

# Biometric Enabled Computer-Based Testing System (CBT) With Advanced Encryption Standard (AES)

<sup>1</sup>H. M. Ismail, <sup>2</sup>B. M. Soye

<sup>1</sup>Department of Computer Science

<sup>1</sup>Federal College of Agricultural Produce Technology, Kano, Nigeria

**Abstract:** The rapid progress of Information and Communication Technologies (ICT) in teaching and learning has moved the paradigm from paper-pencil-based to computer-based testing system of examinations. Universities and tertiary institutions are registering and conducting electronic examination for their students through the electronic and other networking gadgets. With the introduction of e-exams, institutions still grapple with serious issues including poor integrity of the result due to examination questions passes through so many hands and impersonation in the examination hall. A desktop application has been developed by the integration of Java Programming language – JavaFX platform and JasperReports. The software runs on Java 1.8 and above and require a database server such as the MySQL Server. For the frontend styling, JavaFX Cascading Style Sheet was used. Security will be more effective since the system includes biometric fingerprint authentication, picture capture and data encryption and decryption, it will also reduce drastically the problems of human interference, impersonation, bribe-taking by lecturers, invigilators and supervisors, too much paper work, examination leakages and also reduce the number of invigilators needed for invigilation.

**Keywords:** CBT, Biometric Fingerprint, Cryptography, AES, JavaFX

## 1. INTRODUCTION

Examination is one of the best methods of evaluating the knowledge and ability of an individual (Adebayo & Abdulhamid, 2009). Jamil & Shami (2012) point out that it is generally recognised that examinations determine the extent to which educational objectives have been achieved as well as the extent to which educational institutions have served the needs of community and society. To this end, various methods have been employed in examining the ability of an individual, starting from manual means of using paper and pencil to electronic, from oral to written, practical to theoretical and many others (Adebayo & Abdulhamid, 2009). The paper-pencil-based (manual) examination, which has been in existence for decades, may not be attractive for use because of the problems usually experienced including examination venue capacity constraints, lack of comfort for examination candidates, delay in the release of results, examination malpractices, cost implication of printing examination materials and human error (Fagbola, Adigun, & Oke, 2013).

The rapid progress of Information and Communication Technologies (ICT) in teaching and learning has moved the paradigm from paper-pencil-based to computer-based system of examinations which are usually termed as Computer Assisted Testing (CAT), Computerized Assessment (CA), Computer Based Testing (CBT), Computer Aided Assessment (CAA) and Computer Based Assessment (CBA) (Jamil & Shami, 2012). The employers are using electronic means for conducting aptitude test for their job seekers; the universities and other tertiary institutions are registering and conducting electronic examination for their students through the internet and other electronic and networking gadgets, various examination bodies in the country like the West Africa Examination Council (WAEC), National Examination Council (NECO), National Board for Technical Education (NABTEB), National Teacher Institute (NTI) etc. register their students through electronic means, recently electronic examination has been widely adopted by nearly all the Nigeria University for post Unified Tertiary and Matriculation Examination (Post-UTME) also known as pre-admission screening (Adebayo & Abdulhamid, 2009). CBT however, is expected to offer several advantages for the institution and the learner. Some of these advantages include: Adaptive testing, where the next question to be posed is determined by prior response(s); question banks and randomization of questions and response orders to reduce cheating; automated analysis of results from entire candidate cohorts; immediate feedback can be given. (Fagbola, Adigun, & Oke, 2013). With these aforementioned, many more educational bodies engaging in electronic examination and registration for testing the ability of their candidates, which determine the future of this great country and our dear youth, there is a need for serious examination of the system which has great impacts on the populace (Adebayo & Abdulhamid, 2009).

