ISSN 2047-3338

Cryptography – Analysis of Enhanced Approach for Secure Online Exam Process Plan

N. Samba Siva Rao[1], P. Harshita[2], S. Dedeepya[3] and P. Ushashree[4]

[1,2]Varadhman College of Engineering, India
[3]PRRM Engineering College, India
[4]P. Indra Reddy Memorial Engineering College, India

***Abstract*– To conduct the exam for thousand people offline process have several problems, to avoid those problems with gone for the process online exam is a field that is very popular and made many security assurances. Even though it fails to control cheating, online exams have not been widely adopted well, but online education is adopted and using all over the world without any security issues. Education learning from online process not have any problem and don't disturb to any one, through online test plan we need to control so many things here our work proposes an enhanced secure filled online exam management environment mediated by group cryptography techniques using remote monitoring and control of ports and input. The target domain of this is online exams for any subject's contests in any level of study, as well as exams in online university courses with students in various remote locations. An easy solution to the issue of security and cheating for online exams and uses an enhanced Security Control system in the Online Exam (SeCOnE) which is based on group cryptography with an e-monitoring scheme. This paper also determines the comparison effects of existing system, and the proposed processes involved in handling failures.**

***Index Terms*– Online Exam, Cryptography, SeCOnE, Security and Cheating**

I. INTRODUCTION

NOW a day's education becomes online process even the offline is usually chosen as the evaluation method for both off line education and online education. We have more benefits on online examinations but security remains a problem such this person writing the exam on a networked computer is monitored by a proctor at some predetermined location. Requirement for an exam location goes against the accessibility the major attraction of e-learning or distance learning may also negate cost savings generated by e-learning or pose obstacles [1] for remote students.

Remove the requirement for human intervention in secure online exam management so as to capitalize on the advantages of online processes. Security [2] control system in the online exam is based on group cryptography with an e-monitoring scheme cryptography supports enhanced security control for the authentication and integrity provides a proctor function to remote examinees to prevent cheating and thus removes the requirements of having to go a fixed location. Our work shows the online exams for all subjects in UG & PG university courses with students at remote locations and also addresses the problem of monitoring an on line exam at a fixed time with same question paper jumble format for all examinees just like an off-line exam but without restricting the physical location of the examinees to improve the quality of education.

Actually an exam proctor is either a person or a machine. Remote Proctor (RP) is supposed to verify the student's ID (thumbprint) and eliminate cheating through a motion detector. Suspicious motion by a student taking an online exam causes a video to record the student's actions. Instructors then review these exam videos for evidence of student cheating. Proctor is similar to RP in that one electronic proctor in a control room monitors up to six or eight students taking exams. The teaching faculty does not review videos unless the proctor notes something questionable regarding student honesty.

Some universities provide electronic proctoring devices such as Remote Proctor to graduate and undergraduate students asserting that it will be required in their courses. Faculty members are then told that they should use Remote Proctor since their students have purchased it and are expecting to use it. University management scenario is rife with conflicts of interest and circular reasoning. Some faculty members probably use Remote Proctor just to avoid being labeled uncollegial or non-team players. Professors who refuse to use electronic proctoring tools may find themselves excluded from online teaching assignments.

II. BACKGROUND

Offline exam become more hectic everything we need to do manually. For secure online exams based on a secure exam protocol with an omnipotent central manager who controlled all the information for students, teachers problem answer sheets and grades. The weakness of this system was that the manager was assumed to be absolutely honest. Moreover, a restricted room was required for the exam, to prevent cheating.

A. Survey on Online Exam

Related security problems to online exams include not only unauthorized access to the problem sheets before the exams but also modification of the questions answers and the grades. Different cheating patterns exist including copying the answer of the another person, number 2 is writing number one person exam searching the internet for answers using the data and software saved on the students local computer and discussing in the hall or email or message chat. Have many problems combating this includes giving a different one to ser each student, restricting the exam room or limiting the number of answer submissions to one. We focused a method to identify and to communicate securely [3] between teachers and students rather than on countermeasures against cheating on online exams.

