iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VI **Month of publication:** June 2020

DOI: http://doi.org/10.22214/ijraset.2020.6276

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

Designing Security Framework for Secure Exam System based on QR Code

Ms. Ikhar Shruti[1], Ms. Kanhurkar Pratiksha[2], Ms. Mahalunkar Jyoti[3], Ms. Nikhal Snehal[4], Prof. Dhage Vaibhav[5]
[1, 2, 3, 4, 5]*Department of Computer Engineering, P.K technical campus, Pune University, India*

Abstract: ***Today, Online Examination System is considered a fast-developing examination method because of its accuracy and speed. The main objective of our project is to efficiently evaluate the candidate thoroughly through a fully automated system that not only saves time but also give a fast result. In this automated system, there is no need for paper and pen. The user can write the exam without going to the exam centre. The project includes two modules namely, administrator and user. The control for all the process of the examination belongs to the administrator module. Now a day, require for fast accessing of data is increasing with the exponential increase in the security field. QR codes have served as a useful tool for fast and convenient transferring of data. But with increased usage of QR Codes have become insecure to attacks such as phishing, pharming, manipulation, and exploitation. The goal of designing applications is to hide candidate details with the help of QR code, to recognize cheating at the time of examination by taking a screenshot and photo of that particular candidate through a web camera. Online Exam Software is the best solution to improve every educational centre.***
Keywords: Security, QR-Code, AES, Encryption, Decryption, M- learning, E-learning.

I. INTRODUCTION

Online Examination System is also required minimum manpower to handle the examination. Today, almost all organizations demands
to manage their exams by online examination system since it precise time. Organizations easily monitor the progress of the student through an examination. The online examination system is significantly important to the educational institution to prepare the exams, saving the time and effort that is required to check the exam papers, and prepare the results reports. The online examination system helps the educational institutions to monitor their students and keep eyes on their progress. At the time of online Examination, the Candidate is given a limited time to answer the questions and after the time expires the answer paper is disabled automatically and answers are sent to the examiner. The examiner will evaluate answers, either through an automated process or manually and the generated results will be forwarded to the candidate through email or made available on the web site. In the current online system, the Candidate can able to use any other site for getting information related to the questions and select the correct answer. This system unable to catch the cheat and cheaters get full freedom to misuse the online exam system. To avoid the above situation, this project designs a secure system which helps the particular organization to detect cheating during the exam and terminate the exam at that time. The system will also provide digital authentication to avoid any fraud candidate who appeared for the exam. At the admin side, the generated QR code gets scanned and all details related to candidates get present on his/her console. Candidate can appear for both exam mode online as well as offline. In offline, questions are generated uniquely for each candidate. The manual procedure used for conducting an exam is a time-consuming process and error disposed of due to human limitations.

II. EXISTING SYSTEM

In the process of conducting the online examination, the student can easily open a new tab and find out the answer to this question and also does not terminate the exam. These cheating details are not known to examiner or admin. In this way, student activities are not traced. We found that the existing system was a manual entry of up keeping of the details of the student who are registered already. And it is very difficult for every student to come to the examination centre. An online examination system is needed to prepare registration form, question paper for the students, and need to print a lot of numbers manually. For calculating how many students registered, and validating details of every student in a month by hand is very difficult and time-consuming. It does not only require lots of time but also a loss of money as it requires quite a lot of Manpower to do that. Another thing that takes into account is the possibility of mistakes. The limitation of the existing system is that it is not personalized. It cannot be used for personal and immediate reference. This system is not compatible with all kinds of devices. Even the staff members can make quick entries if the responsible person is absent. It also requires the teacher to monitor the examination centre.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

III. PROPOSED SYSTEM

The modern computerized system is enlarged with the target to conquer the disadvantages of the existing manual system. The proposed system has obtained many advantages. People from different parts of the world can register conveniently. The new system is better personalized. It is developed in a quick and easy referential approach. The benefits of the proposed system are that security is nourished in the new system. Securities to the important data are maintained confidentially. In comparison to the existing system, the proposed system will be less time consuming, easily understandable, user friendly, and more efficient. The result will be very precise and accurate and will be declared in a very short period. The proposed system is secure as no any chances of paper leak as it is operated by the administrator only. To keep track of this, the logs of candidates and their response are stored and can be backup for future use.

In this proposed system, while going to conduct an online examination, students carry QR code which is obtained through Gmail, and this QR code scanned by examiner. Examiner checks all credentials correct are not. If it is correct then the examiner will permit the students for the exam and otherwise not. Throughout the exam time if a student does cheat by opening a new tab then our system will take a screenshot of that screen and take a photo of that particular candidate through a web camera. All cheating details are sent to the admin as well as on the student's Gmail and terminating screen of that particular candidate. If students give the exam without cheating then the results of students will generate successfully.

