A Focus Group Study: Usability and Security of Challenge Question Authentication in Online Examinations

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

Abstract— **Online examinations are open to many security threats. These include intrusion by hackers, and collusion and plagiarism by students. This paper presents a focus group study to understand the views of online programme tutors on security threats to online examinations, authentication approaches and the proposed challenge question method. The findings showed that majority of participants were concerned about impersonation and abetting in online examinations. In the context of collusion attacks, challenge question method was considered a preferred authentication approach. The feedback on usability of different type of challenge questions indicates that dynamic profile questions are more usable than image-based and text-based questions. There was an agreement that the proposed method could influence impersonation attacks. However, some participants showed concern about abetting attacks, and supported the use of remote proctoring and secure browsing tools in addition to the challenge question method.**

Keywords—Online examination, collusion, impersonation, security threats, usability, authentication

I. INTRODUCTION

Online examinations are delivered in a remote web based environment and open to a wide number of security threats [1]. In an attempt to secure them, it is essential to understand and identify the nature of all threats. These threats can be approached in two stages i) threats are analysed, and then, ii) recommendations are introduced and discussed in order to cope with the detected threats [2].

Authentication is a first line of defence in the security of information systems [3]. It is a component of security taxonomy that confirms the identity of remote users. Many authentication methods are implemented to determine whether someone is who they claim to be [4]. The authors proposed and implemented a challenge question approach for authentication of students in online examinations [5].

This paper analyses a focus group study of online programme tutors to understand their perception of security threats, authentication approaches, and usability and security of the proposed challenge question approach.

II. BACKGROUND

Security threats to online examinations may come from different sources, which are motivated by varying objectives. However, research studies agree that cheating contributes to a large number of security threats [6, 7, 8]. It is believed to be a prevailing phenomenon reported by researchers in all forms of education [6, 7]. Given the varying types of threats, they are classified into two main categories: intrusion and non-intrusion attacks, as described in a classification presented in an earlier study [9]. Non-intrusion threats include collusion and non-collusion attacks. Collusion is further classified into impersonation and abetting categories. These threats are difficult to identify and mitigate, because such threats involve legitimate students inviting third parties to impersonate or help them in their online tests.

The proposed challenge question approach collects information during the learning process to build a student's profile, which is used for authentication in the examination. This method implements three different types of questions as described below:

- Text-based questions: are associated with individual's personal information. For example "what is your favourite movie?"
- Image-based questions: utilizes images for authentication. Users are required to identify their previously chosen images in order to authenticate.
- Dynamic profile questions: utilizes student's learning activities, lessons, submissions, grades, forum posts etc. to create and consolidate his or her profile, which is used for authentication.

The authors conducted multiple studies in simulation, as well as real online courses involving both online and on-campus students [5, 9, 10, 11, 12, 13, 14, 15, 16]. The findings of the earlier studies were encouraging. The analysis of text-based questions showed usability issues such as syntactic variation, spelling mistakes, and memorability [11]. The use of image-based questions addressed some of these issues using multiple choice questions [12] and showed improved usability. However, it is anticipated that students may be able to share their text-based and image-based questions with third party impersonators for collusion attacks. The dynamic profile questions are created non-intrusively in the background [10], which is likely to increase difficulty for students to share with impersonators.

The threats classification described in earlier study was based on literature review and it is important to understand views of important stakeholders on security threats and the proposed methods to counter them. With teaching and assessment responsibilities, online programme tutors have a central role in an online learning and examination context. This study presents feedback obtained from a focus group of online programme tutors, who were chosen as experts in this field. They were invited to provide their views on potential threats, authentication methods, usability and applicability of the proposed challenge question approach against identified threats with a focus on collusion attacks, remote proctor, and secure examination browsers.

III. Study Method and Design

This study adopted a mixed methods approach, comprising a focus group (qualitative research technique) and a questionnaire (quantitative technique). Several definitions for a focus group are available in the literature review, including collective activity [17], organised discussion [18], and social events and interaction [19]. In a typical focus group study, a group of representative individuals are chosen and gathered by researchers to discuss their personal experience and comment on the topic under research [20]. The study was performed in multiple phases described below:

A. Participant's Recruitment

A group of online programme tutors from the University of Hertfordshire was invited. A total of nine participants i.e. 5(55%) Male, 4(45%) Female, attended the study. They were highly experienced and experts in the area of online teaching, face-to-face teaching, course design, examinations design, invigilation, research supervision, Human-Computer Interaction (HCI), usability, security, and assessment of students. The session was also attended by authors, research supervisors, and the moderator.

