****

**MASINDE MULIRO UNIVERSITY OF SCIENCE AND TECHNOLOGY**

**SCHOOL OF COMPUTING AND INFORMATICS**

**DEPARTMENT OF COMPUTER SCIENCE**

**EMAIL CRYPTOSYSTEM**

**A Project Report Submitted in partial fulfillment of the requirements for the award of the degree of Bachelor of Science in Computer Science of Masinde Muliro University of Science and Technology.**

**PRESENTED BY: JACINTA GICHUHI**

**REG: COM/0018/14**

**PROJECT SUPERVISOR**

**MR. JASPER ONDULO**

**DATE**

# Declaration and Certification

I *Jacinta Gichuhi*, declare that this Project Report is my original work and has not been published and submitted for any other degree award in any other University before.

Signed: ……………………………. Date: ……………………………….

# Certification

The undersigned certify that they have supervised the project **“*EMAIL CRYPTOSYSTEM”***

Signature…………………………… Date………………………………..

**Supervisor**: Mr. Jasper Ondulo

Lecturer, Department of computer science

## Dedication

I dedicate my project to the school of computing most helping and resourceful lecturers who guided me all along as I was developing the project. Special feeling goes to the MMUST team involved in making requirements such as internet connection and power available to students.

I dedicate this work and give special thanks to my best and ever-helping for being there for me throughout the entire period of my project.

## Acknowledgement

It is a great pleasure for me to acknowledge the assistance and contributions of all the people who helped me to make my project successful. My project would not have been so successful, without the dedicated assistance given by those individuals.

I would like to give my special thanks to Mr. Jasper Ondulo who aid the coordination and supervision of my project. I would also like to thank my colleagues and all other Officials of Department of Computer Science for the assistance and guidance they gave towards this project.

I would like to thank every individual who gave me even the slightest support to make my project successful. *Thank you every one!!*

**Abstract**

## Executive Summary

This documentation highlights the various sections of the project undertaken. The introduction gives an overview of the subject of the project, why the project was chosen, and the main goals of the project. After the introduction, background information will try to explain what necessitated the research and show how technology has been embraced in the current business world.

In the problem definition, the paper explains how the current system works and the various procedures used to carry out various functions of the current system. Thereafter, project justification section explains how the project intends to automate the current system and also justify the desirability of the new system.

Under Methodology, the paper describe the procedure that was followed during the system development, the tasks undertaken in order to achieve the objectives of the project and also identify the data needed and how it was collected. It also covers the full system analysis and design and test cases.

In the implementation and testing section, this paper explains the coding scheme implemented while developing the project, the various levels of testing performed on the system and the various test cases undertaken.

The paper will also mention under system requirements the various resources and equipment that were to develop the system and also an estimate of the cost incurred in the process.

The paper then gives the schedule that was followed during system development process in the form of a Gant chart. Finally, the conclusion emphasizes on the benefits the users will get by using the system developed

# 1. CHAPTER ONE: INTRODUCTION

## 1.1 Introduction

Over past years insecurity of information being shared over the internet such as via emails has been a common global threat. Email encryption and decryption system is meant to curb this threat by ensuring eavesdroppers of information being shared over the internet cannot access and read the emails, cannot alter the emails in any away and can never make the emails unavailable to their recipients.

The system will use Advanced Encryption Standards due to its strong encryption algorithm to ensure mails messages and their attachments confidentiality, Integrity and availability as the sender and the receiver will be communicating over a secure channel. Before sending the email the sender will convert the plain text email content into scrambled message which is unreadable text format by use of an encryption key. On reaching the receiver end the receiver will re-convert the scrambled message into normal plain text by use of a decryption key. This will ensure that only the receiver can access the email.

This application will allow people to share even highly confidential mails among themselves without having to fear about security of the mails due to the strong encryption algorithm used and sharing of the key only among themselves thus avoiding any form of attack.

## 1.2 Statement of the problem

Emails being send over the internet is prone to disclosure of information because they are currently being transmitted in a clear insecure channel. Many cases have been reported of confidential emails being accessed and altered by unauthorized personnels and sometimes they are never received by designated recipients. Alterations of confidential information could results into big loses of resources especially money and lives if there is a security breach of the military information as the enemy would resend the altered wrong information to the designated recipient for his own personal gain.

Email encryption and decryption system is meant to solve all these confusion by ensuring that the original information send can only be accessed by the intended recipient.

## 1.3 Main aim of the project

To design an email system with high level security measures to ensure email information is highly secured. The system will ensure that only the intended people can read the email contents.

## 1.4 Specific objectives of the project

* To analyze the previously developed email encryption systems.
* To design the modern email encryption system using AES algorithm scheme.
* To implement the designed email encryption system.
* To test its working capability using various software testing methods i.e. unit testing, integration testing, acceptance testing etc.

## 1.5 Research questions

* What loses are incurred when there is a security breach in confidential email contents?
* What is the percentage of people using emails as a way of communication?
* What are the existing efforts made by researchers to enhance email security?
* Why security of emails is a vital need globally?
* What can be done to ensure emails confidentiality, availability, integrity and non-repudiation?

## 1.6 Scope of the project

This project covers the encryption of all email contents which includes:

* Text and pdf files
* All types of images
* All types of software
* Audios and videos among others.

The system uses the symmetric key encryption called AES algorithm.

## 1.7 Limitations of the study

* There is no guarantee that the methods of attack on the encrypted email contents such as brute force will not succeed.
* In case the encrypted data is damaged or tampered with, there is no assurance that it will be decrypted successfully.
* The system has limited accessibility as screen readers can have difficulties using it.

## 1.8 Benefits and beneficiaries of the study

This system was majorly designed for military organizations, journals and financial companies. The system can also be used by any regular users who use email as a form of communication.

The following section lists the benefits of using the system:

* Its strong bit encryption algorithm will make sure that others will not be able to hack or change the file/data attributes.
* It ensures guaranteed access to encrypted data by authorized users by automating storage back-up for critical master encryption keys.
* Data encryption guarantees data integrity.
* It helps the encrypted data to be transmitted securely
* Data encryption provides confidence that your encrypted data backups are safe.
* The email cryptosystem can be used to encrypt any size of data whether large or small since it does not have size limitations hence users can have as many email attachments as they wish.
* This system will provide all security check ups which can be performed during encryption and decryption of documents.

## 

## 1.9 Rational of implementing the project (Project justification)

Due to the problem stated above there arises the need for an email encryption and decryption system. The system will protect email messages and attachments sent over untrusted networks. It will ­­­­ ensure that the transmitted email cannot be received by anyone else apart from the designated recipient. This will cut short the number of loses encountered due to email transmission over the insecure channel.

To get rid of loses encountered due to transmission of email messages and its attachment over untrusted network an email encryption and decryption system is required to as Confidentiality, Integrity and Availability of transmitted emails can always be maintained.

## 1.10. Feasibility Study

In order to ascertain the viability of the project, I studied articles online to find out if there is need to create a new email cryptosystem that can replace the existing ones.

### 1.10.1. Economic Feasibility

This was carried out to compare the cost of developing, operating and maintaining the proposed system and if it is economically viable in relation to return on investment. This served as my cost benefit analysis portion. The concern here was:

* How beneficial is the existing system or mode of operation?
* What are the costs associated with the existing system?
* What are the benefits of the proposed new system?
* What are the costs associated with the proposed system?

### 1.10.2. Technical Feasibility

This study was meant to answer the following major concerns:

* Are there enough technological resources to undertake the project?
* Are the processes and procedures conducive to project success?

This would ensure that there a technical capacity to carry out and implement the proposed system

## 1.11. Requirement Capture and Analysis

Having established that the project was worth starting, a detailed description of the functionalities that the system was supposed to accomplish was done. These requirements were then explored to find out the needs or conditions to be met by the new system. Conflicting requirements were then eliminated.

The following activities were undertaken during this process:

* **Eliciting requirements***-*Intensive research over the Internet as well as brain storming with friends was done.
* **Requirements analysis and validation**-The requirements that were cited during the study was then analyzed to check for clarity, incompleteness, ambiguity and also

Contradictions amongst them.

* **Recording the requirements***-*The requirements obtained was then documented

## 1.12. Requirements Specification

These involve:

* Functional requirements – statements of services the system is expected to provide.
* Non-functional requirements- constraints on the services or functions offered by the system.

### 1.12.1 Functional Requirements

The system is expected to perform the following functions:

* Create new emails accounts to new email users.
* Allow users to login using their account details
* Allow users to change their profile details such as changing passwords.
* Allow users to compose emails and add attachments.
* Allow users of encrypt the email contents before sending
* Allow users to use key of their choice while performing encryption
* Provide users with a encryption successful status once the email has been encrypted
* Provide users with a send email successful status once the email has been send
* Enable intended users to decrypt the email contents with a decryption key once the email has been received.

### 1.12.2 Non Functional Requirements

* ***Robustness:*** the system is able to handle error conditions gracefully without failure e.g. invalid data defects and unexpected conditions
* ***Usability:*** The system can be easily used by any computer literate person.
* ***Maintainability:*** The system is easily maintainable as it is not extremely complicated and comes with a help function.
* ***Flexibility:*** The system is flexible and can be modified to suit the changing user’s needs over time.

####  Others include;

* The system should prompt users in case of wrong inputs during account creation
* They system should notify users in case of wrong decryption key
* The system should be able notify users in case of wrong login information
* The system has a help module that will guide new users while using the system.

## 1.13 Materials Required

### 1.13.1 Software Requirement

* Windows XP Professional SP3 operating system and above or Linux Operating System (Ubuntu 14.04 LTS and above)
* Java SE Development Kit (JDK)
* Java Runtime Environment (JRE)
* WampServer 3.0.6
* Netbeans version 7.1.2 and above
* MySQL dbms
* A web browser e.g. *Internet explorer, Mozilla Firefox, Google chrome or Opera mini.*

### 1.13.2 Hardware Requirement

* Pentium IV computers and other higher platforms. Minimum processor speed of 1.5 GHZ, 512MB of RAM and at least 40 GB of disk space.
* Standard peripheral devices of a personal computer system.

### 1.13.3 Others

* An external storage device of at least 1gb
* Wireless/wired Internet connectivity

# CHAPTER 2

2.1 Overview of the Literature review

Nowadays AES algorithm plays a vital role in securing the confidentiality and secrecy of both the static and dynamic information. Many computer scientists have greatly applied the AES in different ways ranging from organization, institutions, schools, banks, military etc. In order to understand this, this chapter gives more prospective and detailed ideas about the performance of the encryption algorithms, this subsection describes and examines previous work done in field of data encryption. This subsection also discusses the results obtained for some of the algorithms.

2.2 Definitions of the terms

The following are the terms used in this chapter;

**Encryption**- This is the process of converting the plain message into cipher text, which cannot be easily understood by anyone except authorized parties.

Decryption-This process of converting the encrypted message (cipher) into plain text, which can easily be understood.

WLAN- This is the wireless local area network.

AES- This is called Advanced encryption standard. It one of the modern symmetric key encryption commonly used for providing data confidentiality.

Blowfish- this is the symmetric key encryption that uses the feistel network to perform the encryption and decryption.

RC4- this is the Rivest Cipher 4, which is the stream cipher.

2.3 Related studies

The following are previous work done by different scientists;

**D. S. Abdul. Elminaam et.al., (2009)** presents a performance evaluation of selected symmetric encryption algorithms on power consumption for wireless devices in their paper named “Evaluating the Effects of Cryptography Algorithms on power consumption for wireless devices.” Following points are concluded by him from his experimental result. If packet size is changing with or without transmission of data using various WLANs protocols and different architectures. It was concluded form the result that Blowfish and AES has better performance than other common encryption algorithms used, followed by RC6. Worm holes are present in the security mechanism of DES and 3DES; Blowfish and AES do not have such worm holes any so far.

**Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati, Mohsen Rahmani**, “A New Modified Version of Advanced Encryption Standard (AES) Based Algorithm for Image Encryption” (2010). The authors proposed an enhanced model of Advanced Encryption Standard to possess good level of security and better range of image encryption. The modification process can be carried out by adjusting the Shift Row Transformation. As the result shown, that the comparison has been made in between the original AES encryption algorithm and the modified algorithm which produces very good encryption results focusing towards the security against statistical attacks.

**P.Prasithsangaree and his collegeue P. Krishnamurthy** 2003 analyze the Energy Consumption of RC4 and AES Algorithms in Wireless LANs. RC4 and AES encryption algorithms performance evaluation is made by their research. The matrices for such evaluation are as follows: CPU work load, encryption throughput, key size variation and energy cost. Experimental results conclude that for encrypting large packets the RC4 is energy efficient and fast. However, for a smaller packet size encryption AES was more efficient than RC4. Therefore it appears that by using a combination of RC4 and AES we can save energy to provide encryption for any packet size.