A. Scope Of The Project

Online Examination System is developed for educational institutes like schools, colleges. It is designed to provide and facilitate the administrator and user. It also provides complete and safe information to the user. This system has a good user interface as well as it satisfies the user requirement.

B. Architecture Design

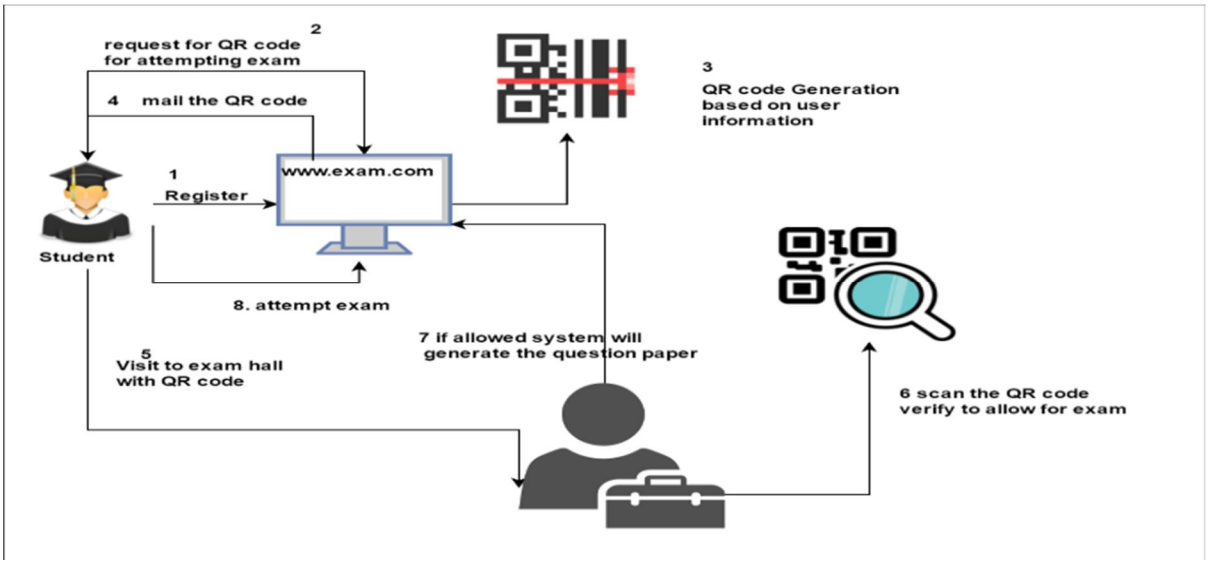


Fig.1 System Architecture

IV. METHODS AND METHODOLOGIES

A. Implementation Of AES 256

In the process of encryption, we have a plaintext of 128 bits, and the size of the key is 256 bits. There are 14 rounds in AES 256. The first round comprises of all the five operations like Pre-round operation, sub byte, shift rows, mix columns, and Add round key operations. From 2nd round to 13th round have four operations sub byte, shift rows, mix columns and Add round key operations and the last 14th round involves of three operations sub byte, shift rows and then add round key.

The process of generating the key as follows:

Input key which is of 256 bit is partitioned into eight parts of 32 bits. The last column is taken and given as input to S box. The achieved output of the S box is given shift rows operation. The output 8 MSB bits are XORed with the round constant. The achieved output is XORed with the 0th column of the input key.

©IJRASET: All Rights are Reserved

The 0th column of the new key is XORed with the 1st column of the input key gives 1st column of a new key and so on. In this way, we generate new keys of 256 bits by joining the eight obtained columns of the new key. In the 1st round, this key of 256 bits is split into two parts each of 128 bits size which is used in the pre-round operation, and the other is used in Add Round key operation. In the end, there will be 128bit output and 256-bit key output. In the 2nd round as we don't have a pre-round operation so the round output of 1st round is carried out as input to sub byte and the remaining operations are the same as round 1. This process of round operation is repeated up to 13th round operation and the last round is similar to the previous round the only change is it does not have mix columns operation. AES Decryption is exactly inverse to AES Encryption Process.

