User Security Issues in Summative E-Assessment Security

Kikelomo Maria Apampa, Gary Wills, David Argles
School of Electronics and Computer Science, University of Southampton, UK

Abstract

Summative electronic assessments embodies enormous advantages such as automated marking, immediate feedback and on-demand tests. User security plays a vital role in summative e-assessments, as it ensures that online tests are delivered to the correct students only. Thus, the existing user security model presents a two-layered challenge to the student; whereby responses to "who are you?" and "is it really you?" questions are solicited. Amidst the usefulness of the existing model, summative e-assessments are susceptible to impersonation challenges. In this paper, we classify the user security concerns into Type A, Type B and Type C impersonation types. We suggest that these vulnerabilities can be linked to a weakness in the user security model. Hence, without discarding the existing model we propose a goal-oriented approach to address the user security needs of the e-assessment system. Furthermore, a review of the existing solutions depicts insufficient capabilities to minimise all the three types of impersonation challenges. Hence, we propose that an appropriate blend of existing methods will minimise the types of impersonation threats and improve user security in summative e-assessments

1. Introduction

Assessment is a major issue in education and one of the key activities in student learning. Influenced by technological advances, assessment has begun to make its way out of the traditional classroom into online environments. Thus, employing online assessments delivers benefits such as opportunities for lifelong learning, automatic marking and immediate feedback. Online formative assessments are designed to improve students' learning and give information about their progress [13]. Online summative assessments are categorised as high-stake examinations which count towards a final course mark. Thus, it may be mandatory for a student to take a summative assessment. In higher education, summative e-assessments can be divided into two: (1) e-assessments in supervised environments and (2) e-assessments in non-supervised environments. Summative e-assessments which are conducted in supervised environments include campus based exams and authorised test centres [48]. In these environments, authorised personnel or proctors are required to monitor and supervise the examination process from start to finish. Non-supervised environments include distance learning examinations and on-demand tests. In these environments, the examination process may be supervised remotely; however the examinee is required to maintain academic honesty. In this paper, we focus on summative e-assessments conducted in supervised/controlled conditions

In their work, Marais *et al*, [36] identify two categories of security in e-assessments: web security and e-assessment security. However, they concluded that web security is a well investigated area but it is insufficient to fulfil the security needs of e-assessment. In addition to the well defined web security areas, we include that data security [16], location security [36, 6], software security [4] and the network security [48] of summative e-assessments are also well researched. However, Klett & Pharow [31] suggest that the user security process of the e-assessment security is a potential research field. This paper explores the existing user security model and its inherent vulnerabilities. Finally, we propose a model that is specific to the user security in summative e-assessments.

2. Confidentiality, Integrity and Availability

A computer-based system has three primary valuable assets to protect; they are the hardware, software and data assets [41]. The computer security threats which exploit the vulnerabilities of computer assets are interception, interruption, modification and fabrication. The fundamental security goals which ensure that the hardware, software and data assets are not compromised by the threats include confidentiality (C), integrity (I) and availability (A) [17]. In literature, it is suggested that a security relationship exists between the C-I-A security goals and the critical assets (hardware, software and data) of a system [41]. Thus, a compromise in the C-I-A security goals may lead to a compromise of the critical assets.

To explain the existing security relationship, we present an example of data stored in a computer. The data is expected:

- To be accessed by only authorised parties; thus, data must be restricted (confidentiality).
- To contain no alterations of the original data; modification should be done by authorised parties only (integrity).
- To be operational and accessible whenever it is needed; except during authorised downtimes (availability).

3. User Security in Summative E-assessments

Due to the high-stake nature of a summative e-assessment, the system bases much of its security on knowing that only a legitimate student can gain access to the online test. Thus, one of the characteristics of an e-assessment system is the ability to securely provide a test which is delivered at the right time and to the correct student. User security plays a vital role in e-assessments; as it ensures that only the correct students write an online test. To fulfil this role, the user security process poses two challenges (identity and authentication) to the students. Thus, the ability of the students to provide the correct responses will give the security system an assurance that the correct students are taking the test. In this section, the questions provided by the security system and the common types of responses are explored. Figure 1 depicts the questions posed to the student during an online assessment.

3.1. Identity

Identity is a term that reflects uniqueness, sameness and distinctness. Hence, when an e-assessment security system solicits an answer to the "who are you?" question; it simply requires that the student provides a unique response which distinguishes him/her from every other student. A typical form of response used in e-assessment is the username (e.g. student log-in name). A username is not secret information and it can be shared or stolen for fraudulent purposes. In addition, providing a username only method makes the e-assessment security system an easy hurdle for the students. In an identity only system, the students are required to provide one answer; however, this response does not ensure correctness of the student. In order to ensure correctness, the e-assessment security system solicits an additional response to confirm the claimed identity. It should be noted that an identity only system is does not exist in summative e-assessment security systems.

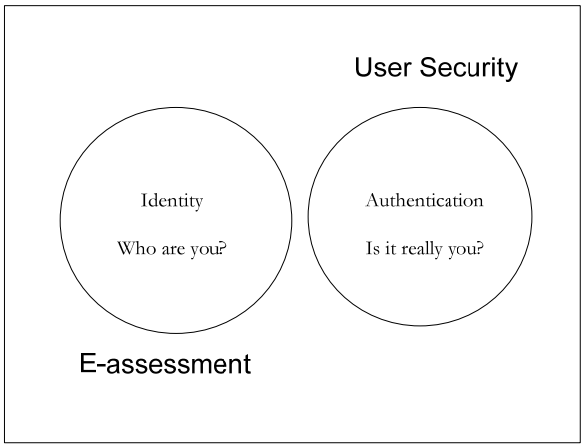

Figure 1. User security in summative e-assessment

3.2. Authentication

In e-assessment, it is insufficient to assume correctness of a student based only on an identity. As depicted in figure 1, the e-assessment security system requires prove that the identity claimed actually belongs to the owner who stored the information. Hence, when the security system solicits an answer to the "is it really you?" question; it simply requests an evidence of the claimed identity. Authentication data is often a secret which should be known to the student and the security system alone. User authentication is a widely discussed subject both in assessment and non-assessment online environments and it is well-researched [12]. In general, user authentication is classified into three categories: (1) Something the user knows (knowledge), (2) Something the user has (possession) and (3) Something the user is (biometrics). Common pairs in e-assessment security depict a username used as a form of identity and one or more of the above authentication methods employed as proof for a claimed identity. By doing this, the user security phase can solicit answers from the students in order to satisfy the requirement of the security system i.e. to ensure that only correct students take the online test.