**Agrawal et al.** Present detailed study of the popular symmetric key encryption algorithms such as DES, TRIPLE DES, AES, and Blowfish. Symmetric Key algorithms run faster than Asymmetric Key algorithms such as RSA etc and the memory requirement of Symmetric algorithms is lesser than asymmetric encryption algorithms. Security of Symmetric key encryption is superior to Asymmetric key encryption. It was concluded that the supremacy of Blowfish algorithm over DES, AES and Triple DES on the basis of key size and security. The F function of Blowfish algorithm provides a high level of security to encrypt the 64 bit plaintext data.

**Seth et al.** made a comparative analysis of three algorithms, DES, AES and RSA considering certain parameters such as computation time, memory usages and output byte. It was concluded that RSA consumes longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm. Based on the text files used and the experimental result it was concluded that DES consume least encryption time and AES has least memory usage while encryption time difference is very minor in case of AES algorithm and DES algorithm.

**Marwaha et al.** discussed three algorithms DES, 3DES and RSA. DES and 3DES are symmetric key cryptographic algorithms and RSA is an asymmetric key cryptographic algorithm. Algorithms have been analyzed on their ability to secure data, time taken to encrypt data and throughput the algorithm requires. Performance of different algorithms was different according to the inputs. It was concluded that confidentiality and scalability provided by 3DES over DES and RSA is much higher and makes it suitable even through DES consumes less power memory and time to encrypt and decrypt the data but on security from DES can be easily broken by brute force technique as compared to 3DES and RSA, making it the last secure algorithm.

2.4 Objectives

* To understand how various algorithms were implemented to encrypted different types of file formats.
* To understand the different types of encryption algorithms used

# 3.0. METHODOLOGY

3.1 Introduction

This chapter elaborates on the methodologies that were used in developing the email cryptosystem. It entails the descriptions of the target users of the product, the sample population and how it was chosen, the methods of data collection, system requirements in terms of software and hardware for the creation of the product and the software development methodology used.

3.2 Target users of the product

This system was majorly designed for military organizations, journals and financial companies. The system can also be used by any regular users who use email as a form of communication. Military organizations have confidential information that needs to be shared which when leaked to the enemy will lead to serious loss of lives therefore this platform will enable them to comfortably pass their confidential information without any fear.

Journalist deals with very personal information about governments and its politics among others. When the identity of the particular journalist is leaked to the person of interest this may result to great enmity between them which might reach to family level. This causes high levels of fear and insecurity in the concerned parties. This system is meant to reduce such cases.

3.3 Target population

This system targets every individual who uses emails as a form of communication and is interested in confidentiality of the information he/she shares or receives.

## 3.4 Methods of data collection

interviews, questionnaires, observation (proof needed). Explain why you chose on that particular method

3.5 System requirements

To achieve the creation of the system the following software platforms and hardware were used

**Software**

* Windows 10 operating system
* MySQL database version 5.7.14
* WampServer 3.0.6
* Net beans IDE version 8.2
* Google Chrome version 61.0.3163.100
* Java and SQL programming language

**Hardware:**

* HP Elite Book 8470p with 4gb RAM and 2.6Ghz clock speed and 500gb hard disk
* Modem

3.6 Software development methodology

Incremental model has been used as the methodology. The incremental model combines elements of the linear sequential model (applied repetitively) with the iterative philosophy of prototyping. The incremental model applies linear sequences in a staggered fashion as calendar time progresses. Each linear sequence produces a deliverable “increment” of the software. The system was broken down into modules. During the initial module development, an initial version of the system was developed. Each module passed through the requirements, design, implementation and testing phases. A working version of software was produced during the first module, so you have working software early on during the software life cycle. Each subsequent release of the module adds function to the previous release. The process continues till the complete system is achieved.

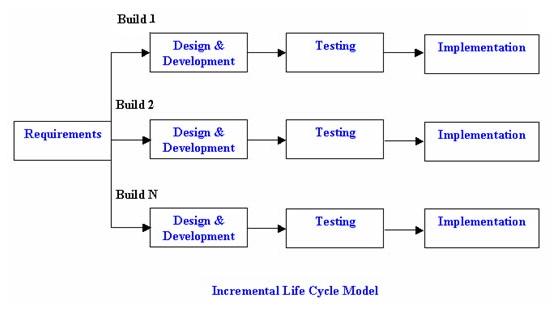


Figure 1.0: Incremental model design.

**Advantages of Incremental Model:**

1. Generates working software quickly and early during the software life cycle.
2. This model is more flexible – less costly to change scope and requirements.
3. It is easier to test and debug during a smaller iteration.
4. In this model customer can respond to each built.
5. Lowers initial delivery cost.
6. Easier to manage risk because risky pieces are identified and handled during it’d iteration.

**Disadvantages of Incremental Model**:

1. Needs good planning and design.
2. Needs a clear and complete definition of the whole system before it can be broken down and built incrementally.

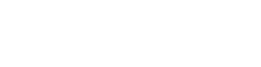
# CHAPTER 3: SYSTEM DESIGN

## 3.0 General Overview

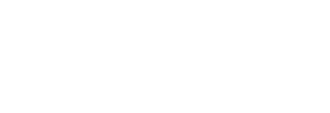
System design is an integral part in any working software worth implementing. In this section we shall look into the data aspect and component interface for the *email cryptosystem*

The system will generally interact with various entities from database server to system users.

Figure 1: General interaction between web server, JSP engine and Clients.



Internet



Web server

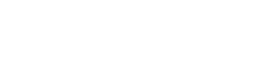


Clients



JSP servlet

engine



Database

The system has two ends;

**System backend*:*** The back end of the system consists of MYSQL database and XAMPP server. MYSQL is used as a storage media for data and processed information. The user is not aware of this as he/she just interacts with the interface provided for them in the front end.

**System front end:**This is the interface part of the system. All data entries are captured here. Java for graphical user interface has been used here.

There levels that were applied in development of the system are;

* Architectural design
* Database design
* Interface Design
* Component design

## 3.1 Architectural Design

In this design level, the basic structural framework that identifies the major components of a system and the communications between these components. Below is a general model for the whole system; **Scenario**

### Email User.

* Register as a user
* login to the system
* compose email
* Encrypt and send
* View inbox
* Decrypt received email and open
* logout

## Figure 2: Architectural design of the system and communication flow between components

EMAIL CRYPTOSYSTEM

LO

LOGOUT

DECRYPT THEN VIEV

OPEN RECEIVED MAIL

ENCRYPT THEN SEND

COMPOSE EMAIL

CHANGE DETAILS/SETTINGS

AUTHENTICATION

LOGIN

REGISTER

## 3.5 Database Design

This involves the design structure of the database. The following is a ER model used to show the relationship between the various entities in the system.

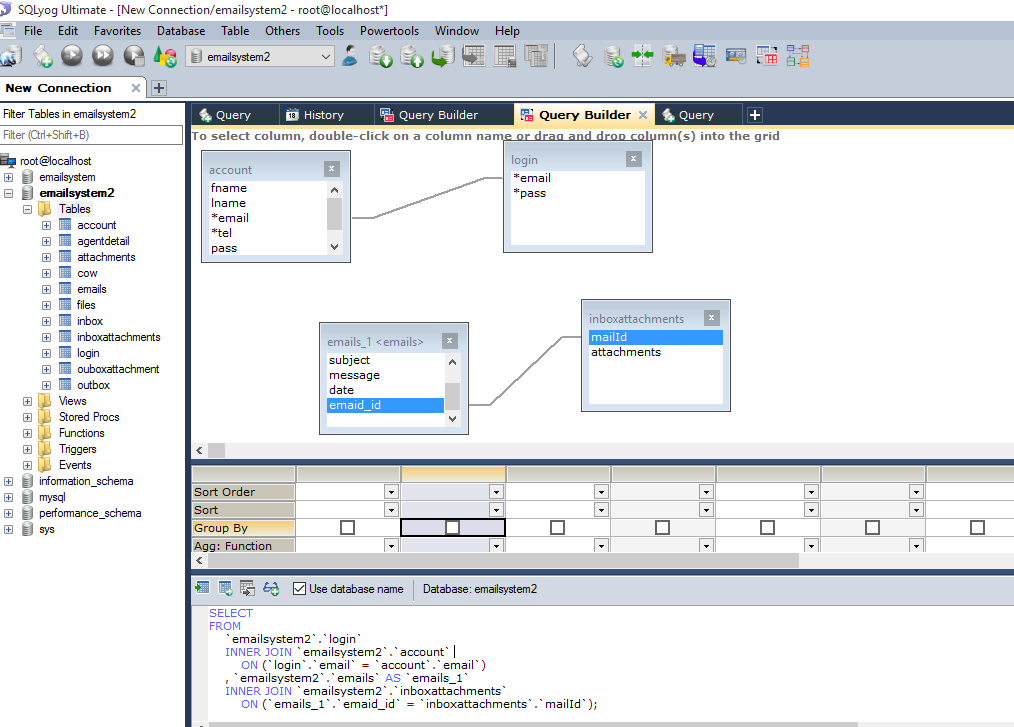


Figure 3: Enhanced Entity-Relationship (EER) model for database entities.

3.6 Interface Design

In designing the systems’ interface, I attempted to emulate Jacob Nielsen’s usability heuristics as described below:

### User control

The interface has been made to adapt to the needs of the user. I provided more than on way of doing same task. This is made possible by provision different links located at different parts for doing the same task

### Match between system and real world

The web-page module was designed to emulate/resemble the normal requirements of guests **Consistency**

Consistency is about making similar things look and behave similar. The front end and the back end of my system are consistent. This provides users with a good chance to learn new contexts (and to detect new contexts), to concentrate on relevant tasks, to feel safe.

**Minimalistic design**

In each form, only information that is directly relevant to the task in hand is displayed.

### Error recognition and diagnosis

While using the system a user can tell when an error has occurred as error messages are displayed and possible ways to get out of the error are suggested.

## 3.7 Component Design

This is the structural design of various modules in the system.

### 3.7.1 Registration Module

This is where new users of the system get registered. Upon submission of successfully entered details, an account activation link is sent to the email provided where the user is supposed to activate their account before logging into the system. Successful activation of the account fully registers the user with the system.



Figure 4: Screen Shot of User Registration page

### 3.7.2 Login Module

This screen shot shows an entry point from where users (administrators and Applicants) get access to the system. Users use valid emails and password to login.

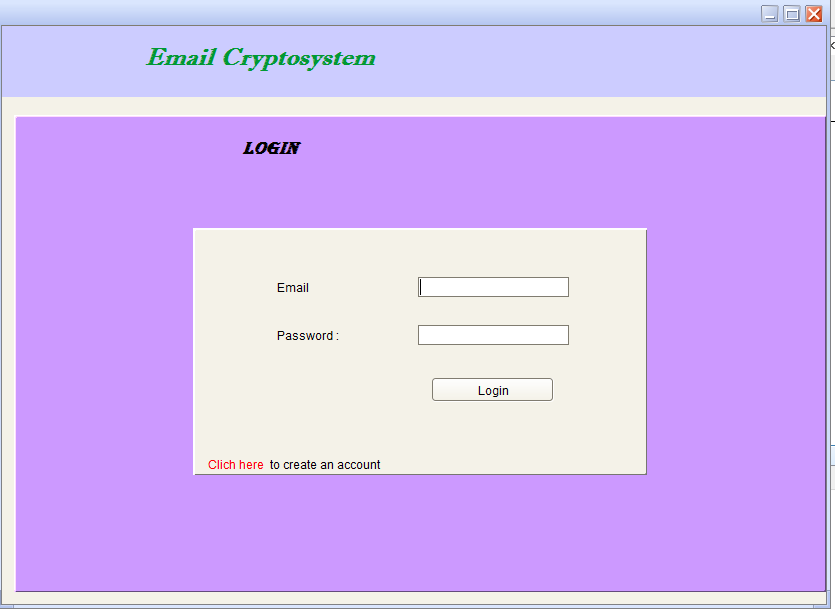


Figure 5: Screen Shot of User Account Login page

After users have successfully logged in, they are directed to their specific main page depending on user category from where they can choose various options to perform the various activities that are provided by the system.

