DOI: http://dx.doi.org/10.26483/ijarcs.v9i1.5276

ISSN No. 0976-5697

Volume 9, No. 1, January-February 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

SECURITY ANALYSIS OF CONVENTIONAL/ELECTRONIC SUMMATIVE ASSESSMENTS

Kissan Gauns Dessai
Dept. of Computer Science
Govt. College of Arts, Sci. & Comm., Sanquelim
Sanquelim-Goa, India

Venkatesh V. Kamat
Dept. of Computer Science & Technology
Goa University
Goa, India

Abstract: Educational institutions worldwide face an ever increasing threat of malpractices during the conduct of summative assessments/examinations. Malpractices are perpetrated by students, controlling authority and the other external agents before, during and even after the assessments. Appropriate measures to deter and detect malpractices are essential to uphold the academic honesty and integrity of the assessment system. The identification of the source of the malpractice and the threat is utmost essential to plan the defence for curbing the malpractices. In this paper, we identify the threats encountered in the conventional/electronic assessments pertaining to the higher education and provide the comparative analysis of countermeasures adopted. We then provide the security analysis of the conventional/electronic assessments to understand the influence of the existing methods in attaining the required level of security to withstand the identified threats.

Keywords: Summative Assessment;Assessment threats;Assessment Vulnerabilities; Assessment Malpractices; Countermeasures; Security analysis.

I. INTRODUCTION

Educational institutions worldwide use summative assessments/examinations to assess the learning outcome of students and to grade the students. Summative assessments are normally high-stake assessments having a tremendous impact on career/employment prospects of students. As the summative assessment is looked upon as a key to success/qualification, it attracts a plethora of academic misconducts and malpractices from the stakeholders concerned [1].

The intensity and pervasiveness of the problem of malpractices can be gauged from the fact that apart from the students, it is also the strong nexus between other involved stakeholders along with the external agents. The summative assessment encompasses collusion, impersonation, leakage of question papers, plagiarism, altering answer-books, misconduct in examination center, approaching supervisors / examiners for a favor, making false entries in the award list / assessment registers and issuing fake certificates/degrees etc. [2], [3].

Some of the embraced measures in controlling malpractices in the conventional summative assessments are enumerated below:

- Appointment of multiple paper setters for preservation of secrecy of question papers and establishing the anonymity of paper setters.
- Submission of a sealed hard copy of the manuscript of question paper to protect integrity of the question paper.
- Monitoring and supervising the examination conduct from start to end to control acts of academic dishonesty such as collusion, plagiarism, cheating etc.
- Use of unique labeled question paper and answers-script booklet or common question paper cum answer booklet in order to link the question paper and answers-script together.
- Eliminating student identity from answer-books and assigning a pseudonym mapped to a student identity to maintain student anonymity from examiners.
- Maintenance of student attendance record to prevent denial of committed action of students/other stakeholders.

The currently employed practices in conventional assessment have many shortcomings; some are more significant than the others [4]. The electronic assessment has the potential to curb most of the shortcomings associated with the conventional assessment. Some of the established strategies for controlling the assessment malpractices in electronic assessments are listed below:

- Generation of the question paper just before commencement of the examination, i.e., Just-in-Time (JIT) generation of question paper [4].
- Encryption of the question paper using symmetric/asymmetric encryption techniques for preservation of secrecy of question papers [5].
- Message Digest/hashing technique to ascertain the integrity of the question paper/answers-scripts [6].
- Digital signatures for non-repudiation, i.e., to prevent the denial of committed action of the communicating entities [5], [7].
- Mixnet servers to keep the identity of the student/examiners anonymous [8].

The currently adopted security practices in conventional/electronic assessments are insufficient to provide comprehensive security cover from the malicious acts as apparent from ever increasing cases of the successful outbreak of malpractices. We, in this paper, explore some of the crucial security requirements for conducting summative assessments. We then identify the threats that target the assessment system and further evaluate the existing countermeasures addressing the threats. The countermeasures considered are based on the study of well-established and common set of assessment rules and regulations followed in most of the higher education institutions in India. We also argue that the current assessment system is exposed to further threats due to inadequate fulfillment of security requirements.

Contribution:

This paper aims to highlight the countermeasures used in combating the incessant threats faced by most of the summative assessment systems (conventional/ electronic). Based on the malpractice reports/ records and formal analysis of the conventional/electronic assessment systems, we provide the security analysis of the conventional/electronic assessment systems identifying the need for further security interventions.

