Improved Security for Online Exams Using Group Cryptography

K. Usha Rani, Ch. Varsha, B. Priyanka, P. Neeharika, Associate Prof. Dr. S.Venkatramulu
Department of CSE,
KITS, Warangal,AP,India

Abstract- Online examination system is a internet-based system. Exam is conducted using the internet. The basic aim is to conduct the online exams more securely. For high security we used group based cryptography. Mail authentication is provided so that user gets username and password. In the database the user credentials and user answers are stored in the form of encrypted format. Only admin have the access to the database. The encrypted form of data in the database cannot hacked by the hacker.

Keywords- high security , cryptography , internet-based system etc.

I. INTRODUCTION

Exam activities including recognizing exam trends with revenue sources, determining exam timers, objective/ subjective test parts, and paperless exam administration can all be streamlined with an online review system. The Online Examination System, which is a low-cost option, can transform traditional pen-and-paper tests to online and paperless exams.

The use of online assessments, the Internet, and online exams is not common. My project provides a more stable Internet exam organization environment using group cryptographic methods and remote port and input monitoring. The proposed system provides a solution to the problem of online examination and hacking that removes the need of staff work, allowing users to benefit from the advantages of online processes. In this method, the Online Exam (second) employs an improved Security Control system based on group cryptography.

An online examination system is that the complete agenda of a web based test which possesses multiple features and functionalities. The online examination system uses online examination software. With help of software the tests are created, conducted. This type of online examination system has multiple benefits. Few of them are that it eliminates the pen and paper work , eliminates any sort of manual work load which is just too much just in case of an offline test, reduces time and examination cost and reduces logistics cost.

II. LITERATURE SURVEY

The recent implementation of electronic surveillance and the resulting widespread awareness among group of students. Few anomalies were discovered after examining the interviews and studying the current electronic online evaluation and assessment system, and a new e-exams system was created to eliminate these anomalies.

To prevent deception in the online test process, the current method uses data protection to secure questions sent to the e-Review centre through the internet or intranet, as well as video conference-based computers. In both learning and instructional contexts, online review has received a lot of interest and has proven very useful. Examining an individual's skill and intelligence is the mosteffective way to assess them. To reach this point, a variety of techniques for assessing a person's competence have been used.

Newly developed system describes the use of computer devices rather than manual or paper systems, which were marked by large test leakages, impersonations, instructor demands for gratification, and inducement- taking by supervisors and exam invigilators. A body of research is focusing on developing better approaches to supervise e-exam processes and e-learning programs.

Any of the study looked at various aspects of the scheme, including: Schramm looked at a web-based e-learning framework that could easily deliver and rate mathematical questions with no complaints.

As a result, itrequires the ability to input and output numerical formulas, generate complex plots, and generate random terms and statistics.This is a web-based online scheme in which the system assessment administers tests and grades students' exams. The method allows for the administration of tests, the compilation of responses, the automatic labeling of entries, and the development of exam reports. It can handle a wide range of queries.

III. EXISTING SYSTEM

There are many online exam systems available in the market today. In existing system every student have to fill the exam form manually and submit to specific course. The process of conducting exam and evaluating the result after the test was done manually till date. Sometimes the results are not accurate. Checking of result is time consuming.

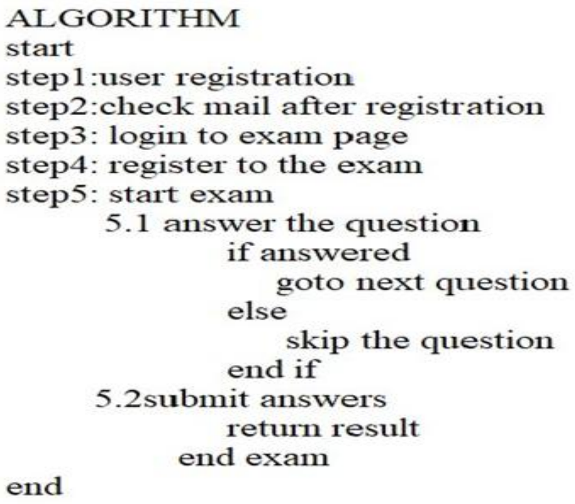
As the examination systemmaintains the database to store the data of question papers and answers given by the students in exam. Hacker can hack the database and download the quesions and he can modify the answers.

Disadvantages of existing system:

- Time consuming
- Manual analyzing is difficult
- Chances of leakage of paper

IV. PROPOSED SYSTEM

The proposed system provides a solution to the problem of online examination and hacking that removes the need of staff work, allowing users to benefit from the advantages of online processes. In this method, the Online Exam (second) employs an improved Security Control system based on group cryptography.



```
ALGORITHM
start
step1:user registration
step2:check mail after registration
step3: login to exam page
step4: register to the exam
step5: start exam
        5.1 answer the question
                if answered
                    goto next question
                else
                    skip the question
                end if
        5.2submit answers
                return result
            end exam
end
```

1. Registration:
In registration phase, user registers for the exam. During registration user fills the registration form. Form contains username, address, street, mobile number, email. User have to give working email id for registration, to the given mail id the admin sends the username and password to take exam.

2. Authentication:
In authentication phase, user has to check the registered mail id for username and password. Mail id should be opened in proper localhost. User get link to the mail, when user click on the link account will be activated and username and password will known to the user. From the activated account user get login into the exam. User password will stored as in encrypted format.