B. Presentation on Threats and Challenge Question Method

At the start, participants were given a power point presentation on remote online examinations, authentication, collusion attacks, and the challenge question approach. Findings of the empirical studies using pre-defined text-based, image-based, and dynamic profile questions were also presented to provide a background to an online examination context, threats, and mitigation methods. At the end of the presentation, participants were handed the paper-based questionnaire for their feedback, as described in the following section.

C. Questionnaire

A 19-question paper-based questionnaire was produced to collect participants' feedback on security threats and collusion, usability of authentication methods, effectiveness of question types, and overall usability and security of the challenge question approach. 5- and 10-point scales were used for all questions. The questionnaire was distributed to participants after the first presentation described above. They were asked for feedback based on their experience associated with the information provided in the first presentation. The questionnaire was filled-in and returned by all participants.

D. Presentation on Remote Proctor and Secure Browser

Participants were given a second presentation on the use of a secure browser and remote proctoring tool, ProctorU [21], to deter collusion attacks. This method has been offered by a number of service providers to conduct proctor-led examinations remotely. This approach was presented as a potential candidate for mitigation of abetting attacks.

E. Focus Group Discussion

After the presentations, seats were arranged in a circle to facilitate group discussion. The moderator welcomed all participants and asked for their consent to record the session on a video. After setting up video cameras, the moderator gave a brief introduction about the research aim and problems. He started the discussion by describing a scenario followed by probes. He posed relevant probes one by one and steered the discussion. Participants responded to each probe in a group discussion.

IV. Questionnaire Analysis

The analysis is derived mainly from three sources to ensure triangulation and validity [22]. One source is participants' feedback to questionnaires, as shown in Table 1, and the second source is findings from the empirical enquiries presented in previous studies [5, 9, 10, 11, 12, 13, 14, 15, 16]. The third source is analysis of the focus group discussion discussed in the next section. The following sections present an analysis of participants' feedback collected on the paper-based questionnaire.

A. Security Threats and Collusion:

The threat of collusion in online examinations has been a rising concern for educational institutions and tutors. There is a prevailing view that online examinations pose a higher threat than face-to-face examinations. Numerous studies [23, 24, 25, 26, 27, 28] reported that online learning offers more opportunities for cheating. Chiesel [p.33029] identifies that 64% of university professors perceive cheating in online examinations to be easier. Table 1 shows an analysis of the questionnaire regarding security threats, including collusion attacks, in the section "Security Threats and Collusion". Online programme tutors have been actively involved in designing and conducting examinations for both on-campus and online students. They were asked about their concerns

Table 1: Questionnaire Analysis

	Questions	M	Med	SD
	Security Threats and Collusion			
1	How concerned are you about the security of a remote online examination?	4	4	0.7
2	How concerned are you about the authentication methods implemented for the security of a remote online examination?	3.7	4	1.1
3	In your view, how difficult is it for a student to cheat in a remote online examination?	2.1	2	1
4	In your view, how difficult is it for a student to cheat in face-to-face invigilated examination?	3.6	4	1.3
5	Consider the threat of a student copying answers from a book or other course material. Please rate the seriousness of this threat in a remote online examination where there is remote student authentication but no invigilation.	3.8	4	0.8
6	Consider the threat of a student copying answers from the Internet. Please rate the seriousness of this threat in a remote online examination where there is remote student authentication but no invigilation.	3.8	4	0.8
7	Abetting – Consider the threat of a student getting help from someone else, based in the same location. Please rate the seriousness of this threat in a remote online examination where there is remote student authentication but no invigilation.	4.2	4	0.6
8	Impersonation – Consider the threat of a student getting help from a third party, based in a remote location. Please rate the seriousness of this threat in a remote online examination where there is a remote student authentication but no invigilation.	4.1	4	0.7
	Existing Authentication Methods			
9	Login Identifier and Password Authentication	3.4	3	0.8
10	Graphical Password Authentication	3.4	3	0.8
11	Security/Challenge Questions Authentication	3.6	4	1.1
	Effectiveness of Different Question Types			
12	How effective would the challenge question approach be to mitigate impersonation attacks?	3.3	3	0.7
13	Pre-defined Text-Based Questions	3.0	3	0.5
14	Pre-defined Image-Based Questions	3.4	3	0.5
15	Dynamic Profile Questions	3.8	4	0.8
	Overall Usability and Security of Challenge Questions			
16	How usable is the challenge question approach?	3.6	4	0.8
17	How secure is the challenge question approach in terms of non-collusion based intruder attacks?	3.6	3	0.7
18	How secure is the challenge question approach in terms of collusion attacks?	2.9	3	0.6
19	Given that security and usability may be considered to be a trade-off, on a scale of 1 to 10, please indicate where you think the best option should be.	3.6	3	1.9

regarding threats and authentication approaches in online examinations.

