

Object Oriented Modelling of Secured E-Assessment System

Nikhilesh Barik , Dr. Sunil Karforma

Abstract— Now day's different multinational and national companies are using E-assessment system for recruiting UG and PG students. Main advantages of this approach are immediate result and feedback, any time students can start their examination during the tenure of availability of question from the server, etc. E-assessment system is an important component of e-learning system, which basically runs over Information and Communication Technology (ICT). The success of E-assessment system is dependent on level of security imposed in the system. Different security services like one time authentication, verification, presence of supervisor are not sufficient to ensure the security of E-assessment system. In this paper we explore a suitable Object Oriented Model to authenticate a student as examinee where authentication is achieved by RSA Digital Signature during sending e-question papers and submission e-answer papers. Proposed model may be used for all kind of E-assessment so that learners will be motivated for online examination .

Index Terms—E-Learning system, E-assessment, Learning Security, Object Oriented Model, Information and Communication Technology (ICT), Online Test, Digital Signature.

1. INTRODUCTION

E-assessment has been a popular term for last few years but it is gaining much more importance recently. From 2011 many national and multinational companies like TCS, Syntel, and Digital Domain etc has applied E-assessment for screening the students for recruitment. E-assessment is automatic examination evaluation system where examination can take place over ICT which can term as online examination. Instead of traditional paper bases classroom examination this test does not require any particular campus. Though supervised system or authorized test centre assure the academic quality and standard of the education system.

The concept of learning using computer of ICT is not new ,but in case of higher education ,to give certificate/grade of particular course/learner always assessment require.

E-learning users dealing with valuable assets like User Profile, sealed e-admit / e-registration certificate, question paper, answer script, Grades, related to E-assessment. It is not so easy to handle these assets smoothly and conduct the fair examination as well as authenticity, integrity privacy and reliability also maintains and also since E-assessment is totally running under internet environment high ended security requires stopping threats and vulnerability of internet. Zamzury has classified threats into six categories Spoofing ,Tampering ,Repudiation ,Information disclosure, Denial of services and Elevation of privilege with respect to e-learning system[7]. All these are very much applicable under E-assessment system also.

Wipple[6] discussed clearly in his paper about four basic security requirements PINA which are Privacy, Integrity, Non-repudiation and Availability.

Privacy related to access of private information of all users. For example an evaluator should not know the mobile number with name for any learner at the time of evaluation the answer sheet where as manager should know. This concept is very much dynamic. Integrity refers authenticity of the users

.Authenticity of the examinee ,examiner and invigilators in different stages of E-assessment can be checked using password, Biometric, Video monitoring ,e-tokens etc. After completion of any operation no user will allow to deny that operation refers the security nonrepudiation which is very important at the time appearing the exam and submitting answer sheet by learner, submission of marks by invigilator, grading the students by manager, etc. Availability is also one of the main security requirement as everything is online. Non available means temporary death of the system which may occur by different type of attacks during transaction of E-assessment material. Then every user will lost their interest with E-assessment as well as in e-learning system. So degree of accuracy that is reliability is also strictly related with this availability[1].

Apampa discuss clearly the Blob (Binary large object) based verification process which ensures that authenticated student starting the E-assessment is the same student throughout the test session[2]

We will mainly consider the object based approach as it contributes to the solution of many problems associated with development and quality of software product. Though Object Oriented Modelling[OOM] in not new concept but it always provides greater programmer productivity, better quality of Software and lesser maintenance cost. Besides these OOM has number of advantages as below[5]

- The principal of data hiding helps the programmer to build the secure programs
- Via inheritance programmer can eliminated the redundant code and extend the use of existing classes
- It is possible to have multiple instances of an object to co-exists without any interference
- It is possible to map objects in the problem domain to those in the program.
- It can be easily upgraded from small to large systems

- Message passing system between objects is more efficient.
So in OOM Software complexity can be managed easily ,which helps to save development time and produce higher productivity and quality.

2. OBJECT ORIENTED MODEL (OOM) OF E-ASSESSMENT SYSTEM.

2.1 Class Hierarchy

End users ,Controller ,Developer and overall authority are the main entities related to the E-assessment system. End users are directly attached with this E-assessment system. So end users are students, managers and Instructors. The following OOM shows the details of the class hierarchy and Sequence diagram shows interaction among different level of users of E-assessment system in the Fig-3 and Fig- 4 [9].