The present problems associated by tertiary institution with the conduct of electronic examination and registration for testing the ability of their candidates are lack of resumption capability when power, network and or physical computer's component failures (Younis & Hussein, 2015); poor integrity of the result due to examination questions passes through so many hands, especially when a private individual is involved (Adebayo & Abdulhamid, 2009). Questions to be uploaded into the server are script which is very tasking and a measure of errors introduced into the questions (Osang, 2012). Valenti, Neri, & Cucchiarelli (2003) point out that most researchers in this field agree on the thesis that some aspects of complex achievement are difficult to measure using objective-type questions. Scripting of the questions to be uploaded into the server is very tasking and a measure of errors introduced into the questions. All questions type in Microsoft word are being converted into the format acceptable by the software (Osang, 2012). Choice randomization distribution within each question must be performed to ensure security, robustness against cheat attempts during examination process and impersonation in the examination hall, as well as conspiracy and collaboration of security agents and officials to compromise the integrity of the examination (Younis & Hussein, 2015; Ayo, Akinyemi, Adebisi, & Ekong, 2007). Scrupulous practices by some administrator in the manipulation of the scores of the students and in ability of the system to keep track of user activities.

## 2. LITERATURE REVIEW

Zhenming et al. (2003) developed a novel electronic examination system based on a Browser/Server framework technology which carries out the examination and auto-grading for objective questions and operating questions, such as programming, operating Microsoft Windows, editing Microsoft Word, Excel and PowerPoint. It has been successfully applied to the distance evaluation of basic operating skills of computer science, such as the course of computer skills in Universities and the nationwide examination for the high school graduates in Zhejiang Province, China. The system is designed specifically for computer science students. It is not designed for general purpose students. The system can be improved on through question encryption and random administration of questions to reduce the level of examination malpractice. Satav et al. (2012) proposed a Structure Query Language (SQL) Based Paperless Examination System (SBPES).

SBPES is a web-based system that can present a descriptive exam format for SQL and Description Model Language (DML) statements. This application requires presenting a highly maintainable, secure platform which provides high robustness, reliable, scalable, and updatable in order to acquire new features to improve user acceptability. SBPES supports secure login, multi-instructor, and portability features. On the other hand, the other features namely: resumption capability, random question selection, question encryption, random questions distribution and random choices distribution are missing. Electronic exam is a difficult part of e-learning security (Husztai & Petho, 2008). The paper describes a cryptographic scheme that possesses security requirements, such that authenticity, anonymity, secrecy, robustness, correctness without the existence of a Trusted Third Party. The proposed protocol also provides students a receipt, a proof of a successful submission, and it is based on existence of anonymous return channels. Another research work proposed a theoretical approach that incorporates available fingerprint biometrics authentication technologies in conjunction with e-learning environments to curb unethical conduct during e-learning exam taking (Levy & Ramim). The proposed approach suggests practical solution that can incorporate a random fingerprint biometrics user authentication during exam taking in e-learning courses. Doing so is hypothesized to curb exam cheating in e-learning environments. Schramm (2008) looked at e-learning web based system that could simply offer and grade mathematical questions with infinite patience. Therefore it needs the capability for in and output of mathematical formulas, the dynamic generation of plots and the generation of random expressions and numbers.

A web-based online examination system that is not limited by time and place was developed by Yuan-Lung et al. (2003) to enable students to arrange their time for examination in accordance with the progress of their lessons. The system had simple fraud protection function by employing a random generation in the order of questions in each student's test, making cheating extremely difficult. The questions could also be in diagram form, animations and other multimedia forms other than textual test questions, therefore making the test questions more diverse. Teachers can make statistical analysis aimed at a particular test to determine the average mark scored by students on a particular test, and this can be used as a reference material for teaching remediation. The design was broadly structured into three areas: the student area, the teacher area and others (includes administrator, production group and comments). Implementation was done using Windows 2000 as the operating system. ASP (Active Server Pages) was used to provide a dynamic web page while the functions required by the online examination system were appropriately processed through the VB (Visual Basic) Script in ASP. The system also used the IIS technology (Internet information Server) to construct an ASP platform while Microsoft Access functioned as the database. The database was accessed using ODBC. Users can arrange their examination time in accordance with the progress of their lessons. Test takers can check the test solutions immediately after the test, thus letting students know their mistakes and work to correct them. With the rise in cybercrimes, the security enhancement of the online examination system should be looked into in order to ensure that the questions for students' assessment are not tampered with or leaked prior to formal examination date.