Outline: The next section provides the background details and overview of the related work. Section 3 provides a description of the summative assessment model. Section 4 and 5 provides the threats, countermeasures and vulnerabilities in conventional and electronic assessments respectively. Section 6 provides security analysis of conventional / electronic assessments based on the reported/recorded malpractice incidents and formal analysis using Proverif tool. Section 7 draws the conclusions and outlines the future work.

II. BACKGROUND & RELATED WORK

Educational institutions use a variety of approaches to verify the learning outcome of students and to assess the attainment of learning objectives of the course [9]. In practice, summative assessment is used to report what students have already achieved in their course curriculum in the form of a grade or a certificate [10]. The conventional assessment / examination is an assessment delivered to the candidate on paper and where the candidate responds on paper [12]. Conventional summative assessments are predominantly used by educational institutions to grade the students based on subjective assessments. On the other hand, electronic examination/e-assessment refers to an automated process where assessment activity is delivered and displayed on a computer screen and candidate responses are uploaded electronically [12]. In a typical electronic assessment setting, tests are objective in nature and can be offered at different locations or different times and the test questions can be randomized to provide a different question paper to each student [13].

Summative assessments are often of high-stake nature as the output of such assessments are used for promotion, placement, certification, and accountability [11]. Thus, reliability is central to summative assessments; since the results may have an enormous impact on students' academic/career future. The summative assessment encompasses malpractices in a variety of forms such as collusion, impersonation, leakage of question papers, plagiarism, altering answer-books, misconduct in examination center, approaching supervisors/examiners for securing favor, making false entries in the award list/ assessment registers and issuing fake certificate/degrees etc. [2], [3].

Numerous e-examination solutions have been designed with the intent of improving the efficiency and eliminating the loopholes associated with the conventional examination system. E-assessments to a great extent simplify the entire examination process and offer many advantages over conventional assessments. The Learning Management Systems (LMS) such as MOODLE (http://moodle.org), Blackboard (www.blackboard.com), Evalcomix (http://evalcomix.uca.es/index.php/index-en.html) include modules for conducting e-examinations.

Any secure computer system is built on 3 main pillars of security, namely: confidentiality (C), integrity (I) and availability (A) [14]. In particular, confidentiality protects the data item from interception, integrity protects data from modification and availability protects it from interruption [15]. In literature, there are proposals towards the deployment of these security goals as a solution for most data security issues in e-examination. The security protocols for e-examinations are proposed by [5], [7], [16] using symmetric/asymmetric encryption for achieving secrecy of question paper exchanged. There exist proposal by [6] that use hash functions to achieve integrity and authentication. One of the main security problems in e-assessment is making students' submissions non-repudiable. The digital signature is used effectively in achieving non-repudiation of any committed action. An internet-based exam protocol is suggested by [18] to ensure authentication and conditional anonymity requirements with minimal trust assumption. A comprehensive formal framework in the applied pi calculus is proposed by [19] to define and analyze authentication and privacy requirements for exams through formalization of several individual and universal verifiability properties. There is a security model proposed by [21], [22], [23] for incorporating presence (and continuous presence), identity and authentication security goals against impersonation threats from students answering the e-examination. Ref. [24], [25] propose an exam protocol without the need of a trusted third party that guarantees several security properties including anonymity for anonymising the student's test.

However, the existing approaches do not provide a comprehensive solution addressing the security requirements of all the stakeholders. We need an all-inclusive approach to tackle the increasing trends towards the use of unfair means.

III. SUMMATIVE ASSESSMENT MODEL

In this section, we describe the essential components of the typical summative examination system followed by the assessment process and then finally the security requirements of summative assessments.

A. Components of Assessment

The summative assessment model under our consideration comprises of five classes of communicating entities, namely: question paper setter (P), examination controller/authority (B), student (A), supervisor (S) and examiner (X).

- **Question Paper Setter (P)** is an entity who sets the questions based on predefined syllabus. Subset of such questions forms part of the question paper (QP).
- **Examination controller (B)** is an entity, in-charge of conducting the examination and controlling examination related activities. Examination controller is responsible for appointment of paper setters, supervisors and examiners, along with delivery of question paper, collection of answers-scripts and finally tabulating the marks/grades and result declaration.
- **Student (A)** is an entity who appears for the assessment and answers the given QP pertaining to each enrolled course as per the predefined schedule.
- **Supervisor (S)** is an entity who is responsible for controlling and monitoring the conduct of assessment during the answering phase of the assessment.
- **Examiner (X)** is an entity who assesses the student answers-scripts at the end of the examination and allots the marks/grades based on the marking scheme.

