

Original Research Article

Addressing Impersonation Threats in Online Assessment Environment Using Temporal Information and System Interactions

^{*1}Kinoti Patrick, ²Dr. Sylvester O. McOyowo and ²Dr. Henry O. Okoyo

Abstract

¹Kenya Methodist University, Faculty of Computing and Informatics

²Maseno University Kenya, Faculty of computing and Informatics

*Corresponding Author's E-mail:
kinotshi@yahoo.com

Online learning mediated by ICT is fast growing in popularity worldwide. There is need to consider modes of assessment using ICT tools which are flexible given that candidates can take assessments anywhere and possibly anytime. However, the main challenge when conducting online assessments is the imminent impersonation threat. It is difficult to know if the correct candidate is the one taking the exam or someone else is taking examination on their behalf. Impersonation threats have been classified into three types: Type A, B, C and this study introduces type D. Majority of existing online assessments systems employ one time authentication using passwords but they are prone to impersonation challenges given that the candidate may willingly share this information with another person to take exam on their behalf. More is required to verify the identity and presence of an authenticated student for the whole examination duration. Potential approaches apply continuous scan of biometrics but they are incapable of addressing concealed impersonation or Type D threats. This proposed Temporal Information and System Interaction (TISI) model will not only address all the four type of impersonation but will also minimize the human involvement.

Keyword: Assessment, Impersonation, Verification

INTRODUCTION

The advancement of Information Communication Technology (ICT) within the previous decades have seen most of learning institutions embrace online learning for supporting education which is flexible for distance learners. However, the existing online learning courses do not offer great flexibility for the learners as they ought to (JISC, 2006). One of the reasons is that most of the e-learning courses operate on the calendar of conventional classes. The students must physically sit for the examination paper or manual exams on the institutions premises or designated testing centers. However, accessing such premises may be difficult for a distance learner. An innovative approach through online assessments promises to provide the required flexibility

to a distance learner. Adopting online assessments in a higher education environment embodies enormous other benefits such as, automatic marking, immediate feedback to students, and opportunities for lifelong learning and improved access for disabilities or geographically dispersed students. But, getting a completely trustworthy online assessment environment that is able to protect examination standards is a major roadblock to its implementation.

Trustworthy electronic assessment has been cited as one of the most difficult challenges in online learning (Maria, 2010). When students score well in an online assessment, does that mean that they know the subject that much? Educators must face the fact that some

students will always look for ways of cheating in an exam given the importance attached to passing exams. The relevance of the assessment process to any academic institution implies that different security mechanisms must be applied in order to preserve some security and academic standards during assessments stages so as to ensure that online assessments builds trust that student performance on exams are an accurate representation of learning and not a result of cheating (Ramu, 2013).

Assessment

Educational assessment is the process of documenting, usually in measurable terms, knowledge, skills, attitudes, and beliefs. Assessment can focus on the individual learner, the learning community (class, workshop, or other organized group of learners), the institution, or the educational system as a whole (Sindhu S, 2013). Assessment does not generally mean testing a student's competence in a subject; however, the use of examination, oral test, essays, quiz and projects are methods of assessing competencies (Knight, 2001). The assessment is at the heart of a learning process.

Online assessment

Online assessment is presented as an alternative to traditional assessments where the assessment task is delivered and displayed on a computer screen via the network. According to the Joint Information Systems Committee (JISC), online assessment is the end-to-end electronic assessment processes where ICT is used for the presentation of assessment activity, and the recording of responses. Brown (1996) suggests that due to paradigm shift in educational technology, it may become unfair to train students online and then use pens for assessments. Thus, in order to provide an alignment between the teaching, learning and assessment processes, it is essential to employ the use of ICT in assessment (Gipps, 2003).

Cheating in Online Assessments

Cheating can be defined as a transgression against integrity which entails taking an unfair advantage that results in a misrepresentation of a student's ability and grasp of knowledge. In the online assessment context, this includes obtaining inappropriate assistance either from an online source, copying from physical material, plagiarism and impersonations. Cheating in examinations is a vice that must be discouraged due to the fact that students who cheat are not likely to have acquired skills necessary for them to use in their professions.

Exams are a measure of qualification increasingly relied upon to gauge an individual's knowledge, skills and abilities. The results of these exams are used by managers for employment decisions and by government agencies and the general public when seeking qualified professionals. Graduating incompetent professionals is likely to cause damage to the society, as incompetent professionals may produce work that fails or even endanger human life like in case of incompetent doctors.