The CBT system developed by Fagbola et al. (2010) was an online examination system that assesses students using multiple choice questions set by the lecturers and is capable of grading students accordingly. The system is expected to provide an effective solution for mass student evaluation and provides functionalities such as auto-submission of examination on expiration of set time, auto-grading of students and examination result report generation. The Waterfall Model of software development Life cycle was adopted and the conceptual design (activity diagram, the use cases, the data flow diagram and the entity-relationship diagram) were presented. Macromedia Dreamweaver 8.0, Microsoft Visual Studio 2012 and Microsoft SQL Server 2008 were the tools used for the development of the CBT system. The system was implemented using C# (C Sharp) and SQL server. The CBT system was composed of six different functional pages which are the student login page, the admin login page, the result summary page, the question page, question upload and configuration page and the student result page. It was expected that the system would proffer solutions to challenges such as examination malpractices, low capacity examination venues, inadequate invigilators and inadequate examination materials. Performance assessment of the CBT system was carried out using 250 students and the statistics proved the system as highly flexible. This CBT system can be improved on through the implementation of essay-based questions. Integration of students' continuous assessment should also be included for it to be effective in a tertiary institution. CBTS supports secure login, multi-instructor, and random question selection features, the other features such as resumption capability, random questions distribution, random choices distribution, and portability are missing.

Indoria et al. (2012) developed a web-based online examination system that generates student's scores on submission of the examination. The Administrator of the system had the privilege of creating, modifying and deleting the test papers. A user can register and login with his/her specific id. The system was structured into two areas which were the administrator area and the operator area (user). System development was achieved using ASP.NET and VB.NET having DB2 as back end (database). Windows 2000 Enterprise was used for the server interface while either of Windows 95/98/2000/NT could be used for the client interface. The system can generate students report based on the 'list of passed students', 'list of students pass with merit' and 'list of failed students'. The limitation of this system is that the teacher cannot enter the questions directly into the system and the questions cannot be generated randomly. Rashad et al. (2015) developed an examination management system that is capable of supporting an institution's faculty, student and administration roles in the examination process. It employs different kinds of questions such as

yes/no questions, multiple choice/single answer questions, multiple choice/multiple answer questions, fill-in the gap questions with a string, numeric answer and essay questions. Examinations are automatically marked on conclusion of the answers and reports for the test are produced. It can be used via the Internet and is therefore suitable for both local and remote examination.

The system could help lecturers, instructors, teachers and others who are willing to create new examinations or edit existing ones as well as students participating in the examination. The system would require a more reliable form of security since it can be used via the internet. However, the other features: resumption capability, random question selection and random choices distribution are missing.

Taşci et al. (2014) proposed an online examination system architecture which provides for integrated management of an examination main functionalities. These include question pool creation and update, examination authoring, execution and evaluation, management of the feedbacks from students, along with ensuring use of analysis reports related to the questions and examination created by an intelligent agent in the decision-making processes. The system architecture includes Administration, Implementation, Finalization and Support layer. A Monitoring Agent was designed to help students through creating reports. Analyses on this system at Sakarya University Turkey, showed that the proposed intelligent agent supports online examination system, detects problems that may arise and enables the instructors to make decisions more easily on such problems in a shorter time. Emary & Abu (2006) developed an online website for tutoring and e-examination of economic courses. This novel software tool was used for online examination and tutorial application of the syllabus of economic courses so as to ensure that students study all the concepts of economics. So, the proposed software is structured from two major modules: The first one was an online website to review and make self-test for all materials of economic course. The second part is an online examination using a large database bank of questions through it the level of students can be evaluated immediately and some statistical evaluations can be obtained. The developed software offers the following features: instructors could add any further questions to maximize the size of the bank of questions; different examinations for each student with randomly selected questions from the bank of questions.