B. QR Code Generation:

QR codes (Quick Response codes) are the extension of the bar code. It is a 2-D matrix code instead of a 1-D barcode. It stores the information by arranging dark and light elements in the matrix. The steps of the suggested technique to generate and read a secure QR code are described below in chronological order:

1) *QR Code Generator:* First of all, Enter a password for encrypting the data. A 128-bit key is generated from the password. Then Enter the data for QR Code. Data is encrypted with AES and embedded in QR Code and finally QR Code is generated.
2) *QR Code Scanner:* Scan the QR Code and enter the secret key. A 128-bit key is generated from a password. QR Code is decoded and data is decrypted using the key. If the password entered is correct then true data is displayed otherwise wrong data.

C. Implementation Details

The general structure of the system:

The system is composed of three-layered structures:

1) A database
2) A server
3) Clients

MySQL database management system is open-coded software and it has improved specifications, It uses the application server layer which is used to generate the question paper when the admin verifies users by scanning the QR image it should, On the client layer side, it is required to employ a web browser. To develop an Online Exam system, a server-based and fast JSP servlet programming language is preferred. For the developed software, Apache is used as a web server which is a strong, knowledgeable, and flexible HTTP server and the open-coded programming language. A web server is a software sending the pages stored under the web address you are connected to. In the adaptive web-based exam system, JavaScript language is used to allow dynamic user access; to let it be feel on the same page, and to perform tasks like presenting resting time for the exam. To develop a scanner i.e. android based application. An android studio version 3.6.3 onwards IDE (Integrated Development Environment) is used with SDK (Software development kit) which contains android plugins, theme plugins, etc. which are used to implement the application.

