Using Challenge Questions for Student Authentication in Online Examination

Abrar Ullah, Hannan Xiao, Mariana Lilley, Trevor Barker
School of Computer Science, University of Hertfordshire, UK

Abstract

With the growth of Internet and technology in the past decade, online learning has become increasingly popular and evolved. Online examination is an integral and vital component of online learning. Student assessment in online learning is largely submitted remotely without any face-to-face interaction and therefore, student authentication is widely seen as one of the major challenges. This study aims to investigate potential threats to student authentication in the online examinations and analyzing the benefits and limitations of the existing authentication approaches. We propose the use of challenge questions for student authentication in the online examinations. For this purpose, we designed a profile based authentication framework (PBAF) together with a user-id and password for the authentication of students during online examinations, utilizing a cohort of personal and academic questions as challenge questions. We conducted an empirical study on a group of online students from local and overseas Universities. The result shows the impact of questions type on the usability, in particular the amount of time taken by the introduction of the proposed approach. We also conducted a post experiment survey to collect student feedback on the proposed technique.

1. Introduction

The growth of Internet has largely evolved teaching and learning from a conventional class room into an invaluable educational resource accessible remotely from disperse geographical locations, beyond physical boundaries. The online learning environments are likely to be accessible, available, updatable, resource efficient, useable, economical [23] and have been widely adopted by a number of educational institutions in various disciplines.

In the online learning, examination is integrated with the teaching and learning components. In an online examination scenario, there may be no face-to-face interaction between students, tutors and administrators [12], thus, security is vital to the credibility of online learning environments. The nature of online learning environments makes it more vulnerable to various security threats. Online examinations being an integral part of the learning environment can be high stake applications, which may fall to impersonation and malicious attacks for higher grades [3]. One of the primary goals of student authentication is to ensure the genuine interaction of individual students with the online examination. The conventional user-id and password authentication is not sufficient to verify the identity of an online student.

This paper discusses existing authentication features, and reviews their benefits and constraints. We have designed and developed a Profile Based Authentication Framework (PBAF) in a Learning Management System (LMS). In order to investigate the implementation of PBAF and analyze the use of profile and challenge questions, we performed an empirical study involving a group of students and professionals. Based on the data gathered and analyzed, we proposed recommendations for profile and challenge questions design presented later in this paper.

2. Importance of Student Authentication

The online examination approach essentially differs from the conventional face-to-face examination. In the online learning environments, technology is harnessed with assessment techniques to assess learning outcomes. Online examination is a fundamental and integral part of the learning environment. The online examinations may include questionnaires, assignments, projects, peer review, essays, quizzes, self assessment and portfolios [15]. In the online learning and examination, students interact and submit their work remotely and therefore, building confidence and trust is of vital importance[17]. The online teaching and learning approaches has largely changed student assessment methods. The two different assessment approaches used in the online environments, are summative and formative assessments.

In the summative assessments, student's learning outcomes are evaluated and their skills are measured against the learning goals using various assessment techniques. In online examinations, summative assessment may be at greater risk of attack due to its high-stakes.

Tutors typically use formative assessment to review feedback on learner's activities [7] and record progression. Formative assessment does not count towards final result or grades and this characteristic is likely to reduce security threat in online learning environments.

2.1. Academic Dishonesty

In spite of the anticipated benefits of online learning, security remains one of the major issues and a threat to the success of online learning [4]. As in [16], online learning offers more opportunities for academic dishonesty from remote locations than traditional face-to-face learning and assessment. Lin [19] suggests that academic dishonesty has always been one of the challenges of higher education and cheating and academic dishonesty is an ongoing issue. Academic dishonesty ranges from cheating in examination session to plagiarism or originality of work submitted.