The main information that is exchanged between any two communicating entities in the summative assessment is: question paper (QP) and answers-script (AS)

- **Question paper (QP)** includes the set of questions organized as per the predefined format based on the course curriculum. QP is generated by the examination controller from any of the set of questions provided by the paper setters.
- **Answers-script (AS)** is the set of answers corresponding to the questions contained in the QP. AS is produced by the student.

B. *Assessment Stages*

Summative assessment is a complex process, involving a multitude of tasks, namely: pre-conduct, conduct and post-conduct (refer fig. 1).

1) Pre-conduct

The pre-conduct stage of the assessment identifies and establishes the basic requirements necessary for conducting the assessment efficiently. The main activities of this stage are: student registration, question paper generation and delivery of QP to assessment centers. Besides these activities, pre-conduct stage of the assessment also carries many other miscellaneous activities such as appointment of paper setters, supervisors, examiners etc.

2) Conduct

In the conduct stage of the assessment, authentication of eligible students', the task of question paper delivery, question paper answering and submission of answers-scripts are carried.

3) Post-conduct

Pos-conduct stage of examination handles activities such as the scrutiny of the unfair means, evaluation, the tabulation of the results, and the issuing of a statement of marks to the students.

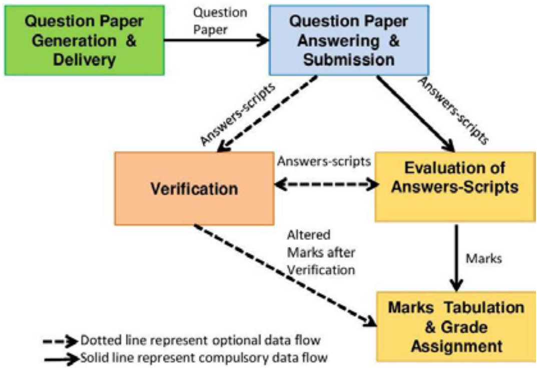

Question Paper Generation & Delivery
Question Paper
Question Paper Answering & Submission
Answers-scripts
Answers-scripts
Verification
Answers-scripts
Evaluation of Answers-Scripts
Altered Marks after Verification
Marks
Marks Tabulation & Grade Assignment
Dotted line represent optional data flow
Solid line represent compulsory data flow

Figure 1. Summative Examination Stages

C. *Assessment Process*

We assume that multiple paper setters electronically submit a wide variety of questions pertaining to a particular course paper forming a question bank. The examination system picks up subset of such questions randomly from the question bank and generate a question paper to the students answering the examination. During conduct stage examination, students are provided with blank official stationary called answer-books to write the answers corresponding to the given questions. Supervisors monitor and supervise the conduct of the examination. At the end of the conduct stage of the examination, students submit the answer-books containing answers to the examination authority. Examination authority allots the collected answers-scripts to examiners for evaluation. Due care is taken to hide the student identity from the examiners and vice-versa. The examiners evaluate the answers-scripts of students and assigns the marks/grades for each answer based on the marking scheme. Finally, examination controller tabulates the marks/grades submitted by the examiners, processes the marks/grades and produces the result.

D. *Security Requirements*

Summative assessment essentially needs to be conducted in a fair and a malpractice free environment as it is of high-stake nature. Some of the crucial security requirements for safeguarding the fairness and reliability of summative assessments are elaborated below:

1) Confidentiality (SR1)

The question paper is extremely important and crucial asset of any summative assessment system. The secrecy of the question paper needs to be preserved before the conduct of the assessment. Any violation of question paper secrecy can affect the sanctity of the entire assessment badly. Along with the secrecy of question paper, it is also essential to safeguard the secrecy of answers-scripts produced by the students from all, except the examiner concerned.

2) Integrity (SR2)

The assessment system must include mechanisms for detecting/preventing unauthorized modification of its assets, namely, question paper, answers-scripts and statement of marks.

3) Non-repudiation (SR3)

Examination authority needs a non-repudiation of origin service (NRO) to prevent student's denial of answers-script origin. Similarly, a student needs a non-repudiation of receipt service (NRR) to prevent examination authority's denial of answers-script receipt. Also, there is a need of maintaining an evidence for non-repudiation of question paper content and answers-script content.