Monitoring offline exams is also a big problem; in some cases communication between teachers and students decreases the tendency to cheat increases. This will effect has direct impact on online exams when students may have little contact with their teachers.

Latest online education uses Web-based commercial course management software [15] such as WebCT [10], Blackboard [9], or software developed in-house. This software is not used widely for online exams, due to security vulnerabilities, and the system must rely on students' honesty or their having an honor code [3]. Existing Web-based approaches to online exams have highlighted easy accessibility and simplified exam management [7], [8]. However, authentication through only a user name and password can be the weak point in the security of online exams. Environment in which students can use a Web browser and the Internet enables them to search the Internet and to communicate with others for help during the exam.

Webcam is used to prevent cheating by randomly transmitting pictures of students during online exams [8]. However, many soundless pictures of a student do not show what that student is doing or why he or she is doing it, or even if cheating is taking place through Web searching, the use of saved data, or chatting. Considerable discussion has taken place on group protocols and group-mediated communications to ensure secure communications among group members [6], [5]. Has included the consideration of secure group composition, secure intergroup communication using a public key, and secure intragroup communication using the symmetric key through the Diffie-Hellman key exchange [4] two groups for secure communication between distributed entities in the online exam system. The intergroup communication is protected through public key infrastructure (PKI), while intragroup communication uses several symmetric Diffie-Hellman keys.

B. Steps Need to Follow to Conduct Secure Online Exam

Requirements need to follow for online security exam are as follows.

- Accessibility Online exams should be possible without regard to location and time.
- Monitoring the absence of proctoring on online exams may relax [2, 9] the examinees and encourage cheating.

Therefore, it is necessary for an online exam management system to have some monitoring method to prevent and to detect cheating.

- Management Online exam management includes problem creation, problem sheet distribution, answer sheet collection, marking, grade posting, and handling of appeals.

The cost savings of online exams mitigate the burden of exam enforcement and induce many examinees located at very remote sites to participate in the exam. Educators can obtain more objective standards for evaluation. The automatic management of exams lets the examinees know their exam performance very quickly. Online exams permit both educators and examinees to achieve their objectives efficiently.

The identities of the examinee, examiner, marker and proctor should be all authenticated at every step in the online exam process because it is difficult to identify them face-to-face online.

Problems and answers should be checked for their integrity to detect unauthorized changes. Only one submission of the answer sheet should be allowed and the submission of answers after the exam has ended should be prohibited. Unauthorized deletion or the modification of the materials related to the exam should be impossible.

The problem sets should be available to the examinees only during the exam period. Answer sheets should be kept securely before grading.

Copy of prevention are getting help from others, using unauthorized electronic material that may be helpful in completing the exam and intercepting or interfering with communications during an online exam

III. ONLINE EXAMS CHEATING PROBLEMS

Online test cheating without using proctors, because we believe that costly proctor supervision provides only minimal assurance of academic integrity. First, we identified the primary methods used to cheat during online exams. Since we cannot totally eliminate this cheating, we next devised internal online exam control procedures to online cheating by making the costs of dishonesty outweigh the benefits. Finally, we devised a comprehensive online testing plan based on eight online exam control process (OECPs) designed to avoid online exam cheating without using proctor supervision. Our technique to creating an online testing plan is similar to how CPAs approach a financial statement audit. First, we assess the risk or potential for fraud (here, online exam cheating). Second, we examine existing internal controls (cheating prevention methods). Finally, we design audit process to detect fraud. The goal is to achieve reasonable [12], [13] assurance that the financial statements contain no material misstatements. In a similar fashion, the online exam professor should use control procedures to achieve reasonable assurance that academic integrity has been maintained and that significant cheating has not occurred during online exams.

A. In What Way Students will Cheat in Exam

In the absence of good online exam control process, how do online students cheat? In some cases, students can obtain exam questions or even exam answers before they take the exam. Some instructors actually make their exams available online for a week so students can take the exam at their convenience. Students then conspire with their network of classmates. A superior student takes the exam first, records the answers, and/or copies the questions. Then the questions are researched, answered, and distributed to the remaining students. If instructors do not periodically revise exams, then student groups develop files for their current and future classmates to use. Students can also illicitly obtain publishers' test banks and related solutions manuals from university libraries, faculty, or underground sources. Online exams that remain open available for access to extended periods of time permit one student to take the exam while receiving help from other conspiring students who then take the exam at a later time. There are many other methods of cheating during online exams. Cheating, as in fraud, seems limited only by one's imagination.

