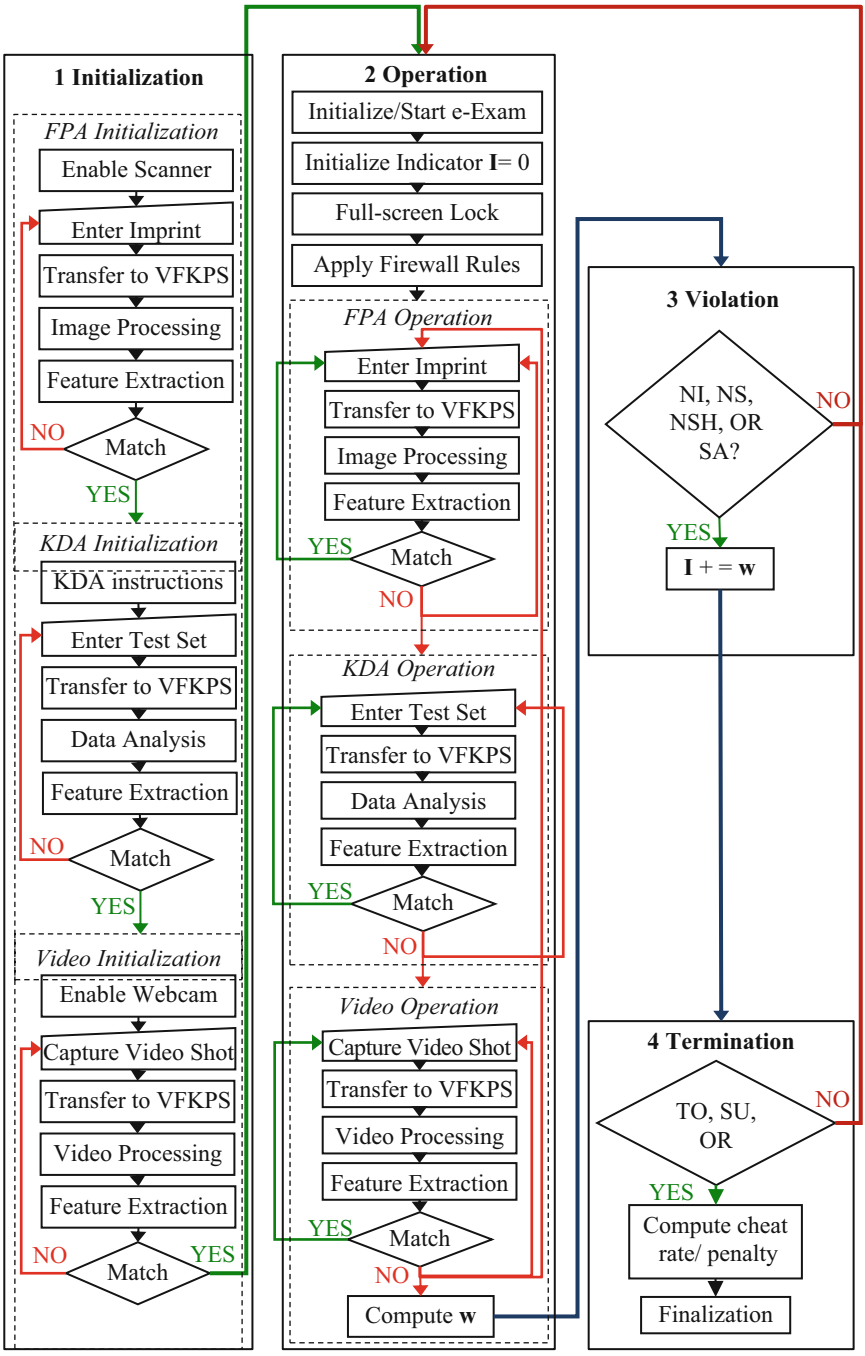

Fig. 21 Phase II (e-Examination Session)

Video Operation This step takes video shots randomly or periodically and sends them to the VFKPS for feature extraction and continuous matching. If matched, a new video shot is captured and the operation is repeated. Otherwise, it continues trying and repeats the operation cycle from the beginning. It also moves to the next step to add a violation with a weight (w) from the list.

Violation

It occurs when some rules are violated, either by the system or the examinee. The exam saves status, pauses, if necessary, and exception handling is followed before the exam can be resumed.

System's Violation This occurs when the keyboard, the mouse or the webcam stops responding, turned off, removed or duplicated. The device checker can detect such violations. Also, power off, internet disconnection and application or operating system errors are considered. If the examinee did not cause any, these errors will not be treated as cheating actions, and no penalty will be applied. Following the state diagram, the exam saves its state, pauses and notifies an agent in the technical support unit (TSU). When the violation reason is detected and corrected, the exam resumes. Restart and shutdown of either hardware or software are allowed to fix the problem. For security issues, the examinee cannot review the previously answered questions after the system is back operational.