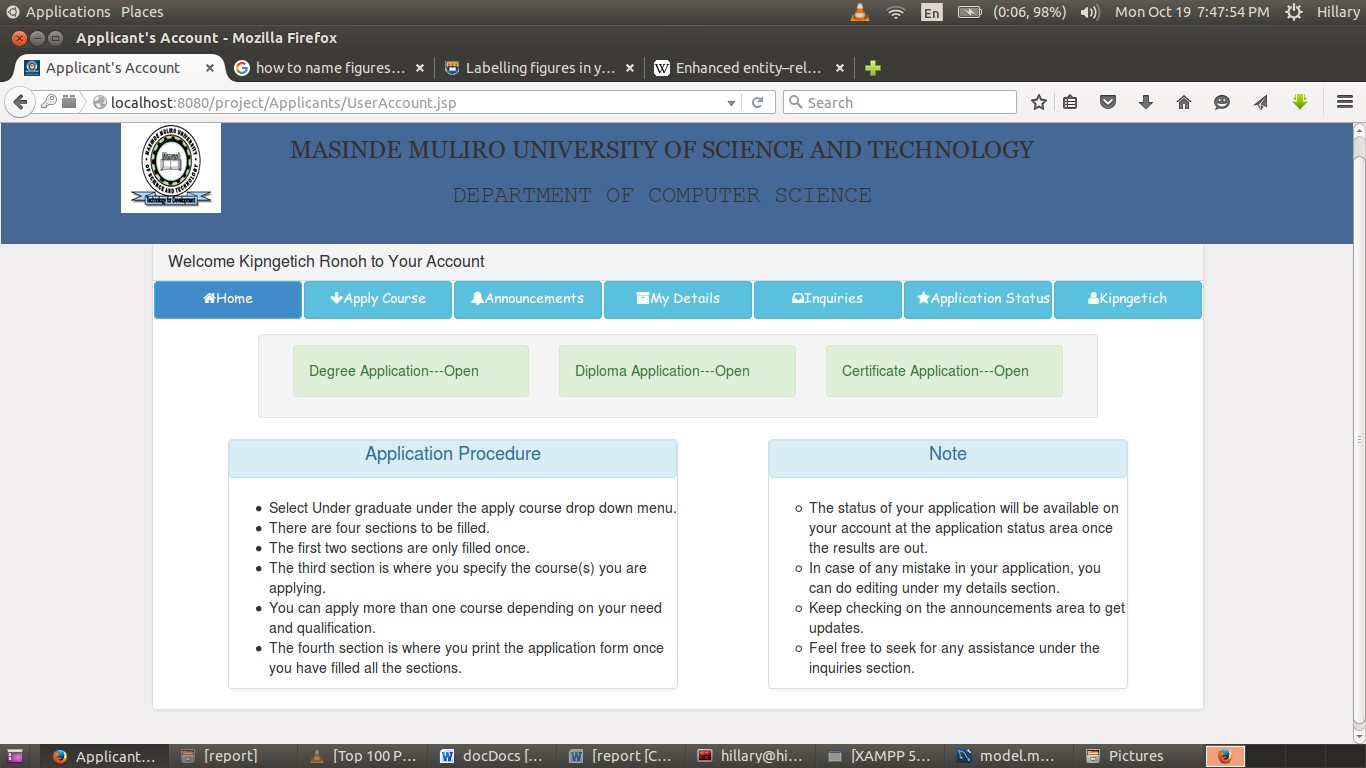
### 3.7.3 Applicant Module

This is one of the main modules of the system. It encompasses all the units that enable the applicant to accomplish his/ her tasks. It has the following sub-modules:

#### 3.7.3.1 Homepage

This page apart from being the applicant’s dashboard also saves as a help area where the applicant is given guidelines on how to apply for a course. It also informs on whether the applications are still opened or closed.

Figure 6: Screen Shot of Applicant’s Homepage



#### 3.7.3.2 Course Application

This is where the applicants do the actual course application. It has four sections namely:

* SECTION A: Personal Details
* SECTION B: Education Background
* SECTION C: Course Details
* SECTION D: Print Form

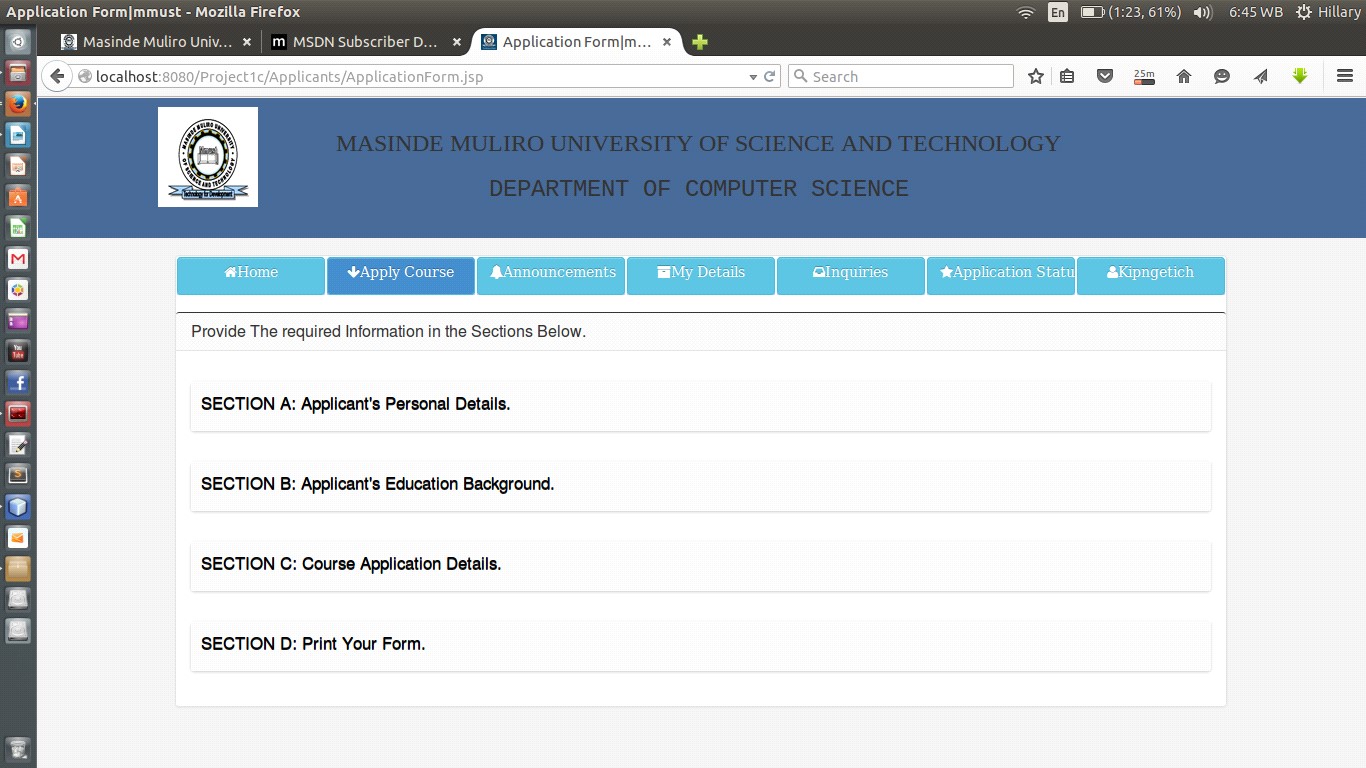


Figure 7: Screen Shot of Course Application page

#### 3.7.3.3 Announcements

Announcements posted by the admin of the system on various issues are displayed here.

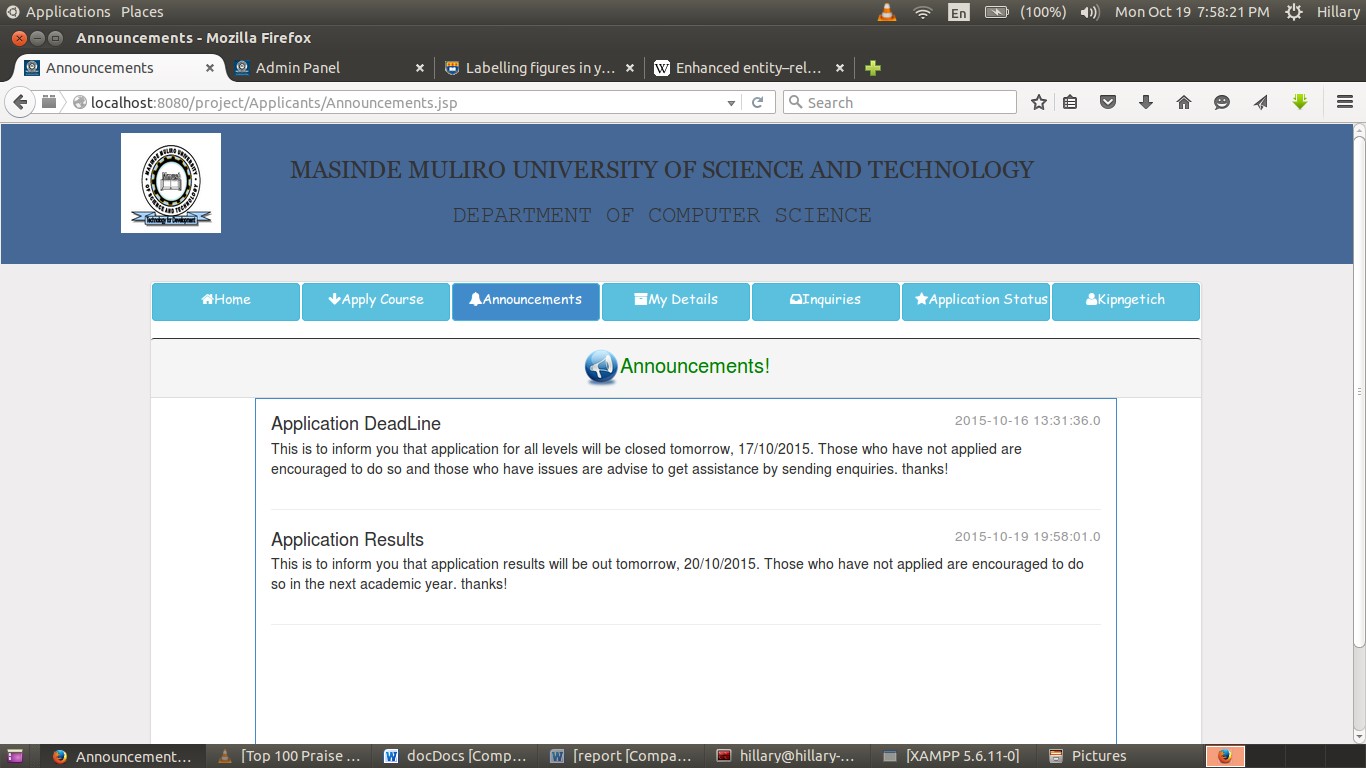


Figure 8: Screen Shot of Applicants’ Announcements area

#### 3.7.3.4 Details

This is where the applicants can view his/her details and edit where necessary. However, the editing option is only active when applications are still open.

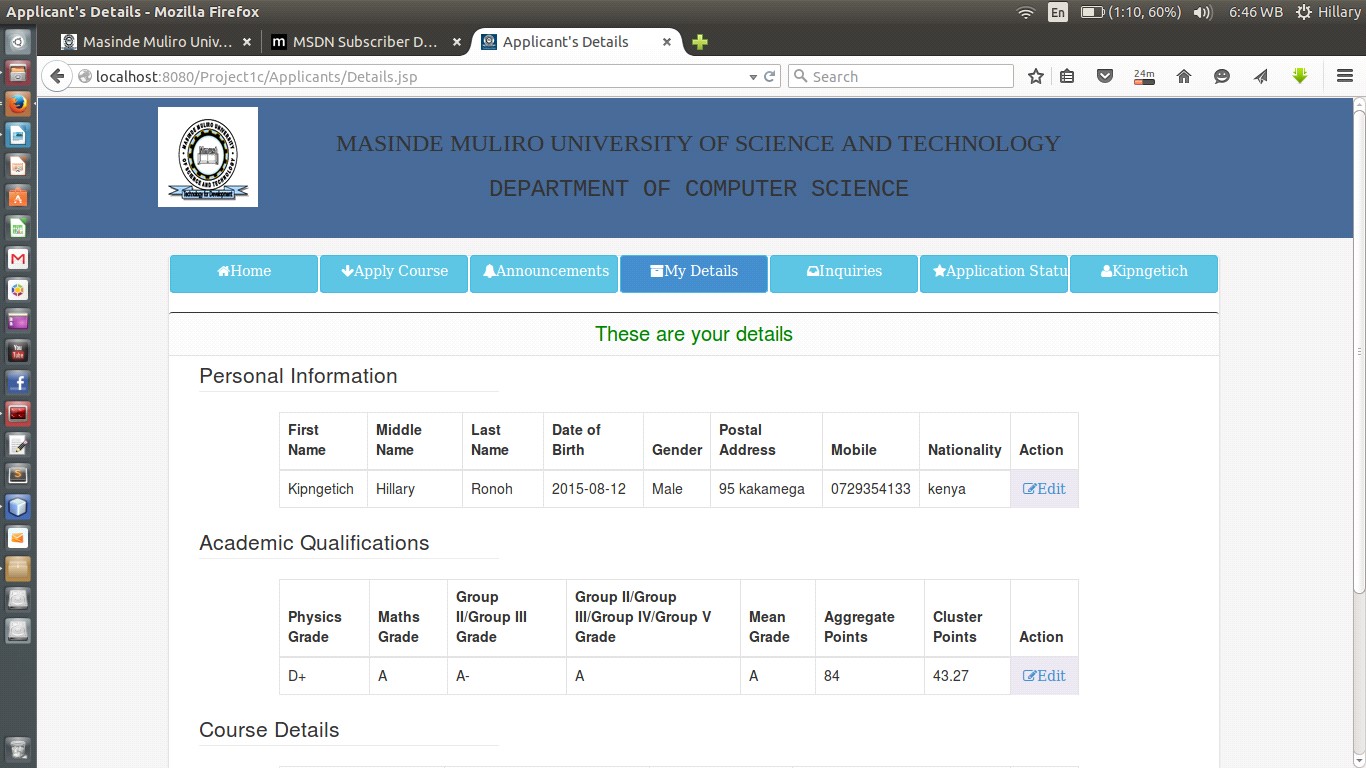


Figure 9: Screen Shot of Applicants’ Details page

#### 3.7.3.5 Inquiries

This module enables the applicant to have a one-to-one chat with the admin of the system. The applicant can make any inquiry from this page.

