Multimodal Biometric Authentication for on-Line Examination : A Robust Approach

Dr. Maithili Arjunwadkar

Director, P.E.S. Modern Institute of Computer Application

Abstract

Information and Communication Technology (ICT) is not very expensive these days. Assessment is a major issue in education but it is one of the key activities in student learning. Due to various advantages of **C**omputer-**B**ased **T**esting (CBT) over the traditional paper-pen based testing, most of the universities or colleges are now moving towards CBT. It led to an increased concern about the security of on-line examination. Traditional approaches to the examinee authentication are not sufficient to avoid misconduct of online examination. This paper proposed a new framework of three layers of security for examinee and two layers of security for invigilators. Using our proposed framework misconduct of on-line examination will be reduced.

Introduction

In today's era, learning capability with concept understanding is judged by the mode of examination in universities or colleges. The Traditional way of examination process used in universities or colleges is based on general paper-pen tests/examination are now slowly being replaced by the online internet based testing system. Assessment is a major issue in education but it is one of the key activities in student learning. Due to various advantages of **C**omputer-**B**ased **T**esting over the traditional paper-pen based testing, most of the universities or colleges are now moving towards CBT. Influenced by technological advances which are largely progressed in learning and evaluation process into invaluable educational resources those are accessible remotely from scattering geographical locations, beyond physical boundaries. The on-line examination environments are likely to be accessible, available, updatable, resource efficient, economical and have been widely adopted by a number of universities in various disciplines. Thus, utilizing online assessments delivers benefits such as opportunities for automatic marking and immediate feedback. The main advantage of online examination is that it can be conducted for remote candidates and evaluation of answers can be fully automated for **M**ultiple **C**hoice **Q**uestions and can be evaluated manually or through an automated system, depending on the nature of the questions and the requirements. Also online examinations can be conducted at any time and does not incur higher cost as traditional exam. Due to the rapid and considerable development in on-line examination, a number of issues are raised in the administration standards, security and control over the testing and evaluation processes. The most important issues is authentication of examiner and examinee or student. Student authentication in on-line examination has been an active research area and a number of authentication procedures have been evolved over time to ensure secure authentication. Recent studies indicate that on-line examinations are reported to be more vulnerable to academic dishonesty and authentication attacks due to lack of physical interaction.

In this paper, we studied the different authentication techniques used in on-line examination and the new approach has been proposed.

Impersonation Threat in the Online examination

Recent studies suggest that the risk of academic fraud in online examination has increased than traditional examination. In on-line environment, one of the major security challenges to user security is the act of impersonation. Impersonation is a fraudulent action with the aim of imitating a legitimate user and defrauding the security system. [1] In the traditional paper-pen examination, the need to correctly identify the student with the help of a student's ID card, hall ticket with photograph and examination

seat number. In on-line environment, students' ID card and login credentials are used normally. This approach claims impersonation threats in the on-line examination.

Impersonation threats are classified into three types, namely type A, B and C [2] [1].

- Type A Impersonation Threat

A connived impersonation is the ability of an invigilator to collude with fraudulent students to allow the fraudulent act. For example, if a student has continually failed a certain test, the tutor/invigilator may respond to human emotions and allow another student to take the online test on behalf of the real student. This type of impersonation can easily go undetected. In addition, there is a possibility of secretly allowed impersonation for monetary purposes. In this situation, the fraudulent students can influence the invigilator to receive a large sum of money to help commit the act. Irrespective of the motives for a connived impersonation, it is essential to find methods to minimize such threats in an on-line examination.

- Type B Impersonation Threat

This impersonation threat poses the question 'is the student really who they say they are?' Impersonation threat occurs when the real student passes his security information to a fraudulent, who use them to answer the exam. Username-Password pairs, for instance, fall in this type. This is a very popular method in the e-assessment. It can be easily shared amongst users. Intentionally or unintentionally real student can share the login credentials with the fraudulent. This academic misconduct can be undetected, especially when the requirement for accessing an online examination is a student's username and password alone.

