Graphical and Text Based Challenge Questions for Secure and Usable Authentication in Online Examinations

Abrar Ullah, Hannan Xiao, Trevor Barker , Mariana Lilley
School of Computer Science,
University of Hertfordshire, Hatfield, UK
{a.ullah3, h.xiao, t.1.barker, m.lilley} @herts.ac.uk

Abstract— **In traditional online examination environments, physical interaction is often replaced with authentication mechanisms. The absence of face-to-face interaction increases the number of authentication challenges. The authors developed and implemented a Profile Based Authentication Framework (PBAF) with the aim to integrate learning and examination processes for secure online examinations. The PBAF approach utilizes the widely used knowledge-based authentication mechanisms: login identifier and passwords and challenge questions. These approaches are reported with a number of benefits and limitations in term of usability and security. Previous studies suggests that the use of image-based graphical authentication may provide usable and secure solution. This paper presents the findings of an empirical study, utilizing a hybrid approach combining image and text-based challenge questions in a real online learning environment. A traffic light system was implemented to improve usability of the PBAF. The traffic light system relaxed authentication constraints for a significant number of users' attempts which would otherwise be penalized (p< 0.01). An abuse case scenario was designed to assess the security of the PBAF method against impersonation attack. The number of participants in abuse case scenario was small, however, results demonstrate that participants were able to share both text-based and image-based questions for impersonation attack.**

Keywords—Online learning, examination, profile, challenge questions, authentication, security, usability

I. INTRODUCTION

Authentication mechanism is an important feature to provide security to systems [1]. A number of authentication features have been used in both offline and web based environments. It is achieved by using known secrets to individuals [2], possession of objects [3] and physical or behavioural characteristics [4]. The various types of authentication approaches provide differing security and usability levels. The "challenge questions" is a widely used authentication approach, which utilizes personal information as authentication token. Using the "challenge questions" approach, users are required to record answers to challenge questions at the outset. These questions are then used for authentication purposes. Challenge questions have been commonly used for credential recovery and banks for identity verification.

In recent studies, the authors implemented challenge questions for security of online examinations against adversary and guessing attacks [5]. However, the findings of these studies suggest that text-based challenge questions were fraught with usability and security challenges. The usability challenges include memorability, syntactic variation, questions relevance, clarity and guess-ability. To mitigate these issues, design for the text-based questions was revived and questions with clarity, ambiguity were replaced.

This study aims to enhance the usability and security of challenge questions in the context of online learning environments to provide adequate security for critical online examinations. The study is part of an ongoing research to evaluate use of challenge questions for security of online learning environments. In response to our previous study [6], which reported the usability challenges of text-based questions, we have implemented image-based challenge questions for authentication purposes.

II. BACKGROUND

Online examinations are integral part of online learning management environments [7]. Online learning can be implemented in a number of ways such as: blended learning, e-learning in a face-to-face course and online learning in a distance learning environment. This work focuses on the security of online learning and examination in a distance learning environment. It is believed that students can exploit the absence of face-to-face invigilation and identification to their benefit and turn to academic dishonesty. Impersonation in the absence of physical invigilation is also reported in online examinations. In impersonation, a student shares access credential with a third party contractor to take examination activity on his behalf in order to qualify or gain extra grades. Student authentication in online examinations is a widely researched area and many argue that online examinations can be more vulnerable to academic dishonesty than traditional face-to-face examinations [8].

A number of authentication mechanisms have been evolved to resist the security threats. Knowledge-based authentication are widely used features, due to its simplicity, availability and compatibility on a wide range of platforms [9]. Users are authenticated by proving knowledge of one or more associated secret tokens. Users are expected to memorize associated

This Research is sponsored by the Wales Deanery, School of Postgraduate Medical and Dental Education, Cardiff University www.walesdeanery.org

secrets. However, studies suggest that memorability and usability have been a rising concern to proliferation of knowledge-based authentication on many online websites. Knowledge-based features are classified into text and image-based approaches. The image-based authentication is seen as a candidate solution to increase the usability and security of online environments. Research in cognitive psychology suggests that humans have better memorability and recognition of images than memorising text-based answers [10]. In the light of above discussion, we have implemented a hybrid approach utilizing text-based and image-based authentication for usability and security evaluation.