Examinee's Violation This occurs when the examinee violates instructions, cheats or tries to cheat. Violation might be impersonation, getting assistance from others, or access to exam resources or material, etc. The violations are weighted and the cheating rate is accumulated using weights (w) and represented on the cheating indicator (I). A violation is weighted if all devices fail to recognize a user, or if a suspicious action (SA) is detected. The examinee's violations in SABBAH can be:

- *FPA violations* include unmatched fingerprint with the stored one, and no imprint (NI) is captured for a predefined period in questions that require a mouse.
- *KDA violations* include unmatched features of keystrokes and keystroke absence, i.e. No strokes (NS), for a predefined period in essay questions.
- *Video violations* are not limited to face and/or head are unmatched, specific parts of the body do not show (NSH) for a predetermined number of tries, suspicious actions (SA) and moves (looking around, sleeping, bending, etc.), and producing noise, speech or voice. On each violation, the system generates relevant warning messages, and the cheating indicator increments ($I+ = w$). If the resultant rate exceeds some violation limit ($I \geq V$), it moves to termination.

Termination

In this phase, the examination session actually terminates, as follows:

Normal Termination This occurs either when the exam's time is over (TO), or when an examinee submits all questions (SU). In both cases, the system saves the session's status-report and video recording. The report includes all violations and the total cheating rate. Finally, it moves to finalization phase that unlocks the full screen, turns off authentication devices and applies penalties.

Abnormal (Cheating) Termination Each time the examinee commits a violation, it appears on his cheating indicator bar. When this rate exceeds a specific limit, say ($I \geq 50\%$), the exam automatically terminates with a zero grade. In fact, this rate depends on the institution's rules and can be configured in the system settings. After termination, the same procedure in (1) is followed.

Phase III: Finalization

The flowchart of this phase is shown in Fig. 22. It includes grading, applying penalties, reporting, and transfer of scores.

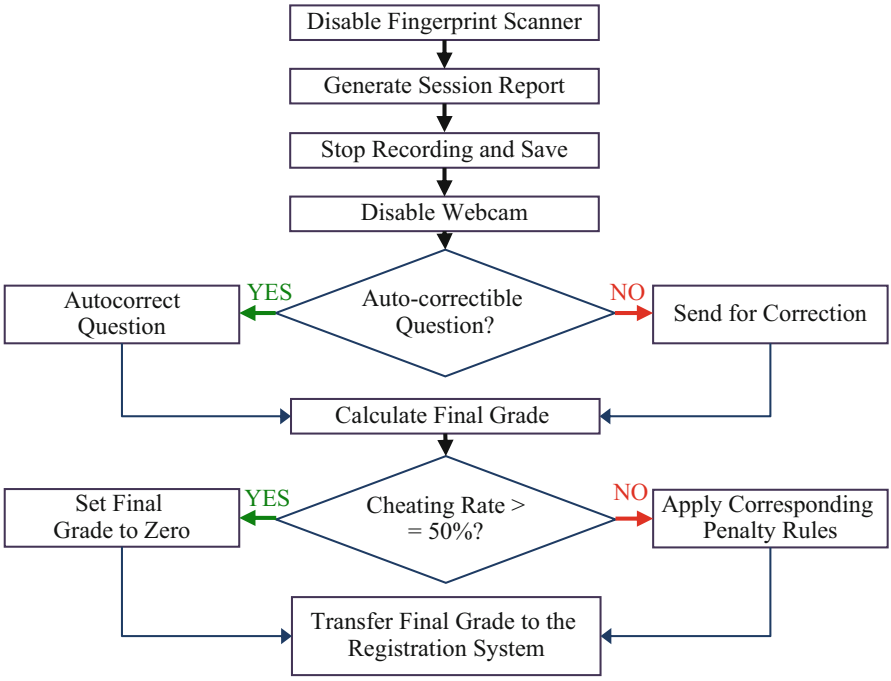

Fig. 22 Phase III (Finalization)

After an exam terminates, a session report is generated, and session recording is stopped and saved. Then the exam is corrected, where auto-correctable questions (e.g. matching or multiple-choice) are corrected. Otherwise, they are sent to the instructor for manual correction. The total grade is recalculated for all questions.

Based on the cheating rate in the generated report, a penalty is applied. For instance, a penalty of 50% cheating rate or more can be a total of zero. Actually, this can be set as a preference according to each institution's policy. In case of uncertainty, a monitoring specialist is notified and given access to an examinee's relevant data and the recorded session. He revises them, evaluates cheating rate, and submits his report, which is considered in recalculating the total grade. The final grade is then transferred to the registration system automatically.

4 Results and Conclusion

In this section, we provide results of a comprehensive risk-analysis that we have conducted against seven security risks. The objective this analysis is to measure our proposed schemes' security and their ability for cheating prevention and detection compared to the previous schemes. The section is divided into five subsections; results, discussion and evaluation, conclusion, challenges and future work.

4.1 Results

For more accuracy in the risk analysis, each risk measures several threats. The distribution of priority on security risks is illustrated in Table 5. It is shown that *Preventing access to resources* achieved the highest priority with a weight of *0.708*, whereas *e-Learning environment security* achieved the lowest priority with a weight of *0.533*. Note that the 5th and the 6th risks have the same priority of *0.567*.

The average score of each scheme is weighted by Eq. (9) [45, 46], where each score is multiplied by its corresponding weight and summed. Then, their summation is divided by the summation of all weights.

$$T_s = \frac{\sum_{i=0}^{n} (W_i S_i)}{\sum_{i=0}^{n} W_i} \tag{9}$$

Table 5 Distribution of priority on security risks

No.	Risk	Weight	Priority
1	Preventing access to resources	0.708	1
2	Satisfying C-I-A goals	0.654	2
3	Satisfying P-I-A goals	0.631	3
4	Impersonation threats (C, D, B, A)	0.613	4
5	Interaction with examinees and feedback	0.567	5
6	Redundancy/fault tolerance of auth. methods	0.567	5
7	Security of e-Learning environment	0.533	6

Where, T_S is the total weighted-score of a scheme s, W_i is the priority weight of a risk i, S_i is the score of a scheme for a risk i, and n is the total number of risks.