4) Anonymity (SR4)

It is also extremely important to keep the identity of certain communicating entities anonymous for ensuring fairness and unbiased assessment. The anonymity needs to be ensured in the following communications:

a) The author of the question paper needs to remain secret from students and others.
b) The student identity needs to remain secret from all the stakeholders before the marking/grading.
c) The examiner of the answers-scripts need to remain secret from all the stakeholders.

5) Associativity (SR5):

Associativity is required to establish the link between the information exchanger and the exchanged information or to link any related information exchanged in a two way communication process (Ex. Link the unique question paper and answers-script received/produced by the student unambiguously). In the examination environment, we need to establish:

a) The connectivity of question paper and answers-script.
b) The connectivity of answers-script and evaluation result.

6) Verifiability (SR6):

Verifiability provides evidence to stakeholders about some event or information. In assessment, the need for verification of certain information or event may arise on multiple occasions such as:

a) A student wishes to verify whether it received a correct question paper.
b) A student wishes to verify whether the answers-script assessed is as submitted by him originally or is modified.
c) A student wishes to verify whether the marks obtained are corresponding to his answers-script.
d) The student needs to verify whether his answers-script is assessed fully.
e) The student needs to verify whether he is marked correctly.
f) Paper setter needs to verify, whether question paper is derived from the questions originally submitted by it.
g) Examination authority wishes to verify during the conduct of examination whether the question paper used is the original question paper provided by it.

IV. CONVENTIONAL ASSESSMENT - THREATS, COUNTERMEASURES AND VULNERABILITIES

Academic institutions use series of measures to control the human errors/lapses as well as malicious activities that can occur during the assessment. In this section, we present a detailed overview of threats, countermeasures and vulnerabilities associated with the conventional assessments.

A. Question paper/Answers-script Leakage

1) Countermeasures

The predominant method used to control question paper leakage, i.e., a threat to the confidentiality of question paper is to use three paper setters for setting 3 different question paper sets. Creating three sets of manuscripts of question paper ensures secrecy of the question paper from the paper setters. Examination authority randomly selects one set of question paper from the given three sets for the particular assessment.

2) Vulnerabilities

Setting three unique and independent sets of question paper ensures question paper secrecy from the generator of the question paper, i.e., paper setters. However, there are many vulnerable points in the method, which can breach the confidentiality/secrecy of the question paper as indicated below:

a) All the 3 sets of question papers are verified by one subject expert.
b) The question paper selected is known during printing.
c) The selected question paper goes through number of eyeballs during printing and production phase.
d) The question paper is exposed during the manual process of sealing.
e) Advance transportation and delivery of question paper to the respective assessment centers.

The answers-scripts produced by the students go through the lengthy supply chain before reaching the examiner. The transportation of answers-scripts from one entity to another entity provides ample opportunities for coercion and cheating.

Example: Any of the staff involved in the question paper selection, printing, production, sealing and transportation can leak the question paper.

B. Alteration of Question Paper/Answers-script

1) Countermeasures

The integrity of the question paper is ensured by submitting the sealed hard copy of the manuscript of the question paper. It is also mandatory to have the signature of the paper setter on each page of the manuscript along with initials on every modification carried.

The integrity of the answers-script is achieved by default as students produce answers-scripts in their own handwriting. The handwriting acts as a deterrent for unauthorized modification of the answers-scripts. As a safety measure, examiners draw lines on blank portions of answers-scripts submitted by the students to prevent any addition later on.

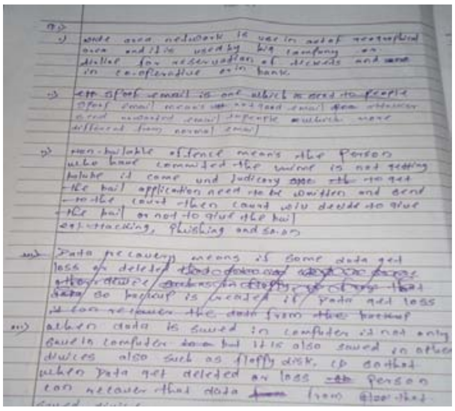
2) Vulnerabilities

If any unauthorized modifications are carried in the question paper, it can come to the light only if the original paper setter sees the final question paper during the conduct of the examination. Even if it is detected, during the conduct phase of the examination the side effects are too many and too costly to revoke the damage suffered.

Since, to disturb the integrity of the question paper, one needs to have access to the question paper, which in turn violates the confidentiality of the question paper. It is quite logical that if confidentiality is broken, there is no need to commit any integrity violation, as question paper is already known.