V. RESULTS

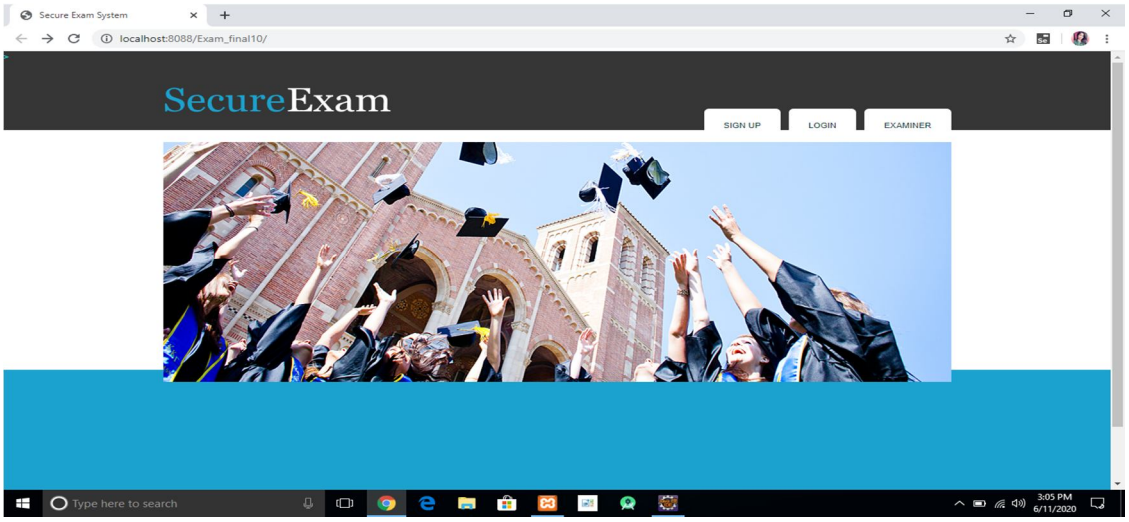


Fig.2 Home Page

©IJRASET: All Rights are Reserved

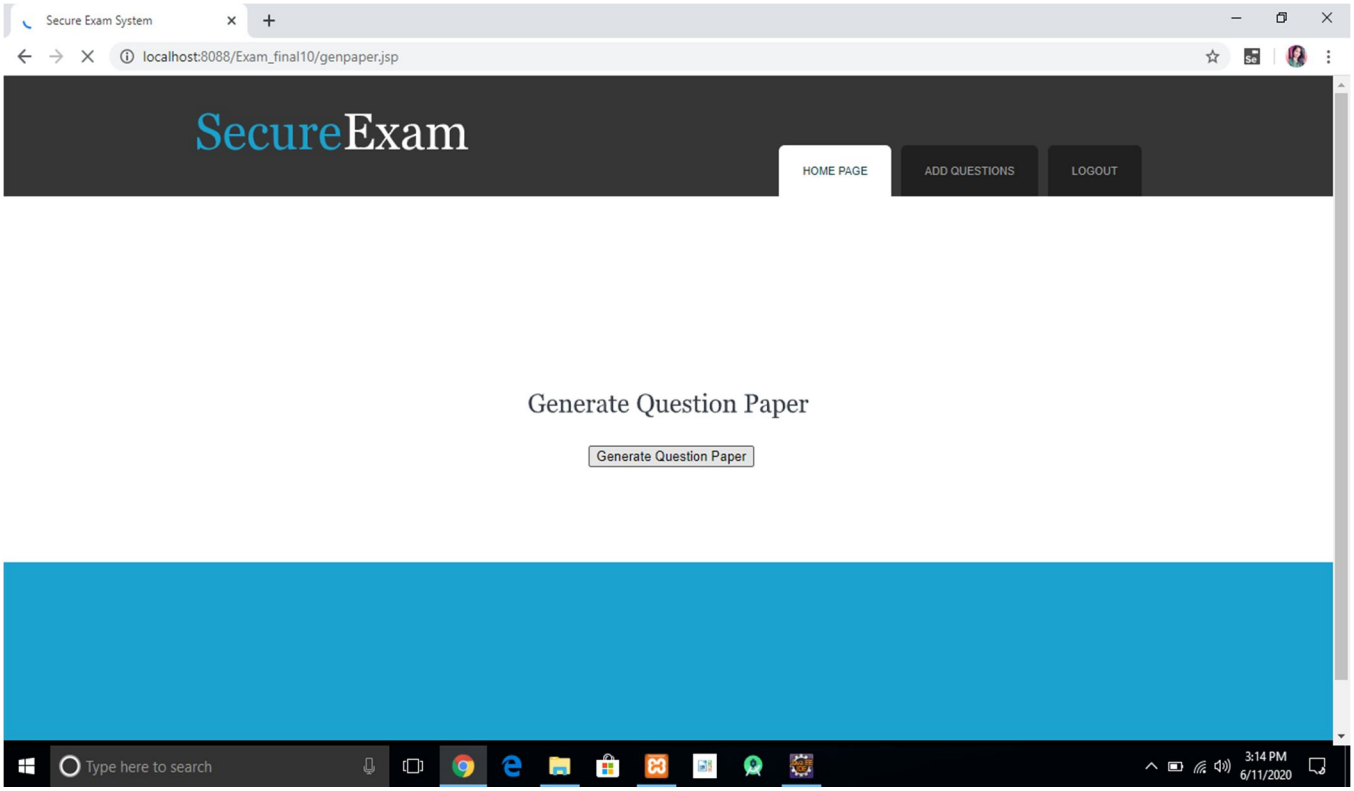


Fig.3 Examiner's Home Page

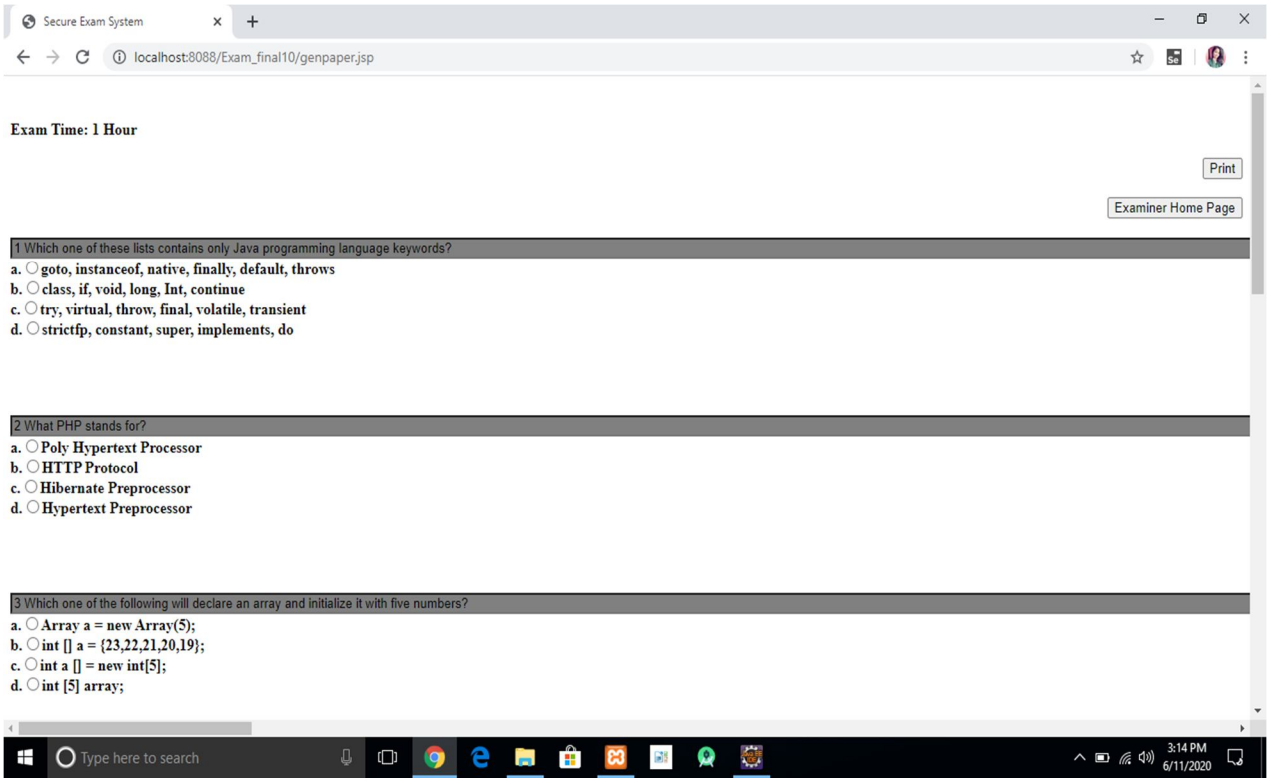


Fig.4 Offline Paper

©IJRASET: All Rights are Reserved

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

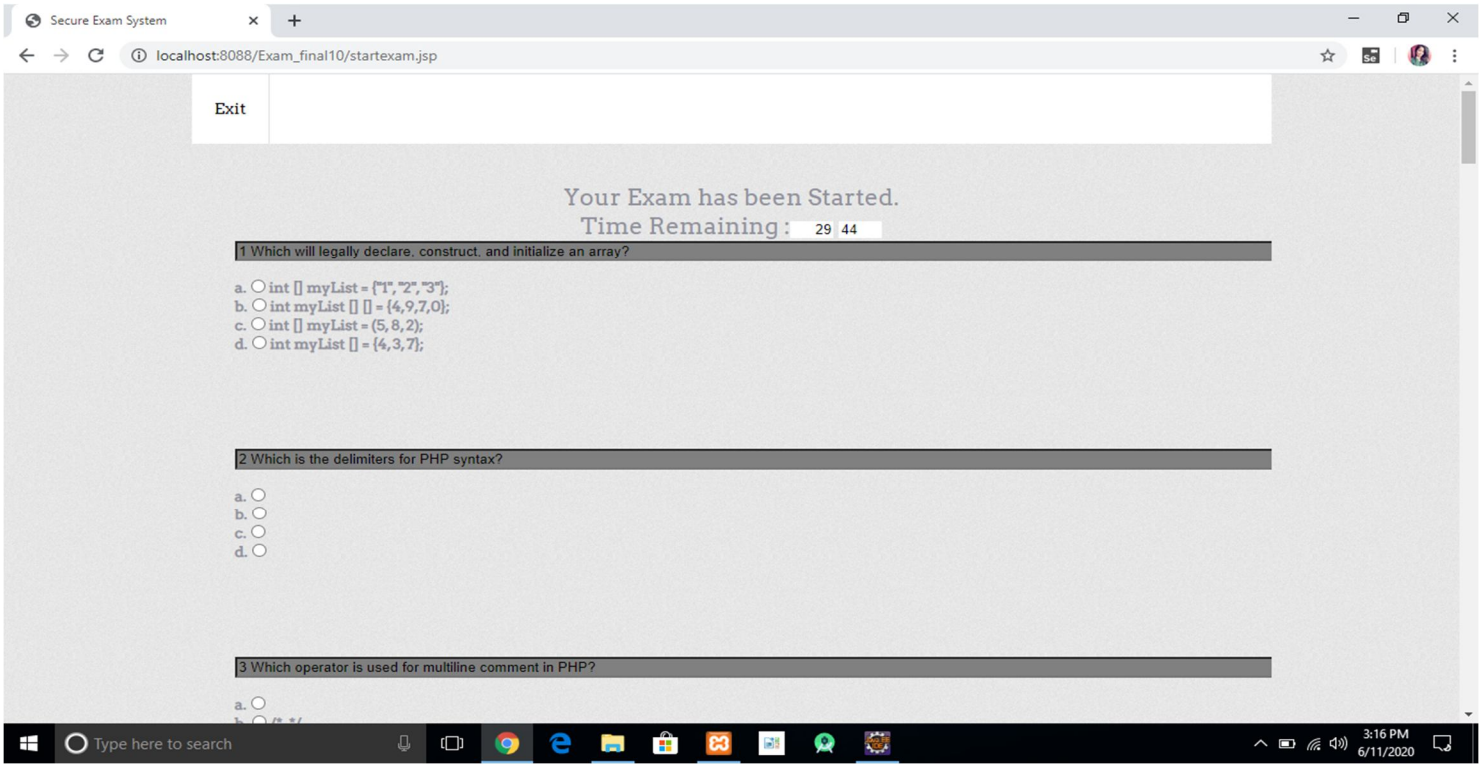


Fig.5 Online Exam

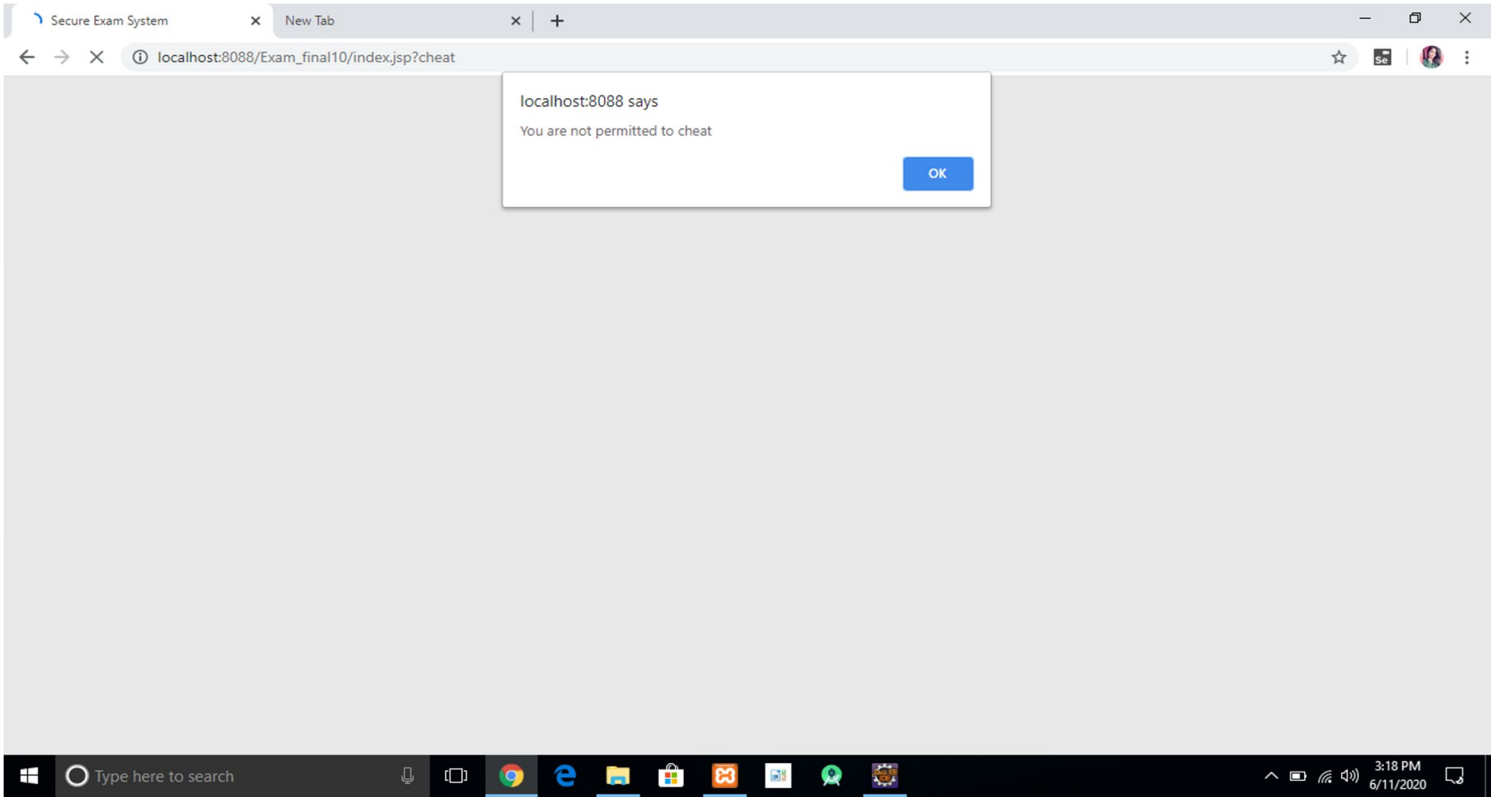


Fig.6 Cheat Detection

©IJRASET: All Rights are Reserved

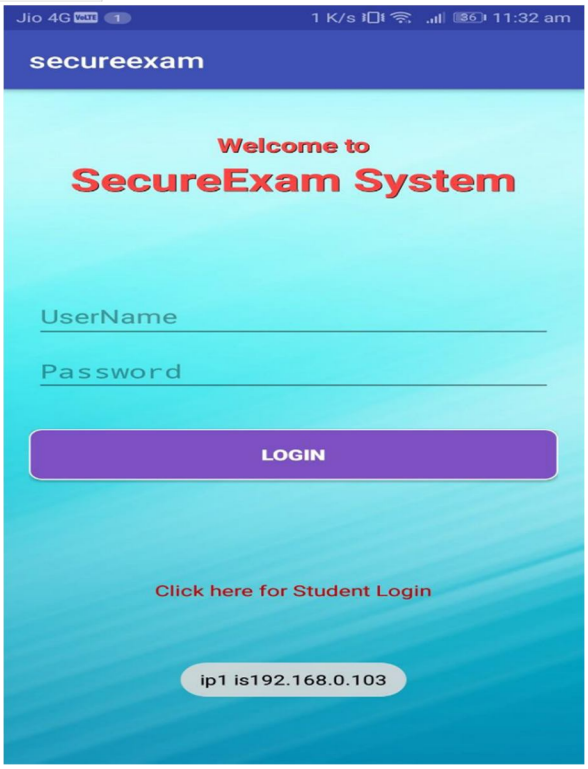


Fig.7 Student Login Page

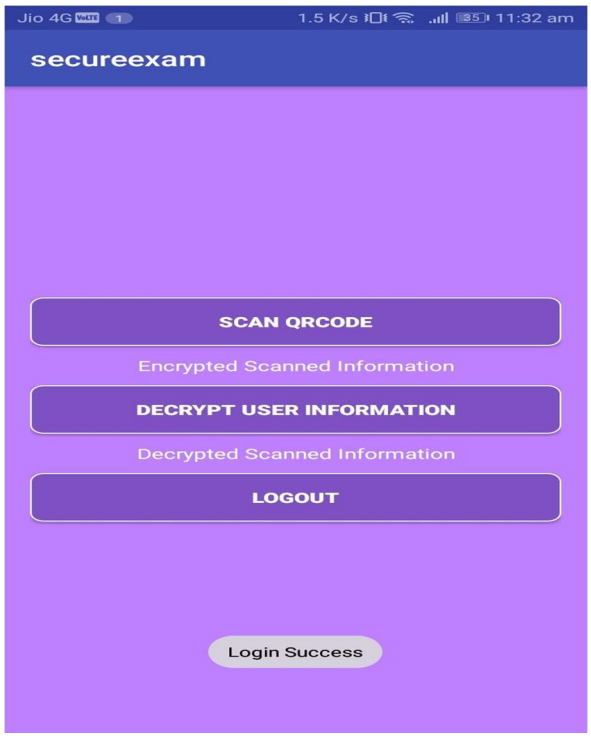