Final results of this risk analysis are shown in Tables 6 and 7. They are also represented by bar charts in Figs. 23 and 24 respectively. In order to compare security of the entire e-Examination schemes, the average scores have been computed. For briefing and simplicity, the scheme with the best score in each category is considered to represent it. Also, both of our proposed schemes are maintained. The remaining lower-score schemes in each category are neglected. Then, results of the remaining schemes are listed within their categories in Table 7. Moreover, their bar charts are illustrated in Fig. 24.

The Italicized scores in the tables indicate that a scheme failed to resolve a risk, i.e. its score is less than 50%. The last row in Tables 6 and 7 show the weighted-average scores of each scheme or category based on Eq. (9). This measures the impact of the risks' priorities shown in Table 5.

4.2 Discussion and Evaluation

Before discussion and evaluation, we start with a previous evaluation study to be compared with our comprehensive evaluation. Apampa [25] has conducted the previous evaluation of the existing schemes against the impersonation threats (e.g. Types A, B and C), as depicted in Table 8. "Yes" means that a scheme solves a threat, "No" means that it is susceptible to a threat, and "SP" stands for strong potential [25].

The previous evaluation show that [25]:

1. The first scheme is vulnerable to Type A threats. Another person else can conduct an e-Exam with connivance of a proctor.
2. The second solves Type B and prevents scenarios of pretending to be the real examinee. It is feasible for Type C if continuous authentication is performed.
3. In the third, fingerprint with mouse dynamics solve Type B, but unclearly solve Type C due to delay in mouse data-capturing. Alternatively, fingerprint with face-geometry detection minimize Type B and Type C threats.
4. The fourth scheme is vulnerable to Type A, B and C. Live video monitoring will fail if the proctor is unfocussed, and video revision needs extra efforts.
5. Fingerprint of the fifth scheme solves Type B, while video monitoring is unclear. Moreover, security will be broken if the webcam is moved.

Unfortunately, the previous evaluation is not accurate, since it considers that any scheme with human interaction is susceptible to connived Type A, and a successful attack creates a route for a Type C impersonation. However, it is impossible to prevent human interaction. For instance, developers, database administrators and network administrators have full access to the e-Examination system, and if connived, the system is circumvented. Moreover, our proposed Type D impersonation was not taken into account, and other important security issues such as access to

Table 6 ISEEU and SABBAH compared with the previous e-Examination *schemes* against security risks

No.	Security risk	Previous scheme								Proposed scheme	
		Proc-LAB	BWA-FR	eTest-LAP	Theo-CFP	FP-MD	FP-HGD	SIE-VM	FP-VM	ISEEU	SABBAH
1	Preventing access to resources	54.5%	*15.2%*	*15.2%*	*24.2%*	*24.2%*	*24.2%*	63.6%	63.6%	100%	100%
2	Satisfying C-I-A goals	66.7%	66.7%	66.7%	66.7%	66.7%	66.7%	66.7%	66.7%	66.7%	100%
3	Satisfying P-I-A goals	100%	*33.3%*	66.7%	66.7%	66.7%	66.7%	66.7%	66.7%	66.7%	100%
4	Impersonation threats	100%	*35.7%*	71.4%	71.4%	71.4%	71.4%	71.4%	100%	100%	100%
5	Interaction and feedback	100%	*30.8%*	*30.8%*	*30.8%*	*30.8%*	*30.8%*	*30.8%*	*30.8%*	69.2%	100%
6	R/FT of auth. methods	100%	*8.7%*	*26.1%*	*30.4%*	*47.8%*	*47.8%*	*21.7%*	*43.5%*	*43.5%*	73.9%
7	Environment security	100%	*20.0%*	*20.0%*	*20.0%*	*20.0%*	*20.0%*	*20.0%*	*20.0%*	100%	100%
Average score		88.7%	*30.0%*	*42.4%*	*44.3%*	*46.8%*	*46.8%*	*48.7%*	55.9%	78.0%	96.3%
Weighted-average score		87.4%	*30.5%*	*42.8%*	*44.9%*	*47.2%*	*47.2%*	50.3%	57.3%	78.4%	96.5%

Table 7 Comparison of our proposed schemes (i.e., ISEEU and SABBAH) and the previous *categories* (i.e., schemes are combined into their categories) against security risks

No.	Security risk	Previous-scheme category					Proposed scheme	
		Proctored-only	Unimodal biometrics	Bimodal biometrics	Video monitoring	Biometrics with VM	ISEEU	SABBAH
1	Preventing access to resources	54.5%	*18.2%*	*24.2%*	63.6%	63.6%	100%	100%
2	Satisfying C-I-A goals	66.7%	66.7%	66.7%	66.7%	66.7%	66.7%	100%
3	Satisfying P-I-A goals	100%	55.6%	66.7%	66.7%	66.7%	66.7%	100%
4	Impersonation threats	100%	59.5%	71.4%	71.4%	100%	100%	100%
5	Interaction and feedback	100%	*30.8%*	*30.8%*	*30.8%*	*30.8%*	69.2%	100%
6	R/FT of auth. methods	100%	*21.7%*	*47.8%*	*21.7%*	*43.5%*	*43.5%*	73.9%
7	Environment security	100%	*20.0%*	*20.0%*	*20.0%*	*20.0%*	100%	100%
Average score		88.7%	*44.3%*	*46.8%*	*48.7%*	55.9%	78.0%	96.3%
Weighted-average score		87.4%	*44.9%*	*47.2%*	50.3%	57.3%	78.4%	96.5%