Guzman & Conejo (2009) proposed an online examination system called System of Intelligent Evaluation using Tests for Tele-education (SIETTE). SIETTE is a web-based environment to generate and construct adaptive tests. It can be used for instructional objectives, via combining adaptive student self-assessment test questions with hints and feedback. The proposed software has been designed to work based on the client-server architecture. SIETTE supports secure login and portability features. On the other hand, the other features: resumption capability, multi-instructor, random question selection, random questions distribution and random choices distribution are missing. Henke (2007) proposed a web-based Test, Examination and Assessment System (WETAS). WETAS is a web-based system designed for integration into existing Learning Management Systems (LMS); this system provides an examination environment and assignments as well to facilitate database supported e-Learning Test, suitable for the pre- and post-tests of Reusable Learning Objects (RLO) as well as the remote lab entry test.

WETAS is implemented using Java Applet and PHP scripts for file handling. The Applet for Knowledge Testing in Laboratory Courses (AKTLC), in contribution with a task assembler, provides tasks from (a randomly selectable) text file and performs an evaluation of the student's result, furthermore, WETAS built to make new types of tasks implemented perceptively by using simple and common available text editors. It is also possible to place additional graphics inside the text of the tasks. WETAS supports secure login, random question selection, and portability features. On the other hand, the other features: resumption capability, multi-instructor, random questions distribution, and random choices distribution are missing. Vasupongayya et al. (2010) proposed an Interactive Examination Management System (IEMS). IEMS is a web-based application test management system, with ease of uses, rich features, flexibility, and extensibility.

### 3. CONCEPTUAL DESIGN

The conceptual design of the CBT system was carried out using the sequence diagram and the use case diagram

#### 3.1 Sequence Diagram

As the name implies, a sequence diagram shows the sequence of interactions that take place during a particular use case or use case instance. Sequence diagrams are primarily used to model the interactions between the actors and the objects in a system and the interactions between the objects themselves. Sequence diagrams document the interactions between classes to achieve a result, such as use case. Because UML is designed for object communications between classes are known as messages. The Sequence diagram lists objects horizontally, and time vertically, and models these messages over time. (Gálvez, et al, 2009)