As shown in Table 1, in response to Q1 and Q2 regarding “Online examinations” and “Authentication approaches”, the majority of participants reported their concern and scored M = 4 and M = 3.7 respectively (1 – No concern at all; 5 – Strong concern). In response to Q3 and Q4, participants felt that it is less difficult to cheat in online examinations (M = 2.1) compared to face-to-face examinations (M = 3.6). While cheating in an online examination has been reported as a risk, collusion is seen as a main concern. Participants were requested for feedback in Q5-8 regarding different types of collusion attacks including “copying from books and other resources”, “copying from the Internet”, “abetting” and “impersonation”. In response to these questions, the majority of participants reported high concern regarding impersonation and abetting, which scored M = 4.1 and M = 4.2 respectively.

B. Knowledge-based authentication approaches:

The knowledge-based approach is the simplest technique employed to fulfil the security requirements. This is an easy to use method, and expected to provide secure authentication. It is a low-cost, accessible, widely acceptable and preferred authentication method [30].

Participants were asked for their feedback on the usefulness of existing knowledge-based authentication approaches in the context of online examinations. These approaches include

‘Login Identifier and Password’, ‘Graphical Passwords’ and ‘Challenge Questions’. Participants rated the ‘Challenge Questions’ approach as M = 3.6 (1 - Not useful at all to 5 - Very useful).

C. *Usability of Challenge Questions:*

Braz and Roberts [31] state that the usability of security systems has become a major issue in research on efficiency and user acceptance. It is important to investigate usability attributes, i.e. the efficiency and effectiveness of the challenge question approach. This method implemented text-based, image-based and dynamic profile questions. In the empirical studies reported in [10, 12], the effectiveness of different question types was analysed by computing correct answers during authentication. Dynamic profile questions were the most usable of all question types, with 99.5% correct answers. Unlike other question types, this was the most efficient method as questions and answers were generated dynamically in the background during the learning process to build profiles, and students were not required to register their answers.

In response to survey questions 13, 14 and 15, participants rated the effectiveness of text-based, image-based and dynamic profile questions as 3, 3.4, and 3.7 respectively (1 - Not useful – 5 - very useful). A one-way ANOVA was performed on the data shown in Table 1: questions 13, 14, and 15, with linear contrasts to find a difference in participants' responses to the usability of different question types. A significant trend was found in participants' responses to the usability of different question types (F (1,754) = 1250.96, p < 0.01). A Pearson correlation was performed on participants' feedback to questions regarding the usability of question types to test the direction of the trend. The result of the test shows a significant correlation (p < 0.01), and (r = 0.46) indicates a positive trend in the usability of questions from text-based, image-based, and dynamic profile questions.

D. *Security of Challenge Questions:*

Mitigation from all types of threat is a priority; however, based on the feedback to questions associated with threats, collusion is reported as a rising concern for online examinations. Participants were requested for feedback on the security of the proposed method to mitigate non-collusion and collusion attacks. There was an agreement on the security of challenge question approach to influence non-collusion threats. However, some participants reported concerns when this approach is implemented to mitigate collusion attacks. Question 18, regarding the security of challenge question approach to mitigate collusion attacks, scored M = 2.9.

In summary, participants felt that impersonation and abetting are challenging threats to online examinations. The proposed method is usable when dynamic profile questions are implemented. There was an agreement that this method could influence impersonation attacks; however, some participants showed concern about abetting attacks, which are discussed in the focus group analysis.

