21st Century Academic Forum Conference Proceeding
2015 Conference at Harvard

Assessments in the 21st Century: No more cheating during e- Examinations!!!

Aarthi Nagappan
Faculty of Education and Distance Learning,
Botho University, Gaborone, Botswana

Abstract

Education has now become more accessible and flexible via e-Learning. As newer technologies become less expensive and more learners want to study from the comfort of their homes, online learning environments are becoming widely used for teaching and learning purposes (Zhang & Kenny, 2010). With the introduction of e-Learning, online examination is a great option for modern life. However e-Examinations are not secure enough in most cases and require invigilation or proctoring mechanisms to enforce secure conduct of an examination. Thus, the future of e-learning is greatly attributed to the credibility of e-Examinations. Today, some of our 21st Century e-Learners travel to test centre to write their examinations, which defeats the purpose of flexible learning. The question for Open and Distance Learning institutions (ODL) is "Are we ready to administer cheating free e-Examinations from home?" so we are sure that these students just don't walk out with online degrees for examinations which they never sat. The problem this research will address is to find solutions to improve security for e-Examinations conducted from Home. Exhaustive literature review, observing test centers, interviews and questionnaires were used in identifying security threats facing e-Examinations and a secure e-Examination model is proposed. Continued presence verification of the candidate for the entire duration of the exam with strong biometric authentication mechanisms is suggested as key to curb impersonation.

Key Words: e-Learning, e-Examination, Authentication, Presence Verification

Introduction

Information and communication technological developments sweeping the globe are rapidly transforming every sector. Education Industry is no different and is getting bigger and brighter with e-Learning. According to Pappas (2013), students and employees are becoming more interested in earning their degrees through e-Learning. As a result, knowledge and skill acquisition is changing with modern use of technology. E-Examinations have become a new and popular phenomenon in Higher Education. The tools and techniques developed for e-Learning are providing learners with flexibility and a more effective medium for instruction.

A survey conducted informs that in the higher education institutions, about 35% of students take at least one online course. Furthermore, 65% of higher education institutions now say that online exam is a critical part of their long term strategy (Chen & He,2013). Security is one of the challenges for both the traditional and online examination system (Sarrayrih & Onyesolu, 2013). E-learning environments are increasingly common as can be seen with the numerous resources spread over the network. At the same time a rise in student cheating practices has been as identified. Institutions are expected to ensure that their students are not cheating and/or indeed the right candidate who should be writing the exam and for the entire duration of the examination. This is important for assuring credibility of e-Examinations, a major stumbling block in promoting e-Learning. One way to mitigate security breach during e-Examination is to identify, authenticate and continuously monitor candidates during the examination. This helps curb impersonation during e-Examinations. Impersonation refers to an act of dishonesty where one person pretends to be another for him/her to gain access to unauthorized resources/assets and this has been reported several times during examinations despite strict measures being put in place.

Identification refers to confirming "who you are?"; authentication verifies indeed "is it really you?"; and continuous monitoring would guarantee that "you are the right candidate who wrote the full examination without any support or assistance" (Sabbah,2011). Authentication factors include ownership (e.g., cards, passport, etc.,), knowledge (e.g., pin, password, security questions) and biometric (e.g., face, iris, finger print recognition) or behavioural dynamics (e.g., keystroke, mouse dynamics, etc.,). It is not sufficient to guarantee CIA goals (Confidentiality, Integrity and Availability) but also achieve PIA goals (Presence, Identity and Authentication) for administering credible examinations.

As much as moving to e-Examinations provide location flexibility to students, it also proves to be much more challenging than originally expected. Improving student authentication in e-Examinations in order to prevent fraudulent activities is seen to be highly important. ODL institutions are asked to guarantee examination standards irrespective of traditional or online medium, as exams continue to remain as primary means for assessing learner's knowledge and skill. This would require building more security into current examination systems. If examinations are designed and administered in such a way that they guarantee 4 types of security namely user security, data security, location and web security, then perhaps that would be a much more reliable online examination system for use in the 21st Century.

The purpose of this paper is to produce the related discussions in the literature, to present an in-depth analysis of the security issues facing online learning. The different threats facing e-Examinations were identified through questionnaire and risks from these threats ranked to see which threats have more impact on online examination. The online learning source can become proactive and knowledgeable as they diminish the security risks found in online learning. Current security for e-learning systems relay principally on the deployment of passwords authentication

system which will no longer stand test of time. Online learning systems need to identify with the state of the art in this energetic field. So as an effort in this direction and in response to increasing threats facing e-Examinations, researcher has come up with a number of counter measures and proposed through a theoretical framework.