B. How to Control in Online Examinations

Honest student conduct is a function of cost getting caught and punished vs. benefit possible better grade choice for the student, which is at the heart of any fraudulent act. To cheat or not to cheat: That is the question. A good control system for managing online examinations should both discourage and detect cheating by students. If deficiencies in the control system are discovered, then new or revised online exam control procedures must be implemented. The control procedures to be used must be consistent with the written exam instructions related to the duration of the exam, any materials that can be used as references, and any permitted forms of communication among students regarding examination questions. The Underground Professor has developed and tested a set of online exam control procedures that will severely reduce although not totally eliminate students' ability to cheat and. A review of exam scores and resulting grades indicates face validity of exam integrity and no grade inflation when using this control

C. Online Testing Plan Developing

Implementing the online exam control process, professors are using the online exams can construct a testing plan that does not require expending resources on proctor supervision. Such plans will not entirely eliminate exam cheating, but a good plan will provide reasonable assurance that academic integrity has been achieved at a satisfactory level.

An exam should be scheduled for a specific date and time.

The exam should close when the allotted time period for work expires.

An exam should be open to Internet access for only a 15 minute time period.

Students can work only one question at a time and cannot access completed questions.

Students can access the online exam only one time.

Online exam access should use Repondus Lockdown Browser or its equivalent.

An exam should randomize (scramble) question sequence and answer choices.

About one-third of objective type questions should be rotated/modified on each exam every term.

D. Check the Student Particular Details before Entering into the Exam Hall

The OECPs described above serve to avoid student cheating on online exams without the presence of a physical or electronic proctor. However, a proctor has two functions to avoid cheating, and to verify the identity of the student completing the exam. Without using proctor supervision, the professor must devise some control procedure to assure the validity of the purported identity of a student who completes and submits online exams and other assignments. Student ID numbers and passwords are frequently used to satisfy this control objective. More elaborate identity tests are available using thumb print technology and cornea scans. Control costs tend to be proportional to the sophistication of the technology used. How many controls are enough and what costs are warranted to achieve the control objectives for online testing depends on the individual circumstances?

IV. PROBLEM DEFINITION

For thousands of people conducting the exam, manual test plan generates several problems such as centre of examinations, paper releases before the exam and cheating process. To avoid all these we have a solution online test process, exam management team sit at one place and they can monitor everything at their same. Online test process solution having the drawback that is cheating, our work analyzes the all these drawbacks in this paper.

A. Preparing the Online Examination

We have presenting few lines how to prepare for online examination her.

Every computer user should have the freedom to download run copy distribute study share change and improve their software for any purpose without paying licensing fees.

Every computer user should be able to use their software in the language of their choice

Every computer user should be given every opportunity to use software even if they work under a disability.

Algorithm for online exam process:

```
1. Start
2. Function Setup_exam_environment ()
3. CE[S (i)] registers with AE
4. AE sends identity of s(i) and IP[s(i)] to AA
5. When CE connects to SS, SS sends identity of
s(i) and IP[s(i)] to AA for authentication
6. IF AA authenticates CE[S (i)] THEN SS sends problem
     e[S (i)] set to the examinee CE[S (i)] along with the
     identity of CT
ELSE
Stop the exam process
ENDIF
7. CE[S(i)] verifies the integrity of e[S(i)] by sending the
     identity of the examiner to AE
8. IF AE satisfies with the integrity of e[S(i)] and the
     examiner
THEN
CE sends "ready" message to SS
ELSE
```

```
Request for the problem set again
ENDIF
9. IF SS receives ready messages from all the
examinees THEN
SS sends “start” message to all the
examinees
CE lets the examinees to see the problem one by one
ELSE
halts the online exam.
ENDIF
10. CE[S(i)] sends answers , problem set and its identity to
    SS
11. IF CE[S(i)] is authenticated by AA THEN
SS saves answers in the database
ELSE
Rejects the answers from the examinee
ENDIF
12. After completion of all the problems/time SS
sends “end” message to all the examinees to end the exam.
13. SS marks the answer sheet with the right answers
    provided by CT
14. SS sends grading to the examinees.
15. IF the examinee is not satisfied his grading then he
    appeals for re-grading THEN
GOTO Step 13
ENDIF
16. END
```