- **Plagiarism:** Plagiarism is seen as one of the major challenges to both online and face-to-face examination. In plagiarism, students imitate or appropriate someone else's original idea or scholarly work and claim to be the original author. The students submit the plagiarized work as part of their assessment. Evidence suggests that plagiarism is on the rise [8] and it can be a potential treat equally to both online and face-to-face learning and examination. A large number of plagiarism detection software's are employed to check originality of the submitted work. Plagiarism can be one of the potential challenges to online learning; however, our research mainly focuses on student authentication in online examination.

- **Cheating:** In online examinations, the students submit their work remotely and it poses a challenge to verify the identity of a person taking online examination as the same person who registered and completed the course work [3]. Cheating and student impersonation have been a serious problem to the reputation of online learning. Agulla [3] identifies the rise in academic dishonesty in online examinations to gain maximum marks as a threat to online learning. The threat level is higher for online systems because it has increased the opportunities for deception due to non rigorous authentication regime. As in [11], unethical conduct have intensified in online learning due to more opportunities for cheating in online examination as a result of use of technology and the Internet.

3. Authentication Methods

Reliable student authentication is extremely relevant to online examinations because of high stakes being involved. Authentication attempts to verify that the users are who they claim to be. In an online examination scenario, authentication aims to verify the identity of online students and plays a key role in security. Unlike face-to-face examinations, authentication in online examinations is not supervised and invigilation is largely different in an uncontrolled remote environment [21]. Authentication guarantees the currency of online examinations, as the legitimate interaction between a student and the online examination is more likely to lead to authentic results. The mainstream authentication techniques are based on user's knowledge, objects possession and biometric features.

3.1. Knowledge Based Authentication

As in [21] , knowledge based authentication verifies identity on the basis of "what you know". It requires personal knowledge to authenticate individual access to the online environment. A user-id and password scheme is a commonly used example. It is a popular authentication method, because passwords are key to authentication and memorable. In a scenario like banking, where users are highly likely to make every effort to prevent illicit access, this scheme can be effective. However, due to the nature of online examinations, students may conveniently share their login credentials with a third party to boost their grades. As analyzed in [13], low entropy passwords are prone to dictionary attacks. Hence, online examinations relying on a user-id and password are susceptible to collusion and malicious attacks.

Challenge questions or security questions are another example of knowledge based authentication. It is generally used in the banking sector [22] for authentication, and corporate email service providers for credential recovery [24]. We will discuss the incorporation of challenge questions in online learning later in this paper.

3.2. Object Based Authentication

In the object based authentication, individuals in possession of identity objects are believed to be authentic. The users are identified by presenting or applying physical objects i.e. electronic chip cards, magnetic cards, and digital keys. It is broadly used in the banking sector, transportation and secure premises access. The identity objects such as electronic and magnetic cards benefit from storage of individual's identification features. In an online examination scenario, the presence of both entities i.e. identity object and student, increases the security. However, objects may be transferred to a third party or compromised, which poses potential threat to the online examinations [5] e.g. collusion. In addition, it may require special purpose devices to take user input for registration and authentication.

3.3. Biometrics Authentication

The biometrics or characteristics based authentication is performed by the verification of an individual's physical or behavioural characteristics [6]. Biometric frees individuals to memorize passwords and carry cards, as the person is the key for identification [10]. A number of biometric authentication features have been evolved from recent research and implemented in online learning systems including finger print, video authentication, face recognition, audio recognition or combination of these features in the form of multi-modal biometrics.

Fingerprint is one of the most commonly used biometrics authentication features [2], which offers a unique global identifier. The fingerprint may offer secure solution and minimize threat of impersonation in online examinations. The wider implementation of fingerprint for online examination requires additional resources i.e. fingerprint scanners and software on the client's location.

Face recognition biometric trait implements image recognition and pattern matching algorithms to verify user identity [27]. It may be a reliable authentication candidate for online examinations. However, face recognition biometric may not be secure authentication for online learning system due to the complexity of face recognition technology [3]. Various aspects such as variable face expression capture point direction, variable light, environment, web camera, weather and other pertinent accessories e.g. beard, glasses can affect the authentication results.