Problem Statement

With e-Learning, E-Examinations seem to be a great option for modern life. However these examinations are not secure enough and poses some threats, it can be difficult to confirm true user authentication and prevent cheating practices during examinations. It is vital that quality standards be met for all examinations.

The problem this study addresses is to determine the various threats and challenges to e-Examinations and to develop a theoretical framework to minimize cheating by student/s during home based e-Examinations.

Research Questions

1. What are security threats and challenges to e-Examinations?
2. How can security be built into current online examination models?

Research Hypothesis

1. E-Examinations are prone to cheating by students.
2. Improving student authentication and continuous monitoring of e-Examination candidates minimizes cheating during the examination.

Research Scope

This research is confined to e-Examinations, the major threats were identified and a model is proposed which upon implementation will assist to administer cheating free home based examinations.

Significance of the research study

ODL institutions as much as they are interested in e-Learning they are still reluctant in seeking full-fledged support from e-Examinations for 2 main reasons

(i) e-Examinations are not secure and students cheat during these examinations

(ii) Effective invigilation involves huge proctoring costs.

Examinations continue to be the primary means of assessing knowledge and skills and hence the responsibility of every institution to assure examination standards are met .In the 21st century for institutions to go fully online it is important that research be carried out to build additional security into existing examination systems. No institution would want their students to walk away with online degrees for exams they never appeared, dishonesty should be curbed at its roots for a sound education system. This research would benefit education sector by allowing students to write examinations from the comfort of their home. The goal of credibility of e-Examinations will have to be achieved at the end of this research study.

Literature Review

Computer-based testing uses information technology for conducting assessments. The aim of these assessments is fair, faster and reliable examinations (Oluwatosin & Samson, 2013). According to Sabbah(2012), much has been said about the "lack of secure and trusted e-

assessment models as the prime reason for failure of e-Learning" . Student Authentication is the key to ensure exams are given by fair means (Alotaibi,2010).

"Traditionally, authentication systems are required to verify a claimed identity only one time at the initial login. However, the Security of online summative assessments goes beyond ensuring that the right student is authenticated at the initial login. More is required to verify the presence of an authenticated student for the duration of the test" (Apampa et al.,2010).

There are various assessment authentication schemes, some of which are currently researched whilst some have been implemented and with others experiments are currently ongoing. (1)Local/Remote Proctored only scheme. (2)Uni-modal biometrics (3)Bimodal biometrics(4) Multimodal authentication (5)Video monitoring ,these present wide scope for research and promises some possible solution for improving security of e-Examinations.

Sabbah(2012) discusses the following types of Impersonation threats

"(1) Type A impersonation, which might occur in two cases, either the proctor could not detect it, or he allowed impersonation by force, sympathy or bribery.

(2) Type B, which occurs when a student passes his security information to another, who uses them to answer the exam on his behalf. Username-password pairs fall in this type.

(3) Type C, which occurs when a student just login to an exam, letting another to continue on his behalf. Non-shareable attributes such as biometrics fall in this type.

(4) Type D, a new threat where a student logins and answer the exam but with an assistant giving him the answers".

According to Sabbah's (2012) model a combination of automatic video matching and continuous bimodal biometric authentication using fingerprint and keystroke dynamics should be used. This ensures that the examinee is the correct person throughout the e-examination without a need for a proctor. A novel blob based presence verification (BlobPV) system which adopts a video blob analysis operation to detect and classify the changes to a student's presence status in the test environment. This helps identify the student that is currently using the system (Apampa et al., 2010) Another biometric solution proposal is to use fingerprints during the examination login and later constant monitoring of the student through the use of a webcam. If any abnormal behavior is found the student is then prevented from writing the exam (Ramim et al., 2009).

A multi model system for authentication of students during examination was discussed in (Asha & Chellappan, 2008). This technology uses a combination of finger prints and mouse dynamics. Finger prints of the student are taken at the beginning of the login. The mouse movements made by the student during the examination period are recorded and later verified for tracking student behavior. According to Fayyoumi & Zarrad (2014), security for an online exam is provided by using face recognition technology to authenticate learners for attending an online exam, the system continuously (with short time intervals), checks learner identity during the whole exam period in order to ensure that the learner who started the exam is the same one who finished. Moreover, this minimise the possibility of cheating by looking at an adjacent PC or reading from an external paper. Another model was based on finger print based biometric system for identification and distributed firewall techniques to monitor candidates and control network packets of all machines incorporating the traditional username and password for authentication (Onyesolu et al., 2013).It was discussed in (Sarrayrih & Ilyas, 2013) to use 360^{o} camera and finger print recognition device for authentication and presence verification. Unauthorized interference of other users in the network is restricted by creating a domain IP addresses, which are different will be prohibited.