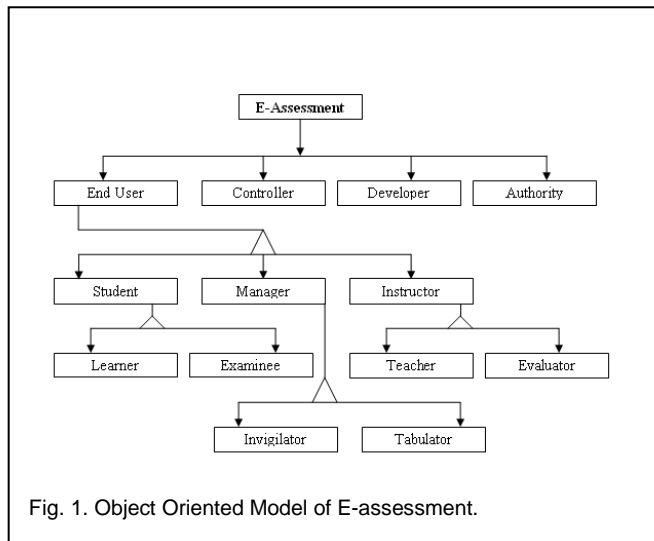


Fig. 1. Object Oriented Model of E-assessment.

A class contains different attributes and functions. In an Object Oriented Model (OOM) overall system is framed by creating by creating objects and establishing relationship amongst objects. This model has been designed keeping in mind that every instruction from the controller has been implemented by the Developer ,who are responsible to design the whole system and without government Authority no certificate is possible to issue to any student for any kind of degree[10].

Role of classes associated with E-assessment system is outlined below:

2.1.1. Examinee

Any students (or learner) after completion of his/her course become examinee , so Examinee can be one of the main user of E-assessment system .The E-assessment system runs only for group of Examinee who have already enrolled in different e-learning courses. There may be different time zone group wise for Examinee for assessment. So this class can inherited from the parent class Student

2.1.2. Manager

Manager represent here as an office administrators or system administrator or any body who are responsible to look after management part of e-learning as well as E-assessment system. The controller of examination is supposed to be the supervisor of the total E-assessment system . They are responsible to communicate to the learner or other manager / invigilator during the examination, create digital signature to the question paper and received answer sheet by verification algorithm from the examinee.

2.1.3. Examiner/Evaluator

Generally Instructor is treated as lecturer or teacher basic objective of instructor should complete the specific syllabus for the particular course and react as an educated router between authors and learners. After completion of E-assessment it is duty to the teacher (become then as examiner/evaluator) to evaluate the copy.

2.2 Use Case Diagram of E-assessment System

For systematic, well-defined and clear understanding of actual implementation we need to use UML(Unified Modelling Language) design[8],[11]. User view version can be describes clearly by the following Use Case diagram. Mr Banerjee, Dr Karforma and Mr Ghosh clearly showed the object based use case diagram as sub system of E-learning system[13],[10]. Here we are representing the role of Examinee ,Examiner and Manager in E-assessment system by use case diagram. Different remedies like Access control using Firewall and Digital Right Management (DRM) can be applied to minimize the risk as the time of E-assessment as discussed by Barik[3]. Access permission is mainly control by the manager by the guidance controller of examination and Digital right management can be implemented by the developer according to the instruction of controller[10].

- Nikhilesh Barik, Research Scholar , Department of Computer Science, University of Burdwan ,West Bengal , India, PH-09434516929.
E-mail: nikhileshbarik@gmail.com
- Dr. Sunil Karforma, Associate Professor, Department of Computer Science, University of Burdwan , India, PH-09474553590.
E-mail: dr.sunilkarforma@gmail.com