Fig.8 Procedure Of QR Code

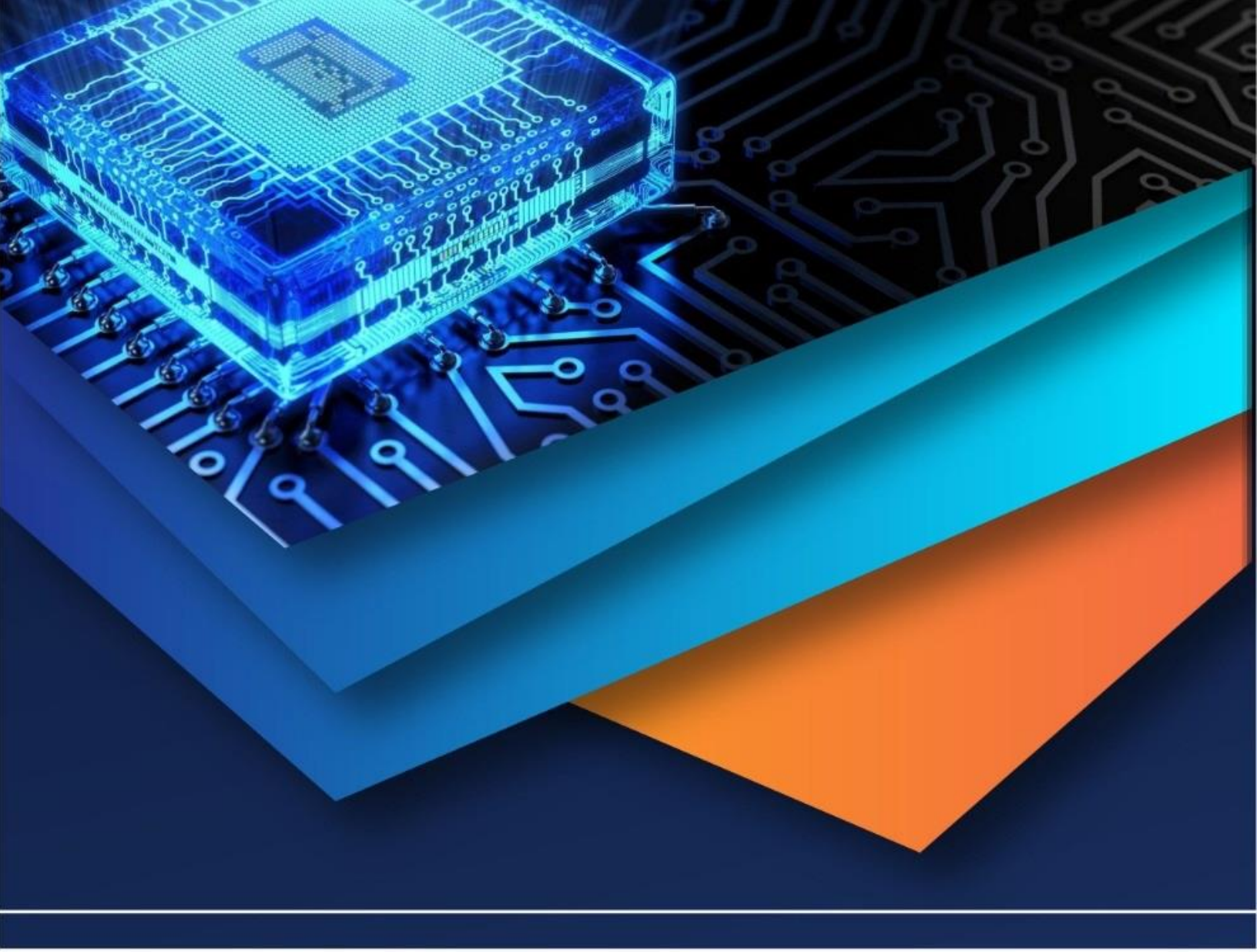
VI. CONCLUSION AND FUTURE SCOPE

The proposed Online Examination System can be easily acquired by universities and institutions to make the exam highly secure. This system is useful to prevent violations that occurred before and after the exam. The system highlights the benefits and future challenges in our educational environments both online as well as offline manner. Future studies may focus on avoiding using any other electronic device or m-learning environment such as moodbile while dealing with