The audio or voice biometric is used both for speech recognition and speaker identification. In this biometric trait, human voice is recognized using automated system based on the data from speech wave. As in [12], intra-individual variations i.e. human voice features like acoustic, voice pitch and speaking style or accent provide a unique identifier for use as a biometric feature. As a behavioural authentication technique, it may be a secure option to shield online examinations. However, varying speaking speed, environmental noises, quality of recording equipments may not result in robust outcome [25]. The intra-individual variation can be a major practical issue in voice recognition. In the context of online learning, user training can be an overhead, when recording voice samples during the enrolment and authentication phase. A user's voice may be recorded for use in replay attacks as the 'liveness' of the user can not be verified [9].

Signature verification is a legacy feature and it has been widely used and highly acceptable in day to day life transactions [1]. However, as in [20], the evolution of technology has enabled the capture and verification of human signature using a combination of computer software and hardware. It is a unique behavioural trait and a potential candidate for user authentication. Purpose built accessories like digital signature pads, tablets and digital pens are used to capture signature information [1]. Unlike some biometric features, signature may not be easily replayed as only the signatory can reproduce the original signatures. However, signature recognition may face other issues i.e. complexities of algorithms, variation in signatures on different occasions, individual's emotional and physical influence on signature and signature forgery [14].

Biometric authentication has its strengths and limitations in terms of usability, cost and security when used in online examinations. It aims to ensure the presence of individual students by verifying physical and behavioural characteristics, which can be a preferred way to counter impersonation. However, it may incur additional cost for using special purpose hardware and software kits, and its wider implementation globally could be a challenge. Unlike knowledge based authentication, the biometric features are not amendable and hence not useable if compromised. Some biometric features may require student training and additional administration to facilitate and monitor various processes. The outcome of the biometric authentication may be affected by variation in human physical and environmental atmosphere, reducing authentication accuracy.

4. Profile Based Authentication

In [26], we proposed a Profile Based Authentication Framework (PBAF) for student authentication in online examinations. The PBAF uses a multi-modal authentication approach to secure online examination. The solution comprises of two layers of authentication i.e. user-id and password, and challenge questions. Initially, a user-id and password can be used to login into the online learning environment to carry out regular learning activities. During the learning process, students are posed with profile questions that are used to extend and refine individual student's profile. When a student requests to access an online examination, the second layer of authentication triggers the challenge questions, which are generated from the student's profile. The profile questions are used to collect answers in order to build and update the student's profile. Challenge questions are used to verify the student's identity. The primary focus of the proposed solution is secure authentication for online examination or summative assessment. "Figure. 1 PBAF Authentication Process Model" demonstrates the PBAF solution.

- **Profile:** The profile is a student's description in the form of questions and related answers. It represents a student by using information received from questions and answers during registration and learning process. The questions and answers in a student profile can pertain to personal information, education, activities, professional experience, hobbies, future objectives, and learning activities.

- **Profile Questions:** The profile questions are presented to students in order to capture additional information, which would in turn be used to extend and refine their profiles. The student is required to provide a user-id and password to pass through initial authentication to access the online learning environment. The student is queried to supply answers to profile questions on each visit to be able to access the learning resources. Answers to profile questions received during the learning process are used to extend or update the student's profile. This is a recurrent process and can be linked to student's online session and date.

- **Challenge Questions:** The challenge questions are randomly selected from the individual student's profile, when a student requests to access a summative online examination. The PBAF generates and presents random challenge questions during the authentication process. When the challenge questions are answered, the framework invokes the authentication process to verify the student's identity against profile answers.