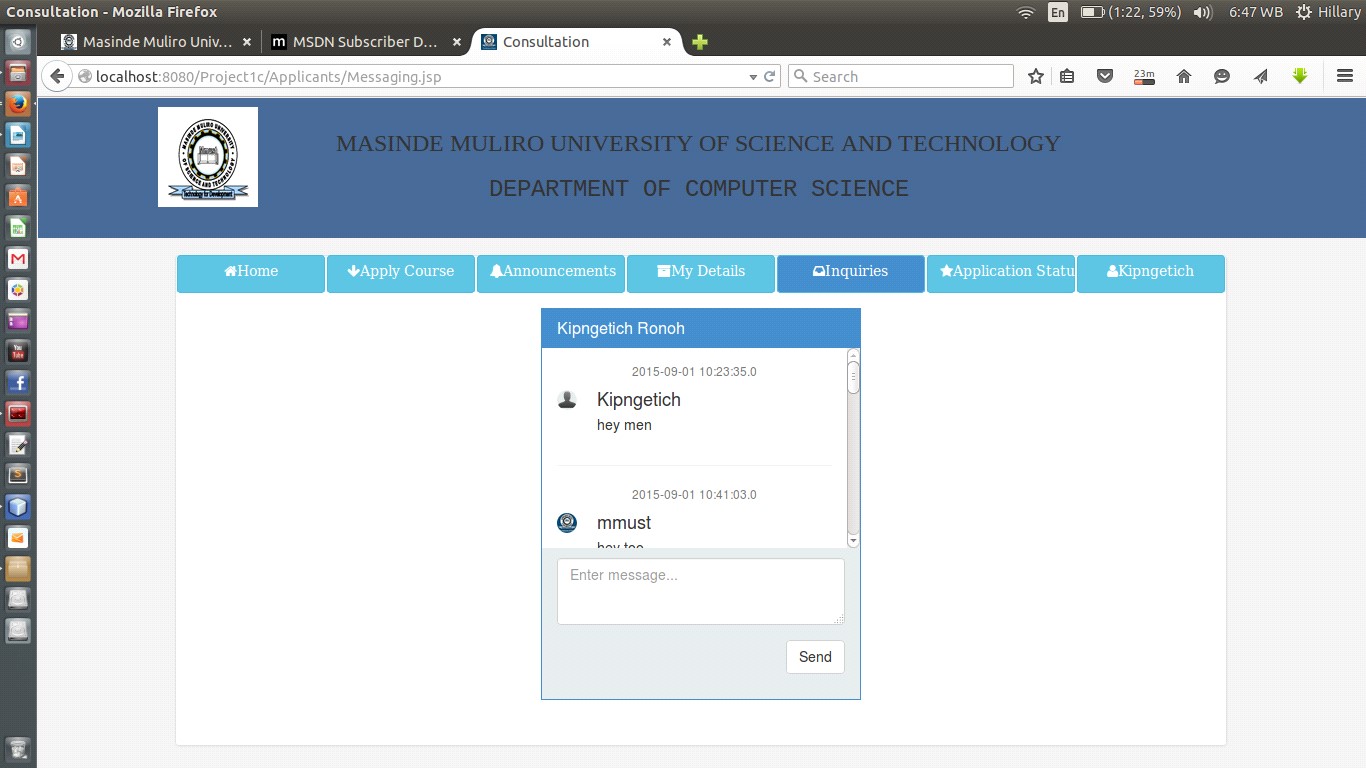


Figure 10: Screen Shot of Applicants’ inquiry area

#### 3.7.3.6 Application Status

This is where applicants receive the status about their application. When ranking has not been done, appropriate message will be shown, when it has been done, a message notifying applicants on their success or failure of their application is displayed.

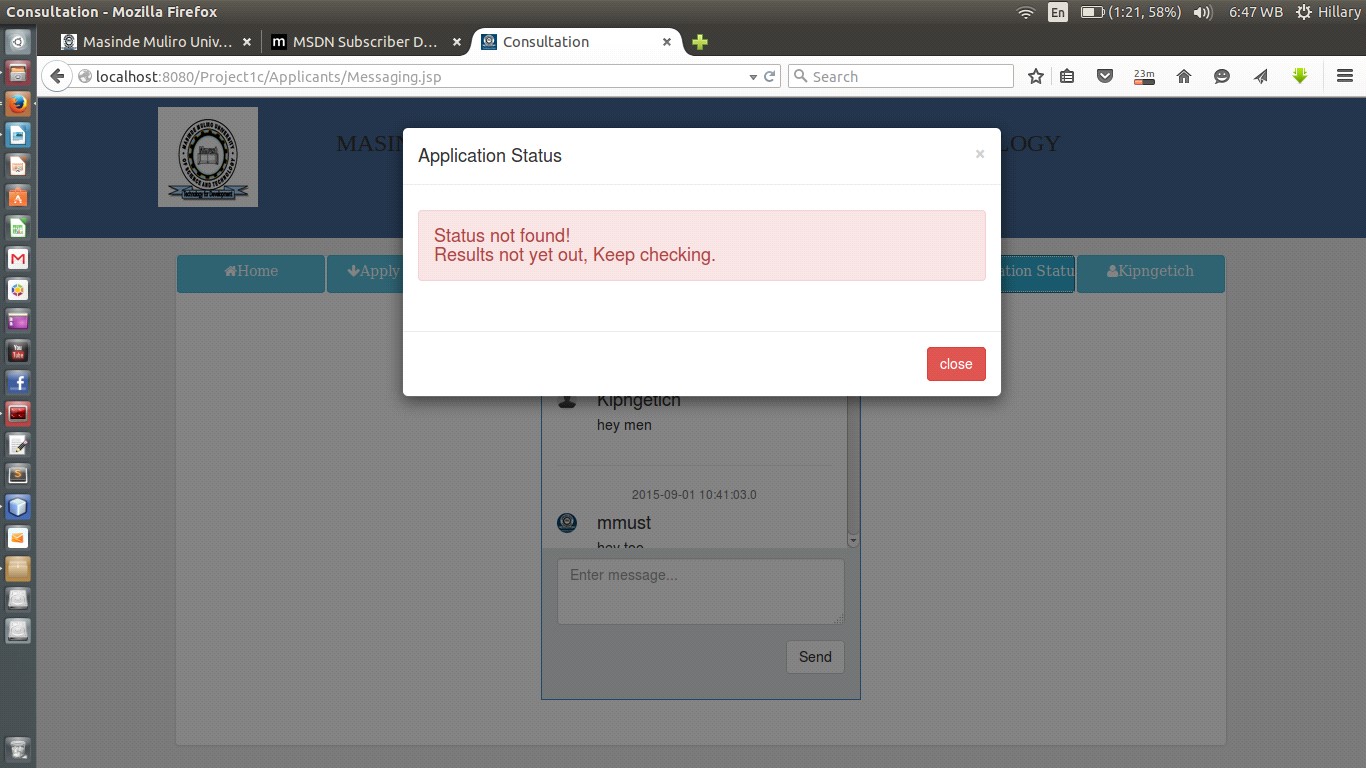


Figure 11: Screen Shot of Application Status dialog

### 3.7.4 Administrator Module

Administrator module form one of the core modules of the system. It is from this module that the admin is able to administer the system. It is composed of the following:

#### 3.7.4.1 Homepage

This is the admin dashboard, various statistical analysis are displayed on this page.

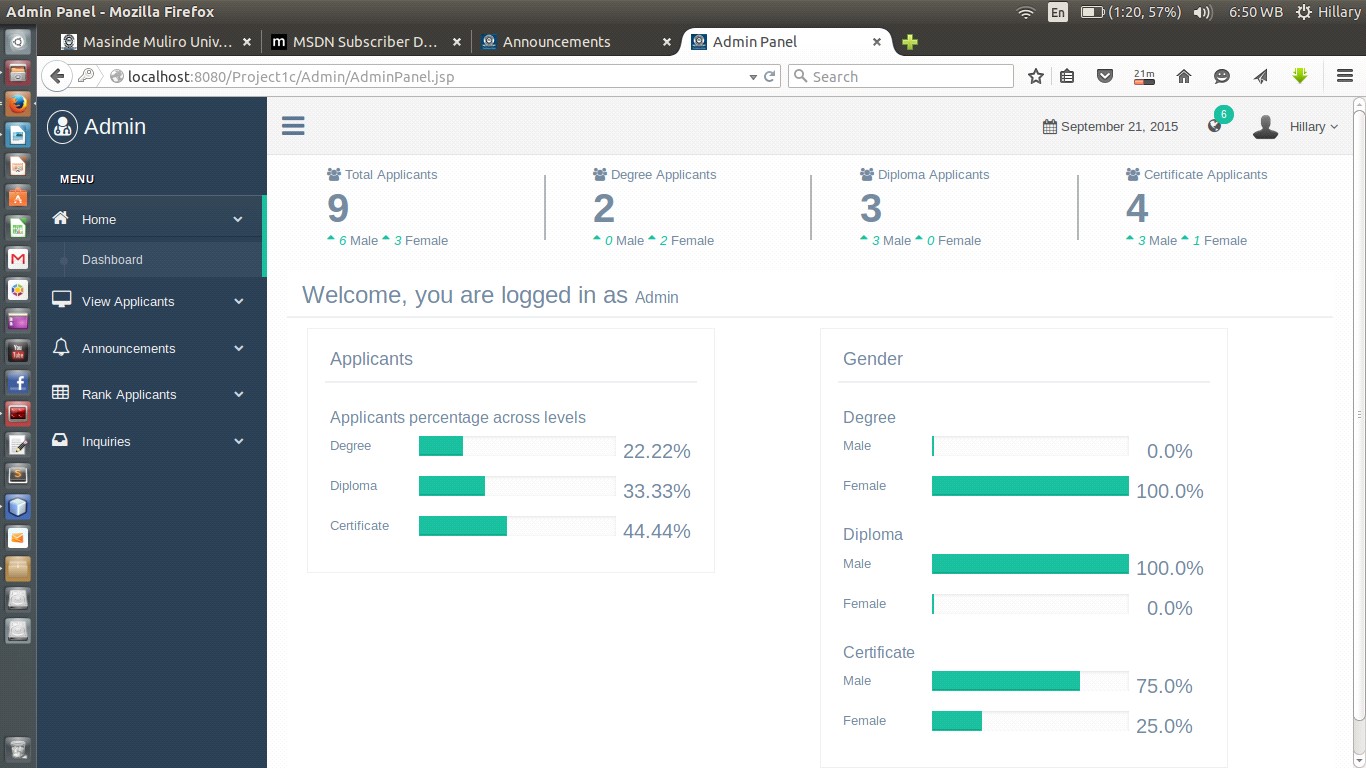


Figure 12: Screen Shot of Admin Homepage

##### 3.7.4.2 View Applicants

This is where the admin is able to view applicants from various course levels. The admin also is presented with the option to delete the applicant.

