



Strathmore
UNIVERSITY

Strathmore University
SU+ @ Strathmore
University Library

Electronic Theses and Dissertations

2016

A mobile based application for verification of legitimacy of degree certificates in Kenya

Ochieng, H. O.

*Faculty of Information Technology (FIT)
Strathmore University*

Follow this and additional works at: <https://su-plus.strathmore.edu/handle/11071/2474>

Recommended Citation

Ochieng, H. O. (2016). *A mobile based application for verification of legitimacy of degree certificates in Kenya* (Thesis). Strathmore University. Retrieved from <http://su-plus.strathmore.edu/handle/11071/4904>

This Thesis - Open Access is brought to you for free and open access by DSpace @ Strathmore University. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of DSpace @ Strathmore University. For more information, please contact librarian@strathmore.edu

A MOBILE BASED APPLICATION FOR VERIFICATION OF LEGITIMACY OF DEGREE
CERTIFICATES IN KENYA

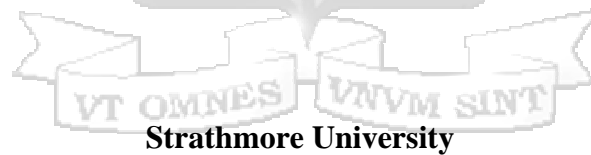
By

Harry Opiyo Ochieng

084953

**A Dissertation submitted in partial fulfilment of the requirement for the award of a Master
of Science Degree in Mobile Telecommunication and Innovation (MSc. MTI).**

Faculty of Information Technology



Strathmore University

April, 2016

This Dissertation is available for library use on the understanding that it is copyright material and that no quotation from the dissertation may be published without proper acknowledgement

DECLARATION

I certify that this research document is my original work and any part of it that is not my own has been duly referenced. I further certify that no material has previously been submitted and approved for the award of a degree by this or any other University. No part of this thesis may be reproduced without the permission of the author and Strathmore University.

Harry Opiyo Ochieng

Signature.....

Date:



This dissertation was reviewed and approved by the following:

Dr. Joseph Sevilla (PhD)

Director, @iLab Africa Research Centre

Strathmore University

Signature.....

Date:

DEDICATION

I dedicate this work to the Almighty God who gave me the favour and opportunity to do this masters, Safaricom and @iLabAfrica for the opportunity, support and training they offered for the attainment of this master.



ACKNOWLEDGEMENTS

First of all I would like to thank the Almighty God for giving me the opportunity to study this master's degree, and also for bringing this very good work he started to completion. This is a testimony that God is very faithful and his promises are yes and amen.

Secondly I thank my Family- my Dad and Mum (Mr & Mrs David Onyoo), my brothers (Mr & Mrs Raymond, Mr & Mrs Ronald and Mr & Mrs Jeffrey, Billy and Amollo) and all my sisters (Beatrice, Mildred, Nancy, Hellaine, Maureen and Terry) for their support, prayers and encouragement during the time I was doing this masters.

Thirdly special thanks go to my Project Supervisor Dr. Joseph Sevilla for his guidance and support that enabled me to finish this project.

I also thank my dearest friend Anne Oyamo and my close friends Collince Wadanda and Cosmas Ayieko for their prayers, encouragement and moral support to see that I successfully complete this project. I also thank my classmate and friend Philip Mudenyio for his spiritual, moral and technical support.

I would also like to thank the MSC.MTI 2014 full-time students and lecturers of Strathmore University for the technical and academic support I got from them to see the project come to completion.

Finally, I do not forget to thank CITAM Woodley Young Professional and Israel Bible study group for their prayers during this project.

ABSTRACT

Every company needs to hire competent and academically qualified staff in order to provide quality service delivery. Therefore companies rely on academic certificates for their prospective employees as a proof and measure of their academic qualifications. However, due to the high number of forged academic certificates in the job market, companies have always ended up hiring unqualified staff with forged academic certificates. This makes the companies to incur huge financial losses and experience low production outputs. Therefore, there is need for employers to verify academic certificates for their prospective employees in order to ascertain their legitimacy. However, these employers lack a uniform process and means for verifying the authenticity of academic certificates. The current systems for verification of academic certificates are time consuming, tiresome and expensive, making only few of the employers to verify certificates for their prospective employees.

This dissertation provides a detailed study of challenges faced in verification of academic certificates, techniques used in verification of academic certificates, how a mobile application for verification of academic certificates can be designed, developed and tested and if the mobile application solves the challenges faced using the current techniques for verification of academic certificates. Data was collected by use of online questionnaires. The data collected was used to find out the challenges faced in verification of academic certificates and the current techniques used in verification of academic certificates. Data analysis was done using Google analysis tools and the results obtained were used to formulate the system requirements and for designing the web and mobile applications. Iterative Software Development was adopted as the software methodology for developing the applications.