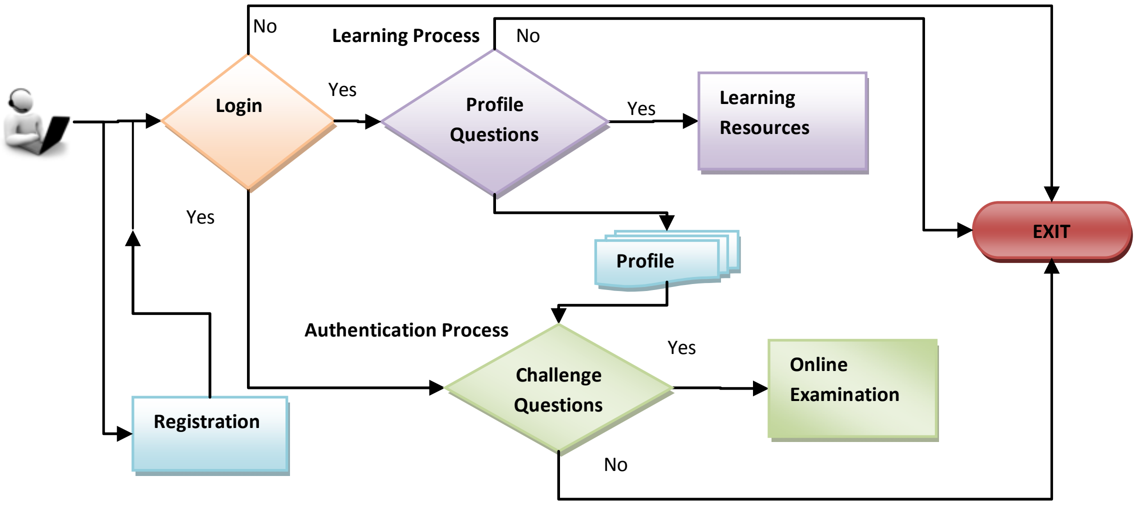

Figure 1. PBAF Authentication Process Model

- **Authentication:** In the authentication process, if the answers to challenge questions matched the stored profile information, student is granted access to online examination. If the answers to challenge question do not match to the stored profile information, student is denied access. The student access is blocked and reported to the system administrator.

5. Evaluation of PBAF

This section focused on the implementation and evaluation of profile based authentication framework in the context of online examination. We planned to analyze the various processes of PBAF, interruption time while answering profile questions and answer trending to different questions types. To do this We need to implement the PBAF first and then collect and analyze participants' answers and responses to the profile questions and challenge questions.

5.1. Implementation of Prototype

The PBAF prototype was developed in PHP and integrated on the MOODLE LMS. A test web server was developed for the purpose of this empirical study. An online simulation course was created and the profile questions were added to the PBAF questions library. Similarly, an online simulation examination was added to the online course. It should be noted that, the online course and examination were not exact simulation with realistic course contents and examination material where a participant can carry out the learning and perform examination questions, as the experiment focuses on collection of answers to profile questions and authentication results.

5.2. Methodology of Evaluation

We performed the experiment in an online environment and were granted the ethical approval by the University of Hertfordshire Research Ethics Board. We recruited local and international IT professionals and undergraduate and postgraduate students from a UK and overseas Universities. The participants were formally informed of the objectives of the research and sent an electronic copy of the guidance notes. The participants were given information on registration process, various access dates to submit their profile questions, online examination and finally a usability and privacy survey. We invited a total of 34 potential participants by email on their consent to participate in the experiment by signing up on the online course.

The design of the challenge questions used in PBAF is of vital importance. We designed a cohort of 20 objective questions, with 10 questions each from their personal and academic domains. We recorded all the information from profile building to participant's authentication. The profile questions response time was recorded in the database for detailed analysis, which is presented later in section 6.

Participants performed the following activities in the empirical study.

- **Registration:** As in "Figure.1", the process starts from completing registration in order to receive login information. The participants created their login accounts and completed online registration on the online course. The "registration" process involves selection of user-id and password for login.