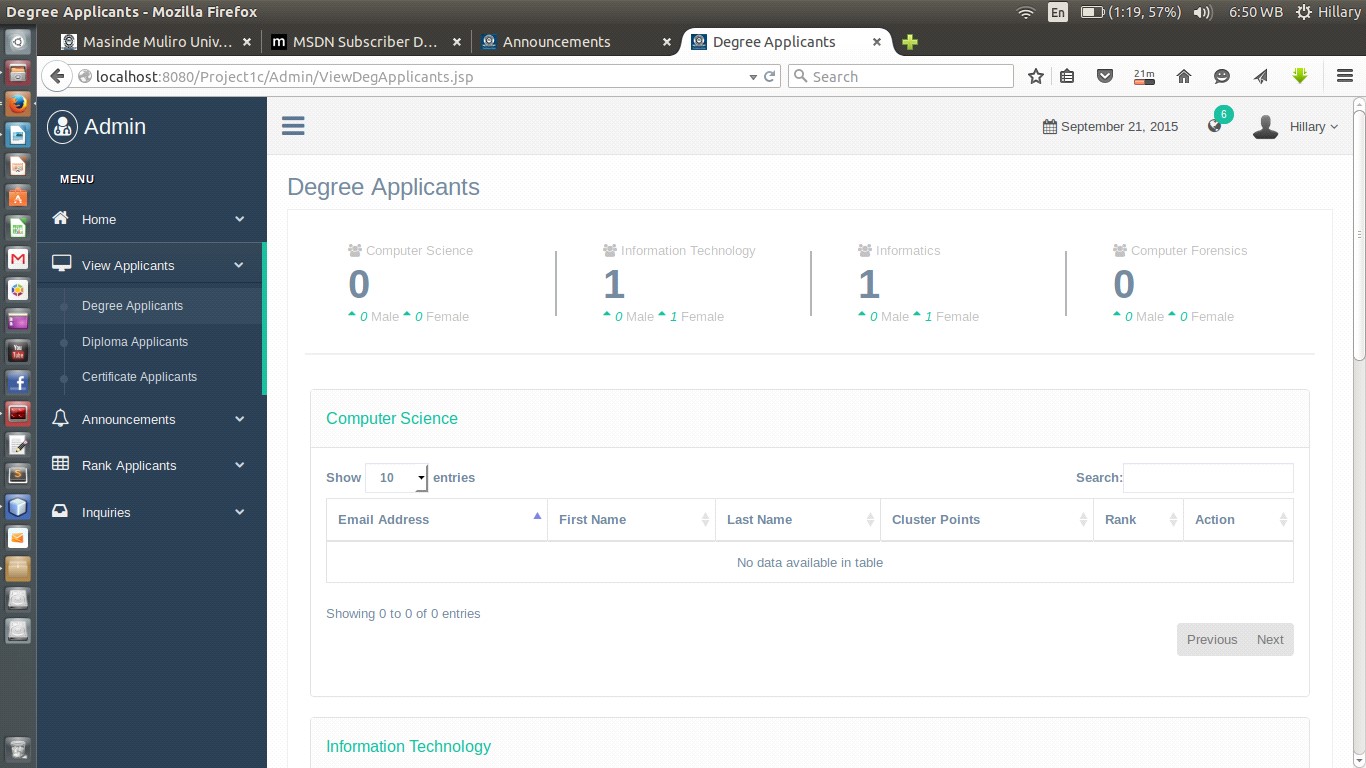


Figure 13: Screen Shot of Degree Applicants

**3.7.4.3 Post Announcements**

The admin posts announcements to applicants from this page.

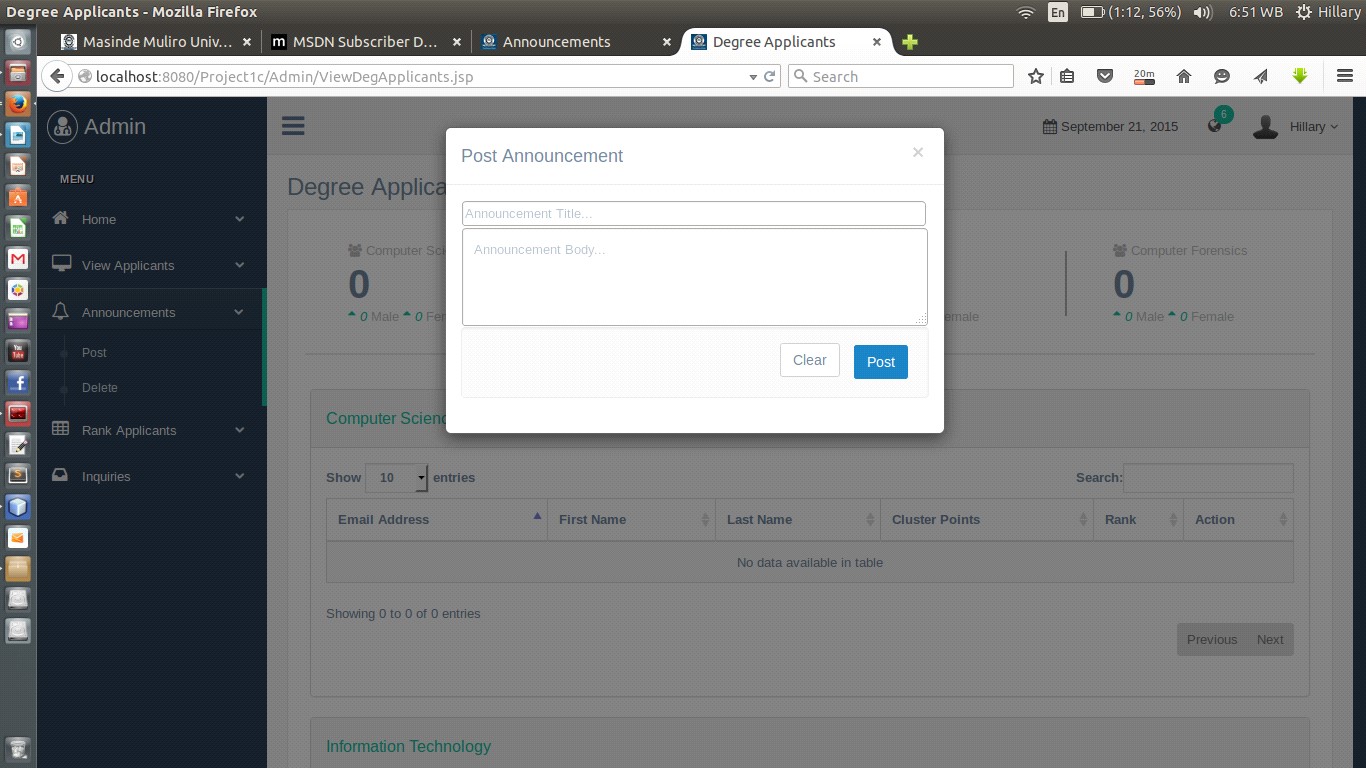


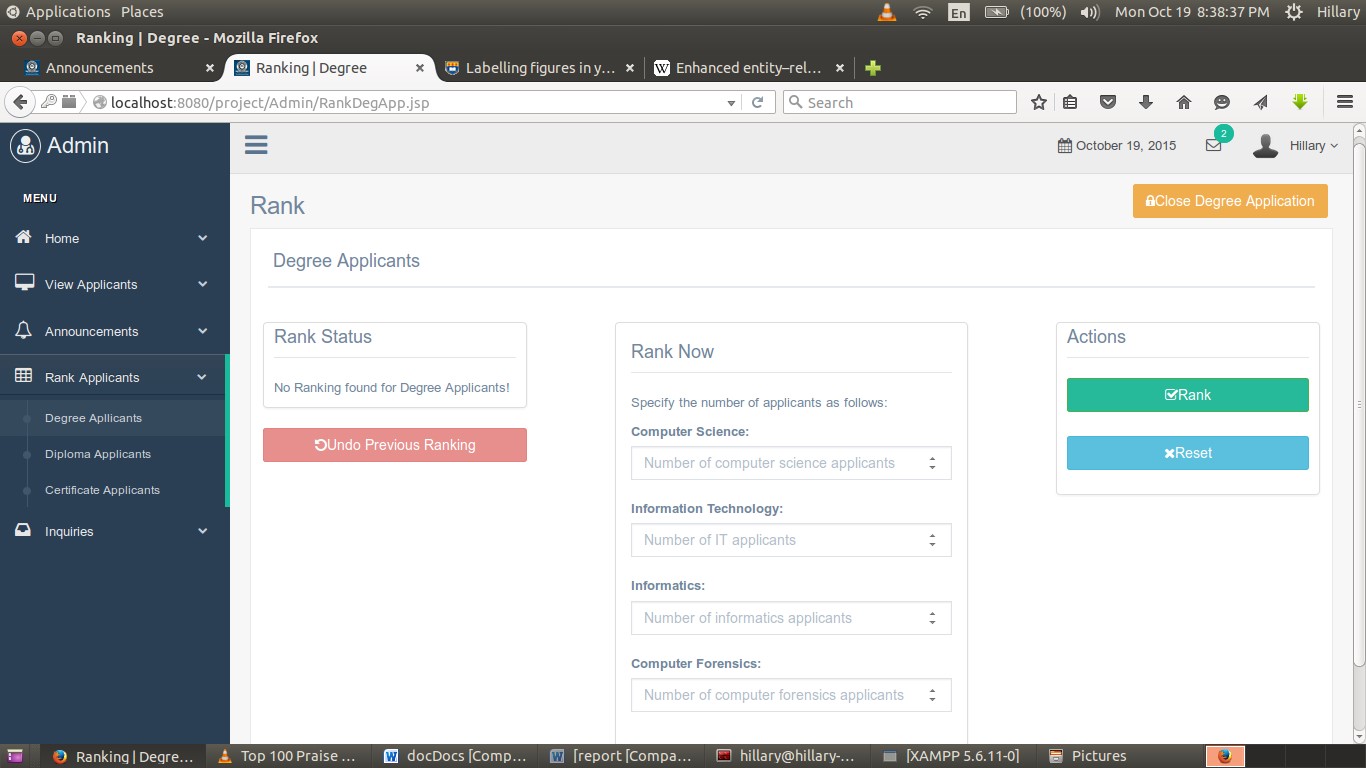
Figure 14: Screen Shot of Announcement posting modal

##### 3.7.4.4 Applicants Ranking

This is where the admin do the ranking of applicants on various course-levels based on the number required applicants.

Figure 15: Screen

Shot of Degree Applicants Ranking



##### 3.7.4.5 Inquiries

Inquiries and chats from the applicants are answered from this section by the admin of the system.

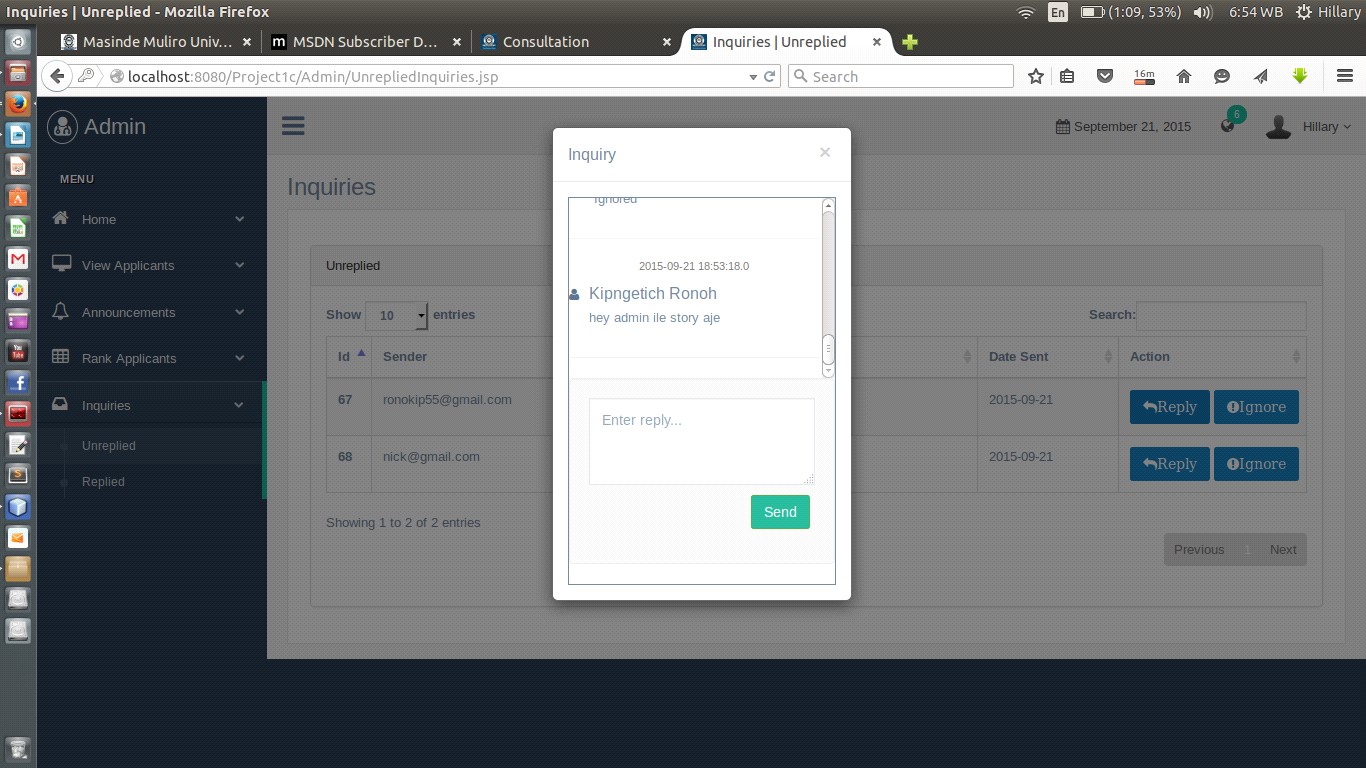


Figure 16: Screen Shot of Admin’s Inquiry area

# 4.0 CHAPTER 4

## 4.1 Implementation and Testing

The stage of implementation is the process of converting a system specification into an executable system. It involves coding, unit testing, module integration and testing, validation testing and documentation.