3.3. The Username and Password Paradigm

In e-assessments, the username/password pair is the most popular and inexpensive method of identifying and authenticating students [45] .The success of the username/password pair is attributed to its ease of use, such that no special device is required for data collection. These have an advantage such that it can be easily implemented using software methods which are conceptually simple for the user to understand. In addition, the students are able to choose an easy-to-remember combination for their convenience [1]. However, Argles *et al* [9] assert

that, when users insist on very short and easy passwords to memorise, a breach in security becomes inevitable. Thus, the simplicity of a password makes it susceptible to a wide range of attacks [18]. A further problem of passwords is that, there is nothing to prevent a legitimate student from sharing their access rights with other people.

Figure 2 depicts a traditional life cycle of a username/password pair. During the registration process, the student registers a username and a unique password for the purpose of the online test. It is essential that the student registration details are linked to module registrations to enable the effective scheduling of online tests to the students. The login process is initiated whenever a student requests access to an online test. The evaluation process validates the identity and authentication responses by comparing the details provided with the stored details. A decision is made at this point and the students are authenticated and allowed access to online test for the entire duration of a test session. If the students are not authenticated, the system determines if a retry will be allowed. The username and password paradigm is perceived to be the preferred method; however, there is need to enhance authentication methods by utilising multiple means of authentication [50]

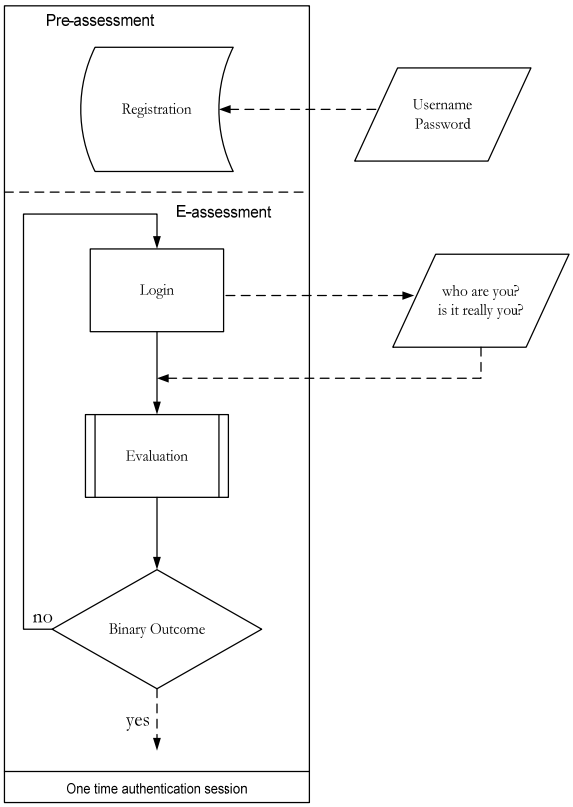

Figure 2. Lifecycle of a username and password pair

3.4. The Biometric Paradigm

Biometrics is a rapidly evolving technology that is used to improve security in a wide range of applications. A biometric architecture consists of the enrolment (user biometric acquired and template is created) and authentication (user biometric data is compared with the stored template) stages. In the quest to implement advanced security measures in summative e-assessment, biometrics is suggested as the ultimate solution for authentication [36]. According to McGinity [37], biometrics systems are simpler and more accurate as an alternative in replacing the conventional password system. The biometric security systems operate in two modes i.e. as an identification or authentication mechanism. A biometric identification system performs a one-to-many match, whilst a biometric authentication is performed against only one possible user [52].

In summative e-assessment security, the fingerprint biometrics is gradually accepted and adopted as a method for student authentication [55]. Employing fingerprints as a method for student authentication requires that an identity is claimed i.e. a username should be associated with the fingerprint. Similarly, if the fingerprints are used for identification, a username can be omitted i.e. the matcher compares the input biometric against all the templates in the database. A biometric authentication system is more common in e-assessments, where biometric fingerprints are used to authenticate the students [23]. The use of fingerprint solutions as against other biometric methods is largely attributed to its convenience. Amidst the potential benefits of biometrics methods; the privacy of the biometric templates is a security concern [26, 44]. Hence, incorporating biometrics for authentication in e-assessment requires that the student's biometric data is kept secret. In our paper [8], we present a method to preserve the privacy of a user's biometric. This method uses an elastic matching algorithm to produce a digest that can be substituted for the raw biometric. Hence, the user's raw biometrics is not exposed during the authentication phase. Biometric template security is beyond the scope of this paper.

3.5. The User Security Model

A summative e-assessment system is perceived as secure, when a student satisfies the identity and authentication security goals. The existing e-assessment user security model (figure 3), is made up of two user security questions and the corresponding techniques for providing responses. It is assumed that, each response method (e.g. password is a member of the goal set) contain an individual level of security. Hence, an intersection of the goal sets (identity and authentication) is sufficient to ensure the security of the summative e-assessments; this is

based on the cumulative security of the response methods. In some e-assessment models, a human invigilator may be required to check a photographic ID card to ensure the correctness of a student. Thus, the invigilator resides in the environment and not included in the goal sets. This is because an invigilator provides an added layer of security for the e-assessment system.

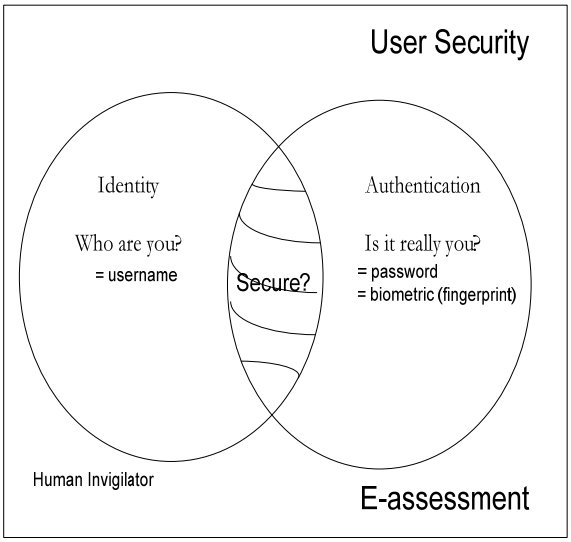

Figure 3. Existing e-assessment user security model

4. Impersonation Threat on User Security

According to the code of practice for the Assurance of Academic Quality and Standards in Higher Education (QAA) for the UK, definitions of academic misconduct in respect of assessment include plagiarism, collusion, impersonation and the use of inadmissible material [42]. In higher education, security considerations do not feature prominently; however, this changes when an online environment is considered [15]. Due to the increased influence of technology in assessments, it is often easier to cheat online [47]. Similarly, the results of a recent study by King *et al* [30], suggests that 73.6% of the students (in the sample population) held the perception that it is easier to cheat in an online course compared to its traditional counterpart. Thus, there exists an increased risk of academic fraud in online assessments versus the traditional assessments. The higher educational sector as constantly focused on plagiarism as a major academic misconduct [40] and there exists an extensive knowledge of plagiarism detectors to curb plagiarism [38]. However, little attention has been given on providing solutions to the other ways of cheating in online assessments.