The authors developed the PBAF authentication approach, which implements challenge questions for security of online examinations. Traditionally, challenge questions feature uses text-based security questions for authentication purposes. However, due to usability challenges reported in a number of studies [6, 11-14], recall and recognition image-based questions were implemented in this empirical study. It was hoped that implementation of text-based and image-based questions would enhance usability and mitigate risks of impersonation in online examinations.

As shown in “Fig.1”, the PBAF uses questions and their answers to build individual student’s profile during the learning process. The profile information is then used to support student authentication during the online examination process.

In previous studies, the authors implemented challenge questions in a simulation online course. The previous work:

- Implemented the PBAF method in a simulation online learning environment, to authenticate students, firstly at a course access level and secondly at examination access level [14].
- Organised an empirical study to research usability of the PBAF method in terms of memorability, clarity of questions, syntactic variation and implementation of a traffic light system [6].
- Conducted an in-depth analysis of the question design and their impact on the usability attributes. The study reported analysis of usability attributes: efficiency, effectiveness and guess ability security analysis in an abuse case scenario [5].

This study aims to:

- Implement the image-based authentication in the PBAF approach in a real online course.
- Perform usability comparative analysis of image-based and text-based questions in the PBAF authentication approach.
- Perform security abuse case analysis of image-based and text-based questions used in the PBAF authentication approach.
- Present findings of a traffic light system and evaluate the effect of relaxing authentication constraints on the usability attributes.

III. Profile Based Authentication (PBAF)

The PBAF is a multi-modal authentication approach, which utilizes login-identifier and password and challenge questions for authentication purposes. Students are provided with a unique username and password for logging into the learning environment. During the learning process, students are required to record answers to questions in order to gain access to learning resources. These questions are referred as profile questions, which are used to build students’ profiles. The authentication process is triggered when a student requests to access online examination. The student is required to answer a set of challenge questions randomly extracted by the PBAF from his profile. A brief description of how the PBAF approach to student authentication works, is given below:

- *PBAF Configuration:* The PBAF method is capable to implement pre-defined text-based, image-based and automated activity-based challenge questions. In this study, predefined text-based and image-based questions were implemented. A set of predefined questions are required to enter the PBAF at the outset. A customized interface is used to upload questions to be used as profile and challenge questions. The PBAF is designed to be configurable and the total number of profile and challenge questions posed during learning and authentication are configured from the PBAF configuration.
- *Profile Questions:* The profile questions are presented to students during the learning process. Students are required to supply answers to profile questions on each visit to be able to access learning resources.
- *Challenge Questions:* The PBAF generates and presents random challenge questions before any online examinations can be accessed. Students’ answers to challenge questions are verified against their profile answers using authentication mechanism.
- *Authentication & Traffic Light System:* The authentication algorithm uses string-to-string comparison to match answers with the stored information. A traffic light system was designed to enhance the usability by relaxing the authentication constraints. The traffic light system was classified into three categories i.e. Red, Yellow and Green. The three colour classification was configurable and reliant upon the number of correct answers to challenge questions. For the purpose of this study, the PBAF configuration was set out and participants were classified as green if all of their 3 answers to challenge questions were matched. Participants providing 1 or 2 matched answers were classified as yellow and presented with more challenge questions to re-authenticate. Participants providing no matched answers were classified red and denied access to the online examination.