- **Learning Process:** The participants were given seven dates to visit the online course and complete the profile questions, with a space of three days between their visits. After the registration, the participants visited the online course and were redirected to answer the "profile questions". The number of "profile questions" requested is configurable and can be set to a value from 1-10. For the purposes of the study reported here, the number of questions was set to 3. This would allow the authors to collect sufficient data for preliminary analysis, without causing fatigue to the participants. The participants can only access the online simulation course, if they submit answers to all their "profile questions". The participants repeated the process on the given dates.

- **Online Examination:** After completing the submission of "profile questions", the participants were notified by email to login and access the online examination link. We set "challenge questions" for online examination authentication to 3, for the purpose of analyzes. However, the number of "challenge questions" is configurable for future experimentation on different frequencies. As in "Figure.1 PBAF Authentication Process Model", the participants visited the online examination link and were redirected by the PBAF system to answer three challenge questions selected randomly from their profiles.

- **Online Survey Questionnaire**: On the completion of experiment, we requested the participants to respond to two online survey questionnaire based on their experience of the PBAF authentication approach. The questions were designed to collect participant's feedback on the user interface, usability of PBAF approach and data privacy.

6. Results and Analysis

Among the total invitees, 77% participated in the initial registration and 60% participated in all the various processes of experiment by providing answers to profile and challenge questions. We used a string comparison algorithm for authentication phase. The answer string can be text, numeric and alphanumeric. The algorithm compares answer of the challenge question with the respective answer stored in the individual's profile to find an exact match in order to authenticate the student. The system locked out participants who could not provide exact answers to all the challenge questions. The participants submitted answers to 285 "profile questions" to construct individual's profile. A total of 13 participants answered 39 challenge questions in the authentication process. Of all the answers submitted for challenge questions, 62% successfully matched, while 38% were unmatched.

We analyzed the data to ascertain the impact of question design on usability and overall usability of PBAF approach.

6.1. Impact of Question Design

As in [18], active recall of answers to questions can affect the users' response time. Response to certain questions can be prompt with active stimulus in memory as opposed to questions, which require extra thinking process to reply. However, further research is suggested to assess active, moderately active and inactive recall based on the user response.

The data on question design was analyzed and results are presented in "Table-1 Questions Analysis on Data from Profile Questions". The results in "Table.1" are based on data collected during participants' answers to profile questions. We used 20 questions for profile and challenge questions, comprising a cohort of 10 personal and academic questions each. We analyzed data based on the mean time taken by participants in submitting answers to profile questions.

- **Personal Questions Analysis:** The results revealed that the participants spent less time in submitting answers to questions requiring a single word response. To questions, "*what is your country of birth*", "*what is your father's surname*" and "*what is your best friend's surname*", the participants responded in the least amount of mean time as 13.58,13.55 and 14.26 seconds largely due to single worded answers. It is worth noting that answers to the first two questions submitted by the participants were 100% single worded and to the third question, 93% were single worded and 7% were multiple worded responses. The formatted answers also resulted in taking extra time by the participants to respond. Answer to a question "*what is your date of birth*" can be a single word however; it took 16.04 seconds mean response time more than other questions of the same type. We noted that all responses submitted to the question were 100% single worded, however, in a date format with "/" symbols, resulted in participants taking more time.

  The mean time taken by participants to answer "*what is your dream job as a child*" was 17.55 seconds, which was the most amount of time spent in personal questions with 55% of responses as multiple words in sentence case. Of the personal questions, the participants took more time on unclear questions, for example, "*What is your home address house name or number*" is unclear and 54% participants submitted their full home address, while the others entered their house name or house numbers and the mean response time was recorded as 16.73 seconds. The personal questions "*What is your home telephone number including country and area code*" and "*What is your mobile number including country code*" were submitted by participants in mean 15.41 and 17.43 seconds with 100% single worded responses, whereas the average length of all answers submitted were 11 digits.