Many experiments have been carried out so far and numerous biometric solutions are being researched every year; though newer and better models are evolving to address security challenges facing e-Examinations. There is no fool proof model that guarantees secure cheating free online examination, because of this it is still difficult to trust e-assessment within an e-learning model. This research aims to improve security for e-Examinations by identifying various threats and developing counter measures to mitigate the risks posed by these threats to e-Examinations. A robust e-Examination model is needed and must confirm PIA goals in addition to CIA goals for assuring credibility of e-Examinations.

Research Methodology

This is a mixed methods research where both qualitative and quantitative data were gathered to answer different research questions. Major findings from both strands were subsequently synthesized to inform future action.

The research questions helped the researcher to choose appropriate research styles in order to seek answers that will guide the research in the right direction. [RQ –Research Question]

RQ(1)- Participatory research was used

(1)Visit test centres and interview test coordinators

(2)Administer questionnaire to students, lecturers, technical and distance learning personnel

(3) Interviews with assessment personnel and exam coordinators who volunteering shared their experiences about student's cheating and different threats to e-Examinations.

Once threats were identified, RQ(2) was aimed at building additional security for current online e-Examination models, this was based on constructivist theory to come up with a framework for secure e-Examination models

The outcome of this paper is a theoretical framework and in future the model will be implemented, tested and evaluated for effectiveness. This is a work in progress and quasi experimental approach will be used in subsequent section of research work to implement the model and the intervention will be reviewed using participatory approach. The findings from future stage will be presented as part of subsequent research papers.

Population and Sampling

Population used for this study included

(1)Exam coordinators

(2)Assessment department personnel

(3)Proctors and Invigilators

(4)Students

(5)Test center administrators

(6)Technical and Distance Learning department personnel

Purposeful and Random Sampling was used in selecting appropriate samples for this research. Researcher chose a random sample of cases from above population (probabilistic) that has already been carefully drawn from a purposive sample (non- probabilistic).

Reasoning for purposive sampling

1. To access knowledgeable people(those with experience in e-Examinations)

2. Random sample without purposive sampling could bring up participants who might be ignorant of issue and hence may not be able to comment on matters of interest to researcher
3. Acquire in depth answers to research questions and better outcomes
4. Typical cases well represented through chosen sample

Instruments and Procedures

Instruments included questionnaires, semi structured interviews and visit to test centre. Access to participants was challenging and needed planning ahead. Careful questionnaire design was critical to seek responses that would guide research and hence questionnaire was internally validated for content and construct by 4 knowledgeable colleagues and pilot run prior to distribution to participants. Though most questionnaires were returned yet not all were returned and some were partially completed and hence could not be included in analysis. Interview and observation schedules were planned early in association with willing participants. It was important to adhere to appointment; however researcher was faced with challenges of cancellation of appointments by some interview participants and was later rescheduled to another date.

The future of this research relies in successfully implementing the proposed model, testing and evaluation. Prototype design will make use of UML and Java coding to develop the prototype. Evaluating effectiveness of prototype and feasibility for use in real time will be carried out by administering home based examinations under controlled conditions for a limited number of participants.

Data Analysis, Findings and Discussion

The review of literature has suggested that security is still not achieved in e-Examinations. In order to confirm this, a visit/s was made to a test center where some students were writing online exams. Observation and interview with test administrators in the center helped to gain insight about the probability of cheating, the various cheating practices and security mechanisms installed in the test center to mitigate risks of student cheating in exams. The security mechanisms put in place to ensure security during online accounting exams was quite strong; however, they were complex systems, expensive and requiring trained personnel to use them and regular maintenance.

Following the visit, semi structured interviews were scheduled with assessment personnel this further revealed cheating exists and there was discussion on various cheating techniques that were normally used by students to cheat during examinations. Botho University has a blended and distance learning (BDL) department which facilitates courses being offered online in order to cater for the needs of a diverse population. The cheating violations which were raised by the assessment personnel during interviews were captured, carefully analyzed and included in the questionnaire administered to students, technical, BDL team and lecturers at Botho University.

