Design Of Computer Based Test Using The Unified Modeling Language

Agus Tedyyana, Danuri and Lidyawati
[1] Politeknik Negeri Bengkalis, Riau, Indonesia
E-mail: agustedyyana@polbeng.ac.id, danuri@polbeng.ac.id, lidyawati@polbeng.ac.id

Abstract: The Admission selection of Politeknik Negeri Bengkalis through interest and talent search (PMDK), Joint Selection of admission test for state Polytechnics (SB-UMPN) and Independent (UM-Polbeng) were conducted by using paper-based Test (PBT). Paper Based Test model has some weaknesses. They are wasting too much paper, the leaking of the questios to the public, and data manipulation of the test result. This reasearch was Aimed to create a Computer-based Test (CBT) models by using Unified Modeling Language (UML) the which consists of Use Case diagrams, Activity diagram and sequence diagrams. During the designing process of the application, it is important to pay attention on the process of giving the password for the test questions before they were shown through encryption and description process. RSA cryptography algorithm was used in this process. Then, the questions shown in the questions banks were randomized by using the Fisher-Yates Shuffle method. The network architecture used in Computer Based test application was a client-server network models and Local Area Network (LAN). The result of the design was the Computer Based Test application for admission to the selection of Politeknik Negeri Bengkalis.

Keywords: Unified Modeling Language, Paper Based Test, Computer Based Test, Fisher-Yates Shuffle, Criptography, Local Area Network

1. Introduction

Politeknik Negeri Bengkalisis one of the vocational colleges and the only State polytechnic in Province of Riau, There are three ways of admissions namely through the search of Interests and Talents, Joint selection admission test Polytechnic and path Self examination conducted Paper Based Test (PBT).

Admission tests of Politeknik Negeri Bengkalis through Joint Selection Examination Polytechnic and independent are using Paper Based Test (PBT), which is through the written test by distributing a booklet and answer sheet to the test takers then answering the test that have been provided by the committee. Paper Based Test (PBT) Model also has some disadvantages, They are the use of too much paper, the possibility of questions leaking to the public, manipulation of test data result and other fraud during the test.

This study is designing Computer Based Test (CBT) application using Unified Modeling Language (UML) which consists of *Usecase diagrams*, *Activity* and *Sequence diagrams*. Computer Based Test, is defined as a test or assessment given by the computer whether they are *stand-alone* or dedicated network, or with other technologies devices which connected to the Internet or *World Wide Web (WWW)* and mostly use the

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

Multiple Choice Questions (*MCQS*), Computer Based Test itself has been applied since 1960 for the knowledge test and problem-solving test, Recent Computer Based Test has been adopted in some schools in Indonesia for the national exam High School level. In this study using the Fisher-Yates Shuffle method into computer-based exam application in randomize the problems so that the problems raised are different. And using the RSA cryptographic algorithm for security exam questions.

2. Method

2.1. Unified Modeling Language Diagrams

graph shaped Diagram showing the symbol of model elements arranged to illustrate certain parts or aspects of the system. A diagram is part of a particular view and generally described to a particular view. The type of diagram such as:

a) Use Case Diagram describes a number of external actors and their relation to the *use case* provided by the system. *Use case* is a description of the functions provided by the system in the form of text as documentation of the use case symbol but it can also be done in diagrams activity. Use case described only seen from the outside of an actor (the state of the system environment the user visits) and not how to function in the system

b) Class diagram described the static structure of classes in the system. Class represents something that is handled by the system. Class can be connected to one another through a variety of ways: associated (connected to each other), dependent (a dependent class / using other classes), specialed (one class is a specialization of other class), or package (a unit group), a system usually has several class diagrams.

c) State Diagram describes all states (state) owned by an object of a class and the circumstances which led the state change. The events can be another object that sent the message. State class is not described for all classes, only the state has a number of well-defined and class conditions changed by a different state.

d) Sequence Diagram Illustrated the dynamic collaboration among a number of objects. Their role is to show a series of messages sent between objects is also interaction between object, something that happens at a certain point in the execution system.

e) Collaboration Diagram describes dynamic collaboration such as sequence diagrams. In order to show the message exchange, collaboration and connection diagrams describe object (refer to the context). If the emphasis is on time or sequence, sequence diagrams are used, but if the emphasis on the context collaboration diagrams are used.

f) Activity Diagram Describes a series of flow of activity, it is used to describe activities that are formed in an operation that can also be used for other activities such as the *use case* or interaction
Component Diagram describes the physical structure of the code's component. The compoenent may include source code, binary component, or executable component. A logic's component contains information about the class or classes that are implemented to make the mapping of the logical view to the component view.

g) Deployment diagrams describe the physical architecture of the hardware and software show the relationship between computer and the devices (nodes) to one another and the type of the relationship. In the nodes, the executable component and object allocated for showing units of software executed by the particular node and dependence components.