- **Academic Questions Analysis:** The results revealed that the academic questions need more attention and clarity. Of all the 10 academic questions, the shortest

Table 1. Questions Analysis on Data from Profile Questions

Personal Questions			
	Mean time (seconds)	% of students answers by no. of words	
Questions		Single	Multiple
What is your date of birth?	16.04	100%	0%
What is your country of birth?	13.58	100%	0%
What is your father's surname?	13.55	100%	0%
What is best friend's surname?	14.26	93%	7%
Who is the favourite hero of your childhood?	14.70	43%	57%
What was your dream job as a child?	17.55	57%	43%
What is your home address house name or number?	16.73	54%	46%
What is your home address town?	16.83	58%	42%
What is your home telephone number including country and area code?	15.41	100%	0%
What is your mobile number including country code?	17.43	100%	0%
Academic Questions			
What is your student number?	14.27	100%	0%
What is the name of your last school attended?	14.60	43%	57%
What was your highest qualification before starting this course?	16.58	75%	25%
What were your grades in your highest qualification before starting this course?	15.14	93%	7%
In which year were you awarded your highest qualification?	14.92	100%	0%
In which month have you started the current course?	15.61	100%	0%
In which year have you started the current course?	16.18	100%	0%
What is the first name of your favourite tutor ever?	15.06	46%	54%
[1]What is your favourite module on this course?	17.82	67%	33%
[2]Where did you find about this course e.g. Internet, Friend etc.?	14.14	86%	14%

[1]47% unrealistic answers i.e. (NA/Nil/Unknown); [2]78% were same answers;

mean response time recorded was 14.27 seconds for a question "*What is your student number*" with 100% single worded answers. To a question "*what is your favourite module on this course*", 47% responses were unrealistic information including "*Nil*", "*NA*" and "*None*", largely because of the absence of *modules* in question on the simulation course. Of all the 20 questions, this question took the largest mean response time as 17.82 seconds. Of all the 10 academic questions, the shortest response time was 14.16 seconds to a question, "*Where did you find about this course e.g. Internet, Friend etc*". However, 78% responses were all identical as "*Friend*", which can be a potential security threat.

- **Questions Design and Authentication:** Analysis of data collected from the "challenge questions" authentication suggests that, of the total 15 unmatched answers received during authentication, 47% failed challenge questions with design issues largely related to questions design. The 47% unmatched answers were formed by the questions "*what is your home address name or number*", "*what is your favourite module on this course*" and "*what is your mobile number including country code*", which lacks clarity and generated multiple word responses. In a learning environment, where learning is a primary focus for the learners, clarity of profile and challenge questions and length of anticipated answers can be important for effective usability.

  Designing of profile and challenge questions for authentication can be an important step towards optimising usability and security of PBAF approach.

6.2. Usability Results and Analysis

The participant's feedback on the usability of PBAF is presented in "Table.2 Usability Results". A total of 16 participants completed a PBAF usability survey. The survey questionnaire was based on a five-point Likert scale from 1 to 5, where 1 specifies "strong agreement" and 5 specifies "strong disagreement". We also used a 3 point scales for a question related to participants distraction, where 1 indicated "*A great distraction*" and 3 indicated "*no distraction*". The survey was designed to collect feedback in the following aspects of the PBAF.

- **Usability and Visual Interface:** The participants submitted a useful feedback based on the "*usability interface"* of PBAF application. A positive feedback was received to the questions, "*it was easy to use the software*" with a mean score of 1.5 (1.5 median) and "*overall, satisfaction on the use of software*" with a mean score of 1.5 (1 median). However, response submitted to questions pertaining "*aesthetic interface*" and "*questions layout*" suggests further improvements. The mean score for related question were 2.3 and 2.4 (median 2). The overall results indicate a positive acceptance to PBAF application and authentication approach, however slight improvement is recommended in the interface and visual design. The feedback received on the user interface, number of questions, and learning interruption was found positive.