- Type C Impersonation Threat

Impersonation threat occurs when the real student just login with his credentials or using any other authentication methods including biometrics, letting a fraudulent to continue the exam on his/her behalf. It indicates that real student is physically present in the on-line examination hall, carried out login procedure and hand over the computer to fraudulent to attempt the examination.

Recent studies pointed out that a major security problem of an on-line is the inability to know that who is there attempting examination or someone else has attempted the test on their behalf. For robust security different authentication techniques are used in an on-line examination. We have studied those in the next section

Existing solutions

Various existing authentication methods, as well as security approaches and their weaknesses, are studied in this sections [2] [1] [3]. Reliable student authentication is extremely important in on-line examination. Authentication attempts to verify that the user who they claim to be. In an on-line examination environment, authentication aims to verify the identity of on-line examines and plays a key role in security.

- **Invigilation**

Invigilation is the act supervising, monitoring students during an examination. For online examination, invigilation is one of the strong security technique can be used. The invigilator is the teacher of that university or college who should be a strict and reliable person. When the examination is taken under the invigilated environment, it ensures that the authentic student has attempted an on-line examination.

The use of an invigilated examination addresses the vulnerable to a Type A impersonation threat i.e. a connived environments. Similarly, invigilator is not serious with his/her duty then Type B impersonation threat i.e. fraudulent use credentials of real student and Type C impersonation threat i.e. logged by the real student and attempted by fraudulent is also possible.

Thus, as long as a connived impersonation goes undetected, there exists a likely occurrence of impersonation threats and attack creates a successful route for a Type B and type C impersonation to be committed. But if invigilator's authentication is used for respected session or slot of on-line examination then it will reduce the three impersonation threats.

- **Profile-based authentication**

Ullah et al [4] proposed Profile Based

Authentication for examinee authentication in online examinations. This type of authentication possesses user credentials i.e. user-id and password, and challenge question. Initially, a user-id and password can be used to login into the on-line environment to carry out regular activities. When an examinee requests to access an online examination, the second layer of authentication triggers the challenge questions, which are generated from the examinee's profile. Challenge questions are used to verify the examinee's identity. The questions and answers in a student profile can pertain to personal information, education, activities, professional experience, hobbies, future objectives, and learning activities. In the authentication process, if the collection of answers to profile questions and answers to challenge questions matched the stored authentication results then the student is granted access to online examination. If the answers to challenge question do not match to the stored profile information, the student is denied access. Challenge questions are generated through profile information, the chances of intentionally or unintentionally share their login credentials and profile information with a fraudulent to boost their grades.

- **Biometric Authentication Scheme**

Biometrics frees examinee to memorize passwords and carry out the cards, as the person is the key for identification. The biometric solutions are commonplace during student login; hence, they are better suited to solve a Type B impersonation threat. Using biometric methods like fingerprint or retina scanning to solve a Type C impersonation threat is practically difficult, as the random authentication of the student will be required for the time of the on-line examination. The random authentication of a student is one feasible approach to solve the Type C impersonation threat. But it can be observed as a means of distraction during the test.

Due to weaknesses of unimodal biometrics, a multimodal biometrics for authentication of the examinee is suggested by researchers. Asha et al proposed the combination of biometric fingerprint recognition with mouse dynamics [5].

- **Video monitoring**

A video monitoring is a system where the examinee is monitored by CCTV or video camera during the entire examination. This is one of the best solutions to rectify the problem of cheating during the examination. According to Lin et al [6], a promising approach to ensure security during online examination is the monitoring of examinee activities via video images. The video streaming of slot-wise entire on-line examination is stored on different hard drivers for future use.

Proposed Framework

The fig. 1 shows the proposed framework of secured multimodal biometric authentication in on-line examination. The solution contains three layers of authentication for examinee and two layers of authentication for invigilator.

Three layers of authentication for examinee comprises biometric like fingerprint recognition, login credentials and another biometric like face detection of the examinee. Two layers of authentication for invigilator comprises biometric like fingerprint recognition, login credentials of invigilators.