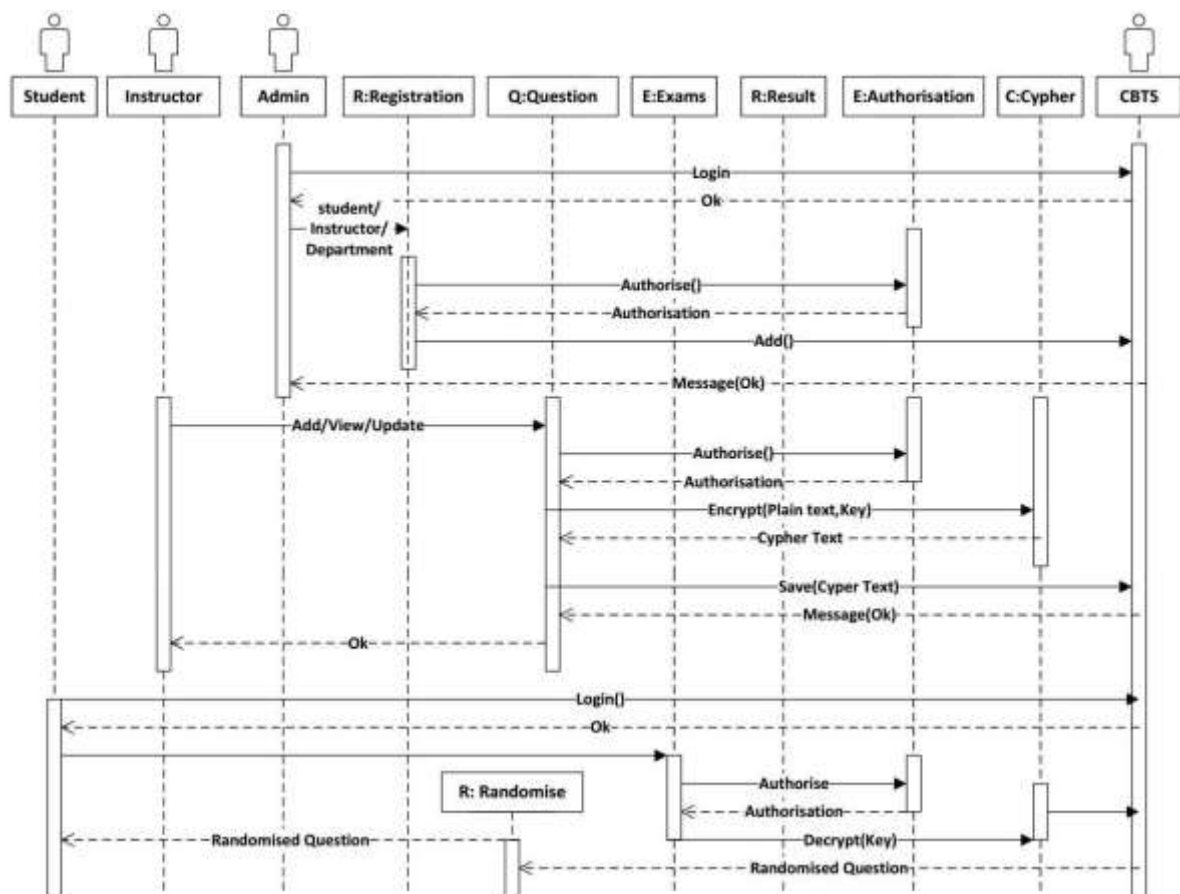


Fig 1. Sequence Diagram

### 3.2 Use case Diagram

Use case diagram for each entity present in the CBT system is presented here. These include use cases diagram for the administrator, lecturer, system and student. The use cases diagram for the administrator shows the activities that are required of the administrator including the upload of lecturer's details, upload of student's details and creation of default passwords for users. The lecturer use cases diagram depicts the process of setting examination instructions, insertion of questions into database, insertion of options as well as the specification of correct answer(s) to question(s). The use cases diagram for student shows that the student can access the system and write his or her examination (Fagbola, et al, 2013)