2.2. Computer Based Test (CBT)

Computer Based Test (CBT), is defined as a test or assessment given by the computer whether they are stand-alone or dedicated network, or with other technologies devices that are connected to the Internet or World Wide Web (WWW) and mostly use the Multiple Choice Question (MCQs). Computer Based Test itself has been applied since 1960 to test the knowledge and problem-solving test.

2.3. Fisher Method Yates Shuffle

Fisher-Yates Shuffle (named after Ronald Fisher and Frank Yates), also known as the Knuth Shuffle (named after Donald Knuth), is an algorithm to generate a random permutation of a finite set, in other words, it is used to shuffle some of the set. A variant of the Fisher-Yates shuffle, known as algorithms Sattolo it can be used to generate a random cycle of length instead. The basic process of Fisher-Yates shuffling is similar to randomly choose a numbered ticket out of the cab, or a card from a deck, The use of the Fisher-Yates Shuffle can be in two ways: original and modern methods, the basic method used to generate a random permutation of number 1 to N is as follows (Ibijola and Olu, 2012):

a) Write down the numbers from 1 to N.
b) Choose a K random numbers between 1 to the number of digits that have not been crossed out.
c) Calculated from below, strike figure K that has not been crossed out, and write that number in other places.
d) Repeat step 2 and 3 until all numbers already crossed.
e) The order of the numbers written in step 3 is a random permutation of the previous numbers

In the modern version, the numbers chosen are not crossed, but its position has exchanged with the last digit of the numbers that have not been selected. The following are examples of the modern version. Range is the number of digits that have not been selected, the roll is the random numbers, scratch is a list of numbers that have not been selected, and the result is a permutation results to be obtained.

2.4. *RSA Cryptography Algorithm*

Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message (Alice) shared the decoding technique needed to recover the original information only with intended recipients (Bob), thereby precluding unwanted persons (Eve) from doing the same. The cryptography literature often uses Alice ("A") for the sender, Bob ("B") for the intended recipient, and Eve ("eavesdropper") for the adversary.[5] Since the development of rotor cipher machines in World War I and the advent of computers in World War II, the methods used to carry out cryptology have become increasingly complex and its application more widespread

Cryptography is derived from the Greek, crypto and Graphia. Crypto means “to hide”, while Graphia means “writing”. In general, Cryptography is the study of mathematical techniques related to aspects of information security, such as data confidentiality, data authenticity, data integrity, and authentication of data. However, it is not all aspects of information security can be solved by cryptography. Additionally, cryptography can also be interpreted as a science or art to maintain the security of the message. RSA is an algorithm based on public-key cryptography scheme. RSA stands for the initials of the inventors: Ron Rivest, Adi Shamir, and Leonard Adleman. The security of the RSA algorithm lies on the difficulty of factoring large numbers into prime factors. Factoring is done to obtain the private key.

2.5. *Web Server*

web Server is a software that provides data-based services and functions to accept the requests from HTTP or HTTPS from the client and usually known as web browser which then sends the results back in the form of multiple web pages and generally will be in the form of HTML documents. In the simplest form, web server will send the HTML data to the web browser, so the request will look like in general, ie a website display. The most common use is the web server for placing the web site, but in practice its use expanded as a data storage or to run a number of business-class applications, Web servers are not only used for serving the World Wide Web. They can also be found embedded in devices such as printers, routers, webcams and serving only a local network. The web server may then be used as a part of a system for monitoring or administering the device in question. This usually means that no additional software has to be installed on the client computer, since only a web browser is required (which now is included with most operating systems)

3. Results and Discussion

UML (Unified Modeling Language) is a modeling language for systems or software that the object-oriented paradigm. Modeling actually used for the simplification of complex issues in a way that is easier to learn and understand. Types of diagrams in UML is the Use Case Diagram, activity diagrams and sequence diagrams, UML is a language to specify, visualize, construct and document the artifacts (part of the information that used to be produced by the process of making software, the artifact can be a model, a description or software) of the software system, such as the modeling business and non-system devices other software. Besides UML is a modeling language that uses the concept of object orientation. UML made by Grady Booch, James Rumbaugh, and Ivar Jacobson under the banner of Rational Software Corps. UML provides a notation that help model the system from various prespetktif. UML is not only used in the modeling software, but almost in all fields that require modeling.

3.1. Use Case Diagrams

Iin the use case diagram the actors are the admin, prospective students and supervisors. Administration staffhas 13 use case, the supervisor has four use cases and new students have 7 case. use case scenario described the sequence of steps describe between the user and the system.