Questionnaires

It was not easy to come with the questionnaire, lot of thinking was needed, once the draft was ready it was validated for content to confirm indeed it will assist in fetching answers to research question 1, then it was validated for construct to see if it is was carefully designed relevant to population chosen and then for grammatical mistakes. There were a number of valid suggestions passed which were incorporated and questionnaire was pilot run ,again few corrections were needed prior to administering to chosen sample(Final questionnaire is included

in the Appendix). Though researcher was interested in large sample from various institutions, due to time constraints and commitments it was restricted to Botho University, for the future questionnaires there is a plan to administer at other institutions as well to get a broader perspective.

The validated and pilot run questionnaire was distributed to 100 participants chosen from the population. Purposeful and random sampling was used to identify the sample participants, of the distributed questionnaires. 72 questionnaires were returned (several follow ups were required) of which only 60 had all questions answered, 10 returned were partially answered and 2 had several check boxes ticked and hence were treated void and was not included during data analysis. Below is data analysis and findings from 60 questionnaires considered for the purpose.

Data Analysis

Below are the results of the questionnaire Section A, which provides general information about the research participants

ITEM CATEGORIES	**COUNT**
GENDER	
MALE	34
FEMALE	26
AGE	
<25	1
25-35	34
36-45	14
46-55	8
>55	3
INSTITUTION-BOTHO UNIVERSITY	1
OCCUPATION	
LECTURER	54
STUDENT(students were on their semester holidays)	3
TECHNICAL STAFF	1
DISTANCE LEARNING STAFF	2
FAMILIARITY WITH E-LEARNING AND E-EXAMINATIONS	
NOT FAMILIAR	2
MODERATE	12
GOOD	21
VERY GOOD	18
EXCELLENT	7
NUMBER OF E-LEARNING COURSES YOU HAVE ATTENDED	
NEVER	7
ONE	13
TWO	10
THREE	10
ABOVE FIVE	20
NUMBER OF E-LEARNING COURSES YOU HAVE TAUGHT	
NEVER	33
ONE	12
TWO	7
THREE	1
ABOVE FIVE	7
ANY EXPERIENCE IN STUDENTS CHEATING DURING TRADITIONAL OR E-EXAMINATIONS?	
YES	30

NO	30
This question was also enquiring on number of times cheating was caught, not all respondents indicated scores and for those who had mentioned, it was not clear whether this cheating was caught during traditional or e-Examination as no comments was included by some participants, this made it difficult. This has pointed out the need to researcher to revisit questionnaire to see how best this question could be rephrased to get accurate answer.	-
ANY CHANCES FOR CHEATING DURING E-EXAMINATION?	
IMPOSSIBLE	2
MODERATE	12
LOW	6
HIGH	23
VERY HIGH	17
IS THERE A NEED FOR PROVIDING SECURITY FOR CHEATING FREE E-EXAMINATIONS?	
NOT NECESSARY	3
LOW PRIORITY	4
IMPORTANT	20
HIGH PRIORITY	26
URGENT	7

Table 1 General information of participants

There were 34 males and 26 females who responded to the questionnaire, age wise count has been furnished in the above table. As can be seen, most were lecturers by occupation and falling in the age range of 25-35. With regards to their familiarity with e-Learning and e-Examination, 21 scored it good and 18 very good which is quite impressive. There were 40 out of 60 participants who have attended 2 and more e-Learning courses. There were 20 participants who have said they have attended more than 5 courses which is good for a middle income developing country like Botswana. However, not many have taught e-Learning courses except for 27 participants out of 60. 33 have never had the opportunity to teach an e-Learning course. 7 claim they were fortunate to teach more than 5 online courses. The question addressing the participants' experience with cheating students during examinations brought about interesting results of 50:50. A significant number of participants (66.6%) feel there are chances for cheating during e-Examinations and 88.3% see the need for providing improved security during e-Examinations. This questionnaire was very insightful and has clearly confirmed that cheating during e-Examinations exists and there is need for a robust and secure e-Examination model for administering cheating free home based e-Examinations. Literature reviewed, Interviews and visit to test center also was confirming the same to the researcher and was an additional evidence strongly motivating this research.