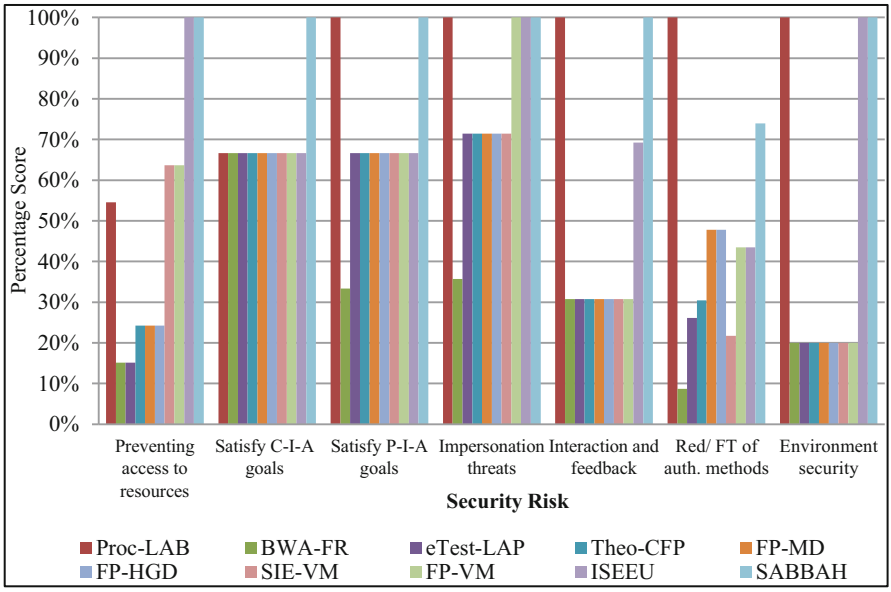

Fig. 23 ISEEU and SABBAH compared with the previous e-Examination *Schemes* against security risks (Percentage Scores)

resources, C-I-A and P-I-A goals were not considered. Therefore, we present a more accurate and comprehensive evaluation below.

Our evaluation and discussion assume that the proctor-based scheme (i.e. traditional) has the highest security in the optimal case. In general, e-Examination schemes compete with it to achieve, at most, the same security. The proctored-only (Proc-LAB) scheme is the most similar to a traditional one, except that it is computer-based and conducted in computer labs.

Nevertheless, *SABBAH scheme* (i.e. our proposed scheme) achieved the *first rank* and the *best security* with an average score of *96.3%*. The following justify this distinct rank of SABBAH in the measured seven-risks:

1. *Access to exam resources (100%):* Exam resources are protected by several methods:
   - The full-screen lock prevents access to local disks, storage media, Internet, Intranet, LANs and WANs.
   - Video matching detects cheating actions such as copy from textbooks, cheat sheets and PDAs (e.g. Phone Calls/MMS/SMS).
   - Exam questions are randomly generated from a large pool (e.g. a question bank).
   - The exam repository is protected with fingerprint and the security module (e.g. SSL/TLS, firewall, anti-x, XXS/SQLI detection, etc.).

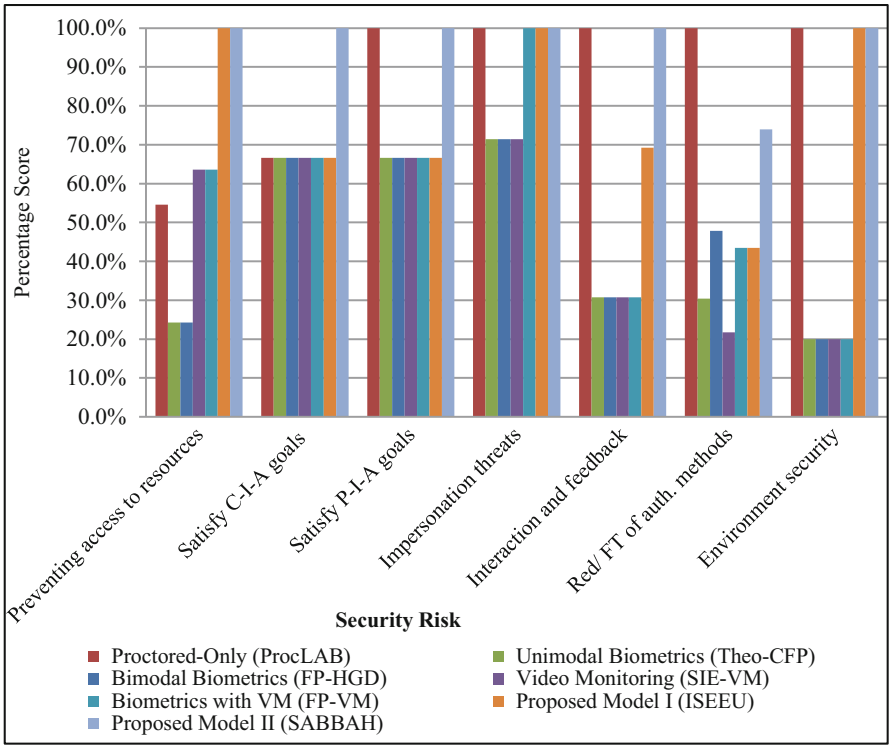

Fig. 24 Comparison of our proposed schemes (i.e. ISEEU and SABBAH) and the previous *Categories* (i.e. combined schemes) against security risks (Percentage Scores)

