Asian Journal of Information Technology 14 (5): 166-175, 2015
ISSN: 1682-3915
© Medwell Journals, 2015

Review of User Authentication Methods in Online Examination

Nader Abdel Karim and Zarina Shukur
National University of Malaysia, Selangor, Malaysia

Abstract: User authentication is a very important online environment issue. Further, investigation is needed to focus on improving user authentication methods for the sake of improving e-Learning security mechanisms; especially in the field of online exams. This study is the result of a systematic literature review which will answer the following three main questions of online exam user authentication methods, systems and threats. The results cover four main directions. First, it shows complete authentication methods that have been used in online exam systems; whether they are classified as knowledge, possession or biometric based. Second, it summarizes the online exam systems and authentication techniques used whether they are classified as user identification, authentication or continuous authentication. Third, it explores the threats that may occur during exam sessions and specifically classifies impersonation threats. Finally, it investigates existing commercial user authentication products that are used to observe online exams.

Key words: User authentication, online examination, authentication methods, online exam threats, online exam authentication system

INTRODUCTION

Internet use has led to an increased use of the World Wide Web which is a computer technology invention that has changed the mode of human communication and information sharing. A new concept that has emerged from the World Wide Web is that of getting educated about the web (e.g., e-Learning) (Alavi and Leidner, 2001; Takahashi *et al*., 2005). e-Learning can lead to a better future as we advance in all areas of science that are needed in this modern life the global e-Learning market is projected to reach $107.3 billion by 2015; according to a new report by the global industry analyst. Therefore, e-Learning tools need to be enhanced with effective and reliable security mechanisms to ensure that this medium can be dependable.

Examinations as a major part of education are a key activity of student learning (Apampa *et al*., 2010). An examination (or exam) is an official test that shows knowledge or ability in a particular subject. Two assessment approaches are used in online examination environments, namely summative and formative. Summative assessments evaluate learning outcomes, whereby student's skills are measured against learning goals using a set of assessment techniques (Ramu and Arivoli, 2013). When summative assessments are focused on grading or classification, students are likely to do their best to obtain good grades and appear competent in comparison with their peers (Gathuri *et al*., 2014). Formative assessment is usually used to survey feedback of learner's activities and record progression. This assessment does not count towards final results or grades and this characteristic possibly decreases security risks in online learning environments (Ullah *et al*., 2012). Therefore, in online examinations, summative assessments may be in more serious danger of misuse due to its high-stakes such as cheating, impersonation threats, etc. Chula G. King's research study shows that 73.6% of students thought that it was easier to cheat online than in traditional courses (King *et al*., 2009) in the authentication of online exam takers, it is very important to make sure that the exams are given fairly (Ullah *et al*., 2012), user authentication is a widely discussed subject in online environments (Basu and Muylle, 2003) and online exams follow identifications such as username, password and biometric identification (Sarrayrih and Ilyas, 2013). In general, user authentication is classified into three main categories: something the user knows known as knowledge based authentication (e.g., password, PIN, pattern), something the user has known as possession based authentication or token (e.g., ATM card, smart card, mobile phone) and something the user is known as biometric based authentication (e.g., biometric characteristics such as fingerprints and face). This study explores the existing and potential authentication techniques that can be used in an online environment to protect exams from potential threats.

SYSTEMATIC LITERATURE REVIEW

To survey existing state of the art associated online exam authentication methods, a Systematic Literature Review (SLR) was performed utilising the procedures mentioned by the EBSE technical report

Corresponding Author: Nader Abdel Karim, National University of Malaysia, Selangor, Malaysia

(Kitchenham and Charters, 2007). For the purpose of our research, we pose the following research questions:

- Question 1: What existing authentication methods/techniques can be used to authenticate users in online exams?
- Question 2: What potential user authentication threats affect online exams?
- Question 3: What are the existing solutions related to implementing online exam user authentication?

This review was performed on several scientific digital libraries and databases in English. The publishing date range was defined as June 2004 through to the end of November 2014. The focus was established as articles identified with online exam authentication or threats. All other insignificant articles were omitted. The scientific digital libraries and databases searched were Scopus, Springer link, IEEE Xplore, Science Direct, ACM and Google Scholar. The search keywords used in the above-mentioned digital libraries is as given below:

- {Online exam, e-Exam, e-Assessment} authentication methods
- Authentication of online examination
- {Authentication, verification} of {online exam, e-Exam, e-Assessment}
- {Online exam, e-Assessment, e-Exam} threats
- Biometric authentication of {online exam, e-Assessment, e-Exam}

Table 1: Number of found articles

Database name	No. of articles	Filter based on title	Filter based on abstract
Scopus	65	30	21
IEEE xplore	42	28	23
Springer link	87	19	9
Science direct	52	11	3
ACM	123	15	4
Google scholar	434	123	68

The search was initiated in November 2014. Table 1 shows all results related to each source. The selection of study involved multiple phases. First, possible relevant articles were identified using search strings and then the publication's article titles and abstracts were screened. As a result, a huge number of publications were omitted; based on their insignificance to the research questions. Next, if there was any doubt about the potential publication's inclusion, the full paper would be obtained for further evaluation (Kitchenham and Charters, 2007).