Section B – Ranking Cheating violations during e-Examinations

The second part of the questionnaire was intended to seek answers to the first research question, which was to identify threats to e-Examinations. Here the participants weighed each of the cheating violations by weighing the risks on a scale of 1-5, where 1 stood for lowest risk and 5 was for serious high risk. The below table presents consolidated findings and helps to identify major threats to e-Examinations.

No	CHEATING ACTION	Risk Rating: Count(n)					Total
		1	2	3	4	5	
1	Impersonation(someone replaces the candidate)	8	7	11	11	23	**60**
2	Someone offers to help with answers(sitting beside or nearer to candidate)	6	5	13	17	19	**60**
3	Notes and other material in possession	2	4	15	16	23	**60**
4	Using search engines eg.Google	8	7	14	15	16	**60**
5	Support using mobile devices(sms,call)	5	13	16	16	10	**60**
6	Paid expert help during exam(FB and other web pages)	10	13	15	14	8	**60**
7	Looking for answers from notes stored on PC or Laptop	8	10	16	15	11	**60**
8	Re-directing webcam	16	17	11	10	6	**60**
9	Looking around or moving head away from webcam	14	12	20	10	4	**60**
10	Projecting questions and seeking help	15	13	13	10	9	**60**
11	Login by another student from different IP address for same exam	17	14	13	7	9	**60**
12	Using Rest room as an excuse	3	9	18	16	14	**60**

Table 2 Risk rating for various identified threats

The highlighted numbers indicates what the risk level is or impact of risk that majority of participants see for each of the listed cheating action. Risks are ranked to identify major threats to e-Examinations which is answer to research question 1. Below table ranks the 12 cheating actions in the order of risk predicated. The main risks are threats: impersonation, use of notes and other materials, and help from others.

No	CHEATING ACTION
1	Impersonation(someone replaces the candidate)
2	Notes and other material in possession
3	Someone offers to help with answers(sitting beside or nearer to candidate)
4	Looking around or moving head away from webcam
5	Using Rest room as an excuse
6	Login by another student from different IP address to continue same exam
7	Re-directing webcam
8	Using search engines eg.Google
9	Support using mobile devices(sms,call)
10	Looking for answers from notes stored on PC or Laptop
11	Paid expert help during exam(FB and other web pages)
12	Projecting questions and seeking help

Table 3 Risk ranking to identify major threats to e-Examinations

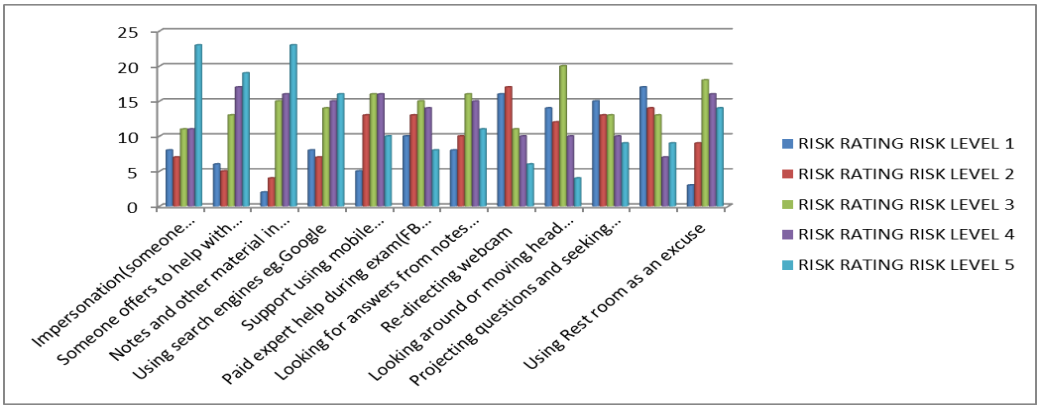

Figure 1 Risk rating by participants to identify major threats to e-Examinations

X axis indicates cheating actions and Y axis number of participants. The blue and violet bars for a cheating action/threat implies a higher the risk of cheating during an e-Examination.

Research question 2 focused on developing counter measures to identified threats and the outcome of this research is a theoretical framework proposed in the next section which will address all of the above listed 12 threats and will provide security for credible e-Examinations meeting security standards. This is work in progress and the proposed model is yet to be developed, pilot run and evaluated for effectiveness of use in real time examinations.

Proposed e-Examination Model

Education is transforming quickly and no doubt there are more and more adult learners who are juggling between commitments but who still want to pursue higher education for professional growth, knowledge and other reasons. Online and distance learning is prospering as a result of the demand from these learners but at the same time diminishing as security standards for e-Examinations are not yet fully achieved. There are numerous threats that have been discussed in previous sections and these are challenging online education.