V. Focus group Analysis

The data analysis of the focus group was performed using a

Table 2 : Focus Group Discussion Analysis

Categories	Raters 1	Raters 2	Score Mean
Collusion Threats			
A user will share access credentials with a third party for a bank account	1.25	1.5	1.4
A user will share access credentials with a third party for an online examination	3.3	3.3	3.3
[1] The risk of sharing bank credentials for a user is…	5.0	5.0	5.0
[1] The risk of sharing online examination credentials for a student is…	2.0	2.3	2.2
[1] The risk of Mobile/Instant Messaging/SMS is…	5.0	5.0	5.0
[1] The risk of Desktop Sharing is…	5.0	4.0	4.5
[1] The risk of inviting third party to exam location is…	5.0	5.0	5.0
Challenge questions method using dynamic profile questions			
Secure against collusion	3.3	3.3	3.3
It can make it hard to collude	4.5	5.0	4.8
As a programme tutor, I will use the dynamic profile question approach in an online exam for my students	4.5	4.4	4.5
Mitigates mobile collusion when answers are timed	4.0	3.5	3.8
[1] Risk of using time factor to penalise students	3.0	2.6	2.8
Timing answers make it hard to collude	5.0	4.0	4.5
Course Design to Prevent Collusion via Mobile SMS	5.0	4.3	4.7
Secure browser and remote proctoring (ProctorU)			
Secure against collusion	4.0	4.5	4.3
Secure against screen sharing	4.3	4.3	4.3
It can make it hard to collude	4.0	3.5	3.8
As a programme tutor, I will use ProctorU in an online exam for my students	4.5	4.7	4.6

[1] 1-Very Low Risk to 5-Very High Risk

qualitative content analysis approach [32]. It is a systematic and reliable technique for compressing many words of text into fewer content categories based on explicit rules of coding [33]. The recording from the focus group discussion was transcribed for detailed analysis. Categories of the main themes associated with this research were identified in the transcription. Phrase analysis was carried out and data were organised into subcategories for further analysis.

The data collected during the study were rated by two independent raters on a scale of 1-5 (1 - Strongly Disagree – 5 - Strongly Agree) and (1 - Very Low Risk – 5 - Very High Risk) as shown in Table 2. The data were evaluated for inter-rater reliability using Cohen's kappa test. The kappa value of 0.583 shows moderate agreement between the raters. The results are discussed in the following section.

A. Participants' Perception of Collusion Threats

To understand the perception of online tutors regarding collusion attacks, it was made a central point of the focus group discussion. While there has been ongoing debate around threats to online examinations and face-to-face invigilated exams, there is agreement that collusion is a potential threat and it is challenging to verify that a student signed up for the course is the same person who is taking the online examination. There was a good discussion on the difference of stakes in online examinations and other web-based applications like online banking. It was discussed that collusion attacks are unique and pose a threat to remote online examinations as well as face-to-face invigilated exams. A participant reported that:

Participant 4:

"There have been occasions when students have colluded and impersonated in the invigilated exams, where both parties were from the university"

Collusion is classified in different types and each type poses a different threat level in an online examination context. A student copying answers from a book or the Internet is not considered collusion because a third party is not involved. Discussion on collusion and types of collusion threats are discussed below.

1) Impersonation in Online Examinations Vs Online Banking

Impersonation is seen as a larger threat to the security of an online examination compared to online banking. There was collective agreement that impersonation poses a different threat to both because of the difference in stakes. As a user of an online bank account, an individual is less likely to share their login credentials or associated information with a third party as it may expose their monetary assets to risk. There was strong disagreement from participants, if they were asked to share their credential for an online banking system, where stakes are different. As shown in Table 2, participants perceived sharing of access credentials in online banking as a high security risk for the account holder and scored M = 5. According to a participant:

Participant 2:

"The potential risk you are exposing yourself to by giving people your banking details is enormous"

Unlike online banking, users of an online examination would share their access credentials with third party impersonators. These users have different stakes than in online banking, and individuals may be tempted to collude in order to boost their grades or qualify a test. The absence of invigilation or monitoring creates more opportunities and students are not challenged. According to many participants, there is a lower risk for a student to collude and share credentials for his online examination with a third party M = 2.2 (1 - Low Risk to 5 - Very High Risk). According to some participants:

Participant 1:

"If you are trying to collude, you would be interested to share your information"

Participant 2:

"Whereas if you are giving your detail to some person who can impersonate, the risk I suppose is potentially quite large, but essentially it is not as large as giving out your bank details"

In summary, there was an agreement that students in online examinations are more likely to collude with third parties and share their access credentials, which is discussed in the following section.