Full content scanning was performed on the last set of journals. Thus, a set of publications was involved in the review, depending on its relevance to the research questions and clearance of their objectives and methodology. The total number of papers used in this review (after removing search redundant and missing information papers) was 54 articles.

DATA EXTRACTION

This study shows several samples of the data extraction. Table 2 summarizes some of collected literatures within four sections; namely method, description of proposed method and strength and weakness of each proposed method.

Table 2: Sample of data extraction

Author/Year	Method	Description	Strength	Weakness
Al-Saleem and Ullah (2014)	Use palm print in addition to user name and password	A new authentication scheme that incorporates username/password with palm-based biometrics. A video capturing technique will also be merged by the system	Good for authentication during the login phase. Merge knowledge based authentication (username, password) with biometrics based authentication (palm print)	Unimodal biometrics are susceptible to impersonation threats (Apampa *et al*., 2010). Need additional hardware for palm print scanning
Ramu and Arivoli (2013)	Use keystroke dynamic in addition to username and password	The researchers proposed system is comprised of two layers of student authentication using biometric authentication (keystroke) in addition to username and password	Can use as continuing and transparent authentication. There is no need for additional hardware	Unimodal biometrics are susceptible to impersonation threats (Apampa *et al*., 2010)
Ullah *et al*. (2012)	Use challenge questions	The researcher proposed a new approach known as Profile Based Authentication Framework (PBAF). Challenge questions are used to authenticate online examination students	Easy to implement and there is no need for additional hardware	Susceptible to impersonation threats because it is considered KBA (easy to share)
Gao (2012)	Use IP address with timestamp	The researcher proposed a new method to monitor student activities using students' IP addresses and timestamps to assist and detect possible cheating behaviour	Easy to implement and there is no need for additional hardware. Allows the examiner to single out cheating online exam suspects	Susceptible to impersonation threats, if the imposter uses the same machine. IP Address can be changed easily
Rudrapal *et al*. (2012)	Use voice recognition	The researcher proposed to use voice recognition through a microphone so that the user can register for online exams	It can be used for continuous authentication of online users. Can be helpful for people who are blind or people who don't use a keyboard for interaction with the system	Unimodal biometrics are susceptible to impersonation threats (Apampa *et al*., 2010)

Table 2: Continous

Author/Year	Method	Description	Strength	Weakness
Bal and Acharya	Use Iris recognition	Biometric authentication and tracking system based on iris recognition	Iris identification is considered one of the most robust ways to identify humans (Bal and Acharya, 2011)	Unimodal biometrics are susceptible to impersonation threats (Apampa *et al*., 2010) Privacy problem of iris templates in the biometric system database (Gao, 2012; Zviran and Erlich, 2006). Storage problems for a huge amount of data. Need a special camera to scan the eye's iris
John, Stewart Monaco, Cha and Tappert	Use keystroke dynamic and stylometry	The researchers investigate keystroke and stylometry biometric systems with the aim of developing a system of authenticating (verifying) test-takers' identities in an online environment	Bimodal biometric authentication system. Can provide continuous and random authentication. No need for additional hardware	Stylometry system has shown limited and inadequate applicability to test-takers Susceptible to impersonation threats (Apampa *et al*., 2010)
Apampa *et al.* (2010)	Use fingerprint and face recognition	The researchers proposed a multibiometric authentication system combination of fingerprint and face recognition techniques. The system re-authenticates when typical behaviours are exhibited	Using multimodal biometric will enhance the security level. The system re-authenticates when typical behaviours are exhibited. Fingerprints are considered a robust way of identifying humans	Need special hardware (fingerprint scanning enabled devices). Privacy problem of fingerprint templates in the biometric system database (Gao, 2012; Zviran and Erlich, 2006). Storage problems for a huge amount of data
Flior and Kowalski (2010)	Use keystroke	The researchers try to present a method for providing continuous biometric user authentication in online examinations via keystroke dynamics	It can be used for continuous authentication of online users No need for additional hardware	Unimodal biometrics are susceptible to impersonation threats (Apampa *et al*., 2010)
Penteado and Marana (2006)	Use face recognition	The author tries to investigate the accuracy of face recognition; captured on-line using a webcam	It can be used for continuous authentication of online users. No need for additional hardware	Unimodal biometrics are susceptible to impersonation threats (Apampa *et al*., 2010) Storage problems for a huge amount of data
Asha and Chellappan	Use fingerprint and mouse movement	The researchers proposed an authentication system with multi-biometrics (fingerprints, mouse movement) to support various e-Learning services	Uses bimodal biometrics. Fingerprints are considered a robust way of identifying humans Can be used for continuous user authentication (mouse movement)	Need special hardware (fingerprint scanning enabled devices) Privacy problem of fingerprint templates in the biometric system database Storage problems for a huge amount of data
Ko and Cheng (2008)	Using Zip disk (token) to secure e-Test	The researchers proposed a secure and reliable examination system that depends on a single zip disk. This system only requires a simple stand alone computer for the taking of a test and provides a secure and reliable examination platform. The system provides security through encrypting all data and student registration files and checks the unique network card address of the PC on which the test is being run	Depends on a special token that the user must have All students' data (within Zip disk) is encrypted	Susceptible to impersonation threats; the Zip disks can be shared easily Needs special hardware (Zip disk). Can only applied in the lab
Kikuchi, Furuta and Akakura	Using handwriting biometric	The researchers try to authenticate exam takers who use pen tablets that depend on a handwriting biometric	The method can only be applied on pen tablets	Unimodal biometrics are susceptible to impersonation threats (Apampa *et al*., 2010) Needs a special hardware (pen tablet)
Levy and Ramim (2007)	Using fingerprint	The researcher uses fingerprint biometrics on e-Exam and investigates its effect on the exam-taker's grade and length of exam time	Fingerprints are considered a robust way of identifying humans	Unimodal biometrics are susceptible to impersonation threats (Apampa *et al*., 2010) Need special hardware (fingerprint scanning enabled devices) Privacy problem of fingerprint templates in the biometric system database Storage problems for a huge amount of data