A mobile and web applications were developed to make verification of academic certificates faster, easier and affordable. The final prototype was tested to check if the requirements are met. Testing was conducted by both the developer and potential users of the application. Other tests included user testing and compatibility testing.

Keywords: Forgery, Academic Certificates, Universities, Counterfeit, Verification, Legitimate

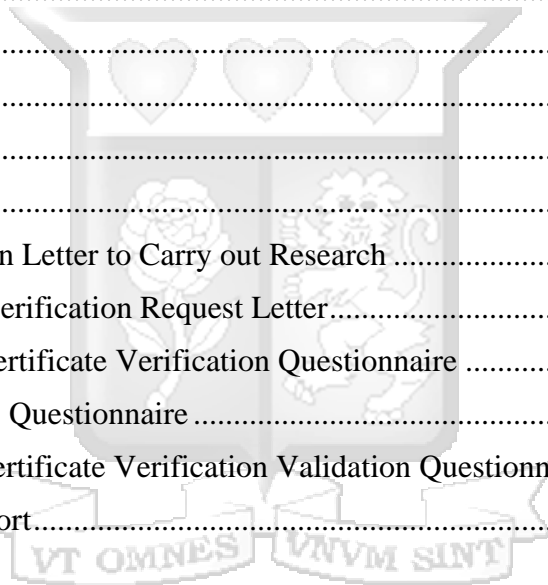
TABLE OF CONTENTS

DECLARATION	ii
DEDICATION	iii
ACKNOWLEDGEMENTS	iv
ABSTRACT	v
LIST OF TABLES	x
LIST OF FIGURES	xi
ABBREVIATIONS	xiii
CHAPTER 1: INTRODUCTION	14
1.1 Background	14
1.2 Problem Statement	14
1.3 Research Objectives	15
1.4 Research Questions	15
1.5 Research Justification.....	15
1.6 Scope and Limitations	16
CHAPTER 2: LITERATURE REVIEW	17
2.1 Introduction	17
2.2 Forgery of Academic Certificates	17
2.3 Types of Forged Academic Certificates.....	18
2.4 Existing Techniques for Verification of Academic Certificates	19
2.4.1 Radio Frequency Identification (RFID)	19
2.4.2 2D Barcodes	21
2.4.3 Online Verification.....	24
2.4.4 Manual Verification of Academic Certificates.....	25
2.5 Advantages and Disadvantages of Techniques for Verification of Academic Certificates	26
2.5.1 RFID.....	26
2.5.2 2D Barcodes	28
2.5.3 Manual Verification.....	28
2.6 Gaps and Limitations	29
2.7 Conclusions	29
CHAPTER 3: RESEARCH METHODOLOGY	31

3.1 Introduction	31
3.2 Agile Development Methodology	31
3.2.1 Planning Phase.....	32
3.2.2 Requirement Analysis Phase	32
3.2.3 Designing Phase	35
3.2.4 Building Phase.....	36
3.2.5 Prototype Evaluation and Testing.....	37
3.3 Conclusions	38
CHAPTER 4: REQUIREMENT ANALYSIS.....	39
4.1 Introduction	39
4.2 Functional Requirements.....	39
4.3 Non Functional Requirements.....	40
4.4 Type of Organisations	40
4.5 Departments	41
4.5 Roles in the Department.....	42
4.6 Number of Years Performing the Roles.....	42
4.7 Techniques for Verification of Academic Certificates	43
4.8 Academic Certificate Verification Process	43
4.9 Parameters Used for Verification of Academic Certificates.....	44
4.10 Time Taken for Verification of Academic Certificate	44
4.11 Cost Incurred in Verification of Academic Certificates.....	45
4.12 Cases of Academic Certificate Forgery	45
4.13 Challenges Experienced in Verification of Academic Certificates.....	45
4.14 Mobile Phone Ownership.....	46
4.15 Mobile Device Operating System	46
4.16 Use of Mobile Applications	47
4.17 Suitability of a Mobile Application for Academic Certificate Verification.....	47
4.18 Proposed Features for the Academic Certificate Verification System.....	48
4.19 Conclusions	48
CHAPTER 5: DESIGNING PHASE.....	50
5.1 Introduction	50
5.2 Systems Architecture.....	50