On the other side, it appears that answers-script tampering is comparatively easier to achieve for the supervisor/ examination authority /examiner.

Example: Supervisors can easily manipulate the answers-scripts submitted by the students. It is a matter of just drawing a line on content of the answers-script for making a particular answer as canceled. The examiner will not assess those portions of the answers-scripts which are cancelled (refer fig. 2). Such act leave no trace/evidence to prove whether alteration in the answers-script was carried by student or somebody else.



Q.)
i) wide area network is use in a lot of geographical area and it is used by big company or [illegible] for reservation of tickets and [illegible] in co-operative [illegible] bank.
ii) ~~[illegible] spoof email is one which is send to people~~
Spoof email means [illegible] not good email [illegible] send unwanted email to people which were different from normal email
iii) non-bailable offence means the person who have commited the crime is not getting bailable it come under judiciary [illegible] to get the bail application need to be written and send to the court then court will decide to give the bail or not to give the bail
e.g. hacking, phishing and so on
iv) Data recovery means if some data get loss or deleted ~~[illegible]~~ so backup is created if data get loss ~~it can recover the data from the backup~~
v) when data is saved in computer it not only save in computer ~~[illegible]~~ but it is also saved in other devices also such as floppy disk, CD so that when data get deleted or loss ~~[illegible]~~ person can recover that data ~~[illegible]~~ from [illegible] saved device

Figure 2. Integrity Violation in Conventional Examination

C. Denial of Action

1) Countermeasures

Examination authority maintains student attendance records for each course paper during assessment. Also, supervisor signs on the hall ticket/admission card carried by the student on each day of the examination, confirming the presence of the student for the particular course paper.

Since the answers-script submitted by the student bears their own handwriting, there is no scope for students to disown their own answers-script.

2) Vulnerabilities

If the practice of supervisor signing the hall ticket confirming the presence of student for a particular course paper is not implemented, the student has no way of proving his presence in the said course paper. Also, the student is not provided with any documentary evidence to prove the exact copy of the submitted answers-script. In such situation, if answers-script is modified, there exists no evidence/protection for students to defend their case.

D. Favoritism, Coercion and Biased Evaluation

1) Countermeasures

If the identity of the communicating entities is hidden from each other certain act of favoritism, coercion, bias, threats, etc., can be controlled. In order to maintain secrecy of the question paper and the anonymity of the actual paper setter, the custom of three different paper setters to set three different question papers is followed.

The student identity needs to be hidden from all till the completion of the assessment. This goal is usually achieved by hiding the roll no./seat no. recorded on the answer-book through a process called as coding. In the coding process, student identity is taken over by a pseudonym. The un-coding, i.e., revealing student identity is done during the declaration of the result.

Examiners conduct evaluation in an isolated environment. Multiple examiners assess the answers-scripts pertaining to each course paper and care is taken not to reveal the identity of the examiners.

2) Vulnerabilities

The manual process of appointment of paper setter makes the identity of paper setter known in advance. The coding process used for hiding the student identity from the examiner is naïve and susceptible to disclosure of student identity. If a single examiner assesses the answers-scripts, then the identity of the examiner is also known without any guesswork. Even in the multi-examiner assessment, the manual appointment process makes the identity of the examiners known.

E. Plagiarism and Collusion

1) Countermeasures

In the conventional assessment, with the common question paper, the given answers-script always corresponds to one common question paper. The services of supervisor are used to control and monitor student behavior and acts of collusion and plagiarism.

Answers-script plagiarism and collusion can be controlled to a great extent, if a unique question paper is provided to each student. In a system with unique question papers for each student/group of students, we require an unambiguous binding between the unique question paper and the student answers-script. The link between unique question paper and answers-script is established using common question paper cum answer booklet or separate but identically labeled question paper and answers-script booklet.

It is also necessary to link the marks assigned and corresponding answer/answers-script. This connectivity is achieved in a conventional examination system by recording marks directly on the answers-script corresponding to the given answer. In such a system, any act of unauthorized modification/impersonation/forgery in the marks can get detected easily, if answers-scripts are verified.

2) Vulnerabilities

If the common question paper is used, we have a many to one mapping from the student answers-scripts to the question paper. Dishonest students exploit this vulnerability and collude or plagiarize the answers-script of neighboring student. Students get the opportunity for plagiarism, even in the supervised environment due to use of common question paper and large examination blocks. Since neither the examination authority nor student maintains any undeniable evidence which can prove the given answers-script is plagiarized or not, it is not possible to fully endorse the claim of any of the communicating entities in the event of any dispute.