2. *C-I-A goals (100%)*: Strong authentication and security module assure confidentiality, integrity and availability. Availability might be slightly degraded when the number of examinees exceeds some limit, if not scheduled carefully.
3. *P-I-A goals (100%)*: Continuous authentication using fingerprint, keystroke dynamics and video matching ensure presence, identification and authentication.
4. *Impersonation threats (100%)*: All types of impersonation threats are solved:
   - *Type A*: never occurs, since there is no manual intervention. Also, sessions are recorded for more processing on uncertainty.
   - *Type B*: never occurs, since biometrics authentication is used, such that no way to pass security information to fraudulent persons.
   - *Type C*: similar to type B, continuous authentication is used to prevent allowing fraudulent to get exam-control, since this scenario will be detected.
   - *Type D*: video matching catches local assistants, while remote assistants are prevented by the security module, which closes all vulnerable ports.

Table 8 Impersonation threats and solutions of existing schemes [25]

No.	Scheme category	Solution to impersonation threat		
		Type A	Type B	Type C
1	Proctored-only environment [18, 30, 39]	No	No	No
2	Unimodal biometrics [12, 24, 28, 40, 41]	Yes	Yes	No
3	Bimodal biometrics [25, 42, 43]	Yes	Yes	SP
4	Video monitoring (+password) [44]	No	No	No
5	Biometrics + webcam monitoring [35]	Yes	Yes	No

5. *Interaction and feedback (100%)*: Two effective tools of interaction with examinees are provided; the cheating indicator and warning messages. The indicator measures the cheating rate and appears on the exam's interface. At the same time, warning messages appear to examinees on each violation.
6. *Redundancy/fault tolerance of authentication devices (73.9%)*: If one of the three authentication devices fails, another continues working. The device checker, in the security module, checks devices, detects failures and fixes them. It also assures a single device only for each authentication method.
7. *Environment security (100%)*: The security module provides a typical secure environment for the whole system. The LCMS (i.e. Moodle) is protected with SSL/TLS encryption. The firewall, the access lists, the XSS and SQLI detectors reduce attacks. Moreover, attachments are checked for viruses, malware, spyware, etc. If any is detected, it will be recovered, quarantined or deleted.

Proctored-only (Proc-LAB) comes next by achieving the second rank with an average score of 88.7%. It scored 54.5 and 66.7% in the 1st and the 2nd risks respectively and 100% in the last five risks. However, proctored-only cannot be considered a pure e-Examination scheme.

Our proposed scheme *(ISEEU) is ranked the third* by achieving an average score of *78%*. Although it failed in the 6th risk with a score of 43.5%, this risk has a lower priority and its impact is not considerable. Justification for this reasonable result is:

1. *Access to exam resources (100%)*: The same as SABBAH, but video monitoring replaces video matching for cheating prevention.
2. *C-I-A goals (66.7%)*: The security module provides high confidentiality and integrity. Availability is degraded when the number of examinees exceeds some limit, since each session needs a new channel. This reserves more memory, CPU and bandwidth. Therefore, it should be scalable and kept under monitoring.
3. *P-I-A goals (66.7%)*: Continuous video monitoring guarantees presence, identification and authentication, but using username and password to login is still weak and vulnerable.
4. *Impersonation threats (100%)*: All types of impersonation threats are solved:
   - *Type A*: exam sessions are monitored and recorded for uncertainty cases.

Type B: continuous monitoring detects the scenario of plagiarism (i.e. conducting exams on behalf of others) using their security information.x*Type C*: allowing others to get exam-control can be detected with continuous video monitoring.

– *Type D*: video monitoring catches local assistants, and closing vulnerable ports and protocols, other than those required, prevents remote assistants.

5. *Interaction and feedback (69.2%)*: ISEEU employs a cheating indicator bar and warning messages. It also uses text and audio chat for more interaction.
6. *Redundancy and fault tolerance of authentication devices (43.5%)*: It uses passwords for login to the LCMS. Moreover, video monitoring and recording are used for continuous authentication. If the webcam fails, the exam pauses until being fixed. Otherwise it is terminated.
7. *Environment security (100%)*: ISEEU exists in the same environment of SABBAH model described above.

Finally, biometrics with video monitoring (FP-VM) ranked the fourth with *55.9%*. Video monitoring (SIE-VM), bimodal biometrics (FP-HGD) and unimodal biometrics (Theo-CFP) failed with *48.7%*, *46.8%* and *44.3%* respectively.

The average scores were used in the previous discussion, in which risk priority was not considered. The weighted-average scores of the seven risks are illustrated in Fig. 25 in descending order. Accordingly, *SABBAH* achieved the *1st rank* with a weighted-average score of *96.5%*, whereas *ISEEU* achieved the *3rd rank* with *78.4%*. Proctored-only achieved the *2nd rank* with *87.4%*. It is being emphasized here that Proctored-only is not a pure e-Examination scheme, since exams could not be conducted at home. The 4*th* and the 5*th* ranks are achieved by biometrics with VM and video monitoring with *57.3%* and *50.3%* respectively. Finally, bimodal biometrics and unimodal biometrics failed with *47.2%* and *44.9%* respectively.