- **Interruption of Study:** The PBAF introduces a technique to collect answers to profile questions during the learning process. To survey questions on participant's interruption while answering the profile questions, we received a mean score of 2.1 (2 median) to "*interruption of study*" and 1.7 mean (2 median) to "*time of interruption*". To another question "*number of questions asked during profile building was a distraction*", 62% participants indicated "Not a distraction", 32% "a slight distraction", and 6% suggested "a great distraction". Given the fact that 62% suggests a positive

Table 2. Usability Results

Usability and visual Interface	**Mean**	**Median**
It was easy to use the software.	1.5	1.5
It was easy to use the Registration Form on initial login.	1.4	1
The interface of this system was aesthetically pleasant.	2.3	2
I am satisfied with the layout of questions posed soon after the login.	2.3	2
Overall, I am satisfied with the use of the software.	1.5	1
Interruption of study		
I could effectively carry on with the learning activities while answering the questions.	2.1	2
I was able to complete answering the questions quickly which were posed on each login.	1.7	2
[3]I was distracted by the number of questions asked after the login.	3.2	3
The occurrences of profile questions should be once per day instead of one per user session.	2.6	3
It was easy to respond to the challenge questions	2	2

[3]Reverse scale

acceptance, however a combine effect of participants concern makes 38%, indicates a further test on reduced number of questions. Also, to collect more information on "*interruption*" and "*response time*", more experiments are warranted on a real online course.

The overall feedback looks satisfactory both on the conceptual and interface design with indications to improve the layout. The above analysis identified the need for a better question design to implement secure authentication and ensure optimum usability. The result suggests that participants spent more time in replying questions with design anomalies. The poor question design also resulted in usability issues during authentication process

7. Conclusion

The popularity and growth of online learning has also led to an increased concern about security of online examinations. The threats to online examinations can have a detrimental impact on the credibility of online learning courses that make extensive use of online examinations.

Conventional approaches to student authentication are unlikely to be sufficient to counteract collusion and malicious attacks to online examinations. This paper reviewed various authentications traits, their feasibility in the online learning environments, and their strengths to deal with collusion and malicious attacks.

This paper proposed PBAF and the findings from the empirical study reported here suggest, that *challenge questions* based authentication can be an effective technique, if the questions are designed effectively to meet both the usability and security challenges. The collections of answers to *profile questions* are performed during the learning process hence the student response time, anticipated length of answer, difficulty and clarity of questions shall be considered in the questions design. The participants' responded positively to a post experiment online survey on the PBAF application interface and the proposed technique for online examinations authentication.

The results identified that the design of questions has a proportionate effect on the time spent and usability of the PBAF approach. Future work would therefore, concentrate on the usability, security, privacy and reliability aspect of the PBAF authentication.

8. References

[1]Adamski M., Saeed K. "Online Signature Classification and its Verification System", 7th Computer Information Systems and Industrial Management Applications2008, p. 189-94.

[2] Aggarwal G., Ratha N., Jea T. Y., Bolle R. "Gradient based Textural Characterization of Fingerprints", Biometrics: Theory, Applications and Systems, 2008, IEEE.

[3] Agulla E. G., Rifón L. A., Castro J. L. A., Mateo C. G. "Is My Student at the Other Side? Applying Biometric Web Authentication to E-Learning Environments", Eighth IEEE International Conference on Advanced Learning Technologies, 2008, IEEE.

[4] Alwi N. H. M., Fan I. S.,"Threats analysis for e-learning", *International Journal of Technology Enhanced Learning*, 2010,2(4),358-71.

[5] Apampa K. M., Wills G., Argles D. "An approach to presence verification in summative e-assessment security", International Conference on Information Society (i-Society 2010), 2010, IEEE.

[6] Asha S., Chellappan C. "Authentication of e-learners using multimodal biometric technology", International Symposium on Biometrics and Security Technologies 2008, IEEE.