If separate answers-script is used with unique question paper, then it is not possible to prove which student received which question paper in case of a dispute.

Example: A student can commit an intentional/unintentional error in recording roll no. /seat no. amounting to having two answers-scripts with identical roll no. Similarly, two students with hand in glove with each other can write each other's seat no. on the answer-book for maliciously providing benefit to one amongst them.

V. ELECTRONIC ASSESSMENT - THREATS, COUNTERMEASURES AND VULNERABILITIES

The electronic assessment is perceived to offer in general an efficient and effective mechanism for conducting entire assessment and specifically provide state of the art instrument for controlling most of the anomalies and malpractices observed in conventional assessments. We now analyze the e-assessment with reference to the e-assessment system, Remark! [8].

A. Question paper/Answers-script Leakage

1) Countermeasures

In e-assessment, question papers are generated just- in-time (JIT) from the available question bank. The public key infrastructure (PKI) is used for encryption of the question paper. Each student/group of students gets unique question paper. At the end of the examination students submit the encrypted answers-scripts corresponding to the question paper to the examination authority. Examination authority sends the collected answer-books in encrypted form to the examiners for evaluation.

2) Vulnerabilities

Since, the question paper is generated JIT, the problem of question paper leakage is altogether weeded out from the system. However, as the examination authority receives the answers-scripts encrypted with its own public key, examination authority can easily manipulate the answers-scripts.

B. Alteration of Question Paper/Answers-script

1) Countermeasures

The integrity of the question paper is ensured by using digital signatures. Examination authority sends the encrypted question paper with the signed hash of the question paper. Student verifies the hash before answering the question paper. Similarly, students send the signed answers-scripts to the examination authority. Examination authority verifies the hash to ascertain the correctness of the received answers-scripts. If any unauthorized modifications are carried to the question paper/answers-script, it can get detected immediately for taking the remedial action.

2) Vulnerabilities

An unauthorized entity cannot tamper with the question paper/answers-script as normally it is assumed that modern encryption and digital signature methods are difficult to break.

However, as answers-scripts are available to the examination authority in an unencrypted form, there is a scope for alteration of the answers-scripts.

C. *Denial of Action*

1) Countermeasures

In a fair and non-repudiable assessment system, both communicating entities maintain the evidence to prevent the denial of action of the other party. Examination authority maintains acknowledgement of the question paper sent by student and student maintain acknowledgement of the answers-script sent by the examination authority. The hash value ascertains the receipt of exact content. In other words, both parties maintain non-repudiation of origin (NRO) and non-repudiation of receipt (NRR) to prevent each other from denying their action.

2) Vulnerabilities

If one party aborts the protocol before committing the receipt of the content, then there is a risk of denial of receipt by the other party. In e-assessment, if examination authority aborts the protocol after receiving the answers-script and before sending an acknowledgement then the student is in a disadvantageous position. In this way, most assessment protocols are biased towards examination authority and are unfair to the student community.

D. *Favoritism, Coercion and Biased Evaluation*

1) Countermeasures

The e-assessment with just-in-time (JIT) generation of question paper from a large question bank addresses the issue of establishing paper setter anonymity. Anonymous mixnet servers are used to create pseudonyms to hide the real identity of the student from the examiners and the identity of examiners from the students. The identity of the student is revealed only during the result declaration. The identity of the examiner is always kept hidden.

2) Vulnerabilities

Although, mixnet servers successfully establish anonymity of student and examiner from each other, the process of generating pseudonyms through mixnet server is costly and infeasible, in an assessment system with large number of students.

E. *Plagiarism and Collusion*

1) Countermeasures

Question paper leakage, answers-script plagiarism and collusion can be controlled to a great extent, if a unique question paper is provided just-in-time (JIT) to each student/group of students. In an e-assessment with unique question paper for each student/group of student, the association between the student, unique question paper and answers-script is ensured by pairing the question paper and answers-script before sending it to the examination authority.

2) Vulnerabilities

The question paper and answers-script pair is available in unencrypted form to examination authority, where the association can be dismantled. The better approach would be to provide only the necessary part of the information to the party concerned with required level of associativity.

VI. SECURITY ANALYSIS

The conventional/electronic summative assessments suffer from series of threats as discussed in section IV and V. We used the Proverif tool [26] to model both conventional and electronic assessments and to understand the security vulnerabilities associated with the current assessments. The security analysis discussed below is based on the Proverif verification and manual analysis of the cases of malpractices reported/recorded in the conventional/electronic summative assessments pertaining to the higher education based assessments.