the current environment. So in the future, we can develop more secure software by using advanced technologies.

REFERENCES

[1] Kevin Peng, Harry Sanabria, Derek Wu, Charlotte Zhu, “Security Overview of QR Codes”, Massachusetts Institute of Technology 6.857 Computer and Network Security.
[2] Sumitra, Comparative Analysis of AES, and DES security Algorithms.
[3] D. Jackson, “A semi-automated approach to online assessment,” in Proc. 5th Annu. SIGCSE/SIGCUE ITiCSE Conf. Innov. Technol. Comput.Sci. Educ. (ITiCSE), Helsinki, Finland, 2000, pp. 164–167.
[4] P. Rogaway and T. Shrimpton, “Deterministic authenticated-encryption” in Advances in Cryptology—EUROCRYPT, vol. 6. Springer, 2007.
[5] X. Zhang and K. K. Parhi, "On the optimum constructions of the composite field for the AES algorithm," IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 53, no. 10, pp. 1153–1157, Oct. 2006.
[6] S. Parihar et al., “Automatic grading and feedback using program repair for introductory programming courses,” in Proc. ACM Conf. Innov. Technol. Comput. Sci. Educ. (ITiCSE), Bologna, Italy, 2017, pp. 92–97.
[7] Diaa Salama Abdul. Elminaa1, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, Performance Evaluation of Symmetric Encryption Algorithms.
[8] J. Sheard et al., "Exploring programming assessment instruments: A classification scheme for examination questions," in Proc. 7th Int.Workshop Comput. Educ. Res. (ICER), Providence, RI, USA, 2011, pp. 33–38
[9] J. W. Howatt, “On criteria for grading student programs,” ACM SIGCSE Bull., vol. 26, no. 3, pp. 3–7, 1994.
[10] D. Canright, “A very compact S-box for AES,” in Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst. Berlin, Germany: Springer, 2005, pp. 441–455.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)