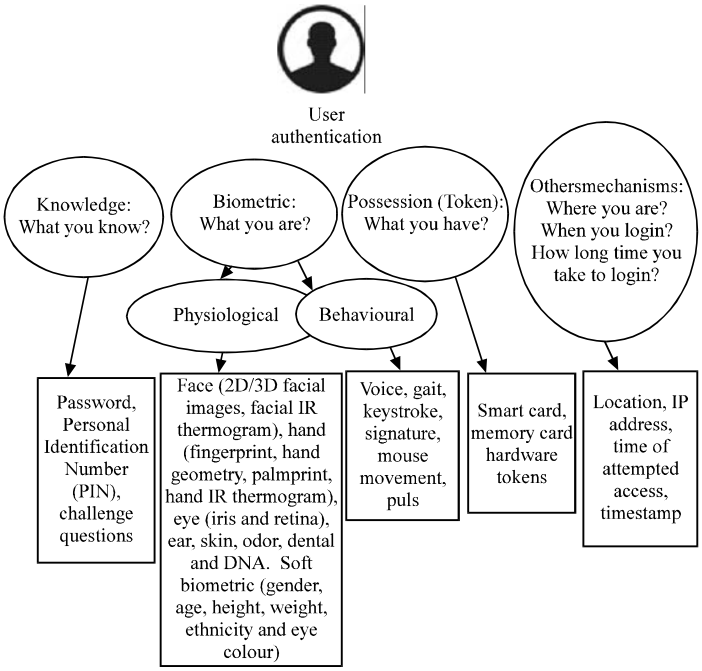
User
authentication
Knowledge: What you know?
Biometric: What you are?
Possession (Token): What you have?
Othersmechanisms: Where you are? When you login? How long time you take to login?
Physiological
Behavioural
Password, Personal Identification Number (PIN), challenge questions
Face (2D/3D facial images, facial IR thermogram), hand (fingerprint, hand geometry, palmprint, hand IR thermogram), eye (iris and retina), ear, skin, odor, dental and DNA. Soft biometric (gender, age, height, weight, ethnicity and eye colour)
Voice, gait, keystroke, signature, mouse movement, puls
Smart card, memory card hardware tokens
Location, IP address, time of attempted access, timestamp

Fig. 1: Online user-authentication methods with its techniques

DATA ANALYSIS

This study addresses the analysis of the systematic review results. Figure 1 represents the answers found regarding research question 1: What existing authentication methods/techniques can be used to authenticate users in online exams?

Figure 1 shows the classification of available authentication methods that can be used in online examinations in addition to several examples of each method.