The value attached on examination results have brought in threats to the security and validity of the assessment process. Candidates who are not well prepared and/or unqualified may be tempted to seek credentials through any fraudulent means such as cheating in exams. Furthermore, some students feel it is very necessary to cheat to get ahead of other students in today's competitive environment and it can be argued that, some student take online classes to enhance their chances of being able to cheat (Bedford, 2011). Educators must face the fact that students will always look for ways of cheating in an exam given the importance placed on passing exams and also in quest to get ahead of others in job market.

A major problem when conducting online 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 (Wisher et al, 2005; Aojula et al, 2006; Levy & Ramim, 2007; Hernandez et al, 2008). This has informed this study to focus on impersonation threat.

Impersonation Threat in Online Environment

Identity and presence verification is meant to address impersonation threats. 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 (Ramu, 2013). There exists an implicit consideration of impersonation threats in online assessments (Wisher et al, 2005; Hernandez, 2008; Ramu, 2013). According to Maria (2010) impersonation threats can be classified into three types, namely Type A, B and C. This study introduces Type D impersonation threat which can even be more difficult to detect and address. The types are as below:

Type A Impersonation Threat

A connived impersonation is the ability of an invigilator to collude with fraudulent students to allow the fraudulent act. For example, the tutor/invigilator may respond to human emotions of assisting a poor student or due to financial gains to allow another student to take the online test on behalf of the right candidate. This type of impersonation can easily go undetected.

Type B Impersonation Threat

This impersonation threat poses the question “is the student really who they say they are?” Impersonation threat occurs when the real student pass his security information to a fraudulent, who use them to answer the exam on their behalf. Systems that only use username-password pairs are susceptible to this type of threat. However, strength of authentication method and use of biometrics can reduce this threat.

Type C Impersonation Threat

Impersonation threat occurs when the correct student logs in, and then lets fraudster to continue with the exam on his/her behalf. Even if a system is using biometrics approaches such as fingerprint and other stronger authentication mechanism, they can still be susceptible to type C threat. Much more is required to ensure that the correctly authenticated student is one taking the online examination for the whole duration of the examination. One biometric trait such as fingerprints may be insufficient for correctly authenticating test taker for the whole duration due to high likelihood of failed authentication. Approaches that use a combination of biometrics such as face and fingerprints or keystroke dynamics can reduce this threat.

Type D Impersonation threat

Impersonation threat occurs when there is concealed or no observable user information such as their biometrics. A fraudster may take advantage of lack of user information to trick the system that the candidate has left the station and answer the exam. Thus, there is a need for an improved online assessment system which is sufficient to ensure that only the correct students take an online test for the allocated duration of the examination.

Schemes for Addressing Impersonation in online assessment

There are many schemes that have been adopted by institutions of learning for addressing impersonation challenges in online assessment environment. However, they have shown various limitations in addressing all types of impersonation threats.

Human Invigilators

Traditionally, examinations have relied on human invigilators to supervise in order to maintain standards. In human supervised environment and with proper controls,

it is difficult for impersonation to take place. But, it is not feasible for online assessment for as the number of student studying online continues to increase, the human invigilator may not be able to monitor large number of candidates taking exam at the same time who are geographically dispersed. Secondly, institutions have contracted external invigilators to supervise examinations in centers due to logistical challenges. This may create an opportunity for impersonation type A threat in which a rogue invigilator may collude with a candidate to allow another person to take exam on his/her behalf either for financial gain or due to human sympathy to assist weak candidate.

Username and Passwords

In recent past, automated systems have been adopted but they typically authenticate candidate only at the initial log-in session using user names and passwords. As a result, it is possible for another user, to access the system resources, with the permission of the signed-on user and take examination hence Type B impersonation threat.

Biometric Authentication

The process of authentication has always relied on verifying association between a person and one of either something the user knows (e.g password), something the user has (smart card) and something the user is (e.g biometrics). The first two involves logical or physical secrets which are subject to theft and identity transfer while the third, which is the use biometrics, is difficult to steal or transfer. In general the authentication methods can be divided into three categories according to Yousef (2011): knowledge factor which entails something the user knows, ownership factor which specifies something the user possesses and inherent factors which includes something the ‘user is’ such as facial image, fingerprint, DNA and something the user does such as typing rhythms.

Biometrics is defined as the identification of an individual based on physiological and behavioral characteristics (Qinghai, 2012). Commonly used physiological characteristics include face (2D/3D facial images, facial IR thermogram), hand (fingerprint, hand geometry, palmprint, hand IR thermogram), eye (iris and retina), ear, skin, odor, dental, and DNA. Commonly used behavioral characteristics include voice, gait, keystroke, signature, mouse movement and pulse. Uses of biometrics are ultimate solutions for authenticating candidate because they rely on physical characteristics that may not be transferable (Yousef, 2011). The most commonly used biometrics for authentication are the fingerprints, A special device which might be a portable

Table 1. Summary of existing schemes and their weaknesses.