In generic (non-assessments) online environments, one of the major security challenges to user security is the act of impersonation. Impersonation is a fraudulent action with the aim of imitating a legitimate user and defrauding the security system. For example, in online banking, customers refrain from divulging their assigned login details to prevent others from accessing their bank account. However, there is a possibility that the customer's login details can be stolen, eavesdropped or hijacked without the knowledge of the customer. Thus, when a service is requested, the system grants access to the impersonator believing the details presented originates from the customer. In an approach to minimise impersonation in online environments, the banking industry invest in a second layer of protection to ensure risks are minimised [11].

In e-assessments, the issue of impersonation is considered as a major cause of concern and it is perceived as an even greater risk by the academic community [28]. Weippl [53] assert that students who want to cheat willingly reveal their login details to another person for the purpose of impersonation. Hence, this shows a striking departure from other online environments (e.g. e-banking) where people will not knowingly cooperate with someone who tries to steal money out of their bank account [32]. According to Stoner [49], a student cannot 'accidentally' impersonate another during an online assessment. In traditional (pen and paper) exams, the need to correctly identify a student is well understood and the requirement is to produce a student ID card which includes a photograph. The traditional approach of using a photo ID card and matching it with a student's login details in online environments is generally adopted [51]. This approach provides an added security layer, whereby a human invigilator ensures the correctness of the student taking the test. Based on exiting literature, [10, 23, 48, 56] there exists an implicit consideration of impersonation threats in summative e-assessments. In this section the impersonation threats are classified into three types, namely Type A, B and C.

4.1. Type A impersonation Threat

A tutor/invigilator is assumed trust worthy for the purpose of the online test; however, there exist the possibility of a connived impersonation (a.k.a. Type A impersonation threat). A connived impersonation is the ability of an invigilator to collude with fraudulent students to allow the fraudulent act. A connived impersonation may originate from a sympathetic feeling towards the student and it should not be overlooked especially when the assessment counts towards a student's degree or qualification. For example, if a student has continually failed a certain test, the tutor/invigilator may respond to human emotions and allow another student to take the online test on behalf of the initial student. This type of impersonation can easily go undetected. A

successful connived impersonation reduces the 'equal opportunity' or 'fairness' requirement for all students [22] and it hinders the integrity of the test. In addition, there is a possibility of a connived impersonation for monetary purposes. In this situation, the fraudulent students can influence the invigilator to receiving a large sum of money to help perpetrate the act. Irrespective of the motives for a connived impersonation, it is essential to find methods to minimise such threats in a summative e-assessment system. This paper does not eliminate totally the use of a human invigilator; however, measures should be taken to ensure that the correctness of a student is independent of an invigilator.

4.2. Type B impersonation Threat

The following example introduces a scenario which will be used to illustrate the Type B impersonation threat. This impersonation threat poses the question "is the student really who they say they are?"

Example 1: *Consider that Alice has initially registered for the COMP101 online test. Thus, Alice has an account on the e-assessment system which includes a user profile. Alice's user profile on the database includes her name, date of birth, year of study, registered courses and login details. The online test is scheduled to commence at 10am for the duration of 60mins in the departments' computer laboratory. At 10am on the assessment day, Eva walks into the test room with the knowledge of Alice's login details and other information required. Eva satisfies the identity and authentication goals by inputting Alice's login details. The online security system believes that Alice has requested to gain access to the online test; as a result of a match between the stored login details and the login details presented. However, the security system is oblivious to the swap between Alice and Eva; hence, Eva is not really who she claims to be for the purpose of the online test.*

In the scenario illustrated above, it is directly observed that Alice is absent for the online test; however, Eva has the ability to produce Alice's login details when requested by the security system. In order to analyse the scenario, the identity and authentication paradigms specific to e-assessments are recalled (see section 2). A username and password is classified under the knowledge in which a user has; thus, it can be easily shared amongst users. This academic misconduct can be undetected, especially when the requirement for accessing an online test is a student's username and password alone. However, in past and recent times employing the username and password alone has proven to be the most convenient and popular method in the e-assessment. In exploiting this weakness, students can perpetrate a Type B impersonation threat by not showing up for the test; but sharing their details with another student. It can be argued that, using a tutor/invigilator can curb a Type B impersonation; however, a Type A threat readily comes into mind. By employing a tutor/invigilator in the scenario above, the occurrence of a connived impersonation cannot be totally eliminated.

In order to minimise a Type B impersonation threat it is observed that the problem is peculiar to the *strength of the authentication method*. Employing a username and password paradigm for an online test makes a Type B threat more appealing to impersonators. It is observed that due to the inherent attributes of a password scheme (shareable), it is unable to resist an impersonation threat. In addition, a student's access is authenticated once at the login for the duration of the test session; however, the repeated authentication is performed based on the password cached in the browser [33]. Hence, a method which would increase the difficulty of responses solicited by the security system is required.

Table 1. Type B Impersonation: Password

Authentication	Password
Registration	Alice
Login	Eva
Evaluation	Eva
Implication	Impersonation

4.3. Type C impersonation Threat

In a continuing description from the example above, example 2 illustrates a scenario to depict one approach that can be employed to minimise the Type B impersonation threat. However, the solution presents a potential security challenge which is explained in example 3. Thus, the Type C impersonation threat poses the question "who is there?"

Example 2: *Consider that a biometric fingerprint authentication method is employed for a student login; thus, Alice is required to scan are fingerprint on a capture device and await a positive confirmation before continuing with the online test. This implies that, Alice needs to be present to carry out the login procedure.*

In summative e-assessment, a biometric fingerprint authentication method is suggested as the ultimate solution and it is becoming popular [33, 36]. An advantage of a biometric scheme as opposed to a password scheme is its non-shareable attributes.

Using the scenario above and given a biometric fingerprint method for login, it is impossible for Alice to provide Eva with a finger to gain access to the test. This implies that, during enrolment Alice has enrolled her fingerprint and a template is stored in the database alongside her user profile. Thus, access to the online test can only be granted when there is a match between the raw biometric fingerprint presented and the stored template. It is suggested that adopting this method will deter the impersonators and the impersonated students from the act. Hence, using a biometric method, Alice will be obliged to take the online test herself instead of employing Eva.