[7] Birenbaum M.,"Assessment 2000: Towards a pluralistic approach to assessment", *Alternatives in assessment of achievements, learning processes and prior knowledge*, 1996,3-29.

[8] Born A. D.,"How to reduce plagiarism", *Journal of Information Systems Education*, 2003,14(3),223-4.

[9] Eveno N., Besacier L. "Co-inertia analysis for liveness test in audio-visual biometrics", Proceedings of the 4th International Symposium on Image and Signal Processing and Analysis, 2005, IEEE.

[10] Gil C., Castro M., Wyne M. "Identification in web evaluation in learning management system by fingerprint identification system", Frontiers in Education Conference (FIE), 2010, IEEE.

[11] Harmon O. R., Lambrinos J., Buffolino J.,"Assessment design and cheating risk in online instruction", *Online Journal of Distance Learning Administration*, 2010,13(3).

[12] Hayes B., Ringwood J. "Authenticating student work in an e-learning programme via speaker recognition", 3rd International Conference on Signals, Circuits and Systems (SCS) 2009, IEEE.

[13] Huiping J. "Strong password authentication protocols", 4th International Conference on Distance Learning and Education (ICDLE), 2010, IEEE.

[14] Jazahanim K. S., Ibrahim Z., Mohamed A. "Online zones' identification using signature baseline", Second International Conference on the Applications of Digital Information and Web Technologies, 2009, IEEE.

[15] Joosten-Ten Brinke D., Van Bruggen J., Hermans H., Burgers J., Giesbers B., Koper R., et al.,"Modeling assessment for re-use of traditional and new types of assessment", *Computers in Human Behavior*, 2007,23(6),2721-41.

[16] Jung I. Y., Yeom H. Y.,"Enhanced security for online exams using group cryptography", *IEEE Transactions on Education*, 2009,52(3),340-9.

[17] Karvonen K. "Creating trust", In Proceedings of the Fourth Nordic Workshop on Secure IT Systems, 1999, Citeseer.

[18] Laufer B.,"The development of passive and active vocabulary in a second language: Same or different?", *Applied linguistics*, 1998,19(2),255-71.

[19] Lin C. H. S., Wen L. Y. M.,"Academic dishonesty in higher education—a nationwide study in Taiwan", *Higher Education*, 2007,54(1),85-97.

[20] Meshoul S., Batouche M. "Combining Fisher Discriminant Analysis and probabilistic neural network for effective on-line signature recognition", 10th International Conference on Information Sciences Signal Processing and their Applications (ISSPA), 2010, IEEE.

[21] Moini A., Madni A. M.,"Leveraging Biometrics for User Authentication in Online Learning: A Systems Perspective", *IEEE Systems Journal,* 2009,3(4),469-76.

[22] Rabkin A. "Personal knowledge questions for fallback authentication: Security questions in the era of Facebook", In SOUPS 2008: Proceedings of the 4th Symposium on Usable Privacy and Security, 2008, 23, New York, NY, USA, ACM.

[23] Ruiz J. G., Mintzer M. J., Leipzig R. M.,"The impact of e-learning in medical education", *Academic medicine*, 2006,81(3),207.

[24] Schechter S., Brush A. J. B., Egelman S. "It's No Secret. Measuring the Security and Reliability of Authentication via", 30th IEEE Symposium on Security and Privacy, 2009, IEEE.

[25] Shaver C. D., Acken J. "Effects of equipment variation on speaker recognition error rates", International Conference on Acoustics Speech and Signal Processing (ICASSP), 2009, IEEE.

[26] Ullah A., Xiao H., Lilley M. "Profile Based Student Authentication in Online Examination", International Conference on Information Society (i-Society 2012), 2012, IEEE.

[27] Zhao Q., Ye M. "The application and implementation of face recognition in authentication system for distance education", 2nd International Conference on Networking and Digital Society (ICNDS), 2010, IEEE.