IV. Reasons For Using Image-based Challenge Questions

Image-based authentication has been widely researched area [15]. Stemming from people’s ability to remember images over words, the PBAF implemented various graphical

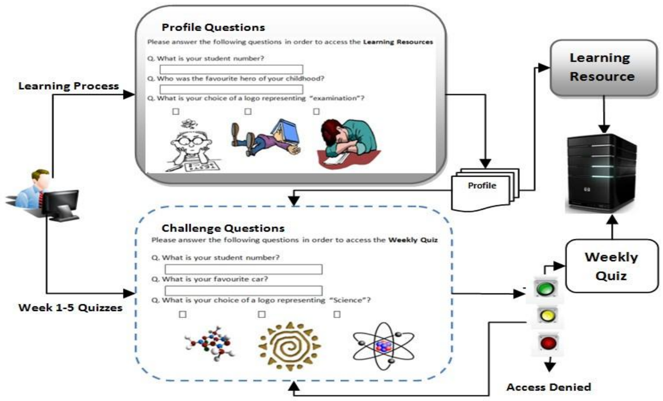

Profile Questions
Please answer the following questions in order to access the Learning Resources
Q. What is your student number?
Q. Who was the favourite hero of your childhood?
Q. What is your choice of a logo representing "examination"?
□ □ □
Learning Process
Learning Resource
Profile
Challenge Questions
Please answer the following questions in order to access the Weekly Quiz
Q. What is your student number?
Q. What is your favourite car?
Q. What is your choice of a logo representing "Science"?
□ □ □
Week 1-5 Quizzes
Weekly Quiz
Access Denied

Figure 1. PBAF Authentication during Learning and Examination Processes

authentication methods. This study reports on the usability of text-based and image-based (hybrid) questions after analyzing the results from an online course. The method of authenticating with images over words can be a usable and memorable approach when compared to traditional text-based authentication. On their own, graphical passwords do have weaknesses, such as shoulder surfing, therefore, text-based questions were combined with graphical approaches which may alleviate this concern. This study implemented a hybrid approach and utilized text-based questions, recall image-based questions and recognition image-based questions. The PBAF authentication method is capable of utilising different types of challenge questions. Description of challenge questions of various types is given below.

A. Text-Based Questions

The text-based questions are posed in plain text format such as "*What is your favourite colour?*" It is a widely used question type implemented by a number of email service providers for authentication purposes [11]. Questions are based on individual's personal and professional information. The text- based questions are further classified into fixed and open type questions [16]. The fixed-type questions are pre-designed. Questions are presented to users from a pool of pre-defined questions. In contrast, open questions are created by users. Users have full control over choosing question's description and answer. The text-based challenge questions faces a number of challenges such as memorability, clarity, syntactic variation, which may cause security and usability issues [17]. Besides the image-based questions, this study implemented fixed type text-based questions. These questions were uploaded during the PBAF configuration process.

B. Recall Image- Based Questions

The recall image-based authentication uses images of objects, nature and abstracts etc. to verify identity of users. Users are presented with previously chosen image to recall and identify their selection in order to authenticate [18]. The recall image- based authentication was implemented as recall image-based multiple choice questions in the PBAF approach. "Fig 1" is an example of recall image- based question. Research suggests that image-based questions have advantage over the text-based questions in terms of memorability.

C. Cued-Recall Image- Based Questions

The cued recall image-based authentication relies upon individual's recall ability, however, it is aided with a cue to help recall image selection [9]. The cued recall can either be a text-based information stored by the user [4] or automated retrieval cues [18]. Cued-recall image-based authentication can be implemented as cued-recall based multiple choice image questions in the PBAF approach, however, this study does not cover cued-recall based authentication.

D. Recognition Image- Based Questions

The recognition image-based authentication relies upon individual's recognition ability and authenticate on the basis if an individual has seen or chosen a image before [9]. The correct image is presented with a set of distraction images and user is challenged to recognize a previously viewed or selected image. The recognition based authentication was implemented as recognition based multiple choice questions in the PBAF approach.