Example 3: *It is assumed that Alice, successfully gains access to the online test; hence, the security system believes that Alice has initiated the request due to a match between the scanned fingerprint and the stored template. At a certain time t during the duration time T of the online test, Eva takes over Alice's test. However, at these times the security system is unaware of the academic misconduct; hence Eva is the student seated there instead of Alice.*

In example 3 above, it is observed that there is an increase in the difficulty of the authentication challenge; thus, Alice's physical presence is required to carry out the login procedure. Additionally, it is observed that there exists a possibility for Eva to take over Alice's test after the login procedure. Hence, the responsibility of the e-assessment user security does not terminate at ensuring the correctness of the student; rather, it extends to verifying that the correct student is there taking the test for the period of time. As pointed out in recent studies [5, 23, 27], a major problem of the summative e-assessments is the inability to know who is there taking the exam i.e. to know if the correct student is there taking the exam or someone else has taken over the test on their behalf.

Table 2. Type B Impersonation: Fingerprint

Authentication	Fingerprint
Registration	Alice
Login	Alice
Evaluation	Alice
Implication	Correct Representation

5. Revisiting the User Security Model

One aims of this paper is to investigate the sufficiency of the existing e-assessment user security model in ensuring that only correct students take an online test for the allocated duration of the test. Based on a qualitative review of existing literature on user security during online tests, it can be summarised that impersonation threats is a major challenge in summative e-assessment systems. The existing user security model requires that a student identity and authentication goals only are satisfied prior to accessing the online test; thus, this implies that the student accessing the test is the correct student. However, it is observed that the authenticated student is sometimes not the expected student or the expected student begins a test but does not complete it. Hence, it is concluded that the existing e-assessment user security model is insufficient to ensure that only the correct students take an online test for the allocated duration of the test (figure 4).

In an attempt to address this issue, this paper suggest that satisfying the identity and authentication security goals only is not enough to assure user security during summative e-assessments. Much more is required to ensure that the authenticated student is the expected student and that the correctly authenticated student is taking the online test un-assisted for the duration of the test time. Thus, there is a need for an improved e-assessment model which is sufficient to ensure that only the correct students take an online test for the allocated duration of the test. This paper proposes that, one of the ways to assure correct user security during online tests is to combine the presence goals (and non-intrusive continuous authenticated presence) with the existing identity and authentication security goals. This implies that a student will be required to satisfy the presence (and non-intrusive continuous authenticated presence), identity and authentication security goals prior to and during the online tests. In this section, the e-assessment security assets, threats and security goals are proposed

5.1. E-assessment Security Assets

An asset refers to something that is valuable which needs to be protected [25]. In this paper, it is suggested that the valuable assets of a summative e-assessment system extend beyond the hardware, software and data needs. It should be noted that, the importance of the hardware, software and data assets are not discarded; however, assets specific to user security is considered. A foundation for our proposal exists on the constructivist perspective of e-learning. Based on the existing learning theories, assessment in a constructivists approach forms an integral part of the learning process [24]. Thus, in a constructivist's mind, the student plays the centre role in the learning process. According toWild [54], in e-learning the constructivist's focus is not wholly on the course

content but rather on the student. Hence, in a student-centred approach, the students need to be correctly assessed and securely authenticated in the e-assessment environment. In addition, a summative e-assessment system is perceived busy when delivering an online test and a student taking a test depicts an activity on the system. Thus, it may be pointless to develop an online summative assessment system if the students' participation is excluded. A student taking a test is an indispensable component of the e-assessment system; hence, it is proposed that a student is a valuable asset of the e-assessment user security process [7].

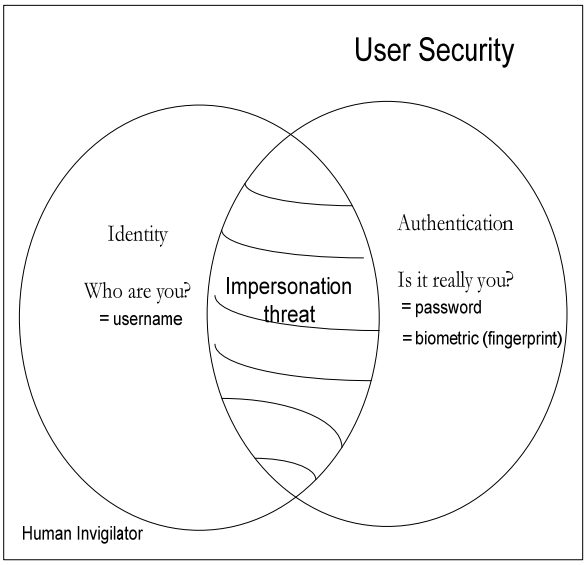

Figure 4. Impersonation threat

5.2. E-assessment Security Threats

A threat is the potential for misuse/abuse of an asset that will cause harm in the context of the system [20]. The level of harm that can occur depends on the asset type; thus, it is appropriate to identify the relevant threats that may apply to each asset type. For example, the storage of assessment data in a university may be under threats from unauthorised exposure and unauthorised alteration. A major threat plaguing the summative e-assessment user security is the threat of impersonation. As described in section 4.1, the Type A impersonation threat can be minimised by ensuring that the correctness of a student is independent of an invigilator; similarly, the Type B impersonation threat is overcome by employing a strong authentication method. However, it is noted that a Type C impersonation threat presents a greater security challenge than its counterparts.

One aim of the Type C impersonation threat is to subtly permit an incorrect and illegal student to take an online test on behalf of the correct student. Thus, a successful impersonation (threat) launched on a student (asset) will reduce the credibility of the online test (harm) in an e-assessment context. Hence, the security system is required to set security goals which can be used to protect the students from impersonation threats. Simultaneously, the e-assessment system is also secure from the fraudulent act. In the C-I-A goal model, the interception threat is an attack on confidentiality; the modification threat is an attack on integrity and the interruption threat attacks availability. Similarly, the threat of unauthorised exposure is converted to the goal of protection from unauthorised exposure, commonly known as confidentiality [39]. Hence, the threat of impersonation is converted to the goal of protection from impersonation, known as presence, i.e. an impersonation threat is an attack on presence. It is concluded that the exclusion of the presence security goal in online summative tests will increase impersonation threats in summative e-assessments.

5.3. E-assessment Security Goals

A goal can be interpreted differently, based on the diversity in job descriptions. For example, a goal would mean different things to a footballer, psychologist, engineer etc. In general, a goal expresses what is desired. It can also refer to a specific, measureable occurrence that any business or system plans or intends to achieve or avoid. According to Haley *et al* [19] security goals are presented in form of a desire and they aim to protect the assets from harm (threats). In computer system security, the confidentiality, integrity and availability security goals ensure that the hardware, software and data assets of a system are not compromised (see section 2). This implies that a compromise in the C-I-A security goals may lead to a compromise of the critical assets.