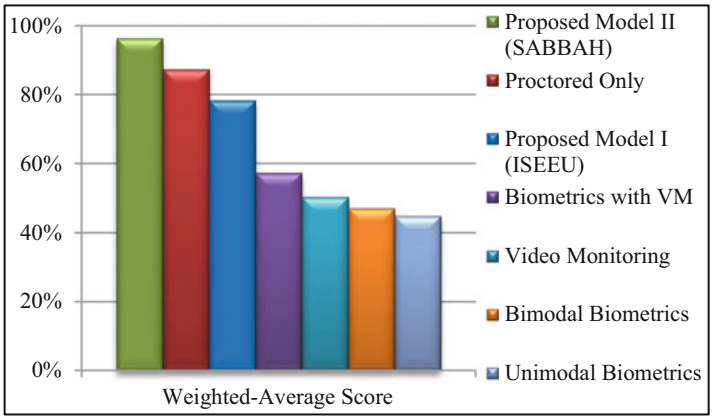

Fig. 25 Weighted-average scores of ISEEU and SABBAH against the previous categories

4.3 Conclusion

It is shown that security is vital for e-Learning systems, since they are operational and contain sensitive information and operations. One of these operations is e-Examination, which has been given higher attention recently. If an institution decides to offer pure e-Courses, it will be faced with untrusted e-Examination. Several efforts have been made in order to provide trustful e-Examination by proposing new schemes to improve security and minimize cheating. Even though, those schemes could not compete with traditional proctor-based examination.

This work contributes to solving the problem of cheating and other security issues, taking into account most of the possible vulnerabilities. It is believed that our proposed e-Examination schemes, i.e. ISEEU and SABBAH, present a major contribution in the field. They are highly secure, simple and easy to be implemented. They are the strongest competitors to the traditional examination scheme, or even beat it with its new features. This is exactly what we proved in our results.

Results show that our proposed schemes proved reasonable security compared with the previous ones. *SABBAH ranks the first*, and *ISEEU ranks the third* in the risk analysis. Results show that the proctored-only scheme (i.e. traditional examination) ranked the second after SABBAH. This rank is considered satisfactory, since our objective was to propose a scheme that competes with the traditional one. The reason for superiority of SABBAH is its higher security and its high ability to prevent/detect cheating actions.

However, the claim that traditional exams are 100% secure is theoretical, and the literature shows that over than 70% of high-school students in USA admit cheating, where 95% of them are never detected. Also, they are inflexible in place and time and economically infeasible. Moreover, all procedures, such as exam delivery, monitoring, grading, scoring and data entry, are manual, which are time-consuming and need manpower.

Both *SABBAH and ISEEU* schemes satisfy the *C-I-A* (Confidentiality, Integrity and Availability) and the *P-I-A* (Presence, Identity and Authentication) goals. Also, they resolve security issues that were neither resolved nor mentioned previously:

- Access to exam resources, such as textbooks, worksheets, local computer, the Internet and remote assistance. Both prevent this by fullscreen locks, interactive-monitoring or video matching, and continuous authentication.
- Our schemes are interactive based on cheating indicator and warning messages to stopp cheating when detected, while the previous schemes lack to this feature.
- Webcam failure pauses the exam until it is fixed to resume, while this scenario leads to system failure in the previous video monitoring schemes.

Regarding plagiarism or impersonation threats, our schemes resolve all types of threats. In addition, they have many advantages over the previous schemes. For instance SABBAH scheme is:

- *Fully automated*: a proctor is no longer needed. Also, grading, cheating penalties, and data transfer all are executed automatically.

- *Fully secure*: solving impersonation threats, satisfying P-I-A goals, interaction with examinees, preventing access to resources, and preventing collaboration.
- *Highly efficient*: a virtual examination session, but with similar efficiency in cheating detection and prevention as actual proctored-sessions.
- *Reliable and redundant*: three synchronized authentication devices. If one fails, another passes. Also, a device might never or rarely been used while using another.
- *Reasonable and relatively inexpensive*: it substitutes proctors who are paid for monitoring.

4.4 Challenges

Although they have many advantages and resolve several security issues, our schemes encounter some challenges. The main challenges can be summarized in:

- *Internet speed/backbone bandwidth and robustness*: high-speed and stable internet connection are required, especially at peak times.
- *Performance and capacity*: they require servers with huge memory and storage/disk space, and SABBAH requires a VFKPS with a high processing power.
- *Implementation complexity*: implementation of automatic video matching is not easy, and its algorithms are still under development. Performance and accuracy in feature extraction and matching are still challenging. Also, users on the client side require a special hardware for fingerprint scanning.
- *Failure penalties*: on unrecoverable failures, the answered questions cannot be reviewed by an examinee after being back, for security issues.

However, who keeps track with the fast advancement in information and communication technology (ICT), discovers that all challenges are to be resolved very soon. For instance, proponents claim that cloud-computing concept fits this type of applications and will overcome many of these challenges. Accordingly, this claim was tested in a small range, where ISEEU was deployed on cloud control; computing platform as a service (PaaS). This test was limited, since we used a trial version with limited services. Regarding special hardware requirement, most of modern computers have fingerprint scanners, and touch-screens can provide more options for secure and interactive e-Examination schemes.