Research question 1 helped in finding the various threats to online examination and Research question 2 assisted in finding counter measures for each of the identified threats. All threats regardless of major or minor needs to be paid attention as even small loophole can break the trust stakeholders have on e-Learning and e-Examinations.

No	CHEATING ACTION	COUNTER MEASURE
1	Impersonation(someone replaces the candidate)	Multifactor Authentication (Photo verification, Finger Print Authentication and challenge questions)
2	Notes and other material in possession	Video Monitoring
3	Someone offers to help with answers(sitting beside or nearer to candidate)	Video Monitoring
4	Looking around or moving head away from webcam	Video Monitoring
5	Using Rest room as an excuse	Jumbled questions released one at a time
6	Login by another student from different IP address to continue same exam	Domain login allowing one IP address per student
7	Re-directing webcam	Video Monitoring
8	Using search engines eg.Google	Blocking all ports and Browser except for exam window
9	Support using mobile devices(sms,call)	Video Monitoring
10	Looking for answers from notes stored on PC or Laptop	Laptop is locked and allows access only to examination window
11	Paid expert help during exam(FB and other web pages)	Blocking all ports and Browser except for exam window
12	Projecting questions and seeking help	Blocking all ports

Table 4 Countermeasures for each cheating action posed as a threat

Having identified the counter measures to various threats, a theoretical framework has been proposed in this paper. The aim of developing this framework was to minimize and if possible eliminate cheating completely during e-Examinations. This proposed theoretical risk driven model uses Multifactor authentication: Login-Password, Finger print, Challenge questions and believes in use of video monitoring, blocking of ports , restricted IP addresses to provide adequate security during e-Examinations. The activity flow of the proposed model is

shown below and indicates the steps a student needs to go through prior to successfully starting the examination.

Identification, Authentication and Presence verification are extremely important to assure right candidate is writing the entire exam. The proposed work ensures both PIA and CIA goals are met in developing a secure and robust e-Examination model.

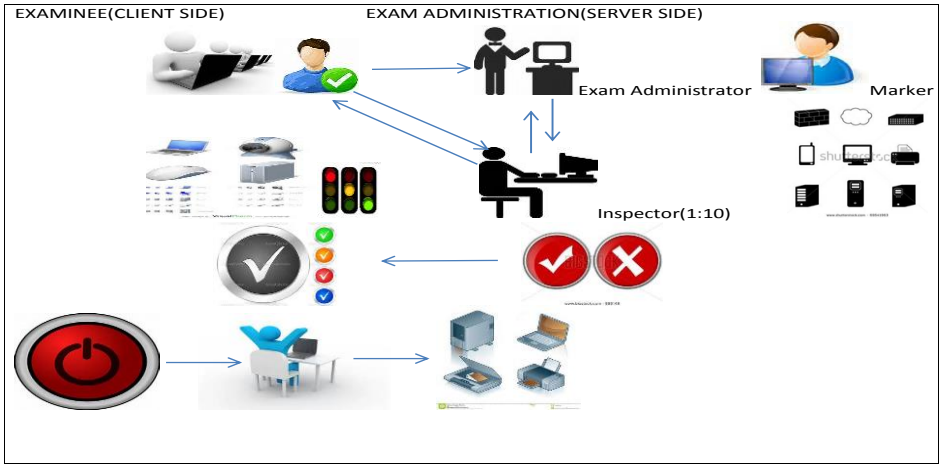

Figure 2 Proposed e- Examination Framework

The online examination in the proposed model is based on client server architecture where students are expected to connect to examination server controlled by the exam administrator. He/ She verifies Inspectors (also called proctors or Invigilators) and grants them permission to access the media server through which student exams will be relied to these inspectors for monitoring purposes.