Initially, every examinee has verified by fingerprint recognition system against the fingerprint template which is stored at the time of filling examination form. Slot or session is allotted to every examinee as per the batch size. So only those students can attempt the examinations that have enrolled in the fingerprint recognition system of the college or university. It confirms that only authentic examinee can enter in on-line examination lab for given slot. After that examinee has logged on examination server using his/her login credentials which are given by college or university after verified his/her examination form. This is the second security layer. If he/she logged successfully the start time of examination is recorded and random questions will be displayed on examinee's computer. The third layer of security is face detection of examinee after a certain interval. Now a days a computer with a webcam is not expensive so that can be used as a third security layer. The face template is also enrolled at the time of filling examination form. The first layer with fingerprint authentication is minimized

impersonate type B threat by authenticating students as per batch. Because of that only enrolled students can enter into examination lab. The second security layer is used to logon on computers for examination. It also reduces impersonate type B threat. The third layer of face detection after certain interval minimizes impersonate type C threat. After finishing the slot time or examination time immediately examination result will be generated. This result contains Examinee name, slot date and timing, the name of allotted invigilator, start time, end time and marks.

For invigilator two-layer authentication, invigilator has verified by fingerprint recognition system against the fingerprint template which is stored initially or in the attendance system. Slot or session is allotted to every invigilator for each batch as per the examination schedule. So only that invigilator can enter into examination lab who has allotted duty to respective batches. After that invigilator has logon on examination server with his/her login credentials. It may put more responsibility on invigilator that if any misconduct of examination happens he/she is fully responsible for it. It reduces impersonate type B threat.

Any login of either examine or invigilator fails immediately it has to be informed automatically to Controller of Examination who is appointed by college or university