2) Impersonation

Students employing someone else to take their test instead of them would willingly share their credentials with impersonators, regardless of any rules or regulations [34]. Collusion between a student and a third party impersonator can happen using different communication approaches. A student may share credentials with a third party in real-time or asynchronously before an examination session using email, mobile phone for SMS (Short Messaging Service), or Instant Messaging. Access credentials can be shared using an email before a test, if the authentication method uses simple credentials which are easy to share. Also, a student may use email if an online examination is monitored or proctored remotely. For example, password for logging into an online examination and answer to memorable challenge questions can be shared through email before the test session. However, authentication approaches which implement dynamic and interactive mechanisms may discourage sharing access credentials beforehand. These questions are non-intrusive and created dynamically based on individuals' learning activities, and students would not know the questions beforehand. Another example is a dynamically-created security code sent to a mobile phone through SMS. However, students may share information via mobile phones in real-time. Participants in the focus group discussion identified that mobile phones pose a potential threat to share access credentials or answers to exam questions in real time. According to participants:

Participant 5:

"If I want to share a code, I would use my mobile phone"

"If I have a mobile phone I can receive text with the answers"

As shown in Table 2, participants in the focus group perceived sharing of access credentials using a mobile phone during an examination as a high security risk and scored M = 5.

Another potential threat is when a student colludes with a third party using remote desktop sharing. As in [34], remote desktop sharing software can be used to share the screen with someone remotely to impersonate and take the test. In an online examination scenario, where there is no invigilation, a student may share a screen or access credentials with a third party for impersonation. This was perceived as a serious threat and scored M = 4.5 (1 - Not serious at all – 5 - Very serious). According to a participant in the focus group:

Participant 5:

"I can easily share my screen with someone sitting somewhere else, who can see the same screen as I do"

There was agreement that a student may share access credentials via email, phone, instant messaging, and remote desktop with an impersonator to cheat in an online examination.

3) *Abetting*

In a non-proctored exam, students may receive help from a third party to answer the test questions. In their study, Tindell et al. [35] surveyed 269 students, with 10% admitting to the use of mobile phone for abetting during exams. Absence of remote proctoring or monitoring creates opportunities for students to ask third parties for help. A student and a third party could collaborate and answer the test questions based in the same location or communicate remotely. Participants of the focus group perceived this as a serious threat as there is always a possibility that a student may get someone to sit close by, or in a remote online examination, who is an expert. According to a participant:

Participant 9:

"I would imagine the trick would be to prevent people sitting next to you and doing the test with, and I think that is the biggest problem"

The content analysis in Table 2 shows that participants perceived this a high risk and scored M = 5, if a student invites a third party to the exam location for abetting.

VI. Security Analysis and Discussion

While it is established that collusion is a rising concern in remote online examinations, authentication approaches alone may not provide adequate security to mitigate both impersonation and abetting threats. Different types of collusion threats may need different deterrence approaches.

A challenge question approach, as well as ProctorU (secure browser and proctoring tool), were proposed to influence impersonation and abetting attacks. The focus group discussion on the proposed methods is presented in the following sections.

A. Dynamic Profile Questions to Influence Impersonation

The dynamic profile question approach was proposed as a solution to influence impersonation attacks in the first presentation. In order to explore participants' perception of the use of dynamic profile questions, the moderator asked whether they would use this approach in an online examination for their students. The majority of participants agreed and understood that it would make an impact on impersonation. The content analysis in Table 2 on the use of dynamic profile questions for mitigation of impersonation shows participants' agreement and scored M = 3.8. According to participants in the focus group:

Participant 6:

"Yes, I agree!"

Participant 7:

"Yes, it is better than what we do now"

Participant 8:

"Yes, it is that extra level of security"

Participant 5:

"Yes!"

Dynamic profile questions may influence impersonation attacks using phone and email. However, a student may share answers to these questions in impersonation attacks using mobile phones. It is likely to take extra time to exchange access credentials on mobile phone in real time, which may affect response time to challenge questions. Students are often expected to complete their tests in allocated time and response time can be used as a factor to influence the use of mobile phones. When probed, participants in the focus group provided positive feedback on the use of a response time factor to discourage impersonation. The content analysis in Table 2 shows participants' perception that timing answers may impact impersonation using a mobile phone, which scored M = 3.8. There was agreement that timing answers will deter students from colluding (M = 4.5). According to some participants:

Participant 1:

"If the answers are coming slowly, slower than what you would expect, or in some strange way, we can just say that we are not accepting this, because there is a problem"

Participant 4:

"It makes it very hard for somebody who pretends to be you or collude"

In a practical situation, if a student is taking noticeable time to respond to authentication and questions in an online examination, it could be noticed by the course administrator/tutor. According to some participants, response time could be used as a factor for assessing test questions as well.