It is being emphasized here that our proposed e-Examination schemes will not provide completely cheating-free e-Exams, but they minimize cheating and impersonation threats. With well-developed functions, we believe that our scheme is more efficient and cost-effective than proctor-based in-classroom sessions.

4.5 Future Work

Our research directions of the future is to improve our e-Examination schemes. In order to achieve this, the following are the main ideas intended to be investigated:

- Implement our proposed schemes in a real environment for some courses. This, actually, aims to measure its acceptance, applicability and security. Accordingly, the schemes should be improved in terms of security and performance. This will enable us to examine their resistance to cyber-attacks such as distributed denial-of-service (DDoS), session highjacking, and man-in-the-middle (MitM), etc.
- Develop an efficient video matching algorithm towards being an important biometrics continuous authentication approach, especially for e-Examinations. It detects examinees' violations and cheating actions automatically.
- Apply all parameters of KDA other than typing speed to improve accuracy, such as flight time, seek time, characteristic errors, and characteristic sequences. This enables us to measure its reliability for continuous authentication.
- Deploy our schemes on the cloud to provide the required computational power, and to evaluate its security and performance in terms of storage, memory and CPU usage.

References

1. E. Kritzinger, "Information Security in an e-Learning Environment", 2006. Last access Dec. 2016. http://sedici.unlp.edu.ar/bitstream/handle/10915/24349/documento_completo.pdf%3Fsequence%3d1
2. Y. Sabbah, "Comprehensive Evaluation of e-Learning at Al-Quds Open University", Internal Report OLC-195/2010, Al-Quds Open University (QOU), Open Learning Center (OLC), 2010.
3. M. Hentea, M. J. Shea and L. Pennington, "A Perspective on Fulfilling the Expectations of Distance Education", Proceedings of the 4th Conference on Information Technology Curriculum (CITC4) Lafayette, Indiana, USA, pp.160–167, October 2003.
4. H. A. El-Ghareeb, "e-Learning and Management Information Systems, Universities Need Both", eLearn Magazine, September 2009. Last access December 2016. http://elearnmag.acm.org/featured.cfm?aid=1621693
5. R. Raitman, L. Ngo and N. Augar, "Security in the Online e-Learning Environment", Proceedings of the 5th IEEE International Conference on Advanced Learning Technologies, Kaohsiung, Taiwan, pp.702-706, July 2005.
6. George M. Piskurich (Ed.), "AMA Handbook of eLearning-Effective Design, Implementation and Technology Solutions", AMACOM American Management Association 2003. Last access December 2016. https://www.questia.com/read/119691314/the-ama-handbook-of-e-learning-effective-design
7. M. Bullen, T. Morgan, K. Belfer and A. Qayyum, "The Net Generation in Higher Education: Rhetoric and Reality", International Journal of Excellence in e-Learning (IJEEL), vol.2, no.1, pp.1-13, February 2009.
8. D. Jonas and B. Burns, "The Transition to Blended e-Learning, Changing the Focus of Educational Delivery in Children's Pain Management", Elsevier, Nurse Education in Practice, vol.[8], no.1, pp.1–7, January 2010.

9. W. H. Rice IV, "Moodle e-Learning Course Development: A Complete Guide to Successful Learning Using Moodle", First edition, Packt Publishing 2006.
10. J. C. Taylor, "Fifth Generation Distance Education", Higher Education Series, Report no.40, The University of Southern Queensland, Global Learning Services, 2001.
11. E. R. Weippl, "Security in e-Learning", First edition, Springer 2005.
12. Y. Levy and M. Ramim, "A Theoretical Approach for Biometrics Authentication of e-Exams", Chais Conference on Instructional Technologies Research, Israel, pp.93-101, 2007. Last access December 2016. http://telem-pub.openu.ac.il/users/chais/2007/morning_1/M1_6.pdf
13. National Institute of Standards and Technology. An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12, October 1995.
14. W. Stallings, "Data and Computer Communications", Eighth edition, Prentice Hall 2007.
15. News, "Popular Sites Push Malware", Computer Fraud and Security, Elsevier, vol. 2010, no. 9, pp. 3, September 2010.
16. News, "The Human Impact of Cybercrime", Computer Fraud and Security, Elsvier, vol. 2010, no. 9, pp. 3-20, September 2010.
17. Official Website of Symantec/Norton, "Norton Cybercrime Report: the Human Impact", August 2016, Last access December 2016. http://us.norton.com/theme.jsp?themeid= cyber-crime_report&inid=br_hho_downloads_home_link_cybercrimereport.
18. E. R. Weippl, "In-Depth Tutorials: Security in e-Learning", eLearn Magazine, vol.2005, no.3, March 2005. Last access December 2016. http://elearnmag.acm.org/featured.cfm?aid=1070943
19. K. El-Khatib, L. Korba, Y. Xu and G. Yee, "Privacy and Security in e-Learning", International Journal of Distance Education, vol.1, no.4, pp.1-19, 2003.
20. S. Banerjee, "Designing a Secure Model of an e-Learning System- A UML-Based Approach", IEEE Potentials Magazine, vol.29, no.5, pp.[20]-27, September-October 2010.
21. N. H. Mohd Alwi, and I.-S. Fan, "Information Security Threats Analysis for e-Learning", Proceedings of the First International Conference TECH-EDUCATION, Athens, Greece, pp.285-291, May 2010.
22. 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 e-Learning Systems", Computers and Security, vol.28, no.8, pp.843-856, November 2009.
23. 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 Transactions on Information and System Security, vol.13, no.3, pp.1-30, July 2010.
24. E. Flior and K. Kowalski, "Continuous Biometric User Authentication in Online Examinations", Proceedings of the 7th International Conference on Information Technology: New Generations, Las Vegas, pp.488-492, April 2010.
25. K. M. Apampa, G. Wills and D. Argles, "User Security Issues in Summative e-Assessment Security", International Journal of Digital Society, vol.1, no.2, June 2010.
26. K. Abouchedid and G. M. Eid, "e-Learning Challenges in the Arab World: Revelations from a Case Study Profile", Quality Assurance in Education, vol.12, no.1, pp.15–27, 2004.
27. A. Marcus, J. Raul, R. Ramirez-Velarde and J. Nolazco-Flores, "Addressing Secure Assessments for Internet-Based Distance Learning Still an Irresolvable Issue", Proceedings of the 9th Latin-American Congress of Educational Computing, Caracas, Venezuela, March 2008.
28. S. Alotaibi, "Using Biometrics Authentication via Fingerprint Recognition in e-Exams in e-Learning Environment", In the 4th Saudi International Conference, The University of Manchester, UK, July 2010.
29. Apampa KM, Wills G, Argles D. Towards security goals in summative e-assessment security. InInternet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for 2009 Nov 9 (pp. 1–5). IEEE.
30. N. C. Rowe, "Cheating in Online Student Assessment: Beyond Plagiarism", Online Journal of Distance Learning Administration, vol.7, no.2, summer 2004.