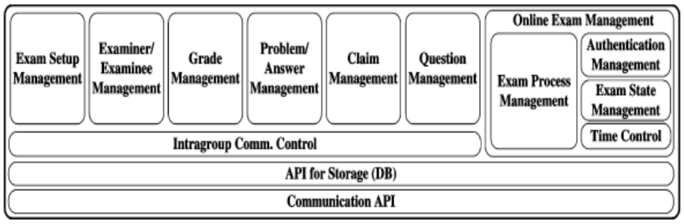

Fig. 1: Shows the online examination process

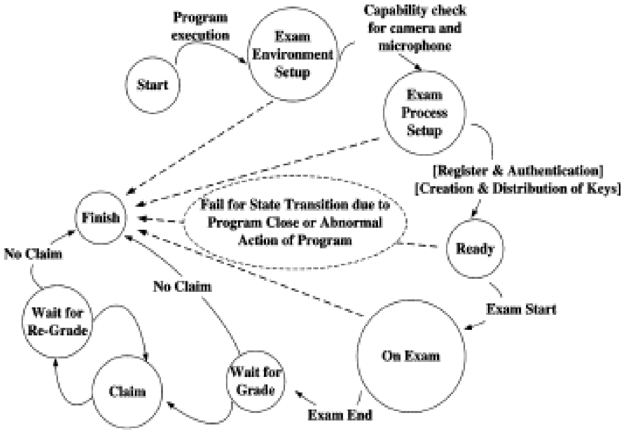
Program execution
Start
Exam Environment Setup
Capability check for camera and microphone
Exam Process Setup
[Register & Authentication]
[Creation & Distribution of Keys]
Ready
Finish
Fail for State Transition due to Program Close or Abnormal Action of Program
No Claim
No Claim
Exam Start
On Exam
Wait for Re-Grade
Claim
Wait for Grade
Exam End

Fig. 2: Shows the online examination flow algorithm/process

B. SeCOnE System Software

It is divided into two parts depending on the role that is whether it is on the client or server side. The operating system of the examinees computers and the proctors’ computer is assumed to be windows family. However the program semantics are not confined to windows because the APIs to control the examinees computer and to handle the multimedia data are also available in Linux and UNIX environments.

C. Proposed Analysis for Online Exam Process

The method e-monitoring examinees can be watched just like in an offline exam. Any cheating that was not noticed during the exam can be detected through the monitor data saved on the monitor server. The enhanced security for the online exam is controlled through the intergroup communication based on PKI, the intra- group communication using symmetric keys and the temporary identity. The exam administrative group and the examinee group are set for every exam. All the entities related to the exam belong to one of those two groups. Agents for the two groups issue the temporary identities to their group members. Neither they nor the group members themselves know the identities of the other group members.

Furthermore, a group member does not know his or her temporary identity, because it is issued in an encrypted form protected by the public key of the verifier, the other group agent. The identities are exchanged by the group agents. Thus, when a group member receives a message, he requests the verification for the sender from the group agent. In addition, message integrity for problems, answers, and grades is guaranteed through the use of digital signatures. Because temporary identities are used in the online exam, it is very important to confirm the identity of someone who is issued a temporary identity. In this paper, that confirmation is performed via a Webcam. An exam administrator connecting to the agent program verifies the person to be authenticated, using the Webcam. In this process, a reference photograph of the group member is taken and saved in the monitor server for later detection of possible impersonation.

The problems are managed by the online exam client after they are issued by the scheduler, but they are not opened before the scheduler sends the message to start the exam. The message is sent only after the online exam environment has been set up and all the online exam clients send the “ready” message to the scheduler. Therefore, it is possible for all examinees to take the online exam simultaneously. The examiners can prepare one set of problems for each of several exam times so that the examinees can choose the time that suits them best.