AUTHENTICATION AND IDENTIFICATION

Most computer systems are protected through a process of user identification and authentication (Zviran and Erlich, 2006). Identification is typically non-private information provided by the user to identify him/her and can be known by other system users (e.g., name, user ID, E-mail address). Authentication provides secret and private information. Authentication methods can be classified into 3 types:

Knowledge based authentication: The most widely used types of authentication are knowledge-based (Zviran and Erlich, 2006), commonly referred to as KBA as a method of authentication that seeks to prove the identity of someone accessing a service such as a website. KBA requires the knowledge of private information of an individual to grant access to protected material. User ID, password and challenge questions are a commonly used. KBA is a common authentication method because passwords are memorable inexpensive, simple to use and attractive to users (Ullah *et al*., 2012; Zviran and Erlich, 2006). However, due to the nature of online examinations, students may share their login credentials to third parties to boost their grades. Hence, online examinations rely on a knowledge base that is susceptible to collusion and malicious attacks (Ullah *et al*., 2012). KBA can be summarized as the following statement: what the user knows.

Possession based authentication (token): Authentication based on private objects that the user has is referred to as Possession-Based Authentication (PBA) or token-based authentication. PBA includes tokens and tickets. A token is typically a hardware device that can be stored in a pocket or on a key chain and carried with the user. However in general, presentation of a valid token does not prove ownership because it may have been stolen or duplicated by sophisticated means (Zviran and Erlich, 2006). Based on the nature of online exams, PBA can be useful if the exam is conducted in a specific place such as a university lab or in accredited testing centres, etc. However, if the exam is conducted at home or in an uncontrolled environment, PBA is useless. The most common examples of PBA are memory cards, smart card tokens, dongles and keys (Flior and Kowalski, 2010; Zviran and Erlich, 2006) and can be summarized as the following statement: what the user has.

Biometrics based authentication: Biometrics is a rapidly developing technology that is used to improve security in a wide range of applications (Apampa *et al*., 2010). It is also defined as the identification of a user that depends on physiological and behavioural characteristics (i.e., what the user is). Behavioural biometrics are based on the user's behavioural attributes that are considered as learned movements (Zviran and Erlich, 2006). Commonly used physiological characteristics include face (2D/3D facial images, facial IR thermograms), hand (fingerprints, hand geometry, palm prints, hand IR thermograms), eye (iris and retina), ear, skin, odour, dental and DNA. Commonly used behavioural characteristics include; voice, gait, signature, mouse movement, keystroke and pulse (Gao, 2012; Zviran and Erlich, 2006). Biometrics can be classified as soft biometrics or hard biometrics. Soft biometrics, e.g., clothing colour, voice, skin, hair colour, signature, height and tattoos are able to be easily changed (Marcialis *et al*., 2009). They can still be used to identify a person quickly but they cannot be used as very firm features (Khan *et al*., 2011) as they exhibit a low discriminant power for recognizing persons (Marcialis *et al*., 2009). Meanwhile, hard biometrics including facial features, fingerprints, palm prints, retinas, iris and vein patterns as strong features for identifying a person. They are not easily changed in a short time (Gao, 2012).

Biometric authentications are technically complex and usually expensive because they require special hardware (Zviran and Erlich, 2006). Biometric authentication systems contains two stages of enrolment (user biometrics acquired and template created) and authentication (user biometrics data is compared with a stored template) (Apampa *et al*., 2010; Gao, 2012). Biometrics are quite secure but not widely accepted by users because they are perceived as intrusive and a violation of personal privacy. In biometric systems, biometric data has to be saved in a centralized database or distributed on smart cards. Potential biometrics users are reluctant to give out their biometrics data because they are worried how their biometrics data will be used for what purpose and whether their biometrics data will be protected adequately (Gao, 2012; Zviran and Erlich, 2006). The appearance of biometrics solved the problems that plagued traditional authentication methods (Gao, 2012; Zviran and Erlich, 2006). They provide the most effective and accurate identification methods because they cannot be easily stolen or shared. Biometric systems can enhance user convenience by lessening the need to design and remember passwords (Ives *et al*., 2004).

Several other authentication mechanisms are able to assist the authentication process such as location, time stamp, IP address and time of attempted access. A brief summary of available identification and authentication techniques that can be used in online examinations are given in Table 3. Table 3 shows the techniques and classifications in addition to the roles that can be played by the techniques in an online examination environment. Finally, a brief description and several example references are given.