3. Exam:
In exam phase, after logging into the exam user has to register for exam for which subject he want to take exam. From the list of exams user register for the exam. User registered exams will be shown in registered exams list. When user starts exam the encrypted question paper will be visible to user.

After submitting the answers the result will be shown to user and user will be automatically logged out from the exam. User answers will be stored in database. User can take one exam only for one time. After taking the exam for registered subject that will not be visible to the user because he/she already taken exam.

V. ENHANCED SECURITY SYSTEM

In cryptography, a gathering key is a cryptographic key that is divided among a gathering of clients. Ordinarily, bunch keys are disseminated by sending those to singular clients, either truly, or scrambled exclusively for every client utilizing either that client's pre-circulated private key.

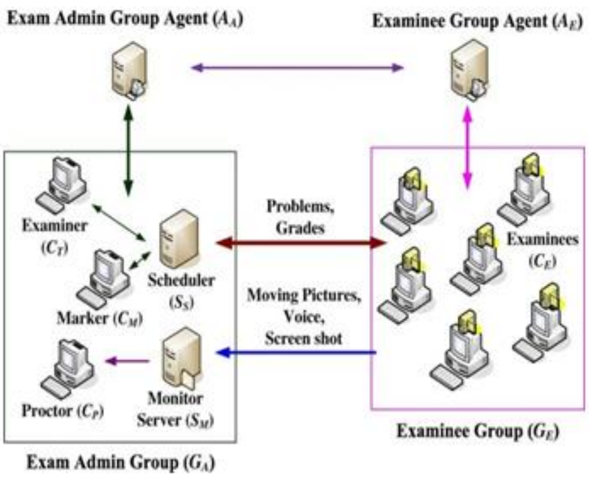


Fig 1. Architecture of security system.

A key in cryptography may be a snippet of knowledge, normally a series of numbers or letters that are put away during a document, which, when handled through a cryptographic calculation, can encode or disentangle cryptographic information. They can be utilized for both encryption and decoding in symmetric cryptography or must be utilized for one or the other encryption or unscrambling with unbalanced cryptography. In view of the strategy, the key can be various sizes and assortments. A key's security strength is subject to its calculation, the size of the key, the age of the key, and the cycle of key trade.

Since the key secures the classification and respectability of the framework, it is imperative to be hidden from unapproved parties. With public key cryptography, just the private key should be kept mystery, yet with symmetric cryptography, it is critical to keep up the secrecy of the key. Kerckhoff's guideline expresses that the whole security of the cryptographic framework depends on the mystery of the key.

Key size is the quantity of pieces in the key characterized by the calculation. This size characterizes the upper bound of the cryptographic calculation's security. The bigger the key size, the more it will take before the key is undermined by a beast power assault. Since amazing mystery isn't achievable for key calculations, investigates are presently more centered on computational security.

Before, keys were needed to be at least 40 pieces long, notwithstanding, as innovation progressed, these keys were being broken faster and speedier. As a reaction, limitations on symmetric keys were improved to be more prominent in size. At present, 2048 digit RSA is usually utilized, which is adequate for current frameworks. In any case, current key sizes would all be broken rapidly with an incredible quantum PC.

“There is numerical design for keys used in the open key cryptography. For instance, public keys utilized in the RSA framework are the result of two indivisible numbers. Subsequently open key frameworks require longer key lengths than symmetric frameworks for a comparable degree of safety. 3072 pieces is the proposed key length for frameworks dependent on figuring and number discrete logarithms which mean to have security identical to a 128 bit symmetric code."

VI. CONCLUSION

We've looked at a lot of security issues in computer-based and online research in this article. We've also looked at a number of different authentication systems for examinees. In addition, we have proposed a new authentication scheme that combines username/password and palm-based biometrics. The proposed scheme would improve the authentication process to the maximum extent possible. Online examination systems have several advantages.

Online assessment is a method of evaluating human abilities, capabilities, attitudes, and attributes in a systematic and objective manner. These evaluations are conducted over the internet using current web technologies. Online testing has become increasingly common. The advantages of online testing include a plethora of evaluation options for both the examinee and the examiner conducting the examination.

If it's a business running certification programs, a college embracing an online mode for performing tests, or a training company planning to scale up assimilation, making the switch to online evaluations will help organizations in a variety of ways. Choosing the right online examination tool, on the other hand, will help you avoid certain disadvantages. You can get reliable results faster with an easy- to-use, stable, and safe examination framework that include all of the new AI- based anti-cheating initiatives.

REFERENCES

[1] J. C. Adams and A. A. Armstrong, “A Web-based testing: A study in insecurity”, World Wide Web, 1998

[2] Al-Mashaqbeh, I.F. Al Hamad, A., “Student's Perception of a web Exam within the choice System Course at Al al Bayt University”, IEEE International Conference on Computer Research and Development, 2010.

[3] Akshada Deshmukh, Harshalata Wadaskar, Leena Zade, Neha Dhakate, Preetee Karmore, “Webcam Based Intelligent Surveillance System”, International Journal Of Engineering And Science, 2012.

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

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

[6] University [Online]. Available: http://www.s cps.nyu.edu/areas-of- study/online/