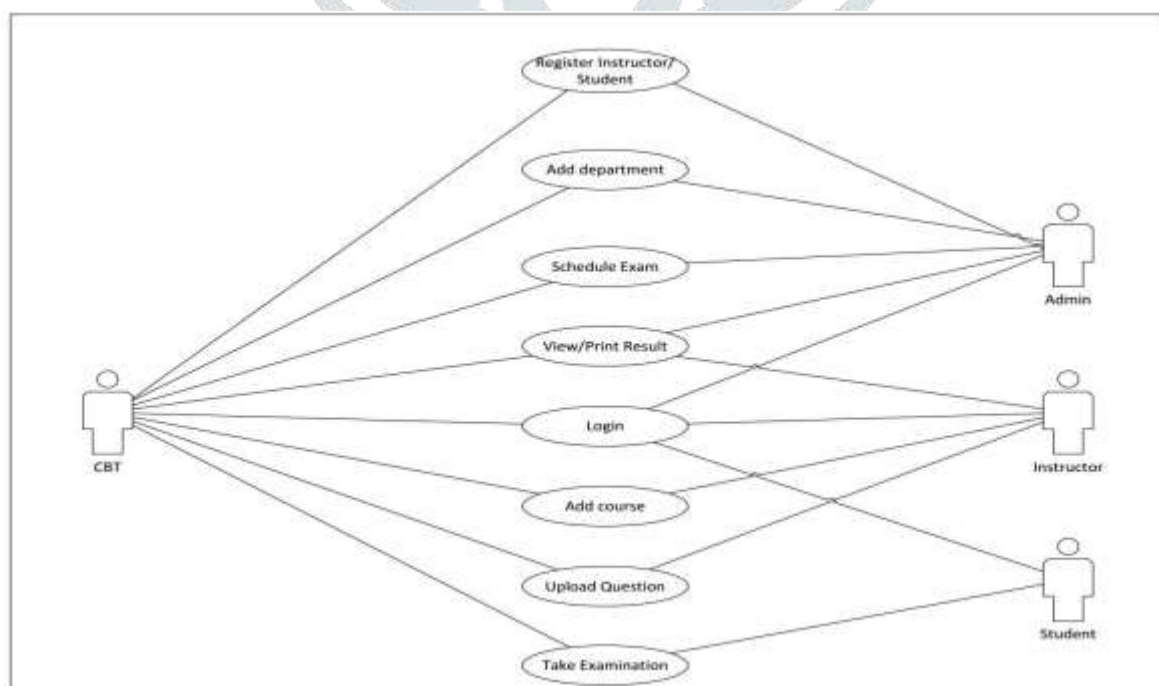


Fig 2. Use case Diagram

#### 4. IMPLEMENTATION

Java programming language was used to build the application logic among various components that they were used to develop the entire system. JavaFX scene builder is another Java related software that was used to build the User Interface for the System alongside NetBeans IDE. MYSQL which is an RDBMS was used to create and manage the database used for the System. Desktop Application are more secure as you can have a total control over the standalone applications and protect it from various vulnerabilities. This may not be the case with web applications as they are open to a large number of users in the internet community thus widening the threat.

##### 4.1. Features

The Systems is designed with high consideration for ease of use. It is flexible enough to allow examinee attempt questions in a stress-less environment. The system provides many features, the most important ones being the following; Student/ Lecturer Registration, Course Registration, Taking Test, Administering test, Question Uploading, Schedule Examination, Result Checking, Multiple user account and role, Full administration capability within the system and Multi-platform compatibility

##### 4.2. Usage

The basic CBT System supports three different user roles:

- Administrator (no restrictions)
- Lecturer (Upload question, Schedule exams, Result checking)
- Student (Take test)

Fig 3. Student registration screen

The CBT System is built to be able to perform different operations ranging from student/staff registration, taking tests, administering test, checking results and many other functionalities. The figure below shows the software's admin home screen. Access to this page is restricted to an administrator whose log in details (username and password) is authenticated by the CBT system.

The Question Upload and schedule Page provides a user friendly platform for the lecturer to input his or her question into the database, while inputting the question into the database, the lecturer also has to specify the answer to the question. Lecturer have the flexibility of choosing from the available examination questions and can upload different picture format. The result page used to display the result of the student in the concluded examination, the result is computed based on the number of options the student provided that matches the correct option specified by the lecturer or answered in a preferred format presented by the lecturer. The result can be filter/search by various columns of the table such as student ID number, his programme of study, course code, semester and session.

A registered student for a test can logon to the system. The student enters his username and the password. The page upon load fetches questions from the database randomly and serves it to the student who can answer the questions by checking the radio button which corresponds to the correct answer in the student's option. The page also initiates a count-down timer which is used to manage the duration of the examination. The timer is activated after clicking on start exam button and the student is automatically logged off the CBT system upon expiration of the timer or submission of the completed test by the student. The CBT system automatically generates the students score for that particular course upon submission.

This module is used serve the questions of the examination to the student. The page upon load fetches questions from the database randomly and serves it to the student who can answer the questions by checking the radio button which corresponds to the correct answer in the student's option or present the answer in the required format required. The page also initiates a count-down timer which is used to manage the duration of the examination.