A. *Confidentiality (SR1)*

The confidentiality of the question paper and answers-scripts is not guaranteed in the conventional assessment as both these crucial assets pass through the weakest link of the system, i.e., the humans. Thus, question paper/answers-script is vulnerable to leakage as apparent from the frequent occurrence of such incidents.

If any such question paper leakage incident comes to light the only option available is cancel and re-conduct the current assessment. However, this option appears to be too draconian for the majority of the innocent and sincere students.

The confidentiality of question paper is achieved in the e-assessment with JIT generation of the question paper and on the assumption that PKI is strong. However, answers-script confidentiality is not fully guaranteed. Examination authority has full access to the answers-scripts received from students.

B. *Integrity (SR2)*

The integrity of the question paper is not met in a conventional assessment because the original manuscript is not available for verification of the integrity of the question paper during the conduct of assessment. Similarly, integrity of the answers-script is not ensured as unsealed answer-books pass through many hands providing ample opportunities for alteration.

The integrity of question paper is achieved in the e-assessment with strong and secure encryption and digital signature schemes. However, integrity of answers-scripts is not ensured as answers-scripts are available to the examination authority in unencrypted form.

C. *Non-repudiation (SR3)*

The conventional assessment does not provide non-repudiation of receipt (NRR) of answers-scripts submitted by the students to the examination authority. In other words, it is impossible for a student to prove the exact copy of the answers-script submitted by it to the supervisor in case of dispute.

Also, non-repudiation and fairness is not met in the e-assessment as most of the time the evidence is built for the protection of examination authority and neglecting the requirements of student community altogether. Ex. Students are not provided any non-repudiation of receipt (NRR) evidence after receiving the answers-scripts.

D. *Anonymity (SR4)*

Anonymity of paper setters, students and examiners are partially met in conventional assessment with the aid of pseudonym. However, the system is subject to failure due to over dependence on a manual process.

Anonymity of paper setters, students, examiners is achieved in e-assessment with the help of mixnet servers. Mixnet guarantees anonymity by generating pseudonyms corresponding to the actual identity of the entity.

E. *Associativity (SR5)*

Associativity of question paper and answers-script is not achieved in a conventional assessment with a common question paper. In conventional assessment, students can produce plagiarized/colluded copy of answers of any other student without getting detected. Associativity is not met even with a unique question paper per student/group of students as question paper/answers-script mapping scheme does not generate any non-repudiable evidence for dispute handling. Intentional/unintentional errors in recording unique student identity can also break the associativity between the given question paper and the answers-script.

Associativity of question paper and answers-script is not attained in the e-assessment as the question paper and answers-script pair is available in an unencrypted form to the examination authority. The examination authority can tamper the answers-scripts breaking the association between question paper and the answers-script.

F. *Verifiability (SR6)*

The status of verifiability satisfaction in some of the key situations in the conventional/electronic assessment is summarized in Table 1:

Table 1. Summary of Verifiability in conventional/electronic assessment

Situation	Conventional	Electronic
Mechanism to permit a student to verify during the conduct phase of assessment, whether he received a correct question paper or not.	Not possible	Verification is possible by matching the hash of the received question paper and the corresponding message digest of question paper.
Permit a student to verify whether the answers-script assessed is as submitted by him originally or is modified in transit.	Not possible	Verification is possible only if the hash value of answers-scripts sent to the examiner is provided to the student.
Permit student to verify whether his answers-script is assessed fully.	The student can request for personal verification of the answers-script.	The student can request for personal verification of the answers-script.

VII. Conclusion

Malpractices in the summative assessments are plaguing educational institutions worldwide. Appropriate strategies are required to deter and detect malpractices to uphold the academic honesty and integrity of the assessment. We investigated two existing assessment systems, namely: conventional assessment and e-assessment to understand the source and type of threats vis-à-vis security requirements. Based on the reported incidents of malpractices, we identified the vulnerabilities associated with the current examination system. The security analysis of the conventional/ electronic assessment indicates that both the systems are a way short of providing the required level of security to the stakeholders concerned. As a future work, we intend to build and analyze a comprehensive security plan for conducting summative e-examination. Also, we plan to devise security protocols for establishing unambiguous and non-repudiable link between the question paper received by the student and the corresponding answers-script produced by the student.