Participant 4:

"If they cannot get through the test in time. Time can be used as a factor to minimise the looking"

Course and online examination design is another important factor to discourage students from taking help. As an example, if an online test consists of multiple choice questions, an expected response time can be easily determined. However, for an open text descriptive question, this may vary. A participant suggested that course and examination design may discourage students from searching the Internet.

Participant 8:

"That's what we have done on the JAVA module. Because some student came and said, I can just search the answer on the Internet and can find the correct answer. I replied, if you do, you won't get enough time to finish the majority of the questions. Basically, those questions cost the time"

However, there are risks associated with the implementation of response time factor for reduction of collusion. This may be challenging to prove a slow response time as the only evidence of a collusion attack. Some participants raised their concerns about using a response time factor to penalise students:

Participant 6:

"I think it is a bit of a hassle to try and prove whether a student has colluded or cheated"

In a practical scenario, students may challenge a decision if they were penalised due to a longer response time, and ask to redo their test. Another participant raised concerns for penalising students based on a response time factor:

Participant 1:

"What if the student wants to protest? If you say, well, I don't accept this answer, and the student says, why not, I dint do anything wrong"

However, the majority of participants agreed to implement additional security factors, including response time, to deter collusion.

Participant 4:

"If we are confident that someone has cheated, we know that the test in invalid, we ask the student to go back and do it again"

B. Secure Browser and Proctoring (ProctorU) to Influence Abetting

The majority of traditional authentication approaches may not detect abetting attacks to ensure that a student is taking an online test without getting help from someone sitting close by or in a remote location. Live invigilation or monitoring may mitigate abetting and discourage a student from communicating with a third party during an online examination session. Participants in the focus group agreed that remote proctoring may influence abetting. According to a participant:

Participant 8:

"I think the remote proctoring possibility sorts out the person sitting next to you to some extent anyway"

A remote proctor and secure browser can be implemented to influence the use of unwanted software e.g. Skype, remote desktop sharing, Internet browser and invigilate an online examination session. One such example is ProctorU, a remote proctoring system for online tests. Trained invigilators at ProctorU watch test-takers by using screen sharing and webcam feeds at offices in Alabama and California [21]. An invigilator verifies the identity of an online student and monitors the examination process. This may be an expensive approach for online tests with a large number of students. In order to explore their feedback on using ProctorU, participants were asked if they would use this approach in an online examination for their students. A large number agreed and understood that it would influence collusion.

Participants suggested that the use of dynamic profile questions and ProctorU together would enhance the security of online examinations to mitigate impersonation and abetting.

Participant 9:

"And by making it harder with challenge questions could have another additional layer. Ok! The name did match, and the photo looks all right, however, how come this part (dynamic profile question) of the authentication did not occur"

VII. CONCLUSION

The study investigated a group of experienced online programme tutors from the University of Hertfordshire. Based on their feedback, impersonation and abetting were identified as common cause for concern. The empirical results in previous studies and feedback from participants suggest that dynamic profile questions are more usable than text-based and image-based questions. This method may influence impersonation attacks. However, authentication approaches including challenge question may not prevent students taking help from someone sitting close by in abetting attacks.

The participants supported the use of secure browser and remote proctoring with dynamic profile questions to prevent impersonation and abetting attacks.

References

[1] Kritzinger E. Information Security in an E-learning Environment. Education for the 21st Century—Impact of ICT and Digital Resources: Springer; 2006. p. 345-9.

[2] Miguel J., Caballé S., Xhafa F., Prieto J. "A massive data processing approach for effective trustworthiness in online learning groups." Concurrency and Computation: Practice and Experience. 2015;27(8):1988-2003.

[3] Furnell S. M., Dowland P., Illingworth H., Reynolds P. L. "Authentication and supervision: A survey of user attitudes." Computers & Security. 2000;19(6):529-39.

[4] Marcel S., Del Millan J. R. "Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation." Pattern Analysis and Machine Intelligence, IEEE Transactions on. 2007;29(4):743-52.