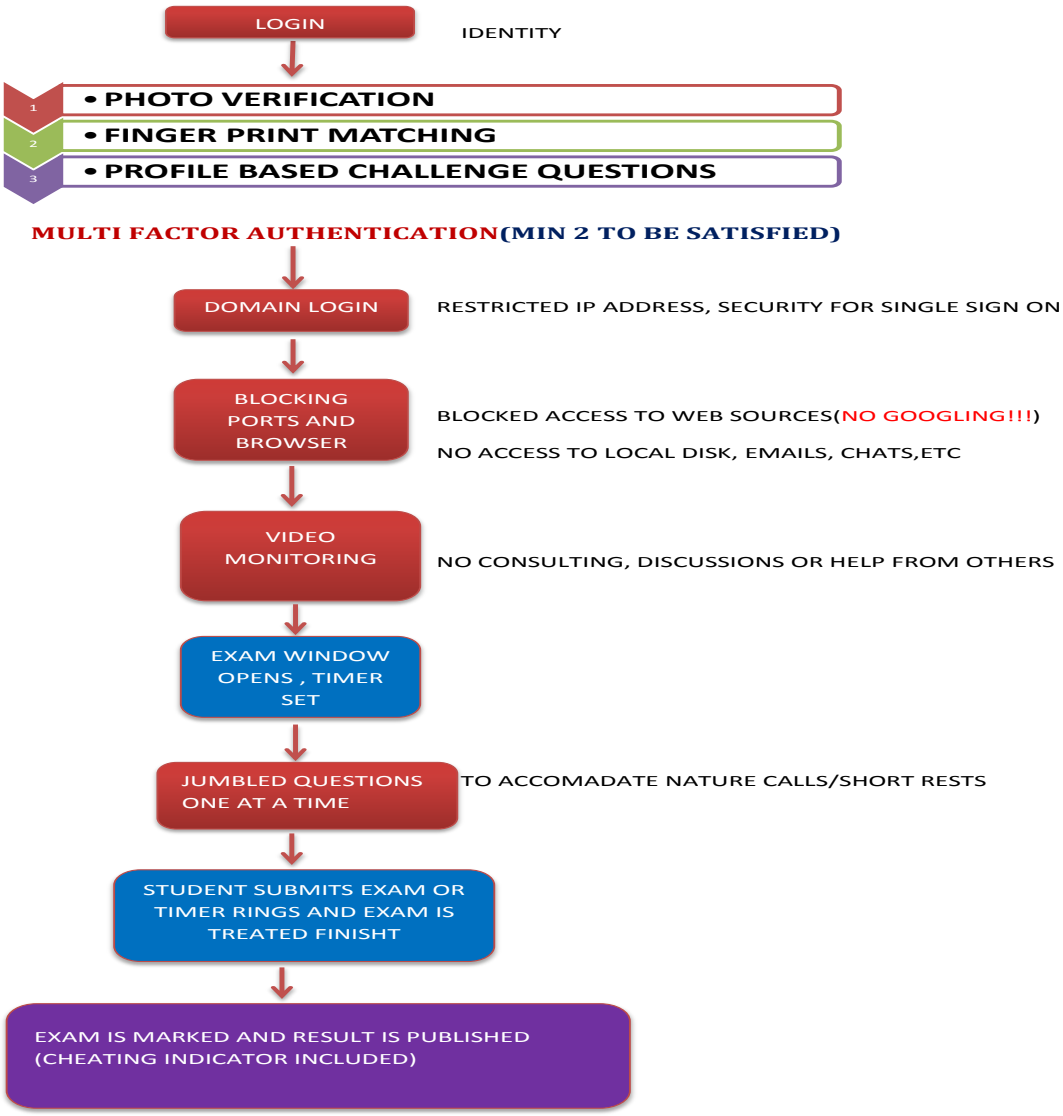

Figure 3 Activity flow for the proposed model

Students connect to the server by entering a username password for identification. Upon successful login, the webcam is turned on and photo verification takes place followed by a finger print which is captured using special device called finger print mouse and matched against a database. Once completed, each student will be asked some challengeing questions for further verification. Finally a traffic signal indicates red-most/all incorrect answers, green-allowed to proceed and yellow-few questions alone answered.

If two of the authentication mechanisms is successfully cleared then the student is granted permission by the inspector to enter the domain using inspector password where only students from valid IP addresses will be granted access to exam server. Upon entering the exam domain, all ports in the laptop and browser are de-activated so the student can only see their examination window. Moreover, students will not be able to google nor access materials stored on the laptop.

During the exam, video monitoring is started and a timer ticks which signals the student to begin exam. Jumbled questions are displayed one at a time. Should a student need to use the rest room he is expected to use a tool that indicates this to the inspector. After submitting the current answer, the student is allowed to use the rest room, while the timer continues to tick. The student is required to return in a defined period of time. When the student returns, he presses the tool again and is now allowed to proceed to the next question. The student will not be able to navigate back. In addition, there is no possibility for a student to know the next questions when leaving to rest room as the questions are randomly jumbled and pop up on the screen one at a time. At the end, the student either submits the completed exam, or a timer rings and the exam is finished.