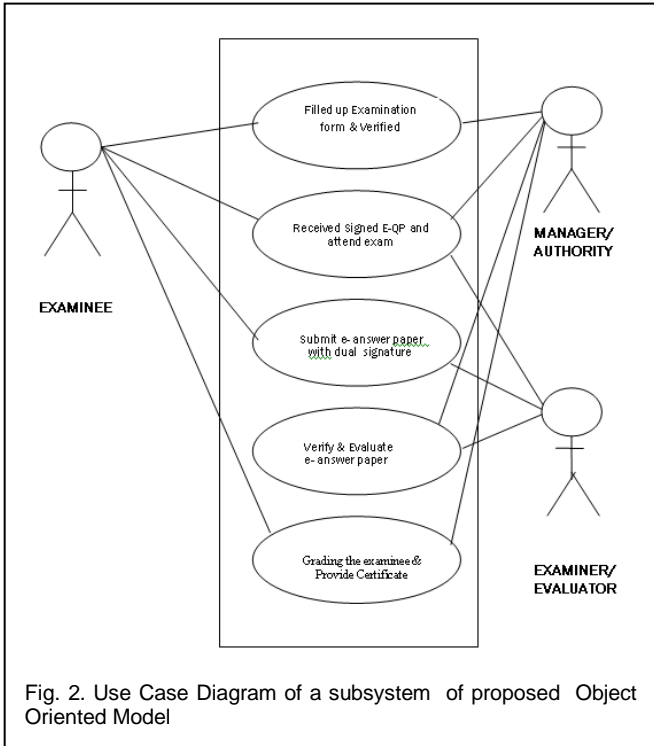


Fig. 2. Use Case Diagram of a subsystem of proposed Object Oriented Model

Above UML diagram is flexible enough and easy to manage where transfer / exchange of data between the two persons is clear. Also relationship among multiple methods E-assessment system is clear enough[9].

2.3 Sequence Diagram

Sequence Diagram clearly explains time dependent message communication among the objects present in E-assessment system. So how processes operate with one another and in which order can clearly understand by the sequence diagram. Here we have discussed by only two subsystems at the time of sending e-question paper and submission of e-answer paper [13].

Digital Signature algorithm can be used to authenticate as well as identifies the concerned authority, which are related during the transaction in E-assessment system. It will be right technology to use digital signature during the transaction of e-documents like Admit card Question paper, Answer paper, Grade Card etc [4]

The following sequence diagram demonstrates authentication of an examinee during transmission of e-question paper.

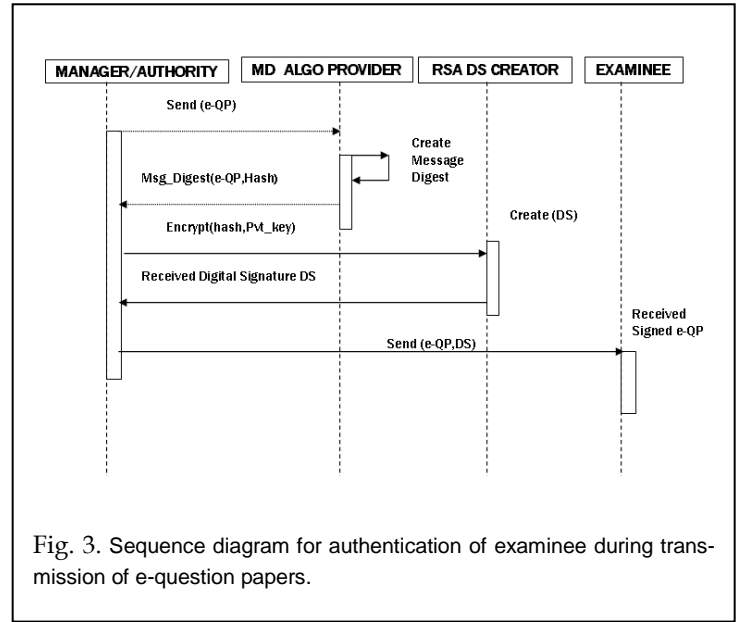


Fig. 3. Sequence diagram for authentication of examinee during transmission of e-question papers.

For authentication of an examiner and examinee during submission of e-answer paper has been displayed in the following Sequence diagram.

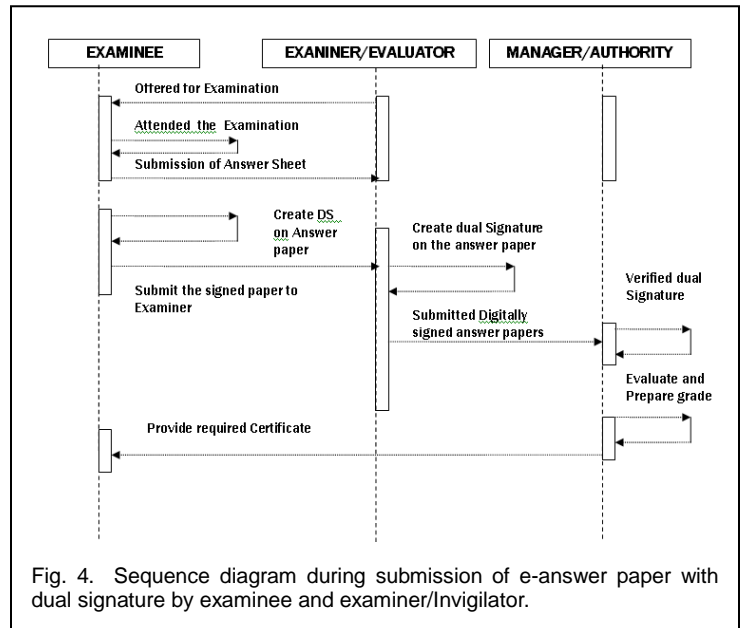


Fig. 4. Sequence diagram during submission of e-answer paper with dual signature by examinee and examiner/Invigilator.