E. Activity Based Questions

The activity-based questions and their answers are generated programmatically based on individual's learning activity during the learning process [19]. In traditional online learning, the learning process is a set of pre-defined activities including lessons, forums, quizzes, assignments, chatting activities to name a few. The questions generator creates activity-based questions, which is trigged on individual's performing any learning activity and used for authentication purposes.

V. METHODOLOHY

This study focuses on the usability and security of profile and challenge questions in the context of online examinations. We performed an experiment using an online learning course. The methodology was approved by the University of Hertfordshire's research ethics board.

A. Particpants Recruitment

A blend of local and international undergraduate and postgraduate students were recruited from UK and overseas Universities. Participants were required to possess basic programming knowledge in order to enrole. 70 students were recruited in order to support the research and learning activities simultaneously.

B. Experiment setup

The experiment was organised into multiple phases. To collect real-time and reliable information, the study was conducted in the 5 week "PHP and MySQL" online learning course. The online course was designed and deployed on MOODLE LMS accessible via the Internet. The PBAF method was built and integrated in the LMS for authentication of participants in the 5 weekly quizzes. An overview of the experiment is given below:

- *Course Design and Participants Recruitment*: A "PHP & MYSQL" course was designed and offered free of cost to attract online students from around the world. The free online course was advertised on the University of Hertfordshire student forum. 70 students were registered in the online course.
- *Questions*: 27 text-based and 13 image-based questions were designed for the study. These questions were uploaded to the PBAF before the registration process.
- *Registration*: Participants were emailed guidance and registration information. Participants created their accounts and completed online registration on the course. The "registration" process involved selection of user-id and password for login. The course content were released conditionally to encourage participants.
- *Weekly Quizzes (Online Examinations)*: Participants were required to complete a quiz on a weekly basis to promote to the following week. Each participant was required to authenticate in order to access a weekly online quiz (examination). Challenge questions were randomly extracted from individual's profile for authentication purpose. A traffic light system was set up to relax the authentication algorithm and minimize the usability challenges.
- *Impersonation Abuse Case Scenario*: An abuse case scenario was undertaken on completion of the online course. To perform an impersonation authentication attack for security assessment, all participants were encouraged to volunteer and share all or maximum answers to their profile questions. The participants were informed about the intended use of the information.

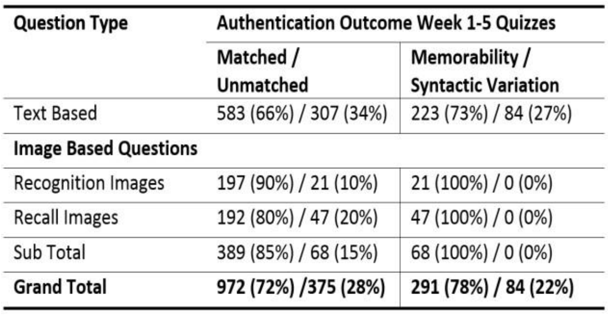
C. *Usability Analysis*

The data collected in the empirical study was stored in a relational database. Participants' answers to questions received at different phases were recorded in the database for *usability analysis*. The usability factors memorability and effectiveness were evaluated. These factors are described below:

i. *Memorability of Text and Image Answers*: Memorability of answers is one of the major concerns of many authentication features. Research studies have reported that memorability is weaker in the text-based challenge questions [20],[6],[21]. Some researcher reported memorability issue in the recall based image authentication, which resulted in introduction of recognition and cued based authentication. In this study, memorability analysis was performed on data collected from the recurrent learning process and multiple weekly quizzes performed as part of the online course. The memorability analysis are presented in the results section.

ii. *Effectiveness of Traffic Light System*: The traffic light system was designed to compensate for usability challenges. To achieve effective authentication with a balanced security mechanism, traffic light system provided extra authentication attempts to individual's providing matched answers to some of their questions.