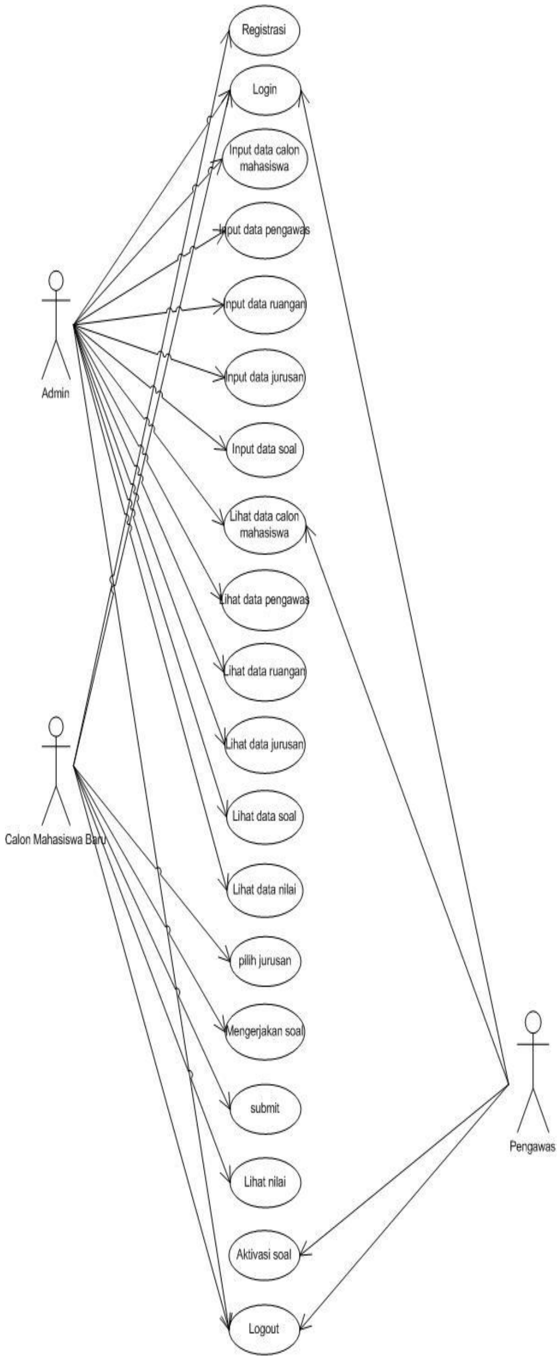


Figure 1. Use Case Diagram

a. Use case scenario login

table 1, Use case scenario login

Use case name	Login	
Use case id	1	
Actor	Administration staff, supervisors and new student candidate.	
pre condition	Actor must fill the username and password first	
triger	Actor can sign in and access the system	
Description	This use case describes the actor that fills your username and password to sign in and access the system	
Typical cource of events	Actor action • Input your username and password	system response • Check the username and password • Showing the page based on the authentication
Alternate courses	If the username and password are correct so the actor would enter into the system if false so the actor would reenter the username and password	
conclution	Actor has successful entered into the system	
Post condition	Showing the main page into the system based on each actors.	

b. Use case scenario registration

c.

table 2, Use case scenario registration

Use case name	Registration	
Use case id	2	
Actor	new student candidate	
pre condition	Actor must fill out and input the registration form for being a new student	
triger	Actor can sign up to be a new student	
Description	This use case describes the actor that fills and input the registration form for being a new student	
Typical cource of events	Actor action Select a menu list of students	system response Showing the form for terms and conditions of registration
	select list	Displays form a list of new students
	Input data registration	
lternate courses	If the students' input do not complete the students can't register	
conclution	Actors can register	
Post condition	Data will be stored into the student registration data	

3.2. Activity diagram

a. Login
In the diagram activity that must be done by administration staff, supervisor and the student is entering usename and password. If the username and password is entered incorrectly then the system will display the username and password is entered incorrectly then do repetition to input a username and password. If the password and user name is entered correctly then it will display the main page or go to the system

b. Registration for new student candidates
In the activity diagram of registration for new students to the things that they must do are logging on, select a menu list of prospective new students on the menu page list of students fill out the form provided to enter data for new students if it is complete then stored.

c. Input the question data
In the activity of inputing data that done by the administration staff is logged in, then select the menu, the menu pages about, administration staff inputing the question data if it is suitable will be saved

3.3. Sequence Diagrams

The Administration staff inputs and adds the question data of the supervisor with taking the steps like log in to enter to the main page that contained the main menu, in the main menu administration staff will select one of the menu like question data, supervisors or room. If you want to add and input the question data so enter into the question menu.. , save and view the question data. If you want to add and input the supervisors data so enter into the supervisors menu. , then input the supervisor data, store and view the supervisor data. If you want to add and enter the data into the room the room menu, then input the room data, stored and viewed the room data.