During summative e-assessment, the C-I-A security goals can be employed to protect the e-assessment system's hardware (PC), software (assessment application) and data (item bank) from potential interception, modification, interruption and fabrication threats. However, it is proposed that the C-I-A security goals are unsuitable to protect the e-assessment security asset from its potential threat [7]. In generic computer security, the people who use or maintain particular applications on a computing system are examples of the valuable assets to the organisational system [41]. This key people are carefully selected because of their skills and potential value to the organisation. For example, a problem would occur if one of the key people decides to leave the organisation (taking away the knowledge) and no other person can fill the position. Based on this description, it is observed that the key people do not depend directly on the C-I-A security goals; instead they would be required to satisfy other goals, e.g. trustworthiness. Hence, we suggest that the C-I-A

security goals are not entirely suited for human assets due to their unpredictable attributes.

In another perspective, it is impractical for a student to satisfy the C-I-A security goals. For example in computer security systems, it is commonplace to apply the C-I-A goals to the data asset; thus, producing data confidentiality, data integrity and data availability. In particular, confidentiality protects the data item from interception, integrity protects from modification and availability protects from interruption. However, applying the C-I-A goals to the student (asset) produces student confidentiality, student integrity and student availability. These terms are defined respectively: student confidentiality refers to privacy of a student's personal information, health records or educational records, which an institution is not required to disclose without prior consent of the student. Student integrity describes an honourable and ethical conduct which is expected from every student during an online test. The student integrity code can be written as a set of policies and sanctions relating to the student's academic conduct during an assessment. Finally, student availability requires that the student is there when needed to take an online test. This paper, does not disregard the importance of the C-I-A security goals; however, security goals specific to e-assessment user security is defined. Hence three security goals of e-assessment user security (figure 5) are proposed:

1. **Presence and continuous authenticated presence:** This reflects a state of a student being at a specific space or place. Only correct and legal students are required to be present for an online test. Continuous authenticated presence ensures that only correctly authenticated students are continually present (from start to finish) for the duration of the test and taking the test un-assisted.
2. **Identity:** This is a distinct attribute which differentiates a student from other students in a given population (e.g. a student's username in a database)
3. **Authentication:** This provides a proof of the identity claimed by a student.

6. Existing E-assessment Solutions

In this section, we summarise existing solutions which addresses the presence security goal in summative e-assessments. We classify these methods under five headings and analyse their suitability in minimising the impersonation threats. Finally, a table which is based on the examples is presented (see table 3).

6.1. Invigilated/Proctored only

Invigilation is the act supervising, monitoring or watching students during a test. In online environments, Rovai [47]; Rowe [48]; Weippl [53] amongst others advocate for the use of human invigilators as a good low-technology means of promoting both identity and academic honesty. According to Harrison [21], impersonation of one student by another is thought to be unlikely when a test is taken under the eye of an invigilator. Hence, adopting an invigilated test environment is the obvious solution to ensure the correctness of a student taking an online test. However, the use of an invigilated testing only environment is susceptible to a Type A impersonation threat i.e. a connived impersonation. A successful connived impersonation attack creates a success route for a Type C impersonation to be perpetrated. Thus, as long as a connived impersonation goes undetected, there exists a likely occurrence of impersonation threats and academic misconduct.

6.2. Uni-modal Biometric Scheme

Most biometric systems deployed in summative e-assessment applications are unimodal; thus, they rely on the evidence of a single source of information for authentication e.g. single fingerprint or face recognition. In their work, Levy & Ramim [33] propose a theoretical approach of using fingerprint biometrics solution for student authentication whilst Agulla *et al* [2] suggest that a face recognition solution is a more secure alternative to conventional authentication mechanisms. These unimodal biometric solutions are commonplace during student login; hence, they are better suited to solve a Type B impersonation threat. Employing unimodal biometric methods to solve a Type C impersonation threat is not practically trivial, as the random authentication of the student will be required for the duration of the test. The random authentication of a student is one feasible approach to solving the Type C impersonation threat; however, it can be perceived as a means of distraction during the test. In an attempt to minimise the impersonation threats by employing a non-distractive unimodal biometric solution, Kikuchi *et al* [29] propose a real-time periodic authentication scheme using biometric handwriting-based samples. Though, behavioural biometrics has been associated with a low error rate in lab settings; further work is required to improve robustness for large scale systems [34]. Moreover, there are limitations imposed on unimodal biometric systems, which can be overcome by multimodal biometrics [46, 27, 50]

6.3. Bimodal Biometric Schemes

Rabuzin *et al*, [43] asserts that it is necessary to combine several different biometric traits in order to implement absolute security in e-learning systems. Thus, adopting multi-biometrics can increase the reliability of the user security beyond the initial student login process and provide ongoing non-intrusive verification for the duration of test session [14, 34]. In literature, few papers exist on the emerging technology of multi-biometrics in e-learning security. Asha & Chelleppan [10], propose the combination of biometric fingerprint recognition with mouse dynamics. In their model, the use of the fingerprint scanner to statically authenticate a user is suitable to solve the Type B impersonation threat; however, minimising the Type C threat using the mouse dynamics is unclear. Ahmed & Traore, [3] asserts that, the data capturing process for mouse biometrics requires some considerably time to accomplish. Hence, for an online test the student is delayed until the data acquisition process is completed; this presents a window to perpetrate a Type C impersonation. Levy & Ramim, [34] propose a theoretical model which combines a fingerprint and web-camera head geometry scanner. Employing this model depicts a promising solution to minimise the Type B and C impersonation threats. However, the paper focused on user acceptance of the technology rather than the actual practical implementation of the solution.

6.4. Video Monitoring of Student

Video monitoring is a proven technology for security monitoring. According to Lin *et al* [35], a promising approach to ensure security during online tests is the monitoring of student activities via video images. Thus, Ko & Cheng [32], propose a secure internet examination system based on random video monitoring. A username and password mechanism is adopted which makes the system susceptible to a Type B impersonation threat. Employing video monitoring, suggests that an invigilator/tutor is required to watch the students taking the test live or view the streaming video at any time. In the first option the invigilator /tutor is obligated to seat at the screen for the duration of the test in order to pick out any unusual activity. A disadvantage is that an invigilator may look away or get distracted whilst watching the screen. The second option depicts a more realistic approach to adopting video monitoring in online tests. Thus, a suspicious grade may imply a suspicious identity; hence, the video footage is retrieved. However, watching a set of video sequences to extract anomalous behaviour may become an extra administrative task.