31. A. Lathrop and K. Foss, "Student Cheating and Plagiarism in the Internet Era: A Wake-Up Call", Englewood: Libraries Unlimited 2000. Last access December 2016. http://www.questia.com/PM.qst?a=o&d=111682012
32. M. Dick, J. Sheard, C. Bareiss, J. Carter, D. Joyce, T. Harding and C. Laxer, "Addressing Student Cheating: Definitions and Solutions", ACM Special Interest Group on Computer Science Education Bulletin, vol.[32], no.2, pp.172-184, June 2003.
33. Murdock TB, Miller A, Kohlhardt J. Effects of Classroom Context Variables on High School Students' Judgments of the Acceptability and Likelihood of Cheating. Journal of Educational Psychology. 2004 Dec;96(4):765.
34. A. Kapil and A. Garg, "Secure Web Access Model for Sensitive Data", International Journal of Computer Science and Communication, vol.1, no.1, pp.13-16, January-June 2010.
35. J. A. Hernández, A. O. Ortiz, J. Andaverde and G. Burlak, "Biometrics in Online Assessments: A Study Case in High School Students", Proceedings of the 18th International Conference on Electronics, Communications and Computers, Puebla, Mexico, pp.111-116, March 2008.
36. C. W. Ng, I. King and M. R. Lyu, "Video Comparison Using Tree Matching Algorithms", Proceedings of the International Conference on Imaging Science, Systems and Technology, Las Vegas, USA, pp.184-190, June 2001.
37. X. Chen, K. Jia and Z. Deng, "A Video Retrieval Algorithm Based on Spatio-temporal Feature Curves and Key Frames", Proceedings of the 5th International Conference on International Information Hiding and Multimedia Signal Processing, pp.1078-1081, September 2009.
38. M. S. Ryoo and J. K. Aggarwal, "Spatio-Temporal Relationship Match: Video Structure Comparison for Recognition of Complex Human Activities", Proceedings of the IEEE 12th International Conference on Computer Vision, pp.1593-1600, Kyoto, Japan, September-October 2009.
39. G. Harrison, "Computer-Based Assessment Strategies in the Teaching of Databases at Honours Degree Level 1", In H. Williams and L. MacKinnon (Eds.), BNCOD, vol.3112, pp.257-264, Springer 2004.
40. E. G. Agulla, L. A. Rifon, J. L. Alba Castro and C. G. Mateo, "Is My Student at the Other Side? Applying Biometric Web Authentication to e-Learning Environments", Proceedings of the 8th IEEE International Conference on Advanced Learning Technologies, Santander, Spain, pp.551-553, July 2008.
41. S. Kikuchi, T. Furuta and T. Akakura, "Periodical Examinees Identification in e-Test Systems using the Localized Arc Pattern Method", Proceedings of the Distance Learning and Internet Conference, Tokyo, Japan, pp.213-220, November 2008.
42. S. Asha and C. Chellappan, "Authentication of e-Learners Using Multimodal Biometric Technology", in International Symposium on Biometrics and Security Technologies, Islamabad, Pakistan, pp.1-6, April 2008.
43. Y. Levy and M. Ramim, "Initial Development of a Learners' Ratified Acceptance of Multi-biometrics Intentions Model (RAMIM)", Interdisciplinary Journal of e-Learning and Learning Objects, vol.5, pp.379-397, 2009.
44. C. C. Ko and C. D. Cheng, "Secure Internet Examination System Based on Video Monitoring" Internet Research: Electronic Networking Applications and Policy, vol.14, no.1, pp.48-61, 2004.
45. N-Calculators Official Website, "Weighted Mean Calculator". Last access December 2016. http://ncalculators.com/statistics/weighted-mean-calculator.htm
46. Wikipedia Website, "Mathematical Definition of Weighted Mean". Last access December 2016. http://en.wikipedia.org/wiki/Average