4. Implementation

The design of the interface is done to allow users to interact with the system. The design interface is done using hypertext markup language (HTML5), Cascading Style Sheet (CSS 3) and jQuery for the system implemented a web-based server.

4.1. Design Interface Login

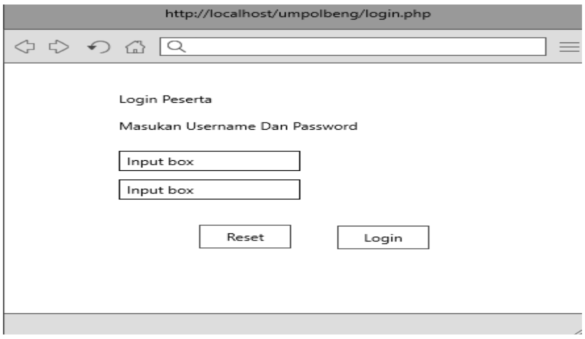

http://localhost/umpolbeng/login.php
Login Peserta
Masukan Username Dan Password
Input box
Input box
Reset
Login

Figure 2. Design Interface Login

4.2. Administration staffInterface Design

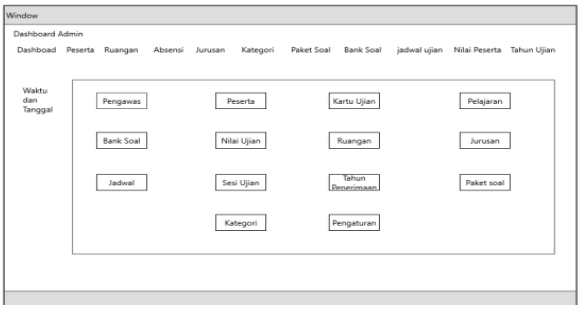
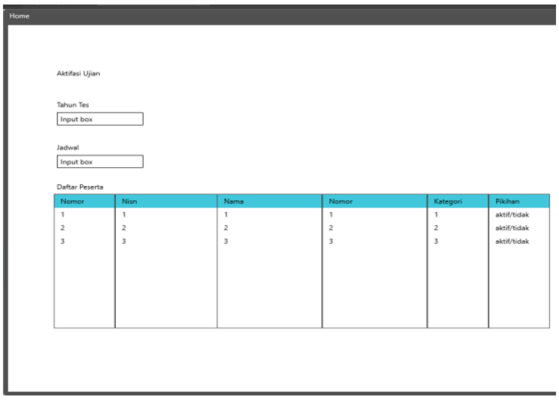


Figure 3. Design Interface Admin

4.3. *Exam Supervisor Interface Design*



Daftar Peserta

Nomor	Nisn	Nama	Nomor	Kategori	Pikihan
1	1	1	1	1	aktif/tidak
2	2	2	2	2	aktif/tidak
3	3	3	3	3	aktif/tidak

Figure 4. Interface Design Supervisor Exam

5. Conclusion

To undertake the designing application of Computer Based Test for admission of Politeknik Negeri Bengkalis. The first step that must be done is analyzing the needs of the system, then making the system design, next is making the system and the last one is testing of the system.

The system will be made with a procedural programming model and a web-based using the PHP programming code and MySQL database. Implementation environment using Apache web server. the network architecture that is used by Computer Based Test Application is a client-server network model with a Local Area Network (LAN). The results of designing in the form of application design Computer Based Test for admission Polytechnic of Bengkalis.

The design of this research using Fisher-Yates Shuffle method in randomize the problems so that the problems raised are different. As a further development suggestion, other randomisation methods can be used to randomize answers that arise so that in addition to raising different questions can bring up different answers

6. References

[1] Sorana-Daniela, B. and Lorentz, J. (2007). *Computer-based testing on physical chemistry topic: A case study. International Journal of Education and Development using Information and Communication Technology*, 3 (1), 94-95

[2] Ibijola, A., and Olu, A., 2012, *A Simulated Enhancement of the Fisher-Yates algorithm for Shuffling in Virtual Card Games using Domain-Specific Data Structures, International Journal of Computer Applications*, Vol.54, No.11 0975-8887 , page24-28.

[3] Arifin, 2009, *A Case Study of Use of Cryptographic Algorithms RSA algorithm As Safe, Mulawarman Informatics Journal*, Vol. 4, No. 3

[4] Maitimu, TR, 2008, *Design and Implementation of Web Server Load Balance Clustring and Scheme Using Linux Virtual Server via NAT*, Journal of Information Technology - AITI, Vol.5, No.1, p. 14-27

[5] Nugroho Adi. 2010. *Object-Oriented Software Engineering method USDP*. Andi offset: Yogyakarta