Even through the proctor, she or he can supervise the examinees with the monitor data saved in the monitor server in near real time for the problems, their right answers, and the answer sheets from examinees are managed by the scheduler. The authentication, which traditionally was based only on a user name and password, is strengthened by the group management. This process includes verification by Webcam and issuance of temporary identities for every exam. No entity can know all the information, such as the real identities of the entities or the cryptographic keys in the system.

This precaution avoids the potential for system compromise due to the failure of a single entity because of maliciousness or an external attack. This application adopts five methods to prevent and detect cheating. First, the identities of entities in the system are verified by a Webcam, and the reference photos taken during the verification process are saved for authentication during the exam. Second, the monitor data for the examinees are recorded and saved during exam. With continuous recording of video and audio during the exam rather than isolated images, a proctor can better understand the examinee's situation and reduce the chance of false-positives or negatives in the determination of cheating, even after the exam. Third, through the screen shots saved in parallel with videos of an examiner, a proctor can better determine what the examinee is actually doing with his or her computer. Fourth, all communications by the examinees, except for those required for the online exam, are disabled through port control. All ports except those required for the online exam are disabled and the ports used can be chosen randomly for each examinee; the ports to be used have only to be sent to the exam administrative group with the IP of the exam client. Therefore, cheating through a fixed port can be rare. Fifth, all other programs except the online exam client are deactivated by controlling the inputs of the examinees. By cutting off electronic communications and disabling other computer programs or inputs on the examinees' computers, the examinees can be prohibited from cheating using their local computer or the Internet.

Online exam take place mainly before and after the exam time. During the exam, only the monitor data, a few messages to check the exam state, and questions, if any, flow to the server side. Communications before exam time are required to authenticate the entities in the proposed system. The proposed browser module presents to the user at startup a full-screen application window that encases a browser window. However, no address bar is provided, nor are there any menus, toolbars, buttons, or other controls that would be seen on a generic browser. The application window is locked in full-screen mode and cannot be resized or minimized until the application is terminated. Timing the exam helps lessen the opportunity that students have to utilize inappropriate material. If the exam has no time limit the temptation to avoid studying and rely instead on looking up answers during the exam would be greater. By providing only forty-five seconds per question, we limit the students' ability to engage in this. We also tend to ask lengthy, application based questions.

V. COMPARATIVE STUDY

Different cheating patterns exists in current system including copying the answers of others, exchanging answers, searching the Internet for answers, using the data and software saved on the student's local computer and discussing the exam by e-mail, phone, or instant messaging and also have many drawbacks such as Level of communication between teachers and students decreases, tendency to cheat by students increases and system must rely on students' honesty or their having an honor code. The system which overcomes our proposed solution to the issue of security and cheating for online exams. This solution uses an enhanced *Se*curity *C*ontrol system in the *On*line *E*xam (*SeCOnE*) which is based on group cryptography with an e-monitoring scheme.

The cryptography supports enhanced security control for the online exam process, as well as authentication and integrity. The e-monitoring provides a proctor function to remote examinees to prevent cheating, and thus removes the requirement of having to go to a fixed location. The target of this project is online exams of any type and exams in online university courses with students at remote locations.

Project proposes administering an online exam at a fixed time with the same questions for all examinees, just like an off-line exam, but without restricting the physical location of the examinees. As the *SeCOnE* system enables many kinds of tests to be given online, it can provide teachers with better evaluation standards for students and may contribute to improving the quality of education with many benefits like Online exam management system having some monitoring method to prevent and to detect cheating, Without regard to location and time and to Avoid intercepting or interfering with communications during an online exam.

VI. CONCLUSION

Our proposed system describes how the techniques provide a secure online exam management and a scheme for the prevention and detection of cheating using e-monitoring. This paper targeted towards exams administered through the Internet at a fixed time with one problem set, but without any restriction on the exam location. A powerful feature of the proposed system is that it can be applied to an exam administered at different times. In this case, the examiner should prepare as many problem sets as there are exam times, in order to prevent cheating during the exam. One overhead cost for this system is in the preparation of the equipment, such as Webcams and microphones, to monitor and to authenticate the entities. Future work extends with distributed online exam process to reduce and prevent all the cheating methods employed by the personnel.