Fig 4. Test Screen

The software is designed to keep log of vital examination variable into the database on the server in real time. Vital parameters such as the login time, logout time, examination remaining time, candidates already chosen answers, questions already attempted before logging out, submit type which can be automatic (upon time expiration) or manual. This helps to know if the candidate was having an ongoing examination, has already completed the exam, or is about to attempt an examination freshly. If the candidate has completed the exam before, he/she will need the admin to enter a retake exam key on his/her behalf. If the candidate is in the process of completing the examination (ongoing exam), he/she will be given the opportunity to continue such. The Systems GUI is designed with high consideration for ease of use. It is flexible enough to allow examinee attempt questions in a stress-less environment.

## 5. CONCLUSION

The system will definitely reduce drastically the problems of human interference, impersonation, bribe-taking by lecturers, invigilators and supervisors, too much paper work, examination leakages and also reduce the number of invigilators needed for invigilation. Especially, security will be more effective since the system includes biometric fingerprint authentication, picture capture and data encryption and decryption have been added to the existing design

## REFERENCES

- [1] Adebayo, O., & Abdulhamid, S. M. (2009). E- Exams System for Nigerian Universities with Emphasis on Security and Result Integrity. *International Journal of the Computer, the Internet and Management (IJCIM)*, 18(2), 47-59.
- [2] Adewale, O. A., Ajadi, T. O., & Inegbedion, J. O. (2015). Perception of Learners on Electronic Examination in Open and Distance Learning Institutions: A Case Study of National Open University of Nigeria. *Formal Education; Quality Issues*.
- [3] Alabi, A. T., Issa, A. O., & Oyekunle, R. A. (2012). The Use of Computer Based Testing Method for the Conduct of