TABLE 1. SUMMARY OF ANSWERS TO TEXT & IMAGE QUESTIONS



Question Type	Authentication Outcome Week 1-5 Quizzes	
	Matched / Unmatched	Memorability / Syntactic Variation
Text Based	583 (66%) / 307 (34%)	223 (73%) / 84 (27%)
Image Based Questions		
Recognition Images	197 (90%) / 21 (10%)	21 (100%) / 0 (0%)
Recall Images	192 (80%) / 47 (20%)	47 (100%) / 0 (0%)
Sub Total	389 (85%) / 68 (15%)	68 (100%) / 0 (0%)
Grand Total	**972 (72%) /375 (28%)**	**291 (78%) / 84 (22%)**

VI. EXPERIMENT RESULTS

Students participated in various learning activities during the online learning process and submitted answers to 2315 profile questions. The learning and weekly quizzes (examination) were organized side by side. Weekly quizzes were secured using the PBAF method and students were required to authenticate using challenge questions before access to their respective quiz. A string-to-string comparison algorithm was utilized in the authentication process. Of the 70 participants, 48 attempted weekly quizzes and answered 1347 challenge questions to authenticate. In weekly quizzes, answer to 972 (72%) of the total challenge questions matched during authentication.

A. *Usability Analysis*

The overall usability analysis shows improvement in the effectiveness of text-based challenge questions compared to a previous empirical study conducted a simulation online course [6]. Questions reported with clarity and ambiguity issues in previous study, were replaced in the current study. The number of matched answers in the previous study was 38 (58%), which increased to 583 (66%). An independent sample t-test shows significant difference in the effectiveness of challenge questions in the current study compared to a previous study (p <0.01). The usability analysis of text-based and image-based questions is presented below.

Effectiveness is measured as a degree of correctness during authentication phase, whereas memorability is measured as a degree of recall. If an unmatched answer was found to be a complete shift from a previously stored answer in individual's profile, it was considered a memorability or recall failure. Overall, the PBAF may be an effective approach. Nevertheless, particular questions may affect the usability of the PBAF method.

Text Vs Image-based Answers: Table 1 shows the summary of authentication in weekly quizzes. The results of text-based questions show 66% matched answers during authentication. Compared to text-based questions, the image-based questions received 85% matched results, which shows an increase in the effectiveness and usability. Psychology research has revealed that human brain is more capable of recognizing images than text [10]. The text-based questions were penalized for both memorability and syntactic variation. Detailed sorting of the total unmatched answers revealed that 223 (73%) was a result of memorability and 84 (27%) syntactic variation. With open text answers, users tend to write their answers in varying formats. The manual sorting of users' answers revealed that 27% unmatched answers were semantically correct but penalized for incorrect spellings, variation in format, and variation in syntax. The text-based questions were fraught with memorability issues. A total of 73% answers were completely different than their original answers registered during the learning process. The results would further improve if syntactic variation was compensated using a more relaxed algorithm including substring and distance algorithms [22]. The image-based questions were multiple-choice options and therefore, syntactic variation was not reported. However, a total of 68 (15%) unmatched answers was a result of answer memorability. This shows that memorability is a common problem with both text-based and image-based questions. The text-based questions are prone to syntactic variation, which can be minimized by implementation of a more relaxed algorithm. Furthermore, text-based questions are reported with privacy issues, which can be addressed using image-based questions [23].

Recall Vs Recognition Based Image Answers: The recall and recognition image-based questions were implemented as part of the hybrid approach in the user study. Summary of the authentication results in table 1 shows that recognition image- based questions received the highest number of matched answers. The recognition image-based questions received 197 (90%) matched answers, which indicate increased effectiveness than the recall image-based questions with 192 (80%), matched answers. The results indicate improvement in usability and a stimulus to recognize a previously seen image presented with distraction images as reported in psychology research [24]. Although, the multiple image questions have improved the usability. However, security evaluation is warranted to analyse the guess-ability of multiple choice image authentication particularly when the number of choices is low (number of choices for this study was set to 3).