## Coding

Coding was done using the following programming languages and platforms **Software**

* Windows 10 operating system
* MySQL database version 5.7.14
* WampServer 3.0.6
* Net beans IDE version 8.2
* Google Chrome version 61.0.3163.100
* Java and SQL programming language

**Hardware:**

* HP Elite Book 8470p with 4gb RAM and 2.6Ghz clock speed and 500gb hard disk
* Modem

To ease the process of coding, the project was broken down into small modules so that each module could be developed, tested and integrated individually. Modularity enhances design clarity which in turn makes implementation easy as well as debugging, testing, documenting and maintenance of the software.

## 4.3 Unit Testing

I carried out this type of software testing during the development of this system. This form of testing ensures that each detail of the implementation is logically correct. This testing helped me to ascertain the correctness of the system in terms of input, processing and output.

## 4.4 Module Integration and Testing

This is a systematic technique for developing a system while at the same time conducting tests to uncover errors associated with interfacing. The main aim is to take untested modules and build a program structure that has been dictated by design. Having written the codes for each module, the modules were integrated and the resulting main module was tested for conformity and completeness.

## 4.5 Validation Testing

With the help of my friends I tested the validity of my system to ascertain that the project was as per the project proposal. . During the process of validation, a number of test cases were carried out as described below.

### 4.5.1 Test Cases

A test case is prepared for each test that needs to be performed. The test cases result in the development of test reports, which is used for test-output analysis. The test cases provided are those of main modules of the system that covers system functionalities.

#### 4.5.1.1 Test Case 1

**Test Id**: Test 2

**Test Name**: Applicant authentication

**Test Description**: This test verifies the email and password to allow access to the system.

**Variables:** Email, password.

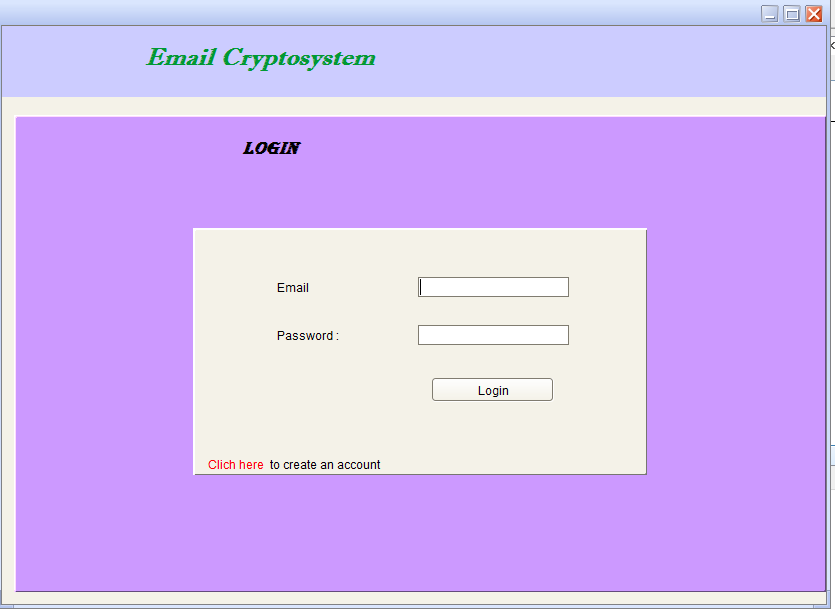


Figure 19: Login Entry Point

1. **Successful login:**

The user (applicant) will be taken to his/her account depending on user type.

1. **Unsuccessful login:**

The following DOM message will be shown to the user:

Wrong login credentials!!

In this state, a user will remain in the login window until he/she provides correct login details.

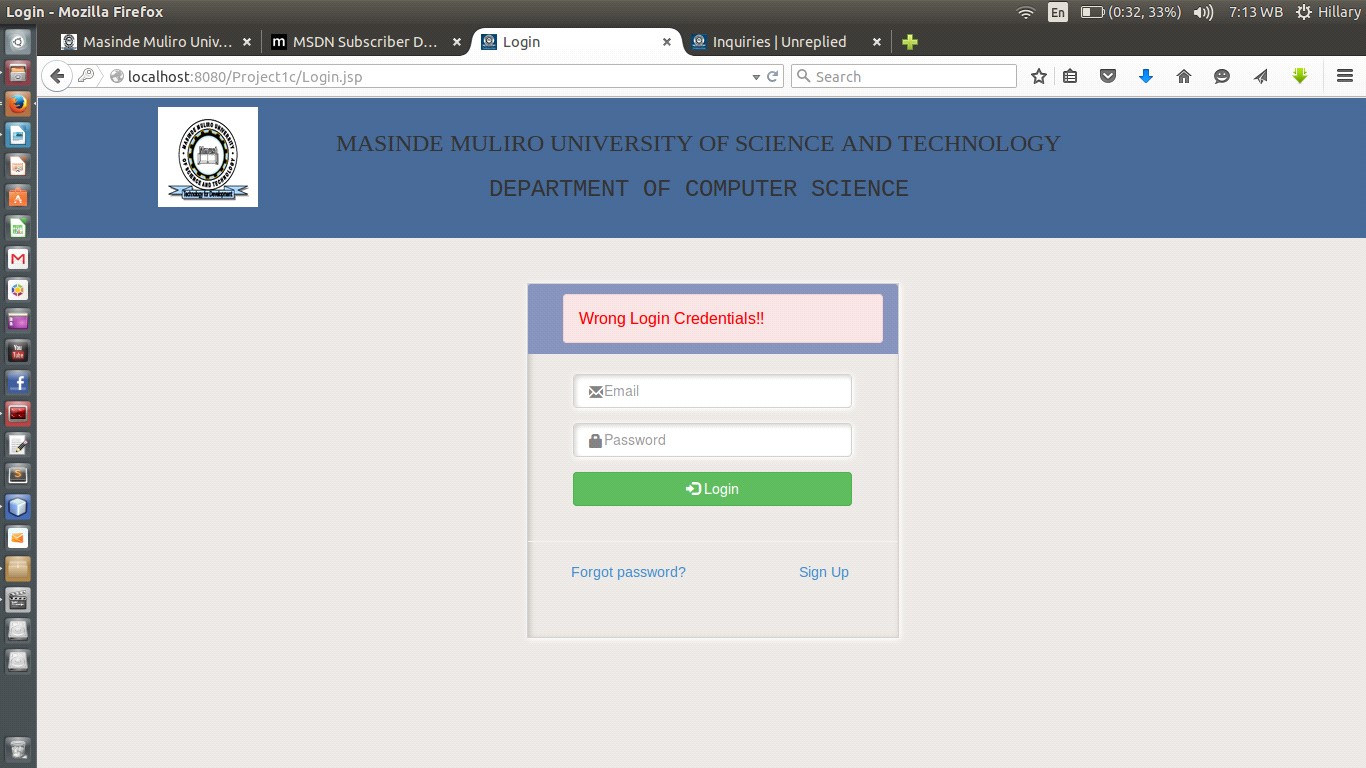


Figure 20: Unsuccessful Login Feedback

#### 4.5.1.3 Test Case 3

**Test Environment**: ACER LAPTOP 500GB HDD, 2GB RAM, Ubuntu 14.04 LTS, Apache tomcat Server, MySQL dbms

**Software**: MMUST ONLINE-COURSE APPLICATION SYSTEM

**Module**: Course application

**Test Id**: Test 3

**Test Name**: Course registration

**Test Description**: Allows an applicant to provide his/her personal details, his/her academic credentials, apply for a course (degree, diploma or certificate) then print the application form.

#### A. Section A: Personal Details

**Variables:** Applicant name (will be provided/already captured during registration), and other personal details (address, date of birth).

**On a Successful application,** a user will be notified as follows:

Details saved successfully…proceed to the next section.

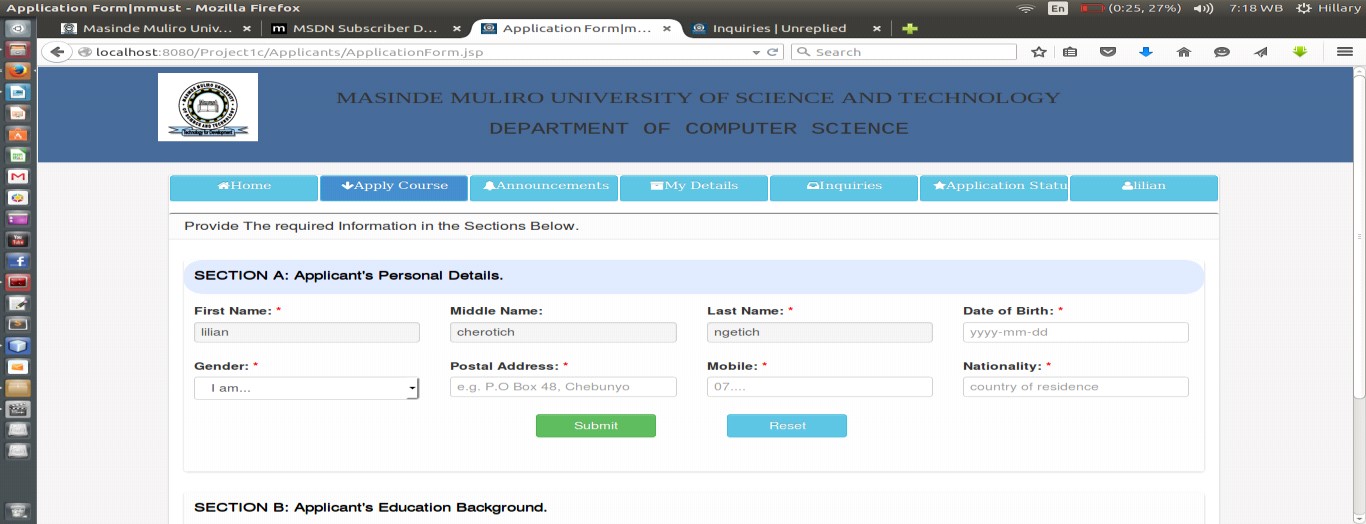


Figure 21

(

a): Personal details entry

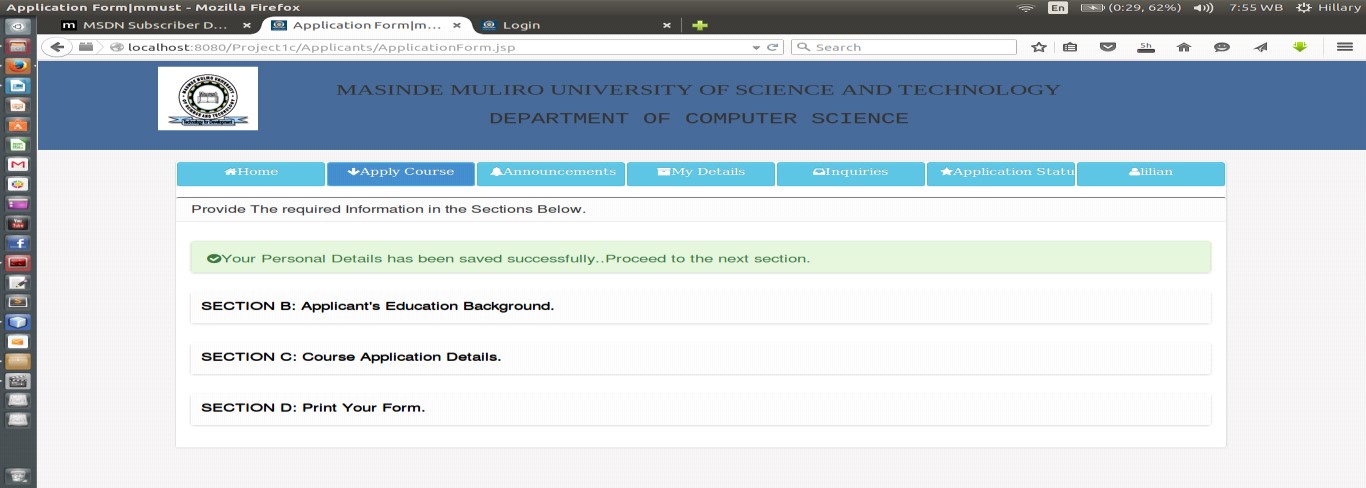


Figure 21(b): successful submission of personal details

#### B. Section B: Education Background

**Variables:** academic qualifications (kcse grades for 7 best performed subjects).

**On a Successful application,** a user will be notified as follows:

Details saved successfully…proceed to the next section.