Table 3: Identification and authentication techniques used in online exam environments

Technique	Technique type	Technique role (online exam)	Description	References example
User_id	Knowledge	User identification	Based on private information supplied by the user	Al-Saleem and Ullah (2014), Bhagat and Katankar (2014), Ramu and Arivoli (2013), Sarrayrih and Ilyas (2013), Sheshadri *et al*. (2013) and Ullah *et al*. (2012)
Password	Knowledge	User authentication	Based on private information supplied by the user	Al-Saleem and Ullah (2014), Bhagat and Katankar (2014), Ramu and Arivoli (2013), Sarrayrih and Ilyas, (2013), Sheshadri *et al*. (2013) and Ullah *et al*. (2012)
Challenge questions	Knowledge	User authentication	Based on private information supplied by the user	Ramu and Arivoli (2013) and Ullah *et al*. (2012)
IP address	Other mechanism*	Location authentication	Can be used to identify the possible location of a user. IP address (together with timestamp) can be used as indicators of possible cheating behaviour during exams	Gao (2012), Ramu and Arivoli (2013) and Sarrayrih and Ilyas (2013)
Timestamp	Other mechanism*	Time authentication	Used to know at which time the exam session started	Gao, Ko and Cheng
Mouse movement	Biometric	User authentication	Behavioural characteristics. Can be used in continuous authentication	Asha and Chellappan, Dehnavi and Fard and Korman
Keystroke dynamics	Biometric	User authentication	Behavioural characteristics. Can be used in continuous authentication	Flior and Kowalski (2010), Kumlander (2008), Ramu and Arivoli (2013) and Sabbah *et al*. (2012)
Face recognition	Biometric	User authentication	Physiological characteristics can be used in continuous authentication	Anusha and Soujanya (2012), Apampa *et al*. (2010) Saevanee *et al*. (2012), Fayyoumi and Zarrad (2014) and Penteado and Marana (2006)

Table 3: Continous

Technique	Technique type	Technique role (online exam)	Description	References example
Fingerprint	Biometric	User authentication	Physiological characteristics. Can be used in continuous user authentication; if it is included with other devices such as fingerprint scanning mouse (Alotaibi, 2010; Levy and Ramim, 2007)	Apampa *et al.* (2010), Gao (2012), Levy and Ramim (2007), Sabbah *et al.* (2012), Sarrayrih and Ilyas (2013) and Sheshadri *et al.* (2013)
Iris recognition	Biometric	User authentication	Physiological characteristics	Bal and Acharya
Video monitoring	Other mechanism*	User presence authentication	Can be used in continuous presence authentication	Al-Saleem and Ullah (2014), Ko and Cheng (2004) Sabbah *et al.* (2012) and Sarrayrih and Ilyas (2013)
Soft biometric	Biometric	User authentication	Gender, age, weight, height, skin colour, clothing colour	Khan
Smart card, memory card and zip disk	Possession	User identification	Based on private objects that the user possesses. May be stolen or duplicated by sophisticated means	Ko and Cheng (2008)
Voice	Biometric	User authentication	Behavioural characteristics. Voice verification using a microphone. Can be used as continuous authentication	Rudrapal *et al.* (2012)
Signature	Biometric	User authentication	Behavioural characteristics	Bhagat and Katankar (2014)
Stylometry	Biometric	User authentication	Behavioural characteristics. Determines authorship from the linguistic styles of the researchers	Krause and John Stewart
Webcam	Other mechanism*	User presence authentication	Can be used in continuous presence authentication	Rao *et al.* (2011)
Eye tracking	Biometric	User authentication	Eye feature tracking for validating users	Song
Brain waves	Biometric	User authentication	ERP (Event Related Potential). Signals used to explain the cognitive information process. Can be used to show differences between e-Learning users	Song
Handwriting	Biometric	User authentication	There are two types of handwriting-based authentication: one based on static information (letter width, density) and one based on dynamic information (x and y coordinates, writing speed, writing pressure and pen angle). Can be applied to online exams using pen tablets or touch screens	Kikuchi
Palm-print	Biometric	User authentication	Physiological characteristics. Needs additional devices to scan (palm print scanning device)	Al-Saleem and Ullah (2014)
Microphone	Other mechanism*	Environment authentication	Can be used to monitor the exam session environment	Rao *et al.* (2011)

*Other mechanisms equate to other authentication methods that may help in user authentication that are not classified as knowledge, possess or biometric based authentications such as user location, IP address, time of attempted access and timestamp in addition to user presence authentication techniques such as webcam and video monitoring

Table 4 shows 38 proposed online-exam user authentication systems with their techniques. From Table 4, we can see that fingerprint and face recognition techniques in addition to keystrokes, user_id and passwords are the most popular authentication techniques used in this field.

Online exam user authentication threats: In order to answer research question 2: What potential user authentication threats affect online exams? Table 3 represents a general illustration of the answers found.

According to the code of practice for the Assurance of academic quality and standards in higher education (QAA) in the UK, the meanings of academic misconduct in respect of assessment include plagiarism, collusion, impersonation and the use of inadmissible material (Bellingham, 2008). In general, one of the major security challenges to user security in online environments; especially in online exams is the action of impersonation (Apampa *et al*., 2010; Rao *et al*., 2011). Impersonation is considered to be a fake action with the aim of duplicating an authentic user and defrauding the security system. In an online exam, the issue of impersonation is considered the most important cause of concern and is therefore, considered to be a greater risk by the academic community (Apampa *et al*., 2010). Based on the literature by Rowe (2004), there is a significant possibility of impersonation threats during online exams.