6.5. Biometric Authentication and Webcam Monitoring

Hernandez *et al*, [23] propose fingerprint recognition to authenticate the students and a webcam which monitors the students in real time for the duration of the test. In their work, an authenticated student is monitored at the beginning of a test whilst the test is terminated when another person is in control. Employing fingerprint recognition is suitable to solve the Type B impersonation threat; however, the use of a webcam to provide dynamic authentication or to control student identity is unclear. Additionally, the security of the suggested model breaks when the student turns the view of the webcam to another

7. Discussion and Conclusion

Based on the results in table 3, it is observed that any solution void of a biometric authentication is insufficient to minimise any of the threats. However, not all the solutions which incorporate a biometric can be used to curb the three types conveniently. Nevertheless, bimodal biometric solutions possess a potential to minimise all threat types to a satisfactory degree. It should be noted that the suitability of a bimodal biometric solution for e-assessment depends largely on the individual biometrics adopted. Lastly, we do not reject any of the existing solutions; rather we suggest that an appropriate blend of the methods will minimise the impersonation threats and improve user security in summative e-assessments.

In this paper, we have explored the existing user security model of a summative e-assessment system. We suggest that the identity and authentication security goals of the existing model are insufficient to ensure security of the student (asset) against impersonation threats. Hence, we propose a user security model which incorporates presence (and continuous presence), identity and authentication security goals. In this paper, we have taken a departure from generalising impersonation threats and have classified the threats into Type A, Type B and Type C. In our analysis, we conclude that a Type A threat can be avoided when the correctness of a student is not totally dependent on a human invigilator. Additionally, minimising a Type B threat rely on the strength of the authentication method adopted. However, solving a Type C impersonation threat is non-trivial. A review of the existing solutions depicts a strong potential towards the use of bimodal biometrics to curb all types of impersonation threats. An example of a bimodal solution is the combination of fingerprint and face recognition techniques. It is assumed that such multi-biometric systems will provide security and deter Type C impersonation threats. However, we suggest

that a bimodal biometric only solution will be highly sensitive in an e-assessment environment. By this we mean that, there exist typical student behaviours that present low risks to e-assessment security; however, such behaviours are seen as anomalous to a biometric system. Examples of typical student behaviours during a test include, placing the head on a desk, leaning to a side of the desk (out of camera view), covering a face with the hand (occlusion) or looking around. Thus, a multi-biometric only system that uses fingerprint for authentication and the face for monitoring may request a re-authentication when typical behaviours are exhibited. It should be noted that there exist some unacceptable student behaviours which presents a breach in security. An example is a student swapping places and a bimodal solution is suitable to deter such unwanted behaviours. However, we want to guard against false re-authentication requests which suggest that the student is no longer there; when indeed the same student is still taking the test.

One of the functionalities of a summative e-assessment system is to provide secure exams that are void of intrusions. Hence, a student's test should be uninterrupted for the duration of the test except in explicit situations. We conclude that, re-authentication requests from a multi-biometric solution which is based on false alarms will reduce the system to a uni-modal biometric solution i.e. authentication is done periodically or randomly during the test. A research direction would be to provide steps that will employ a bimodal biometric solution at a later stage during monitoring. A potential solution will be to incorporate a low level technology at the initial stage of the monitoring process. It is suggested that a low level approach will effectively manage the low-risk acceptable student behaviour without the need for a constant re-authentication. Thus, in the event of an increased risk (e.g. unacceptable behaviour) a high level technology can be employed. This implies that a student intrusion can only occur when it is absolutely necessary. Figure 6 depicts an example of a summative e-assessment architecture which employs a low-level object tracker to monitor the student's presence. The authentication module presents a fusion at the score level to ensure student correctness at the start of the test. The tracking module calculates the difference between the video frames to provide the location and position of the student. The information from the tracker is fed into the classifier module to determine the student risk levels at different times during the test.

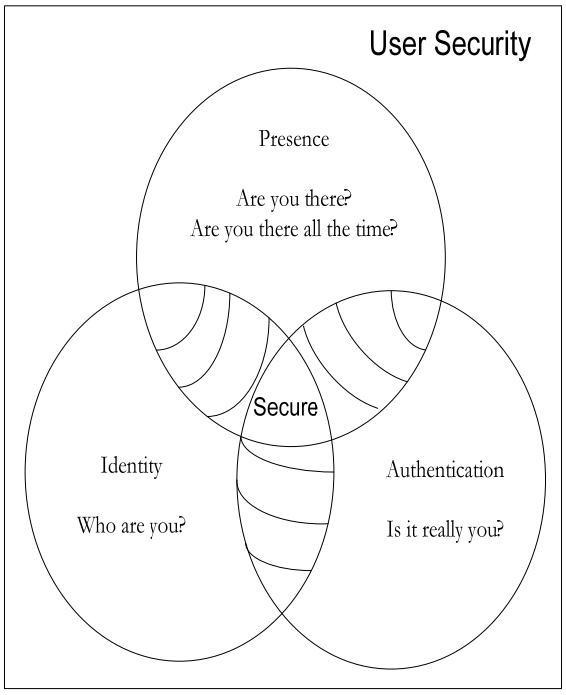

Figure 5. The relationship between presence, identity and authentication

8. References

[1] Adams, A., Sasse, M. (1999). 'Users Are Not The Enemy: Why users compromise Computer Security mechanisms and how to take remedial measures,' *Communications of the ACM*, vol. 42 (12), pp. 41-46

[2] Agulla, E.G., Rifon, L.A., Alba castro, J.L., Mateo, G.C (2008) 'Is my student at the other side? Applying Biometric Web Authentication to E-learning Environments'. ICALT 2008: The 8th IEEE International Conference on Advanced Learning. Spain.

[3] Ahmed AAE., Traore, I. (2007). 'A new Biometric Technology based on Mouse Dynamics', IEEE *Transactions on Dependable and Secure computing* 4(3), pp 165–179.

[4] Allen, J., Barnum, S., Ellison, R., McGraw, G., Mead, N. (2008). *Software Security Engineering: A Guide for Project Managers*, Addison Wesley

[5] Aojula, H., J. Barber, R. Cullen., J. Andrews. (2006). 'Computer-based Online Summative Assessment in Undergraduate Pharmacy Teaching' *Pharmacy Education* **6**(4): 229-236.

[6] Apampa, K. M., G. B. Wills, Argles, D. (2008). 'Electronic integrity issues in e-assessment security'. ICALT 2008: The 8th IEEE International Conference on Advanced Learning, Spain.