Approaches	Impersonation Threats Types				Major Weakness
	Type A	Type B	Type C	Type D	
Human Invigilated	No	Yes	Yes	Yes	-Susceptible to connived impersonation -Not feasible for many online system.
Passwords and smart cards	Yes	No	No	No	-Passwords can be passed to fraudulent candidate.
Unimodal Biometrics	Yes	Yes	No	No	-There is likelihood of many failed verification due to candidate posture, movements, tiredness.
Bimodal Biometrics	Yes	Yes	High Potential	No	-Susceptible to concealed impersonation.

Yes: solution can minimize or solve impersonation threat

No: solution is susceptible to impersonation threat

fingerprint scanner with USB connector is required to scan users imprints and compare with the fingerprint pattern already on the database as captured during registration of candidate. Some laptops and some personal computers already have inbuilt fingerprint scanners. Employing knowledge factors such as biometrics is surest way to address Type B impersonation threat but the scheme may be susceptible to Type C impersonation threat in which the right candidate is correctly authenticated but leaves another person to complete the examination. To address Type C impersonation threat, continuous re-scan of the candidate's biometrics throughout the test session is required.

Majority of biometrics technique relies on single physical characteristics such as finger prints and are referred to as unimodal. Unimodal biometric authentication are effective for authenticating candidate (Is it really you?) and if randomly and/or periodically applied can be a feasible approach for solving the type C impersonation threat. A bimodal biometrics can even be more effective in tackling all forms of impersonation threats. An example of a bimodal solution is the combination of fingerprint and face recognition techniques. Based on that, studies by Jeffrey (2009) and Koichiro (2010), proposes use of a combination two biometrics such as fingerprints and facial recognition as opposed to unimodal biometrics. One challenge of techniques that employ biometrics is that it is expensive in computations given that the signal processing and pattern recognition algorithm involves computation and comparison of biometrics (Koichero, 2010). For one time authentication, the corresponding latencies is not a major concern, but for continuous authentication the concern is substantial. Secondly, employing technologies that can lead to frequent re-authentication requests may become interruptive and distracting to a student (Yousef, 2011) especially if the student is constantly requested for fingerprints for rescanning. Passive authentication such as face recognition is desirable because the system does not require candidate active cooperation to be

authenticated continuously.

Keystroke Dynamics

Monrose and Rubin (2000) proposed the use of keystroke dynamics which is based on measurements and analysis of dynamic aspect of user keyboard interaction and Fliors and kawalski (2010) discusses keystroke dynamics as a method of providing continuous biometric user authentication that can address Type C impersonation Threat. Keystroke dynamics authentication (KDA) proposes that typing rhythm is different from one user to another. One advantage of keystroke dynamics is that, unlike the fingerprint biometrics is less interruptive and also requires less computation than the other biometrics. However, one disadvantage of KDA is the differences that occur over time as a result of changes in typing pattern, tiredness of hands and improvement of skills (Fayyoumi, 2014).

In summary, biometric authentications provide great potential for candidate verification in online assessment and several studies on this topic have been published (Terence S, 2007; Jeffrey, 2009; Koichiro, 2010; Yousef, 2011). Biometric authentication can successfully deal with type A and B threat and if correctly applied, may also address type C impersonation threat which requires continuous user authentication. For a continuous user authentication to be user friendly, passive authentication (e.g., face recognition) is desirable because the system should not require users' active cooperation to authenticate users continuously. In addition, a single biometric trait (unimodal technique) is not sufficient to authenticate a user continuously because the system sometimes cannot observe the biometric information. For example, the systems will not be able to capture a user's face image if he turns his head away from the monitor. In general, to address the limitations of single biometrics, using multimodal biometrics (combining two or more single biometrics, e.g., face and iris) is a good solution. (Table 1)