Table 4: The proposed online-exam user authentication systems and their authentication method

	References										
Authentication techniques	Qinghai	Apampa *et al.* (2010)	Khan	Dehnavi and Fard	Levy and Ramim (2007)	Bal and Acharya	Ullah *et al.* (2012)	Alotaibi and Alotaibi and Argles	Gao (2012)	Flior and Kowalski (2010)	Sabbah *et al.* (2011)
User_id							X				
Password							X				
Challenge questions							X				
IP address	X										
Mouse movement				X							
Keystroke				X						X	X
Face recognition		X	X	X							
Finger print		X			X			X	X		X
Iris recognition						X					
Video monitoring			X								X
Webcam											
Soft biometric			X								
Voice recognition											
Policy dissemination (Moten *et al.*, 2013)											
Stylometry											
Eye tracking											
Brain waves											
Handwriting											
Palm-print											
Microphone											
Timestamp	X										
Zip disk											
Signature											
Photo image											

	References									
Authentication techniques	Asha and Chellappan	Saevanee *et al.* (2012)	Sarrayrih and Ilyas (2013)	Korman	Ko and Cheng (2004)	Agulla	Moten *et al.* (2013)	John C Stewart	Fayyoumi and Zarrad (2014)	Rudrapal *et al.* (2012)
User_id			X							
Password			X							
Challenge questions										
IP address			X							
Mouse movement	X			X						
Keystroke				X				X		
Face recognition		X				X			X	
Finger print	X		X							
Iris recognition										
Video monitoring			X		X					
Webcam										
Soft biometric										
Voice recognition										X
Policy dissemination (Moten *et al.*, 2013)							X			
Stylometry								X		
Eye tracking										
Brain waves										
Handwriting										
Palm-print										
Microphone										
Timestamp										
Zip disk										
Signature										
Photo image										

	References										
Authentication techniques	Song	Hernandez	Penteado and Marana (2006)	Kikuchi	Al-Saleem and Ullah (2014)	Anusha	Rao *et al.* (2011)	Ramu and Arivoli (2013)	Ko and Cheng (2008)	Bhagat and Katankar (2014)	Sheshadri *et al.* (2013)
User_id					X			X		X	X
Password					X			X		X	X
Challenge questions											
IP address								X			
Mouse movement											
Keystroke								X			
Face recognition			X			X					
Finger print		X									X
Iris recognition											
Video monitoring					X						
Webcam		X					X				
Soft biometric											
Voice recognition											
Policy dissemination (Moten *et al.*, 2013)											
Stylometry											
Eye tracking	X										
Brain waves	X										
Handwriting				X							
Palm-print					X						
Microphone							X				
Timestamp								X			
Zip disk									X		
Signature										X	
Photo image										X	

Table 4: Continous

Authentication techniques	References Krause	Ogata	Kumlander (2008)	Yu	Rosen and Carr	Wei
User_id						
Password						
Challenge questions						
IP address						
Mouse movement						
Keystroke			X			
Face recognition						
Finger print				X		X
Iris recognition						
Video monitoring						
Webcam					X	
Soft biometric						
Voice recognition						
Policy dissemination (Moten *et al*., 2013)						
Stylometry	X					
Eye tracking						
Brain waves						
Handwriting						
Palm-print						
Microphone						
Timestamp						
Zip disk						
Signature						
Photo image						

Table 5: Impersonation threats

Threat type	Description	New classification	Justification
Type A	This type occurs in two cases, either the proctors do not notice it or they allow impersonation by force, empathy or bribery	-	Not realistic that the exam can be conducted anywhere
Type B	This type occurs when users pass their security information to others who complete the exam on their behalf	Type 1	Another person attempts to take the exam on behalf of the true user
Type C	This type occurs when a student logs in to an exam and permits another to continue on their behalf		
Type D	This type occurs when a student logs in and completes the exam but with an assistant giving him/her the answers	Type 2	Indirect impersonation where the original user sits to take the exam but the assistant answers the questions