TABLE 2. SUMMARY OF TRAFFIC LIGHT SYSTEM

Attempt Number	Red	Yellow	Yellow	Green
	0/3	1/3	2/3	3/3
1	9(4%)	36(17%)	85(41%)	78(38%)
2	6(5%)	23(21%)	41(37%)	40(36%)
3	2(3%)	10(16%)	28(44%)	23(37%)
4	2(5%)	6(16%)	16(43%)	13(35%)
5	1(5%)	2(11%)	9(47%)	7(37%)
6	1(9%)	1(9%)	4(36%)	5(45%)
7-14	0(0%)	5(36%)	6(43%)	3(21%)
Total	**21(5%)**	**83(18%)**	**189(41%)**	**169(37%)**

Error rate: 10 in yellow classification were 1/1 instead of 1/3

B. *Traffic Light Results*

The traffic light system was designed to compensate for usability challenges: memorability and syntactic variation. Table 2 shows summary of the traffic light system implemented in the PBAF authentication for weekly quizzes. In order to test the significance of any differences in the number matched answers i.e. Yellow (1 out 3), Yellow (2 out 3), Green (3 out of 3) and Red (0 out of 3), a one-way ANOVA test of significance was performed. The results of this analysis showed that there were significant differences in the means F (3, 27) = 52.30, $p < 0.01$. Post hoc comparisons of the groupings yielded the following significant results.

Yellow 1 x Yellow 2, mean difference (MD) =-23.57, Standard Error (SE) = 3.66, p < 0.01, Green x Yellow 1, mean difference (MD) =17.57, Standard Error (SE) = 4.31, p < 0.01, Green x Red, mean difference (MD) =31.14, Standard Error (SE) = 2.90 p < 0.01, Yellow 1 x Red, mean difference (MD) =13.57 Standard Error (SE) = 3.5, p < 0.01, Yellow 2 x Red, mean difference (MD) =37.14 Standard Error (SE) = 1.8, p < 0.01. No other significant differences were found in the post hoc comparisons.

The above findings show that Yellow 1 and 2 have a significant difference with red classification. Participants in the yellow classification would otherwise be penalized for not submitting matching answers to all of their 3 questions during the authentication process. However, participants in yellow classification were re-authenticated due to implementation of traffic light system and minimised the rejection rate in red classification to 21 (5%). Participants provided matched answers to all of their 3 challenge questions in 169 (37%) occurrences. Increase in the green classification was a result of multiple chances to participants falling in the yellow classification. The results indicate that the use of traffic light system significantly affected users' authentication attempts. However, further analysis is warranted to evaluate security of

TABLE 3. SUMMARY OF ANSWERS SHARED FOR IMPERSONATION ABUSE CASE

Students	Number of Answers Shared for Impersonation		Profile to Impersonation	
	Image Based	Text Based	Individual's Profile Question	Impersonation / Profile
S1	1	15	57	**16/57 (28%)**
S2	0	4	57	**4/57 (7%)**
S3	0	5	57	**5/57 (9%)**
S4	0	5	54	**5/54 (9%)**
S5	5	11	44	**16/44 (36%)**
S6	0	3	54	**3/54 (6%)**
S7	0	4	57	**4/57 (7%)**
S8	4	2	57	**6/57 (11%)**
Total	**9**	**50**	**437**	**59/437 (13%)**

the traffic light system.

C. *Impersonation and Security Analysis*

On completion of the 5 week “PHP & MYSQL” course, students were requested to participate in a security evaluation of the PBAF method. Table 3 shows summary of profile questions shared by students during the impersonation abuse case scenario. Columns 1 and 2 show the number of image-based and text-based questions shared for impersonation. Column 3 shows number of profile questions submitted by the individual participated in the impersonation abuse case and column 4 shows the percentage of answers shared for impersonation to profile questions.