[5] Ullah A., Xiao H., Lilley M., editors. "Profile Based Student Authentication in Online Examination". International Conference on Information Society 2012; London, UK: IEEE.

[6] Aggarwal R., Bates I., Davies G., Khan I. "A study of academic dishonesty among students at two pharmacy schools." Pharmaceutical journal. 2002;269(7219):529-33.

[7] Bowers W. J. "Student dishonesty and its control in college." 1964.

[8] Strang R. Behavior and Background of Studentsin College and Secondary Schools. New York: Harper and Brothers; 1937.

[9] Ullah A., Xiao H., Barker T., editors. "A Classification of Threats to Remote Online Examinations". Computing and Communication (IEMCON), 2016 International Conference and Workshop on; 2016: IEEE.

[10] Ullah A., Xiao H., Barker T. Usability of Activity-Based and Image-Based Challenge Questions in Online Student Authentication. Human Aspects of Information Security, Privacy, and Trust: Springer; 2015. p. 131-40.

[11] 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.

[12] Ullah A., Xiao H., Barker T., Lilley M., editors. "Graphical and Text Based Challenge Questions for Secure and Usable Authentication in Online Examinations". The 9th International Conference for Internet Technology and Secured Transactions (ICITST); 2014; London, UK: IEEE.

[13] 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.

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

[15] Ullah A., Xiao H., Lilley M., Barker T., editors. "Design, privacy and authentication of challenge questions in online examinations". IEEE Conference on e-Learning, e-Managementand and e-Services (IC3e); 2013; Malaysia: IEEE.

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

[17] Powell R. A., Single H. M. "Focus groups." International journal for quality in health care. 1996;8(5):499-504.

[18] Kitzinger J. "Qualitative research. Introducing focus groups." BMJ: British Medical Journal. 1995;311(7000):299.

[19] Goss J. D., Leinbach T. R. "Focus groups as alternative research practice: experience with transmigrants in Indonesia." Area. 1996:115-23.

[20] Powell R. A., Single H. M., Lloyd K. R. "Focus groups in mental health research: enhancing the validity of user and provider questionnaires." International Journal of Social Psychiatry. 1996;42(3):193-206.

[21] Eisenberg A. "Keeping an eye on online test-takers." New York Times. 2013;2.

[22] Creswell J. W. Qualitative inquiry and research design: Choosing among five approaches: Sage; 2012.

[23] Vician C., Charlesworth D. D., Charlesworth P. "Students' Perspectives of the Influence of Web-Enhanced Coursework on Incidences of Cheating." Journal of Chemical Education. 2006;83(9):1368.

[24] Olt M. R. "Ethics and distance education: Strategies for minimizing academic dishonesty in online assessment." Online Journal of Distance Learning Administration. 2002;5(3).

[25] Colwell J. L., Jenks C. F., editors. "Student Ethics in Online Courses". 35th Annual Conference Frontiers in Education (FIE '05) 2005; IN, USA: IEEE.

[26] Wielicki T., editor. "Integrity of online testing in e-learning: Empirical study". Fourth IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06); 2006: IEEE.

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

[28] Mcmurtry K. "E-Cheating: Combating a 21st Century Challenge." THE journal. 2001.

[29] Chiesel N. "Pragmatic methods to reduce dishonesty in web-based courses." A Orellana. 2009:327-99.

[30] Hafiz M. D., Abdullah A. H., Ithnin N., Mammi H. K., editors. "Towards identifying usability and security features of graphical password in knowledge based authentication technique". Modeling & Simulation, 2008 AICMS 08 Second Asia International Conference on; 2008: IEEE.

[31] Braz C., Robert J.-M., editors. "Security and usability: the case of the user authentication methods". Proceedings of the 18th International Conferenceof the Association Francophone d'Interaction Homme-Machine; 2006: ACM.

[32] Berg B. L., Lune H. Qualitative research methods for the social sciences: Pearson Boston, MA; 2004.

[33] Berelson B. "Content analysis in communication research." 1952.

[34] Frank A. J., editor. "Dependable distributed testing: Can the online proctor be reliably computerized?". e-Business (ICE-B), Proceedings of the 2010 International Conference on; 2010: IEEE.

[35] Tindell D. R., Bohlander R. W. "The use and abuse of cell phones and text messaging in the classroom: A survey of college students." College Teaching. 2012;60(1):1-9.