Table 6: Today's remote proctor systems with characteristics

Systems	Description (identification and proctoring)	Technical specification	Costs	University example
Secure exam Remote Proctor (SRP) http://www.remote proctor.com	Fingerprint for student identification Video surveillance system/audio recording with SRP device	SRP equipment Computer High speed internet	$125 for SRP equipment and $30 annual fee	Troy University, New York University, Troy University, Alabama University
ProctorU, Axicom Corp http://www.proctoru.com (Virtual online proctoring)	Username, password and ID photo for student identification. Human proctor in real-time and video surveillance system/audio recording	Webcam 640×480 Computer High speed internet-headphones or speakers-microphone Live proctor from ProctorU	$17.50 per 2 h exam	National American University, Andrew Jackson University
ProctorCam http://www.proctorcam.com (Virtual online proctoring)	Username, password and ID photo for student identification. Human proctor in real-time and video surveillance system/audio recording	Webcam 640×480 Computer High speed internet	Average $20 per 1 h exam, discount on groups of students	Loyola University Chicago's, Boston University's, Metropolitan College
WebassesorTM (http://www.kryterion online.com/)	Facial recognition software and pat-terns of keystroke rhythms. Secure browser control video surveillance system	Webcam with audio. Computer with Webassesor ap-plication. High speed internet	Webcam $50-80 plus costs of application	Penn State University
BioSig-ID	Users log into the authentication system by providing a username, first name and last name. They then select the pointing device that will be used to draw their signature (behaviour biometric). It could be a mouse, a stylus or touch pad (Barclay and Yagolnitzer, 2011)	No additional hardware is needed if we use mouse and touch pad. Bio-pen can be used	$12 (which includes a license fee/per student/per semester. If we use a Bio-Pen $90-110	University of Maryland, University of Texas Systems and Houston Community College

Apampa classifies impersonation threats into three types which are A, B and C (Apampa *et al*., 2010; Gathuri *et al*., 2014; Sabbah *et al*., 2012). Sabbah proposed to add a new type, known as type D (Sabbah *et al*., 2012). According to type A as suggested by Apampa *et al*. (2010), we believe it is not realistic because types B, C and D propose that exams can be conducted anywhere without supervision by individuals. Types B and C can be combined into a single type (type 1) as represented in Table 3. Type D will be renamed as type 2 (Table 5) for a better understanding.

COMMERCIAL BIOMETRIC PRODUCTS FOR PROCTORING E-EXAMS

In order to answer question 3, i.e., "What are the existing solutions related to implementing online exam user authentication?" there are existing commercial products that deal with online exam user authentication. According to the literature, there are at least five products that have been received by several universities and colleges for their online courses, namely Securexam, ProctorU, ProctorCam, Webassessor and BioSig-ID.

In general, these products use technological solutions to stop e-Cheating by merging both conventional password-based authentication with new biometrics-based authentication. Table 6 briefly describes each of the five products.

CONCLUSION

User authentication methods can be knowledge-based, possession-based or biometric-based. Each offer both benefits and drawbacks. Biometric based authentication is considered the most accurate and popular method in online exams to authenticate users. Impersonation impacts credibility and is the main threat that faces online exam environments. It can be classified into two types. Several commercial products use authentication methods to protect online exams such as Securexam, ProctorU, ProctorCam, Webassessor and BioSig-ID. For future research, we will classify and order authentication methods and techniques, depending on specific criteria to decide which are more suitable for an online exam environment.

ACKNOWLEDGEMENT

This research was supported by Khazanah Asia Scholarship.

REFERENCES

Al-Saleem, S.M. and H. Ullah, 2014. Security considerations and recommendations in computer-based testing. Sci. World J.

Alavi, M. and D.E. Leidner, 2001. Research commentary: Technology-mediated learning, A call for greater depth and breadth of research. Inf. Syst. Res., 12: 1-10.

Anusha, S.N. and S.T. Soujanya, 2012. Efficient monitoring in online tests using ESDV method. Int. J. Comput. Sci. Inf. Technol., Vol. 4.

Apampa, K.M., G. Wills and D. Argles, 2010. User security issues in summative e-Assessment security. Int. J. Digital Soc., 1: 1-13.

Basu, A. and S. Muylle, 2003. Authentication in e-Commerce. Commun. ACM., 46: 159-166.

Bellingham, L., 2008. Quality assurance and the use of subject level reference points in the UK. Qual. Higher Educ., 14: 265-276.

Bhagat, V. and V. Katankar, 2014. Novel method for student authentication in online examination. Int. J. Res., 1: 974-979.

Fayyoumi, A. and A. Zarrad, 2014. Novel solution based on face recognition to address identity theft and cheating in online examination systems. Adv. Internet Things, Vol. 2.

Flior, E. and K. Kowalski, 2010. Continuous biometric user authentication in online examinations. Proceedings of the 7th International Conference on Information Technology: New Generations, April 12-14, 2010, Las Vegas, NV., USA., pp: 488-492.

Gao, Q., 2012. Biometric authentication to prevent e-Cheating. Instructional Technol., Vol. 3.

Gathuri, J.W., A. Luvanda, S. Matende and S. Kamundi, 2014. Impersonation challenges associated with e-Assessment of university students. J. Inf. Eng. Appl., 4: 60-68.