Before submission the answer paper, examinee use RSA digital signature with his/her private key on it. After that examinee/invigilator also apply RSA digital signature on signed e-answer paper with her/his own private key. This dual signature makes the system more secure. At the time of verification Authority first verify the examiners' / Invigilators' signature. Then once again Authority will verify signature of concerned examinees on that e-answer paper[12]. Same can be apply with two different digital signature algorithms [4],[14] also.

3. CONCLUSION

In this paper we have given emphasis on development of Object Oriented Modelling to ensure the trust of all participants like Examinees, Examiners/Evaluators and Administrators of in E-assessment system. Controllers are supervising the access of information right for different level of users through developers of E-assessment system. Relevant data and procedures has been binded together efficiently through objects such as Examiner, Examinee, Manager etc. We have outlined the behavior of different participants of E-assessment system with the help of Use Case Diagram and Sequence Diagram which are true significant tools of Object Oriented software engineering and also needed for the development of improved quality software. Sequence diagram has been used to show secured transaction with dual digital signature on e-documents'. As two different persons applying the signature on same documents with different private key, it is becoming more secure. So proposed model may be used more learners to do their degree anywhere from world through web with low cost and huge trust in their minds for online examinations. Level of security of the proposed system may be improved further by applying Elliptic Curve version of Digital Signature.

4. REFERENCES

- [1] Weippl Edgar R. "Security in E-Learning", Springer Publication, 2005
- [2] Apampa K M , Gary Wills, David Argles "Towards a Blob-based Presence Verification System in Summative International Journal of E-assessment Vol-1, No-1, 2011
- [3] Barik Nikhilesh and Karforma Sunil "Risks And Remedies In E-Learning System " "International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, January 2012 ,ISSN -0974-9330(OL),0975-2307(P), PP 51-59
- [4] Barik Nikhilesh and Karforma Sunil "A Study On Efficient Digital Signature Scheme for E-Governance Security" "Global Journal Of Computer Science And Technology"(GJCST) ONLINE ISSN :0975-4172 & PRINT ISSN :0975-4350 ,Vol-XII ,ISSUE -II ,Version -I, PP 7-11.
- [5] Balagurusamy E, "Object Oriented Programming with C++" Tata McGraw Hill Education Pvt.Ltd , Fourth Edition 2010
- [6] Weippl Edgar R. " Dependability in E-assessment. "International Journal on E-Learning, 6(2):293{302, 2007
- [7] Z. F. Zamzury et al.(Eds.): "Computer Security Threats Towards the E-Learning System Assets" Communications in Computer and Information Science, 2011, Volume 180, Part 3, PP 335-345.
- [8] <http://www.outsource2india.com/LearningSolutions/articles/usecase-modeling-for-elearning.asp> Accessed on 10th June'2012
- [9] Karforma Sunil and Ghosh Basudeb ; On Designing an e Learning System Model; An Object based approach "NACCS 2010 ,Burdwan University ,Jan 2010.PP 183-190
- [10] Banerjee Sanjay "Designing a secure model of an e-learning system – A UML-based approach ,IEEE , September/October 2010 ,PP:22-27.
- [11] Booch, G,Rumbaugh J , and Jacobson I , "Unified Modeling Language User Guide", 2nd ed. Reading, MA: Addison-Wesley, 2005.
- [12] Khan M Ayoub and Singh Y.P. "On the security of Joint Signature and Hybrids Encryption "IEEE , May 2005 PP 109-112.
- [13] Banerjee Sanjay, Karforma Sunil and Ghosh Basudeb ; Object Oriented

Modelling of E-learning System- a UML Based Approach "NACCS 2012, Burdwan University ,Jan 2012,PP 269-274.

- [14] Menezes A.J., Oorschot PC. van and Vanstone S., "Handbook of Applied cryptography", CRC Press, 1997.s