Figure 22

(

a): Education background details entry

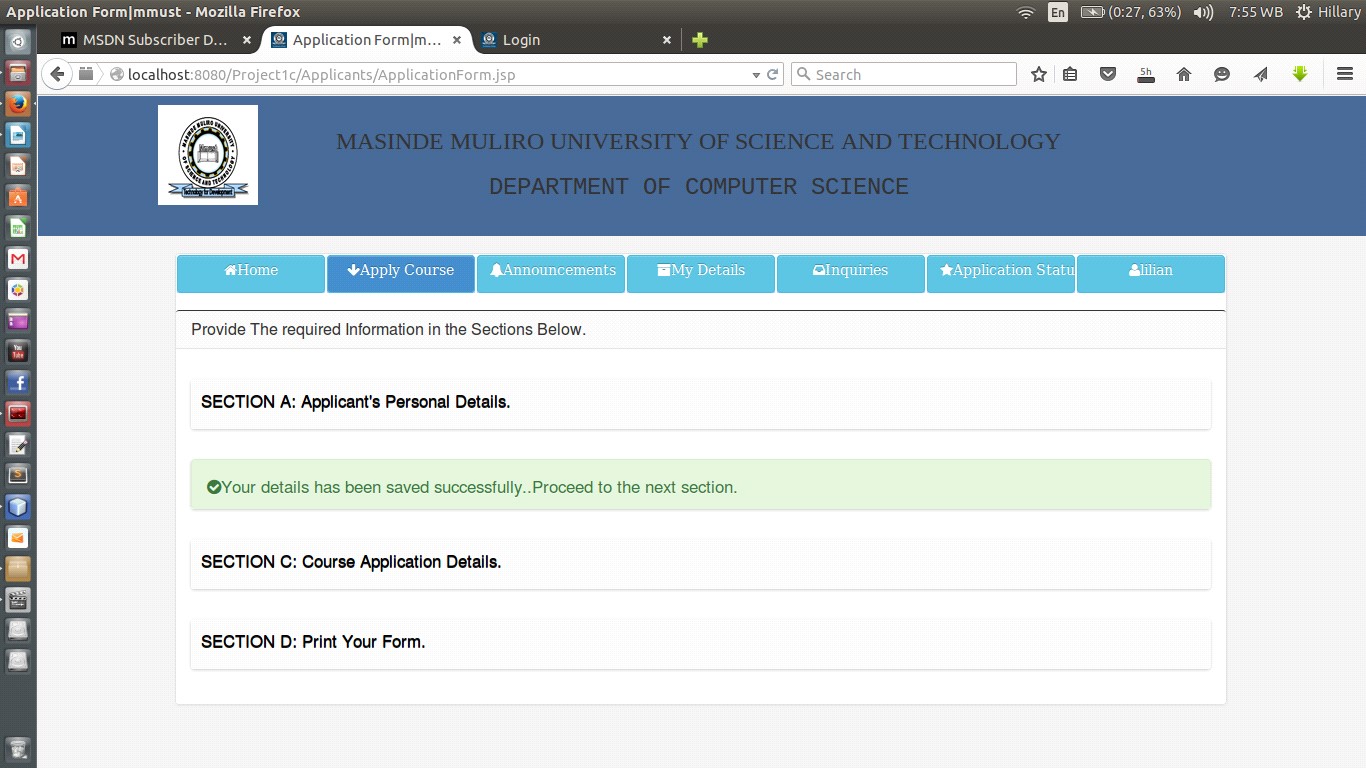


Figure 22(b): successful submission of academic details

#### C. Section C: Course Details

**Variables:** Course details (course level, course name) and campus details (branch name).

**On a Successful application,** a user will be notified as follows:

Details saved successfully…proceed to the next section.

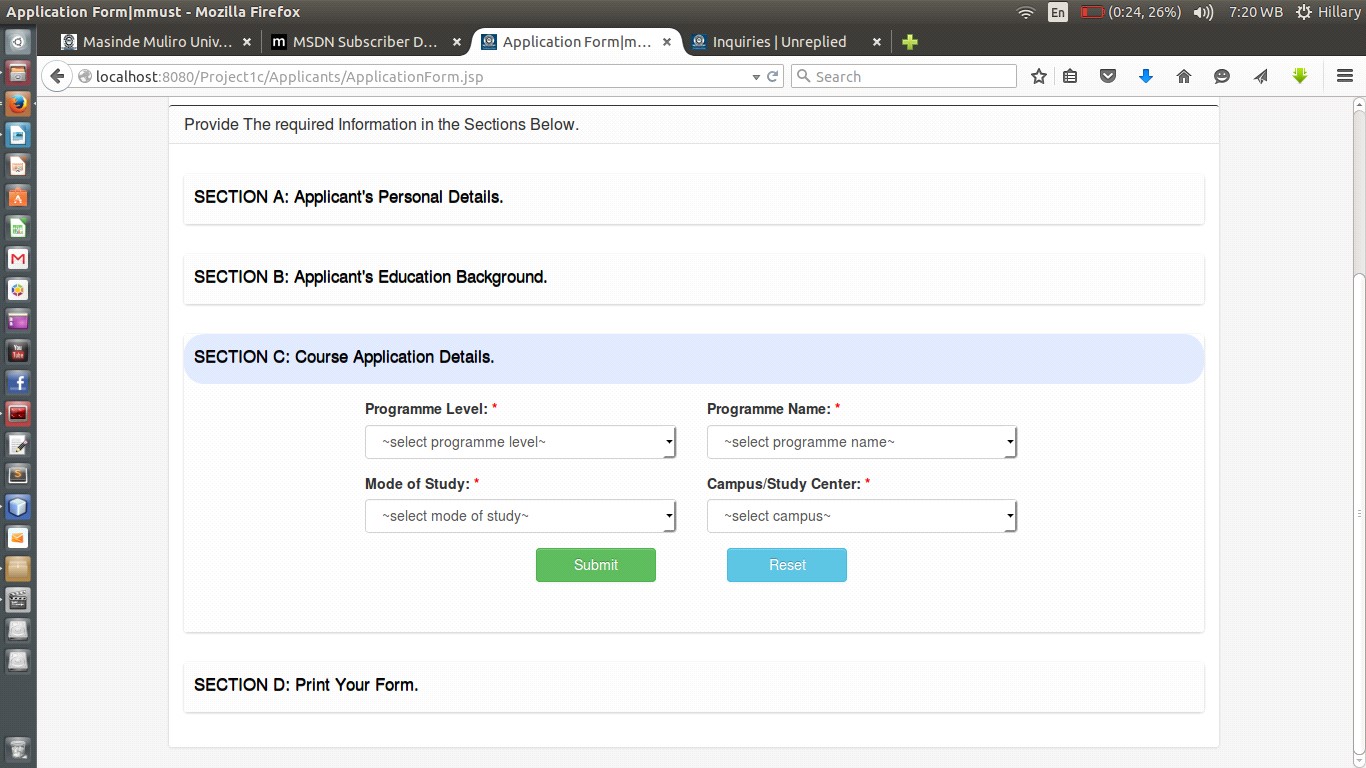


Figure 23

(

a): Course details entry

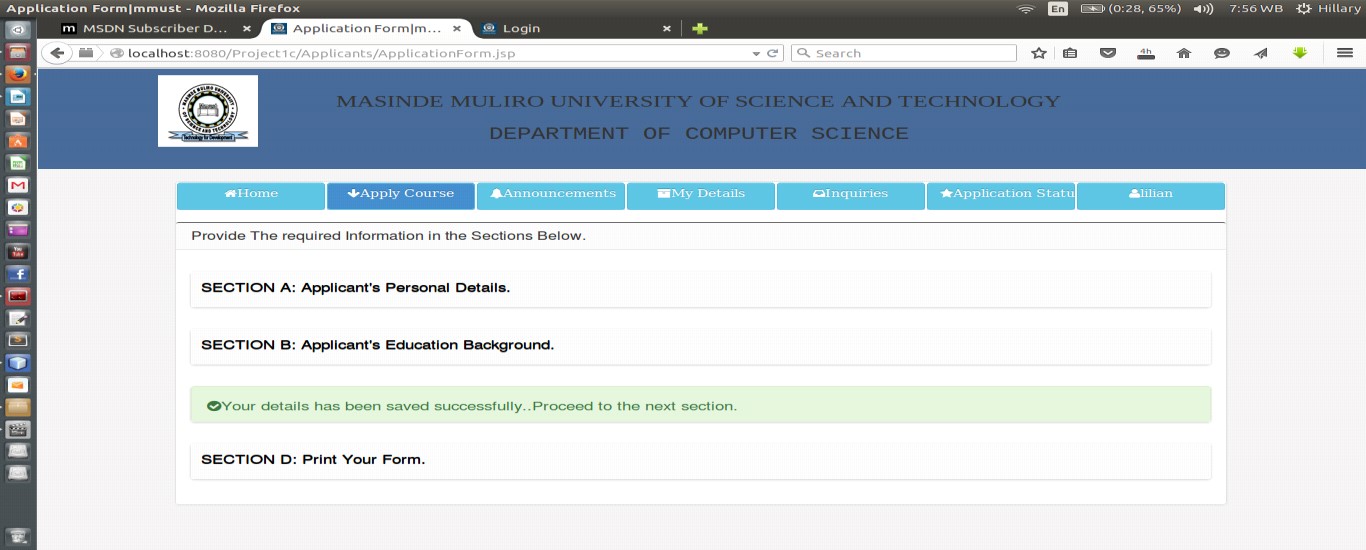


Figure 23(b): Successful submission of course details

#### D. Section D: Print Form

Once the applicants have filled all the three sections above, he can now print his form under this section.



Figure 24

:

Form print

##### 4.5.1.4 Test Case 4

**Test Environment**: ACER LAPTOP 500GB HDD, 2GB RAM, Ubuntu 14.04 LTS, Apache tomcat Server, MySQL dbms

**Software**: MMUST ONLINE-COURSE APPLICATION SYSTEM

**Module**: Applicants ranking

**Test Id**: Test 4

**Test Name**: Applicants ranking

**Test Description**: Admin of the system doing the ranking of the applicants in the various course-levels (have to select the level).

**Variables:** Number of applicants required and based on the number of applicants that have applied.

**On Successful ranking,** the admin of the system will be notified as follows:

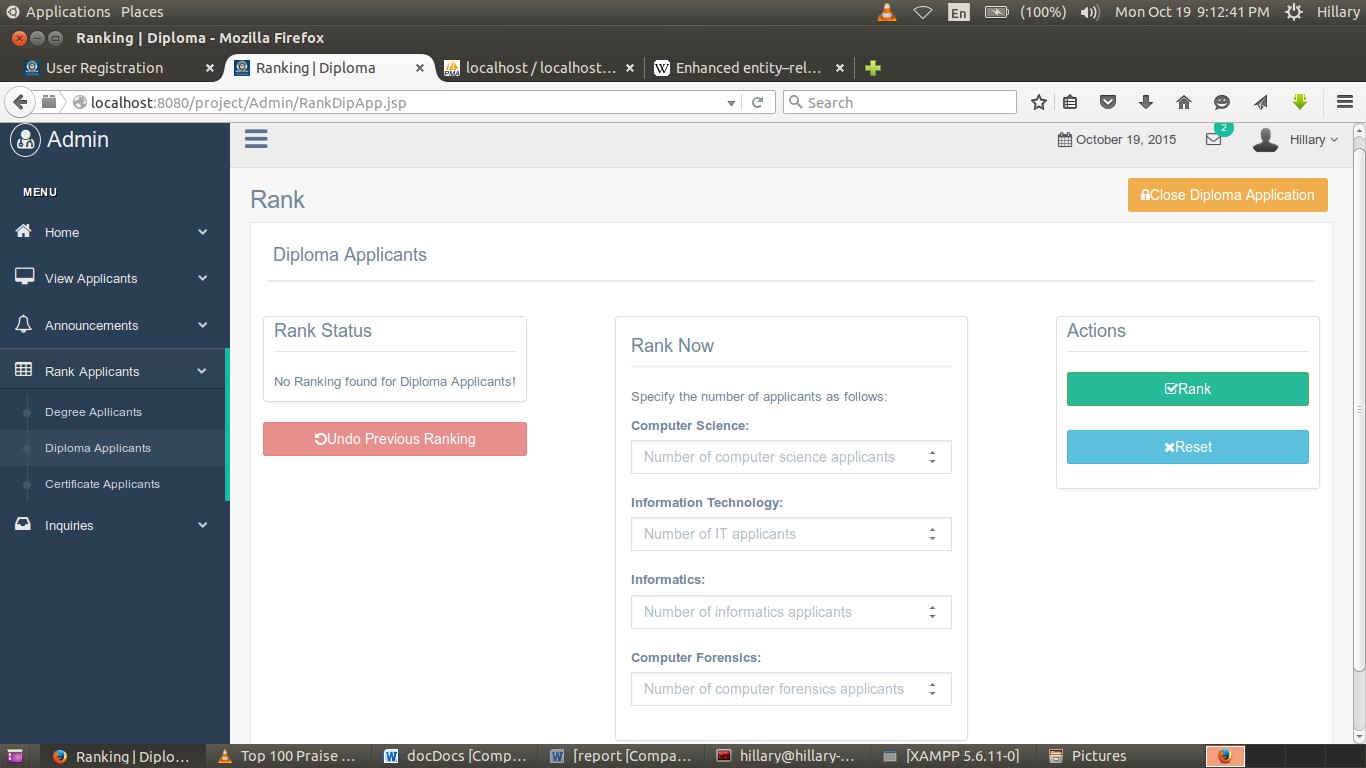
Ranking Successful

Figure 25(a)