Of the 48 students participated in weekly quizzes, only 8 shared 59 questions and their answers with authors. The number of participants was not encouraging and may not produce significant results. A number of conclusion can be drawn from this. There is a possibility that a small number of answers shared for collusion could increase security and participant’s inability to recall for sharing authentication information with a third party. The success of an impersonation attack would depend upon an individual student’s ability to recall and share all or most of their profile questions and answers. The percentage of profile questions to impersonation indicates that students were unable to recall and return all their answers previously submitted during the learning process. The maximum number of answers shared by a student “S5” was 36% of the profile questions. Participants shared 50 (85%) text-based questions for impersonation. We hoped that image-based questions would be difficult to describe verbally, however, participants shared 9 (15%) image-based questions for impersonation. Image-based questions shared for impersonation were not specific answers, but a brief description to identify their selection. Using the image-based information, it would be easy to recognize individual choices in the recognition image-based questions amongst a set of distractor images. Given that none of the 8 students shared answers to all their profile questions, the PBAF may improve the security of online examinations against impersonation. However, particular text-based and image-based questions were prone to impersonation attack and may not completely mitigate the security risks.

Although, an actual attack on the online examination was not performed, however, in a collusion scenario, students can share challenge questions with a third party examination taker to impersonate and access online examination on their behalf. It is important to perform security evaluation of the actual impersonation attack on the PBAF method, if participants were successful to share challenge questions and answers with the attacker for impersonation.

VII. Conclusion

The PBAF approach is a knowledge-based feature, which utilizes challenge questions for authentication in addition to user-id and password for security of online examinations. The text-based questions reported with clarity and ambiguity issues from the previous empirical study were replaced with alternative text-based questions, which increased the usability. Besides the text-based questions, recall and recognition image-based authentication were implemented in the context of online examinations to enhance security and usability of the PBAF method.

The current study was based on a real online course which implemented the PBAF approach for security of the five weekly quizzes. The findings from the empirical study reported in this paper suggest that the usability of text-based questions have improved by introducing a better question design and removing ambiguous and unclear questions. The use of image-based authentication increased the effectiveness of the PBAF method. The image-based questions achieved increased usability than the text-based challenge questions in the online examinations context (p <0.01). Furthermore, the recognition image-based questions achieved increased usability than the recall image-based questions ($p < 0.01$). The traffic light system relaxed authentication constraints for a significant number of attempts falling in yellow classification. The findings of an abuse case scenario show that implementation of the PBAF method, image-based and text-based challenge questions may reduce the security risks, however, particular text-based and image-based questions were prone to impersonation attack. It is imperative to perform evaluation of the challenge questions if participants were successful to share various number of challenge questions and their answers with a third party attacker for impersonation.

Future work would be directed for an in depth security analysis of the PBAF using the text and multiple-choice image questions for authentication.

References

[1] (Nist) N. I. O. S. a. T. Electronic Authentication Guidelines. NIST Special Publication 800-63; March 2006.

[2] Huiping J. "Strong password authentication protocols" in *4th International Conference on Distance Learning and Education (ICDLE)*; 2010; San Juan, Puerto Rico: IEEE.

[3] Deo V., Seidensticker R. B., Simon D. R. Authentication system and method for smart card transactions. Google Patents; 1998.

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

[5] Ullah A., Xiao H., Barker T., Lilley M. "Evaluating security and usability of profile based challenge questions authentication in online examinations." *Journal of Internet Services and Applications*. 2014;5(1):2.

[6] Ullah A., Xiao H., Lilley M., Barker T. "Usability of Profile Based Student Authentication and Traffic Light System in Online Examination". in *The 7th International Conference for Internet Technology and Secured Transactions (ICITST);* London, UK: IEEE; 2012.

[7] Karaman S. "Examining the effects of flexible online [17]Griffith V., Jakobsson M. "Messin’with Texas exams on students’ engagement in e-learning." Deriving Mother’s Maiden Names Using Public Educational Research and Reviews. 2011;6(3):259- Records" in Third International Conference, ACNS; 64. 2005: Springer.