Table 3. Threats and existing solutions

Solution category	Type A Impersonation	Type B Impersonation	Type C Impersonation	Example Reference
Invigilated only environment	No	No	No	21, 48, 53
Unimodal biometric	Yes	Yes	No	2, 29, 33
Bimodal biometric	Yes	Yes	Strong potential	10, 34
Video monitoring (+password)	No	No	No	32
Biometric + webcam monitoring	Yes	Yes	No	23

Yes: solution can minimise or solve impersonation threat
No: solution is susceptible to impersonation threat

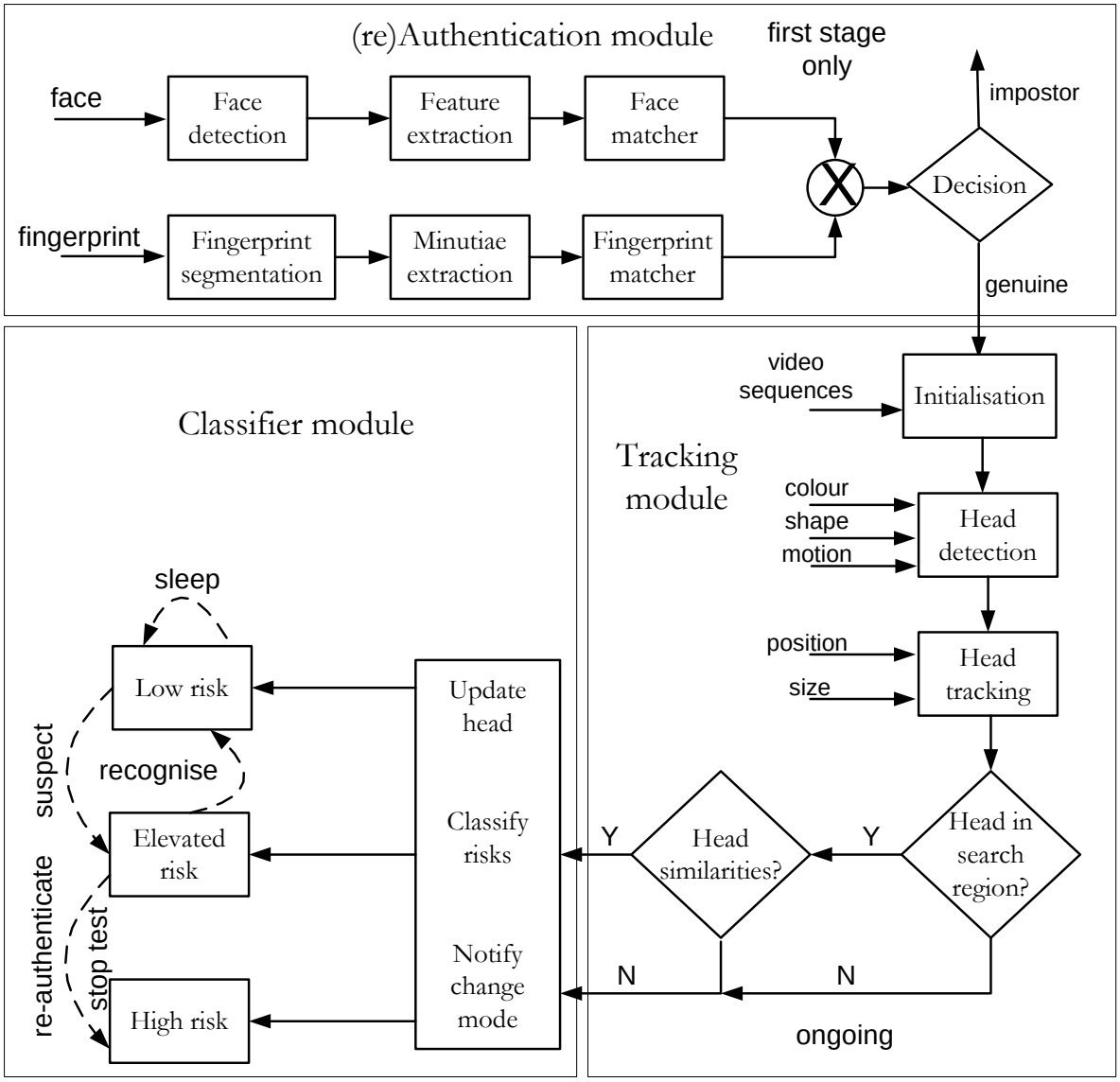

Figure 6. Summative e-assessment security architecture

[7] Apampa, K. M., Wills, G. B. and Argles, D. (2009) 'Towards Security Goals in Summative E-Assessment Security'. ICITST-2009*:* The 4th International Conference for Internet Technology and Secured Transactions, London, UK.

[8] Apampa, K. M., Zhang, T., Wills G.B., Argles, D. (2008). 'Ensuring Privacy of Biometric Factors in Multifactor Authentication Systems', SECRYPT 2008: International Conference on Security and Cryptography (ICETE). Portugal.

[9] Argles, D., Pease, A. and Walters, R. J. (2007) 'An Improved Approach to Secure Authentication and Signing. FINA 2007: International Symposium on Frontiers in Networking with Applications, Canada.

[10] Asha, S., Chellappan, C**.** (2008). 'Authentication of e-learners using multimodal biometric technology' ISBAST: International Symposium on Biometrics and Security Technologies, Islamabad.

[11] Bailie, J. L., & Jortberg, M. A. (2009). 'Online learner authentication: Verifying the identity of online user's. MERLOT *Journal of Online Learning and Teaching*, 5(2), 197-207.

[12] Basu, A., Muylle, S. (2003). 'Authentication in Electronic Commerce', *Communications of the ACM* 46(12), pp. 159–166.

[13] Challis, D. (2005). 'Committing to quality learning through adaptive online assessment', Assessment in Education 30(5): 519-527.

[14] Clarke, N.L., Furnell, S.M (2007). 'Advanced User Authentication for Mobile Devices', *Computers & Security*, 26(2), pp.109-119

[15] Furnell, S., P. Onions, U. Bleimann, M. Knahl, H. Rder, P. Sanders. (1998). 'A security framework for online distance learning and training', *Internet Research* 8(3): 236-242

[16] Gilbert, L., Gale, V., Wills, G. and Warburton, B. (2009). JISC Report on E-Assessment Quality (REAQ) in UK Higher Education. Technical Report, University of Southampton, UK.

[17] Gollman, D. (2006). *Computer Security*, West, John Wiley & Sons, Ltd. Sussex, England

[18] Goyal V, Kumar V, Singh M, Abraham A, Sanyal S. (2005). CompChall: Addressing Password Guessing Attacks. ITCC'05: IEEE International Conference on Information Technology: Coding and Computing.

[19] Haley, C. B., Laney, R. C., Moffett, J.D., Nuseibeh, B. (2008). 'Security Requirements Engineering: A Framework for Representation and Analysis,' *Transactions on Software Engineering (IEEE)* 34(1) pp. 133-153

[20] Haley, C. B., Laney, R. C., Nuseibeh, B. (2004). 'Deriving Security Requirements from Crosscutting' Software Development (AOSD'04). Lancaster, UK: ACM Press pp. 112-121.