Ives, B., K.R. Walsh and H. Schneider, 2004. The domino effect of password reuse. Commun. ACM., 47: 75-78.

King, C.G., R.W. Guyette and C. Piotrowski, 2009. Online exams and cheating: An empirical analysis of business students' views. J. Educ. Online, Vol. 6.

Kitchenham, B. and S. Charters, 2007. Guidelines for performing systematic literature reviews in software engineering. Joint Technical Report Software Engineering Group, Dept. of Computer Science, Keele University, UK and Empirical Software Engineering, National ICT, Australia, pp: 45-56.

Ko, C.C. and C.D. Cheng, 2004. Secure Internet examination system based on video monitoring. Internet Res., 14: 48-61.

Ko, C.C. and C.D. Cheng, 2008. Flexible and secure computer-based assessment using a single zip disk. Comput. Educ., 50: 915-926.

Kumlander, D., 2008. Soft Biometrical Students Identification Method for e-Learning. In: Advances in Computer and Information Sciences and Engineering. Sobh, T. (Ed.). Springer, Netherlands, pp: 114-118.

Levy, Y. and M.M. Ramim, 2007. A theoretical approach for biometrics authentication of e-Exams. Proceedings of the Chais Conference on Instructional Technologies Research, February 20, 2007, Raanana, Israel, pp: 93-101.

Marcialis, G.L., F. Roli and D. Muntoni, 2009. Group-specific face verification using soft biometrics. J. Visual Lang. Compu., 20: 101-109.

Moten, Jr.J., A. Fitterer, E. Brazier, J. Leonard and A. Brown, 2013. Examining online college cyber cheating methods and prevention measures. Electron. J. e-Learn., 11: 139-146.

Penteado, B.E. and A.N. Marana, 2006. A Video-Based Biometric Authentication for e-Learning Web Applications. In: Enterprise Information Systems. Filipe, J. and J. Cordeiro (Eds.). Springer, Berlin, Heidelberg, Germany, ISBN: 978-3-642-01346-1, pp: 770-779.

Ramu, T. and T. Arivoli, 2013. A framework of secure biometric based online exam authentication: An alternative to traditional exam. Int. J. Sci. Eng. Res., Vol. 4.

Rao, N.S.S., P. Harshita, S. Dedeepya and P. Ushashree, 2011. Cryptography-analysis of enhanced approach for secure online exam process plan. Int. J. Comput. Sci. Telecommun., 2: 52-57.

Rowe, N.C., 2004. Cheating in online student assessment: Beyond plagiarism. Online J. Distance Learn. Administration, Vol. 7.

Rudrapal, D., S. Das, S. Debbarma, N. Kar and N. Debbarma, 2012. Voice recognition and authentication as a proficient biometric tool and its application in online exam for PH people. Int. J. Comput. Appl., 39: 6-12.

Sabbah, Y., I. Saroit and A. Kotb, 2011. An Interactive and Secure E-Examination Unit (ISEEU): A proposed model for proctoring online exams. Proceedings of the 10th Roedunet International Conference (RoEduNet), June 23-25, 2011, Romania, pp: 1-5.

Sabbah, Y., I.A. Saroit and A. Kotb, 2012. A Smart Approach for Bimodal Biometrics in Home-exams (SABBAH model). CIIT Int. J. Biometrics Bioinf., 4: 32-45.

Saevanee, H., N.L. Clarke and S.M. Furnell, 2012. Multi-Modal Behavioural Biometric Authentication for Mobile Devices. In: Information Security and Privacy Research. Gritzalis, D., S. Furnell and M. Theoharidou (Eds.). Springer, Berlin Heidelberg, Germany, pp: 465-474.

Sarrayrih, M.A. and M. Ilyas, 2013. Challenges of online exam, performances and problems for online university exam. Int. J. Comput. Sci. Issues, Vol. 10

Sheshadri, R., T.C. Reddy and N.A. Kumar, 2013. Web-based-secure Online Non-choice-based Examination System (WONES) using cryptography. J. Discrete Math. Sci. Cryptography, 15: 353-368.

Takahashi, Y., T. Abiko, E. Negishi, G. Itabashi, Y. Kato, K. Takahashi and N. Shiratori, 2005. An ontology-based e-Learning system for network security. Int. Conf. Adv. Inform. Networking Appl., 1: 197-202.

Ullah, A., H. Xiao, M. Lilley and T. Barker, 2012. Using challenge questions for student authentication in online examination. Int. J. Inf., Vol. 5.

Zviran, M. and Z. Erlich, 2006. Identification and authentication: technology and implementation issues. Commun. Assoc. Inf. Syst., Vol. 17.