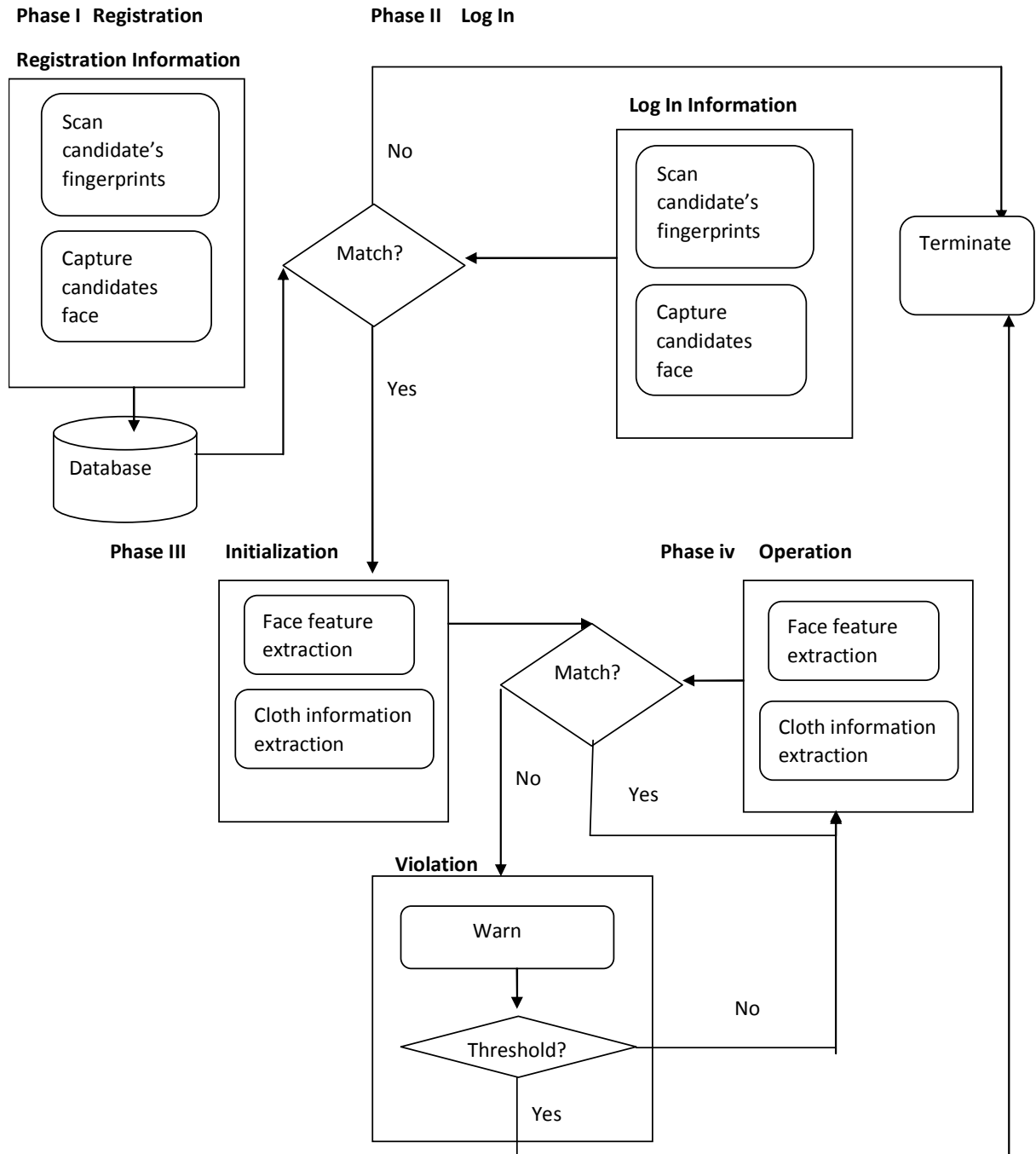


Figure 1. Proposed TISI Model: Kinoti Patrick (2015)

Temporal Information and System Interactions (TISI) Model

The study proposes a model for later implementation; that recognizes the identity of candidate in online assessment, continuously verify their presence status and take necessary action to stop or discourage any kind of impersonation. Specifically, the model proposes methods of dealing with impersonation Type D which was not previously envisioned by previous studies. The model

is inspired by studies by Koichero (2010) who proposed use of soft biometrics such as face color and color of clothing and Fayyoumi (2014) on modification of user behavior through warnings. (Figure 1)

Candidate registering for examination will have their fingerprints and face image taken and stored in a database. During examination, the log in system will verify the candidate's identity by comparing their fingerprints and face with the one in the database. Afterwards, the system will automatically register the

distinguishable features of face and color of clothing and then store the features as a template for continuous verification. The system then continuously applies matching algorithm of the two features throughout the session with the stored information templates. The face features and clothes color are not expected to change during the assessment duration. A sudden change of the face features during the session can be concluded as impersonation. Loss of face features for example when the candidate changes posture such as looking sideways but clothes color information is available, will trigger the system to issue warnings to discourage the behavior. A complete loss of the two features is taken to mean that the candidate has abandoned the exam workstation. This creates an opportunity for Type D impersonation Threat in which a fraudster may conceal his/her presence or abstract the camera to disguise that the candidate has left in order to take the exam on their behalf. In such event, the system should respond by disallowing any activity on the assessment system until correct biometrics is available. However, the loss of biometrics can also be as a result of normal human behavior of movements or misread by sensors. The loss of biometrics is timed and systems issues warnings to discourage candidate movements. A certain threshold will automatically trigger locking of the assessment system which may require another verification process using fingerprints and stored face.