[21] Harrison, G (2004) 'Computer-based Assessment Strategies in the Teaching of Databases at Honours Degree Level 1'. H. Williams and L. MacKinnon (Eds.): BNCOD 2004, LNCS 3112, pp. 257–264, 2004, Springer-Verlag Berlin Heidelberg 2004

[22] Heinrich, E., Milne, J., & Moore, M. (2009). 'An Investigation into E-Tool Use for Formative Assignment Assessment – Status and Recommendations', *Educational Technology & Society*, 12 (4), 176–192.

[23] Hernandez, J.A., Ortiz, A.O., Andaverde, J., Burlak, G. (2008). 'Biometrics in Online Assessments: A Study Case in High School Students'. CONIELECOMP: 18th International Conference on Electronics, Communications and Computers., Puebla

[24] Holt, D. G. & Willard-Holt, C. (2000). 'Lets get real – students solving authentic corporate problems'. *Phi Delta Kappan* .pp 82

[25] ISO/IEC (1999) 'Information Technology - Security Techniques - Evaluation Criteria for IT Security – Part' *Introduction and General Model*, 15408-1. Geneva, Switzerland.

[26] Jain, A. K., K. Nandakumar, Nagar, A. (2007). 'Biometric Template Security', *EURASIP Journal on Advances in Signal Processing*, Hindawi Publishing Corporation.

[27] Jain, A.K., Ross, A., Prabhakar, S. (2004). 'Special Issue on Image- and Video-Based Biometrics', IEEE *Transactions on Circuits and Systems for Video Technology*, 14 (1)

[28] Kerka, S., Wonacott., M. (2000) 'Assessing Learners Online', Practitioner File. ERIC, ED 448285.

[29] Kikuchi, S., Furuta, T., Akakura, T. (2008) 'Periodical Examines Identification in e-Test Systems using the Localized Arc Pattern Method'. The Distance Learning and Internet Conference 2008, Tokyo

[30] King, C.G., Guyette, R.W., & Piotrowski, C. (2009). 'Online exams and cheating: An Empirical Analysis of Business Students Views', *The Journal of Educators Online*, *6*(1).

[31] Klett, F., Pharow, P. (2006) 'How to Achieve User Satisfaction in Complex E-Learning Environments', *ITHET'07:* 7th International Conference on Information Technology Based Higher Education and Training Sydney.

[32] Ko, C. C., Cheng, C. D. (2004) 'Secure Internet Examination System Based on Video Monitoring'. *Internet research* 14(1): pp. 48–61

[33] Levy, Y., Ramim, M. (2007) 'A Theoretical Approach For Biometrics Authentication of E-Exams', Chais Conference on Instructional Technologies Research, The Open University of Israel, Raanana, Israel.

[34] Levy, Y., Ramim, M. (2009) 'Initial Development of a Learners' Ratified Acceptance of Multibiometrics

Intentions Model (RAMIM)', *Interdisciplinary Journal of E-learning and Learning Objects* (IJELLO).

[35] Lin, N.H., Korba, L., Yee, G., Shih, T., Lin, H.W (2004). 'Security and Privacy Technologies for Distance Education Applications', AINA: 18th International Conference on Advanced Information Networking and Applications

[36] Marais, E., D. Argles, von Solms, S.H (2006). 'Security Issues Specific to e-Assessments', 8th Annual Conference on WWW Applications, Bloemfontein.

[37] McGinity, M. (2005). 'Staying connected: Let your fingers do the talking'. *Communications of the ACM*, 48(1) pp. 21-23.

[38] McLafferty, C. L., Foust, K. M. (2004). 'Electronic Plagiarism as a College Instructor's Nightmare Prevention and Detection: Cyber dimensions. *Journal of Education for Business*, 79(3) pp.186-190.

[39] Moffett, J. D., Nuseibeh, B. (2003) 'A Framework for Security Requirements Engineering', Department of Computer Science, YCS368. University of York, UK.

[40] Naude, E., Hörne, T. (2006). 'Cheating or collaborative work: Does it pay?' Issues in Informing Science and Information Technology, 3(1) pp. 459-466.

[41] Pfleeger, C. P., S. L. Pfleeger (2003). *Security in Computing*, Upper Saddle River, Prentice Hall, New Jersey.

[42] Quality Assurance Agency (2000), 'Section 6: Assessment of Students'; http://www.qaa.ac.uk (12 Dec 2008)

[43] Rabuzin, K. Baca, M. Sjako M. (2006). 'E-Learning: Biometrics as a Security Factor'. ICCGI: International Multi-Conference on Computing in the Global Information Technology, Bucharest.

[44] Ratha, N. K., S. Chikkerur, Connell, J.H, Bolle, R.M. (2007). 'Generating Cancelable Fingerprint Templates', *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29(4): 561-572

[45] Rodwell, P. M., Furnell, S. M., & Reynolds, P. L. (2007) 'A Non-intrusive Biometric Authentication Mechanism Utilising Physiological Characteristics of the Human Head', *Computers and Security*, 26(7) pp. 468-478.

[46] Ross, A., Jain, A.K (2003) 'Information Fusion in Biometrics', *Pattern Recognition Letters*, 24(13) pp. 2115-2125

[47] Rovai, A. P. (2000). 'Online and Traditional Assessments: What is the Difference?', *The Internet and Higher Education* 3(3) pp.141-151.

[48] Rowe, N. C. (2004). 'Cheating in Online Student Assessment: Beyond Plagiarism', *Online Journal of Distance Learning Administration* VII (II).

[49] Stoner, G. (1996) 'Implementing Learning Technology' *Learning Technology Dissemination Initiative*. Heriot-Watt University, Edinburgh

[50] Tsalakanidou, F., Malassiotis, S., & Strintzis, M. G. (2007) 'A 3D Face and Hand Biometric System for Robust User-friendly Authentication'. *Pattern Recognition Letters*, 28(16), 2238-2249.

[51] Vollans, T. (2008) 'The Law School with two Masters?', *Web Journal of Current Legal Issues*.

[52] Wayman, J.L (2001) 'Fundamentals of Biometric Authentication Technologies', *International Journal of Image and Graphics*, 1(1) pp. 93-113.

[53] Weippl, E. R. (2005). 'In-depth tutorials: Security in e-learning', *eLearn Magazine*.

[54] Wild, M. (2007). 'Third Generation eLearning', Nine Lanterns Pty Ltd

[55] Williams, J. M. (2002). 'New security paradigms'. Proceedings of the 2002 Workshop on New Security Paradigms, Virginia,

[56] Wisher, R. Curnov, C., Belanich, J. (2005) 'Verifying the Learner in distance learning', 18th Annual Conference on Distance Teaching and Learning 2005