VIII. REFERENCES

[1] R. M. Thomas, Combating academic fraud: Toward a culture of integrity, JSTOR, 2005.

[2] M. A. Eckstein, Combating academic fraud: Towards a culture of integrity, International Institute for Educational Planning, 2003.

[3] V. Maheshwari, Malpractices in examinations–the termites destroying the educational set up, 2011.

[4] D. Varble, Reducing cheating opportunities in online test, Atlantic Marketing Journal 3 (3), pp. 9, 2014.

[5] J. Castella-Roca, J. Herrera-Joancomarti and A. Dorca-Josa, A secure e-exam management system, in: The First International Conference on Availability, Reliability and Security, ARES 2006, IEEE, 2006.

[6] A. Shafarenko and D. Barsky, A secure examination system with multimode input on the www, pp. 97-100, IEEE, 2000.

[7] E. R. Weippl, Security in e-learning, Vol. 16, Springer Science & Business Media, 2005.

[8] R. Giustolisi, G. Lenzini and P. Y. Ryan, Remark! A secure protocol for remote exams, in: Cambridge International Workshop on Security Protocols, pp. 38–48, Springer, 2014.

[9] L. Elton, R. Benjamin and J. Brenda, Assessment in Universities: a critical review of research, LTSN Generic Centre York, 2002.

[10] D. Rowntree, Assessing students: How shall we know them? Routledge, 2015.

[11] A. P. Rovai, Online and traditional assessments: what is the difference? The Internet and Higher Education 3 (3), pp. 141–151, 2000.

[12] JISC, Effective practice with e-assessment, accessed: 2016-09-09 (2007). URL: http:/www.jisc.ac.uk/media/documents/themes/elearning/effpraceassess.pdf

[13] J. Harvey and N. Mogey, Pragmatic issues when integrating technology into the assessment of students. S. Brown, P. Race, & J. Bull (Eds.), Computer-assisted assessment in higher education. pp. 7-20, 1999.

[14] D. Gollman, Computer security. John Wile & Sons, UK, 1999.

[15] C. P. Pfleeger and S. L. Pfleeger, Security in computing, Prentice Hall Professional Technical Reference, 2002.

[16] K.C. Lee, K.N. Chang, S.S. Yu, I.C. Chang, C.W. Shia, W.C. Chen and J.H. Huang, Design and implementation of important applications in a java-based multimedia digital classroom, Consumer Electronics, IEEE Transactions on 43 (3), pp. 264–270, IEEE, 1997.

[17] A.I. González-Tablas, A. Orfila, B. Ramos and A. Ribagorda, Evaweb v2: Enhancing a web-based assessment system, in: Proceedings of the 4th International Conference on Multimedia and Information Communication Technologies in Education, Sevilla, Spain, pp. 837–840, 2006.

[18] R. Giustolisi, G. Lenzini and G. Bella, What security for electronic exams? , International Conference on Risks and Security of Internet and Systems (CRiSIS), 2013, pp. 1–5, IEEE, 2013.

[19] J. Dreier, R. Giustolisi, A. Kassem, P. Lafourcade and G. Lenzini, A framework for analyzing verifiability in traditional and electronic exams, in: Information Security Practice and Experience, pp.514–529, Springer, 2015.

[20] M. Abadi and C. Fournet, Mobile values, new names, and secure communication, In ACM Sigplan Notices,36(3), pp. 104-115, ACM, 2001.

[21] K. M. Apampa, G. Wills and D. Argles, An approach to presence verification in summative e-assessment security. In *Information Society (i-Society), 2010 International Conference on*, pp. 647-651. IEEE, 2010.

[22] K. M. Apampa, Presence verification for summative e-assessments, Ph.D. thesis, University of Southampton, 2010.

[23] K. M. Apampa, G. Wills and D. Argles, towards a blob-based presence verification system in summative e-assessments, International Journal of e-Assessment 1 (1), 2011.

[24] G. Bella, R. Giustolisi, G. Lenzini and P. Y. Ryan, A secure exam protocol without trusted parties, in: ICT Systems Security and Privacy Protection, pp. 495–509, Springer, 2015.

[25] A. Huszti, and A. Petho, A secure electronic exam system, Publicationes Mathematicae Debrecen 77 (3-4), pp. 299–312, 2010.

[26] B. Blanchet, Automatic proof of strong secrecy for security protocols, in: IEEE Symposium on Security and Privacy, Oakland, California, pp. 86-100, IEEE, 2004.