:

Screen Shot of Diploma

Ranking



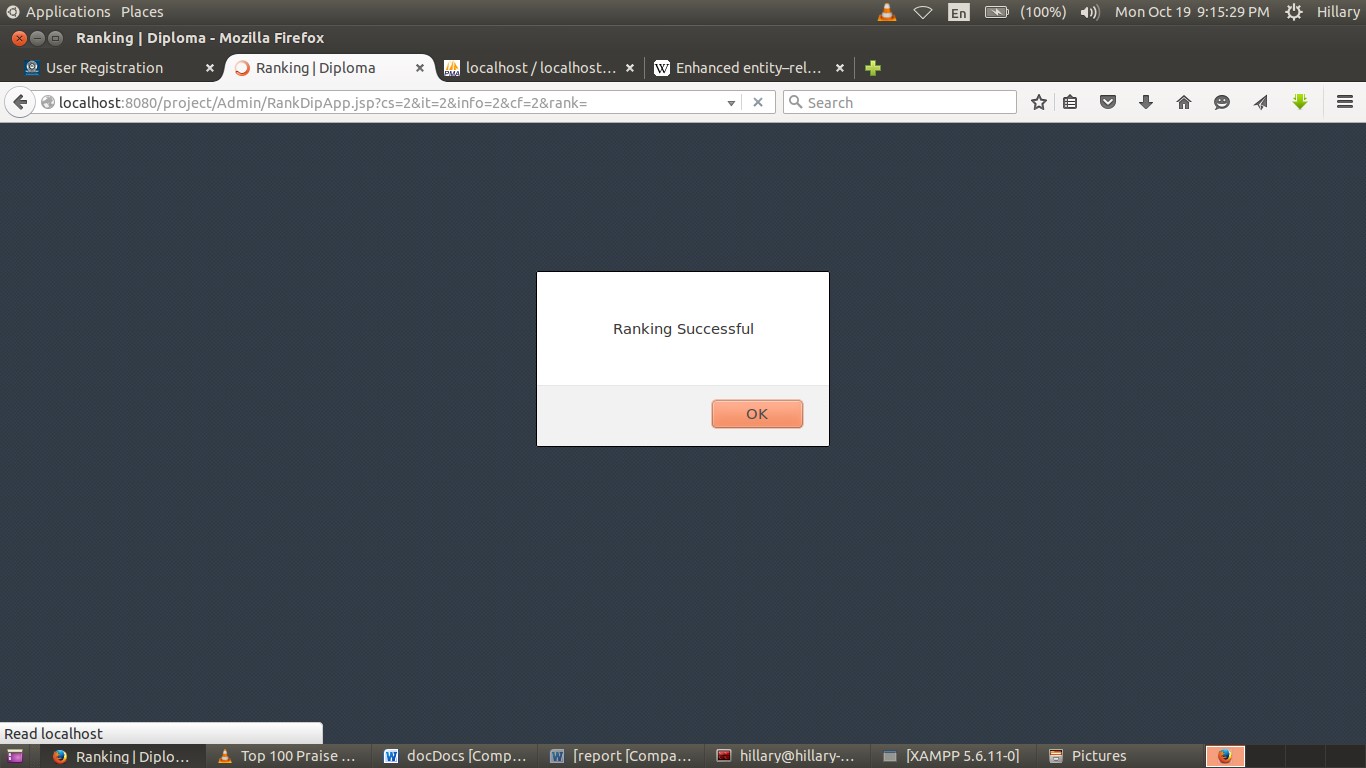


Figure 25(b): Successful Diploma Ranking

## 4.6 Configuration Review

A review of the system was carried out to ensure that all the elements of the software configuration were properly developed cataloged and had the necessary detail to support the maintenance phase of the software life cycle.

## 4.7 Security Testing

Security testing attempts to verify that protection mechanism built into the system will protect it from unauthorized access. This is done by the developer by deliberately inputting wrong usernames and passwords and check on the reaction of the system. Given enough time and resources, good security system will succumb to unauthorized accesses. The designer should then make it such that penetration cost more than the value of the information obtained through penetration

## 4.8 Actual Handover

The final version of the system was presented to the panel after satisfactorily testing it and removing the bugs.

# 5.0 CHAPTER 5

## 5.1 Summary and Achievements

The whole process of analyzing, designing and developing/implementing the information system project has been a fascinating experience. This is because it gave me a chance to apply useful knowledge and skills that had been acquired throughout my programme.

Therefore, the knowledge acquired throughout the system development was of great value in achieving the objectives of the project. Crucial units such as System analysis and design, Programming Concepts, Database Systems as well as IT Project Management proved to be the main source of knowledge and ability in realizing set goals.

The system developed catered for most of the user requirements that were gathered during the datagathering phase. The process of coming up with the system was very challenging and challenging at times. However with the assistance, help and moral support of fellow students, it was possible to overcome these challenges by taking necessary and fruitful solutions. Given the various circumstances, it can only be fair to assert that the system developed is reasonable and meets most of earlier projected objectives.

## 5.2 Constraints

The success of the project was constrained by the following factors 1. Inadequate time to collect all the information about all the records.

1. Limited reference materials.
2. Inadequate funds to undertake a thorough research on the problem domain.

## 5.3 Shortcomings

The system was based on information obtained from various stakeholders of MMUST which sometimes was difficult to find resource persons.

## 5.4 Discussion

This project has enabled me gain a vast experience and knowledge in IT field. It has made me go through a thorough integration of all the knowledge and skills I have acquired in the three years of my study.

To mention but a few, the system have enabled me put in practice Software development life cycle from requirements elicitation to documentation. It has also enabled me to interact and use the various CASE tools that are available to make the whole process easy and efficient. Among the tools that I have been able to interact with is MySQL Workbench which assist in database design, MySQL Database server, Apache tomcat web server and Adobe Dreamweaver CS5 which is one tool that has enabled me in designing good interfaces especially through its inbuilt CSS feature.

The project have also enabled me write proper software documentation and academic papers especially with the help of my supervisor who insisted on good documentation for an easy to maintain software.

The Project have also made me study bootstrap framework and JSP server site language both of which are not covered in the course syllabus and thus have enabled me go through a very intensive research and gain knowledge on various frameworks, languages, plugins and APIs.

## 5.5 Conclusion

The project in my view has been a success amidst a lot of challenges. Full Implementation of the system will pay tangible benefits to the Masinde Muliro University fraternity. It will make the university enjoys a competitive advantage among its counterparts since most of the universities have not implemented such a system.

## 5.6 Recommendations

This project is subject to improvement based on rising requirements. Even though the project was completed on the base of the requirement that were proposed, the system is very much open to improvement.

Masinde Muliro University should embrace and try to implement the systems made by student so that the knowledge body of MMUST can be greatly improved.

Funding of events geared towards solving problems of the society around the university should be harnessed which will improve the image of the university generally.

I would also like to recommend to the department to provide more guidance and materials about the methods of carrying out research and project report writing to students. This will go a long way in preparing students and enabling easy transition between project report writing, together with the rest of the deliverable items.

Finally students who have related projects should be assisted in the process of integrating them so that power of software’s developed locally can be harnessed.

## 5.7 Appendix

### 5.7.1 Project Schedule

Table 1: Project Schedule from week 1 to week 15

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | ***DURATION IN WEEKS*** | | | | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |
| project identification | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Feasibility study | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Requirements capture and analysis | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| General system design | | |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |
| ***Activity*** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| User interface design | | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| System coding | | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Module integration and testing | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Implementation | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| System handover | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Documentation | |  |  |  |  |  | | | | | |  |  |  |  |  |

### 5.7.2 Budget

Table 2: Project Budget

|  |  |  |
| --- | --- | --- |
| **Item** | **Quantity** | **Amount (ksh)** |
| Standard Personal Computer system | 1 | 25,000 |
| Software |  | 2,000 |
| External storage disk | 1 | 800 |
| Stationaries |  | 500 |
| Printing, photocopying, binding and printer |  | 4,000 |
| Internet connection facilitation(modem) |  | 3,000 |
| Miscellaneous |  | 2,000 |
| **Total** |  | **37,300** |

## 5.8 References

* Gerti Kappel et.al (2003): Web Engineering. *John Wiley &Sons Ltd*
* Mark Maslakowski (2000): Sam's Teach Yourself Mysql in 21 Days. *Sams Publishing*
* [www.w3schools.com/bootstrap/bootstrap\_navbar.asp](http://www.w3schools.com/bootstrap/bootstrap_navbar.asp)
* https://github.com/bbottema/simple-java-mail

# Iterative Model In Iterative model, iterative process starts with a simple implementation of a small set of the software requirements and iteratively enhances the evolving versions until the complete system is implemented and ready to be deployed. An iterative life cycle model does not attempt to start with a full specification of requirements. Instead, development begins by specifying and implementing just part of the software, which is then reviewed in order to identify further requirements. This process is then repeated, producing a new version of the software at the end of each iteration of the model.

# Iterative Model design Iterative process starts with a simple implementation of a subset of the software requirements and iteratively enhances the evolving versions until the full system is implemented. At each iteration, design modifications are made and new functional capabilities are added. The basic idea behind this method is to develop a system through repeated cycles (iterative) and in smaller portions at a time (incremental).

# Following is the pictorial representation of Iterative and Incremental model:

# CHAPTER 3

# 

# TUTORIALS POINT Simply Easy Learning Page 8

# Iterative and Incremental development is a combination of both iterative design or iterative method and incremental build model for development. "During software development, more than one iteration of the software development cycle may be in progress at the same time." and "This process may be described as an "evolutionary acquisition" or "incremental build" approach."

# In incremental model the whole requirement is divided into various builds. During each iteration, the development module goes through the requirements, design, implementation and testing phases. Each subsequent release of the module adds function to the previous release. The process continues till the complete system is ready as per the requirement.

# The key to successful use of an iterative software development lifecycle is rigorous validation of requirements, and verification & testing of each version of the software against those requirements within each cycle of the model. As the software evolves through successive cycles, tests have to be repeated and extended to verify each version of the software.

# Iterative Model Application Like other SDLC models, Iterative and incremental development has some specific applications in the software industry. This model is most often used in the following scenarios:

#  Requirements of the complete system are clearly defined and understood.

#  Major requirements must be defined; however, some functionalities or requested enhancements may evolve with time.

#  There is a time to the market constraint.

#  A new technology is being used and is being learnt by the development team while working on the project.

#  Resources with needed skill set are not available and are planned to be used on contract basis for specific iterations.

#  There are some high risk features and goals which may change in the future.

# Iterative Model Pros and Cons The advantage of this model is that there is a working model of the system at a very early stage of development which makes it easier to find functional or design flaws. Finding issues at an early stage of development enables to take corrective measures in a limited budget.

# The disadvantage with this SDLC model is that it is applicable only to large and bulky software development projects. This is because it is hard to break a small software system into further small serviceable increments/modules.

# 

# TUTORIALS POINT Simply Easy Learning Page 9

# The following table lists out the pros and cons of Iterative and Incremental SDLC Model:

# Pros Cons

#  Some working functionality can be developed quickly and early in the life cycle.  Results are obtained early and periodically.  Parallel development can be planned.  Progress can be measured.  Less costly to change the scope/requirements.  Testing and debugging during smaller iteration is easy.  Risks are identified and resolved during iteration; and each iteration is an easily managed milestone.  Easier to manage risk - High risk part is done first.  With every increment operational product is delivered.  Issues, challenges & risks identified from each increment can be utilized/applied to the next increment.  Risk analysis is better.  It supports changing requirements.  Initial Operating time is less.  Better suited for large and missioncritical projects.  During life cycle software is produced early which facilitates customer evaluation and feedback.

#  More resources may be required.  Although cost of change is lesser but it is not very suitable for changing requirements.  More management attention is required.  System architecture or design issues may arise because not all requirements are gathered in the beginning of the entire life cycle.  Defining increments may require definition of the complete system.  Not suitable for smaller projects.  Management complexity is more.  End of project may not be known which is a risk.  Highly skilled resources are required for risk analysis.  Project’s progress is highly dependent upon the risk analysis phase