REFERENCES

[1] Golden Gate University [Online]. Available: http://www.ggu.edu/cybercampus/DegreesCourses/ClassSchedule

[2] Univ. Phoenix Online [Online]. Available: http://online.phoenix.edu/Degree_Programs.asp

[3] New York University [Online]. Available: http://www.scps.nyu.edu/areas-of-study/online/

[4] J. McGough, J. Mortensen, J. Johnson, and S. Fadali, "A Web-based testing system with dynamic question generation," in Proc. 31th ASEE/ IEEE Frontiers in Educ. Conf., Reno, NV, 2001, vol. 3, pp. S3C–23.

[5] C. C. Ko and C. D. Cheng, "Secure Internet examination system based on video monitoring," Internet Res.: Electron. Netw. Appl. Policy, vol. 14, no. 1, pp. 48–61, 2004.

[6] The Blackboard Northern Illinois Univ. [Online]. Available: http://www.blackboard.niu.edu/blackboard/

[7] C. Rogers, "Faculty perceptions about e-cheating during online testing," J. Comput. Sci. Colleges, vol. 22, no. 2, pp. 206–212, 2006.

[8] D. L. McCabe, L. K. Trevino, and K. D. Butterfield, “Cheating in academic institutions: A decade of research,” Ethics Behav., vol. 11, no. 3, pp. 219–232, 2001.

[9] F. DePiero, “Netexam: aWeb-based assessment tool for Abet2000,” in Proc. 31st ASEE/IEEE Frontiers in Educ. Conf., Reno, NV, 2001, vol. 2, pp. F3A–13.

[10] A. Shafarenko and D. Barsky, “A secure examination system with multi-node input on the world-wide Web,” in Proc. Int. Workshop on Adv. Learn. Technol., 2000, pp. 97–100.

[11] J. Burgoon, M. Stoner, J. Bonito, and N. Dunbar, “Trust and deception in mediated communication,” in Proc. 36th Hawaii Int. Conf. Syst. Sci., 2003, pp. 44–54.

[12] W. L. Goffe and K. Sosin, “Teaching with technology: May you live in interesting times,” J. Econom. Educ., vol. 36, no. 3, pp. 278–291, 2005.

[13] J. C. Adams and A. A. Armstrong, “A Web-based testing: A study in insecurity,” World Wide Web, vol. 1, no. 4, pp. 193–208, 1998.

[14] D. Agarwal, O. Chevassut, M. R. Thompson, and G. Tsudik, “An integrated solution for secure group communication in wide-area networks,” in Proc. IEEE Symp. Comput. Commun., 2001, pp. 22–28.

[15] Effective on-line assessment: Workshop support materials. University of New South Wales: Sydney. [viewed 11 Aug 2009] http://www.edtec.unsw.edu.au/inter/dload/flex_ed/resources/Online%20Assessment/Online%20Assessment%20Workshop%20notes.doc.

N. Samba Siva Rao Ph.D (CSE) from Anna University, M.E (CSE) from MNREC, Allahabad, M.Tech (PSE) from REC Warangal. He has 30years of Academic Experience, guided many UG&PG Students, represented Kakatiya University Co-ordinator for NSS summer camp. He have presented papers at National & International Conferences, eights journals published. Currently working as a principal at Varadhman College of Engineering, research areas include Databases, Software Engineering, Networks, Power Electronics and Data Mining.

P. Harshita pursuing M. Tech Software Engineering at Varadhaman college of Engineering B.Tech Information Technology from Teegala Krishna Reddy Engineering College. Her areas of interest include Information Security and Software Engineering.

S. Dedeepya pursuing M. Tech CSE from PRRM Engineering College B. Tech IT from Geethanjali College of Engineering & Technology. Her interest areas include Information Security and Computer Networks.

P. Ushashree pursuing M. Tech CSE at P. Indra Reddy Memorial Engineering College B. Tech CSE from Geethanjali College of Engineering & Technology. Her areas of interest are Computer Networks and Information Security.