The exam is automatically marked where possible, or else it is sent to a marker. The cheating indicator is used during marking to award appropriate marks to student where it could range from reducing few marks to zero marks turning exam void if student attempted seriously to cheating in exam. Thus the above is a very secure e-Examination model which will provide for a brighter and prosperous e-Learning medium to our future students.

Conclusion and Future Direction

E-learning is growing like wildfire mainly because many institutions are becoming interested in e-Examinations. As a critical component in assessing student's knowledge and skill, there is clearly a need to provide adequate security for e-Examinations. It is important that regardless of whether examinations are traditional or online and be it written in a quality assured test center or home, it is important to ensure examination standards are being met.

The researcher in this paper has proposed a secure theoretical framework for administering cheat-free home based e-Examinations. Implementing this model can assist students with writing their examinations from home while institutions are assured of exam credibility. This research is primarily focused on strengthening student authentication as a means to secure e-Examinations and could be extended in future to dimensions of improving security for our online examination servers in order to secure exam question papers, biometric images used for student authentication, untampered results/grades, web security, etc.,

Academic dishonesty needs be curbed at its roots, and as educators, we need to assure only students with necessary knowledge and skills graduate so that they are able to find employment or create new businesses. As such, this is an important way through which a nation can flourish from quality education.

References

Alotaibi, S.(2010).Using Biometrics Authentication via Fingerprint Recognition in E-exams in E-Learning Environment. Proceedings of the the 4th Saudi International Conference, The University of Manchester, UK.

Apampa, K.M., Wills, G.,& Argles, D.(2010).Towards a Blob-based Presence Verification System in Summative E-Assessments. Proceedings of the International Computer Assisted Assessment (CAA 2010) Conference Research into E-Assessment, Southampton, UK.

Asha, S. Chellappan, C.(2008).Authentication of e-learners using multimodal biometric technology in International Symposium on Biometrics and Security Technologies(pp. 1-6), Islamabad, Pakistan.

Cohen, L., Manion, L., & Morrison, K.(2011). Research methods in Education, 6th Edition.

Coughlan, s. How do you stop online students cheating. Retrieved from: <http://www.bbc.com/news/business-19661899>

Fayyoumi, A. and Zarrad, A.(2014) .Novel Solution Based on Face Recognition to Address Identity Theft and Cheating in Online Examination Systems. 4, 5-12, doi:10.4236/ait.2014.42002.

King, C.G., Guyette, R. W., & Piotrowski, C. (2009). Online exams and cheating: An empirical analysis of business students' views. The Journal of Educators Online, 6(1), 1-11.

Oluwatosin, T. & Samson, D.(2013).Computer-Based Test: Security and Result Integrity. Journal of Computer and Information Technology . 2(2), 324-329.

Onyesolu, M.O., Ejiofor, V. E., Onyeizu, D.N.,& Ugoh,D. (2013).Enhancing Security in a Distributed Examination Using Biometrics and Distributed Firewall System.International Journal of Emerging Technology and Advanced Engineering, 3(9),65-70

Pappas, C., Top 10 e-learning statistics for 2014.Retrieved from: <http://elearningindustry.com/top-10-e-learning-statistics-for-2014-you-need-to-know>

Ramim, M.,& Levy, Y.(2009).Initial Development of a Learners' Ratified Acceptance of Multibiometrics Intentions Model (RAMIM), Interdisciplinary Journal of e-Learning and Learning Objects,5, 379-397.

Sabbah,Y., Saroit, I.,& Kotb, A.(2012).Synchronous Authentication with Bimodal Biometrics for e-Assessment: A Theoretical Model. Proceedings of the 6th International Conference in Sciences of Electronics, Technologies of Information and Telecommunications (pp.21-24) ,March 2012.Tunisia, Sousse.

Sabbah,Y., Saroit, I.,& Kotb, A.(2012) A Smart Approach for Bimodal Biometrics Authentication in Home-exams (SABBAH model). CiiT International Journal of Biometrics and Bioinformatics,4(1),32-45.

Sarrayrih, M.A.,& Ilyas, M.(2013).Challenges of Online Exam, Performances and problems for Online University Exam. International Journal of Computer Science Issues. 1(1), 439-443.

Zhang, Z. & Kenny, R.(2010). Learning in an online distance education course: experiences of three international students. IRRODL, 11(1)