[8] Colwell J. L., Jenks C. F. "Student Ethics in Online Wiedenbeck S., Waters J., Birget J.-C., Brodskiy A., Courses" in 35th Annual Conference Frontiers in Memon N. "Authentication using graphical Education (FIE '05) 2005; IN, USA: IEEE. passwords: effects of tolerance and image choice"

[9] Hayashi E., Hong J., Christin N. "Security through a Proceedings of the 2005 symposium on Usable different kind of obscurity: Evaluating Distortion in privacy and security; 2005: ACM. Graphical Authentication Schemes" in Proceedings

[19] Babic A., Xiong H., Yao D., Iftode L. "Building of the SIGCHI Conference on Human Factors in robust authentication systems with activity-based Computing Systems; 2011: ACM.personal questions" in Proceedings of the 2nd ACM

[10] Nelson D. L., Reed V. S., Walling J. R. "Pictorial workshop on Assurable and usable security superiority effect." Journal of Experimental configuration; 2009: ACM. Psychology: Human Learning and Memory.

[11] Just M., Aspinall D. "Challenging challenge questions" in Socio-Economic Strand; 2009: Oxford University UK.

[21] Ullah A., Xiao H., Lilley M., Barker T. "Using questions" in Socio-Economic Strand; 2009: Oxford Challenge Questions for Student Authentication in University UK. Online Examination." International Journal for

[12] Just M., Aspinall D. "Choosing Better Challenge Infonomics (IJI) 2012;5(3/4):9. Questions" in Symposium on Usable Privacy and Security (SOUPS); 2009; CA, USA: ACM.

[13] Just M., Aspinall D. "On the security and usability of Authentication via 'secret' questions" in 30th IEEE dual credential authentication in UK online banking" Symposium on Security and Privacy; 2009: IEEE. in Internet Technology And Secured Transactions

[14] Ullah A., Xiao H., Lilley M. "Profile Based Student Questions Authentication in Online Examination" in Authentication in Online Examination" in The International Conference on Education International Conference on Information Society Technologies and Computers (ICETC2014); 2014; 2012; London, UK: IEEE. Lodz, Poland: IEEE.

[15] Chiasson S., Van Oorschot P. C., Biddle R. Graphical password authentication using cued click points. Computer Security–ESORICS 2007: Springer; 2007. p. 359-74.

[16] Just M. "Designing Secure Yet Usable Credential Recovery Systems with Challenge Questions" in CHI 2003 Workshop on Human-Computer Interaction and Security Systems; 2003. Florada, USA: Citeseer.

[17] Griffith V., Jakobsson M. "Messin'with Texas Deriving Mother's Maiden Names Using Public Records" in Third International Conference, ACNS; 2005: Springer.

[18] Wiedenbeck S., Waters J., Birget J.-C., Brodskiy A., Memon N. "Authentication using graphical passwords: effects of tolerance and image choice" in Proceedings of the 2005 symposium on Usable privacy and security; 2005: ACM.

[19] Babic A., Xiong H., Yao D., Iftode L. "Building robust authentication systems with activity-based personal questions" in Proceedings of the 2nd ACM workshop on Assurable and usable security configuration; 2009: ACM.

[20] Just M. "Designing and evaluating challenge-question systems." Security & Privacy, IEEE. 2004;2(5):32-9.

[21] Ullah A., Xiao H., Lilley M., Barker T. "Using Challenge Questions for Student Authentication in Online Examination." International Journal for Infonomics (IJI) 2012;5(3/4):9.

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

[23] Ullah A., Xiao H., Lilley M., Barker T. "Privacy and Usability of Image and Text Based Challenge Questions Authentication in Online Examination" in The International Conference on Education Technologies and Computers (ICETC2014); 2014; Lodz, Poland: IEEE.

[24] Shepard R. N. "Recognition memory for words, sentences, and pictures." Journal of verbal Learning and verbal Behavior. 1967;6(1):156-63.