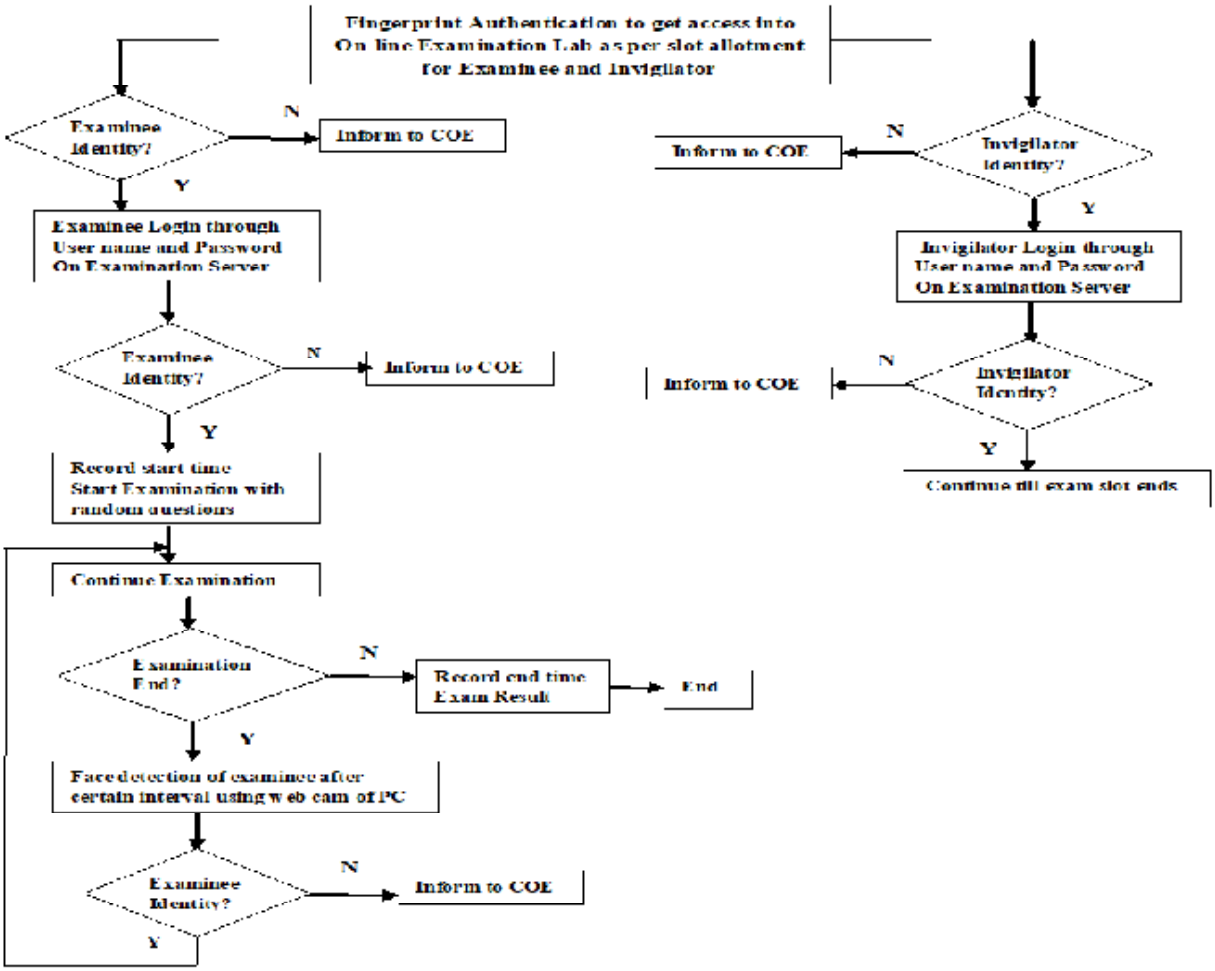
Conclusion

Information and Communication Technology (ICT) is not very expensive these days. Considering the advantages of on-line examination colleges or universities are included it to assess the students for their curriculum. It led to an increased concern about the security of on-line examination. The three types of impersonating threat can have an adverse impact on the credibility of on-line examination. Traditional approaches to examinee authentication are not sufficient to avoid misconduct of online examination. In this proposal, we studied three types of impersonating namely type A, B, C and various authentications approaches with their weaknesses.

This paper proposed a new framework of three layers of security for examinee and two layers of security for invigilators. If colleges or universities are enrolled proper biometrics template of examinee and invigilator then our framework builds robust security. The multimodal biometrics and knowledge-based authentication approach can be an effective technique to increase the security of on-line examination. Using our proposed framework misconduct of on-line examination will be reduced. We know that the cost and time required for on-line examination will be high due to this framework. Future work would be concentrate on how to reduce the cost and time of on-line examination and how to increase the efficiency and effectiveness of on-line examination.

References

1) K. M. Apampa, G. Wills and D. Argles, "User security Issues in summative E-Assessment Security," *International Journal of Digital Society,* vol. 1, no. 2, pp. 135-147, 2010
2) J. W. Gathuri, A. Luvanda, S. Matende and S. Kamundi, "Impersonation Challenges associated with E-assessment of University students," *Journal of Information Engineering and Applications,* vol. 7, pp. 60-68, 2014
3) T.Ramu and Dr.T.Arivoli, "A Framework of Secure Biometric Based Online Exam authentication: An Alternative to traditional Exam," *International Journal of Scientific & Engineering Research,* vol. 4, no. 11, pp. 52-60, 2013.
4) Asha and C. Chellappan, "Authentication of e-learners using multimodal biometric technology," in *Proceedings of the IEEE International Symposium on Biometrics and Security Technologies*, 2008
5) Ullah, H. Xiao and M. Lilley, "Profile-based student authentication in Online examination," in *IEEE International Conference on Information Society* , 2012.
6) N. Lin, L. Korba, G. Yee, T. Shih and H. Lin, "Security and Privacy Technologies for distance Education Applications," in *18th International Conference on Advanced Information Networking and Applications*, 2004


Fingerprint Authentication to get access into On line Examination Lab as per slot allotment for Examinee and Invigilator
Examinee Identity?
N
Inform to COE
Y
Examinee Login through User name and Password On Examination Server
Examinee Identity?
N
Inform to COE
Y
Record start time Start Examination with random questions
Continue Examination
Examination End?
N
Record end time Exam Result
End
Y
Face detection of examinee after certain interval using web cam of PC
Examinee Identity?
N
Inform to COE
Y
Invigilator Identity?
N
Inform to COE
Y
Invigilator Login through User name and Password On Examination Server
Invigilator Identity?
N
Inform to COE
Y
Continue till exam slot ends