- Examinations at the University of Ilorin. *International Journal of Learning & Development*, 2(3), 68-80.
- [4] Al-Amri, S. (2007). Computer-based vs. Paper-based Testing: Does the test administration mode matter? *Proceedings of the BAAL Conference*, (pp. 101-110).
  - [5] Ayo, C. K., Akinyemi, I., Adebiyi, A., & Ekong, U. (2007). The Prospects of E-Examination Implementation In Nigeria *Turkish Online Journal of Distance Education-TOJDE*, 8(4), 125-134.
  - [6] Bassil, Y. (2012). A Comparative Study on the Performance of the Top DBMS Systems. *Journal of Computer Science & Research (JCSCR)*, 1(1), 20-31.
  - [7] Chad, V. M., Zhao, Z., Nan, X., Chen, Y., & Wilkins, D. (2010). A Comparison of a Graph Database and a Relational Database. *ACM Southeast Regional Conference*.
  - [8] Davis, A. M., Bersoff, H., & Comer, E. R. (1988). A Strategy for Comparing Alternative Software Development Life Cycle Models. *Journal IEEE Transactions on Software Engineering*, 14(10).
  - [9] Dhindsa, P. B. (2012). A Comparative Study of Database Systems. *International Journal of Engineering and Innovative Technology*, 1(6), 267-269.
  - [10] Emary, E., A., J. A., & Sondos, A. A. (2006). An Online Website for Tutoring and E-Examination of Economic Course. *American Journal of Applied Sciences*, 3(2), 1715-1718.
  - [11] Fagbola, T. M., Adigun, A. A., & Oke, A. O. (2013). Computer-Based Test (Cbt) System For University Academic Enterprise Examination. *International Journal of Scientific & Technology Research*, 2(8), 336-342.
  - [12] Gálvez, J., Guzmán, E., & Conejo, R. (2009). A blended E-learning experience in a course of object oriented programming fundamentals. *Knowledge-Based Systems*, 279-286.
  - [13] Indoria, V., Sharma, P., & Soni, A. (2012). Online Examination. *International School of Informatics & Management*.
  - [14] Issam, Y. M., & Sameer, H. M. (2015). Construction of an Online Examination System with Resumption and Randomization Capabilities. *International Journal of Computing Academic Research (IJCAR)*, 4(2), 62-82.
  - [15] Jaiswal, G., & Agrawal, A. P. (2013). Comparative analysis of Relational and Graph databases. *IOSR Journal of Engineering (IOSRJEN)*, 3(8), 25-27.
  - [16] Jamil, M., & Shami, P. A. (2012). Computer-Based Vs Paper-Based Examinations: Perceptions of University Teachers. *The Turkish Online Journal of Educational Technology*, 11(4), 371-381.
  - [17] Jovanovich, D. D. (2003). Comparison of software development models. *Proceedings of the 7th International Conference* (pp. 587-592). ConTEL.
  - [18] Kerejeta, M., Larraaga, M., Urko, R., & Arruarte, A. (2007). Web-Based Test, Examination and Assessment System", *Advanced Technology for Learning*, 4(3), 140-145.
  - [19] Kuyoro, S. O., Maminor, G. U., Kanu, R. U., & Akande, O. (2016). The Design and Implementation of a Computer Based Testing System. *Journal of Applied Computation*, 1(1), 1-7.
  - [20] Laura, C. R., Martinez, M., Mora, F., & Alvarez, J. (2009). A Descriptive/Comparative Study of the Evolution of Process Models of Software Development Life Cycles. *Mexican International Conference on Computer Science*. Washington.
  - [21] Levy, Y., & Ramim, M. M. (n.d.). A Theoretical Approach for Biometrics Authentication of e-Exams. 93-101.
  - [22] Maglyas, A., Nikula, U., & Smolander, K. (2010). Comparison of two models of success prediction in software development projects. *Software Engineering Conference (CEE-SECR)*, 2010 6th Central and Eastern European, (pp. 43-49). Eastern European.
  - [23] Malgwi, Y. M., Shelleng, N. B., & Danjuma, K. J. (2015). Analysis of Agile and Multi-Agent Based Process Scheduling Model. *International Refereed Journal of Engineering and Science (IRJES)*, 4(8), 23-31.
  - [24] Osang, F. (2012). Electronic Examination in Nigeria, Academic Staff Perspective—Case Study: National Open University of Nigeria (NOUN). *International Journal of Information and Education Technology*, 2(4), 304.
  - [25] Rashad, M. Z., Kandil, M. S., A. E., & Zaher, M. A. (2015). An Arabic Web-Based Exam Management System. *International Journal of Electrical & Computer Sciences*, 10(01), 35-41.
  - [26] Rashad, M. Z., Kandil, M. S., Hassan, A. E., & Zaher, M. A. (2010). An Arabic Web-Based Exam Management System. *International Journal of Electrical & Computer Sciences*, 10(1), 35-41.
  - [27] Rather, M. A., & Bhatnagar, V. (2015). A COMPARATIVE STUDY OF SOFTWARE DEVELOPMENT LIFE CYCLE MODELS. *International Journal of Application or Innovation in Engineering & Management (IJAIE)*, 4(10), 23-29.
  - [28] Rather, M. A., & Bhatnagar, V. (2015). A COMPARATIVE STUDY OF SOFTWARE DEVELOPMENT LIFE CYCLE MODELS. *International Journal of Application or Innovation in Engineering & Management (IJAIE)*, 4(10), 23-29.
  - [29] Rothi, J., & Yen, D. (1989). System Analysis and Design in End User Developed Applications. *Journal of Information Systems Education*.
  - [30] Ruparelia, N. B. (2010). Software Development Lifecycle Models. *ACM SIGSOFT Software Engineering*, 35(3), 8-13.
  - [31] S. M. Bodmann, & Robinson, D. H. (2004). Speed and Performance Differences among Computer-Based and Paper-Pencil Tests. *Journal of Educational Computing Research*, 31(1), 51 – 60.
  - [32] Sharma, B., & N, S. (2009). Software Process Improvement: A Comparative Analysis of SPI models Emerging Trends in Engineering and Technology (ICETET). 2009 2nd International Conference, (pp. 1019-1024).
  - [33] Taşci, T., Parlak, Z., Kibar, A., Taşbaşı, N., & Cebeci, H. I. (2014). A Novel Agent-Supported Academic Online Examination System. *Educational Technology & Society*, 17(1), 154-168.