CONCLUSION

The TISI Model has been proposed for later validation and implementation as part of ongoing research. The model represents an easy to use, efficient and cost effective technique for addressing all types of impersonation in online assessments. The model is efficient for it eliminates the need for real time streaming and continuous matching is only based on enrolled templates as opposed to using information in database hence may not require very high bandwidth connectivity. It will be cost effective due the fact the distance learner do not require to purchase additional hardware for surveillance but rather the system uses existing webcams in the computers and it is a completely automated solution meaning it reduces the degree of human involvements in supervising examinations. Lastly, the interactive feedbacks and clear procedures make the system easy to use and this allows the candidate to concentrate on answering exam questions. The actual techniques of feature extraction taking to consideration the performance and efficiency of the system will be extensively explored.

REFERENCES

- Bedford DW, Gregg JR, Clinton MS (2011). Preventing online cheating with technology: A pilot study of remote proctor and an update of its use. *J. Higher Edu. Theory and Practice*, Vol 11 (2), Pg 41-59.
- Fabian M, Aviel DR (2000). Keystroke Dynamics as Biometrics for Authentication, *Future Generation Computer Systems* 16, pp. 351-359.
- Fayyoumi A, Zarrad A (2014). Novel Solution Based on Face Recognition to Address Identity Theft and Cheating in Online Examination Systems. *Advances in Internet of Things*, Vol 4(02), Riyadh, Saudi Arabia, Pg 5-8.
- Gipps C (2003). What is the role of ICT-based assessment in university? *Studies in higher education*. Volume 30, Issue 2, 2005, Kingstone, UK. Pg 171-180.
- Hernandez JA, Ortiz AO, 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
- Jeffrey LB (2009). Online Learner Authentication: Verifying the Identity of Online Users. *Merlot Journal of Online Learning and Teaching*. Vol. 5, No. 2, June 2009.
- Joint Information Systems Committee (JISC) (2006). "Effective Practice with online assessment" An overview of technologies, policies and practice in further and higher education. Roadmap for online assessment Report for JISC (Open University, 2006), London UK. Pg 10-20.
- Koichiro N, Klosterman (2010). "Soft biometric traits for continuous user authentication. *IEEE Transactions on Information Forensics and Security*". Volume 5, Issue 4 Pg 771-780.
- Maria Apampa, Gary W (2010). "Security Issues in summative Online assessment Security", *International Journal of Digital Society (IJDS)*, Vol 1, Issue 2, London UK. Pg 135-142.
- Matus K (2010). Behavioral Detection of Cheating in Online Examination; Master's Thesis Information Systems science Lulea University of Technology 2010. ISSN 1402-1552.
- McCabe DL, Butterfield KD, Trevino LK (2006). Academic Dishonesty in Graduate Business Programs: Prevalence, Causes, and Proposed Action. *Academy of Management Learning and Education*, Vol. 5, Iss. 3, pp. 294-305.
- Qinghai G (2012). Biometric authentication to prevent e-cheating. *International Journal of Instructional Technology and Distance Learning*. ISSN 1550-6908 vol 9 no 2.
- Sindhu S (2013). ICT Based Assessment in schools: Teachers Attitude. *Conflux Journal of Education* ISSN 2320-9305 Volume 1, Issue 2.
- Ramu T, Dr. Arivoli (2013) Online Exam Authentication: An alternative to traditional exam. *International Journal of Scientific Research*, Volume 4, issue 11, November 2013, ISSN 2229-5518.
- Terence S, Sheng Z, Rajkumar J, Sandeep K (2007), "Continuous Verification Using Multimodal Biometrics," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 29, no. 4.
- Wisher R, Curnov C, Belanich J (2005) 'Verifying the Learner in distance learning', 18th Annual Conference on Distance Teaching and Learning 2005.
- Yousef Sabbah, ImaneSaroit (2012). Synchronous Authentication with Bimodal Biometrics for online assessment, A Theoretical Model. The 6th International Conference in Sciences of Electronics, Technologies of Information and Telecommunications (SETIT) (2012). Tunisia .Pg 1-5.