5.3 Systems Design	51
5.3.1 Use Case Diagram and Descriptions	52
5.3.2 System Sequence Diagram	58
5.3.3 Partial Domain Diagram	60
5.3.4 Context Diagram	60
5.3.5 Entity Relationship Diagram	62
5.3.6 Database Schema	64
5.3.7 User Interface Flow Diagram	65
5.4 Conclusions	74
CHAPTER 6: PROTOTYPE BUILDING, EVALUATION AND TESTING	75
6.1 Introduction	75
6.2 Implementation Environment	75
6.2.1 Mobile Application	75
6.2.2 Web Application	75
6.2.3 Database	75
6.3 Implementation Details	76
6.3.1 QR-Code Generation	76
6.3.2 The Mobile Application	76
6.3.3 The Web Application	81
6.4 System Testing	90
6.4.1 Introduction	90
6.4.2 Usability Test	90
6.4.3 Functional Testing	90
6.4.4 Compatibility Testing	93
6.4.5 Load Testing	94
6.4.6 Integration Testing	94
6.5 User Testing	95
6.5.1 User Interface Aesthetics	95
6.5.2 User Friendliness	95
6.5.3 Functionality	96
6.5.4 Acceptability	97
6.5.5 Validation	97

6.6 Conclusions	101
CHAPTER 7: DISCUSSIONS	102
7.1 Introduction	102
7.2 Findings and Achievements	102
7.3 Review of Research Objectives in Relation to the Mobile Application	104
7.4 Review of the Application in Relation to Current Methods Used for Verification of Academic Certificates	105
7.4.1 Advantages of the Application	106
7.4.2 Limitations of the Application.....	106
CHAPTER 8: CONCLUSIONS, RECOMMENDATIONS AND FUTURE WORK	107
8.1 Conclusions	107
8.2 Recommendations	107
8.3 Future Work	107
REFERENCES	109
APPENDICES	115
Appendix A: Authorization Letter to Carry out Research	115
Appendix B: Certificate Verification Request Letter.....	116
Appendix C: Academic Certificate Verification Questionnaire	117
Appendix D: User Testing Questionnaire	1
Appendix E: Academic Certificate Verification Validation Questionnaire.....	2
Appendix F: Turnitin Report.....	4



LIST OF TABLES

Table 5.1 Use Case Descriptions 56

Table 6.1 Creating User Account Test Case..... 91

Table 6.3 Logging In and Out Test Case 91

Table 6.4 Verify Certificate Test Case 91

Table 6.5 Reporting Fake Certificate Test Case 92

Table 6.6 View Verification Reports Test Case 92

Table 6.7 Manage Certificates Test Case 92

Table 6.8 Manage Users Test Case..... 92

Table 6.9 Android Platform Compatibility Test..... 93

Table 6.10 Web Browser Test 94



LIST OF FIGURES

Figure 2.1 Radio Frequency Identification (RFID) Adapted from Roberts (2006).....	20
Figure 2.2 Types of 2D Barcodes Adapted from Gao et al. (2007).....	21
Figure 2.3 A Sample QR Code Adapted from Narayanan, 2012.....	23
Figure 2.4 Development of a Degree Certificate Adapted from Singhal and Pavithr (2015)	24
Figure 2.5 Certificate Reference System adapted from Kenya Institute of Management (2016) 25	
Figure 4.1 Respondents Distribution in Different Types of Companies and Organisations	41
Figure 4.2 Respondents' Distribution in Company Departments	41
Figure 4.3 Respondents' Roles on Verification of Academic Certificates.....	42
Figure 4.4 Number of Years Respondents Has Performed the Task	43
Figure 4.5 Techniques Used for Verification of Academic Certificates in Kenya.....	43
Figure 4.6 Parameters Used for Verification of Academic Certificates	44
Figure 4.7 Respondent's Smart Phone Ownership.....	46
Figure 4.8 Respondents' Smart Phone's operating System.....	46
Figure 4.9 Respondents' Use of Other Mobile Applications	47
Figure 4.10 Suitability of the Mobile Application in Verification of Academic Certificates	48
Figure 5.1 System Architecture for The Proposed Application.....	51
Figure 5.2 Use Case Diagram	60
Figure 5.3 System Sequence Diagram.....	62
Figure 5.4 Partial Domain Diagram.....	63
Figure 5.5 Context Diagram.....	64
Figure 5.6 Entity Relationship Diagram.....	66
Figure 6.7 Web Application Dashboard	83
Figure 6.8 Web Application User Login.....	82
Figure 6.9 User Management.....	84
Figure 6.10 Adding a New User	84
Figure 6.11 Add Certificate	88
Figure 6.12 Update and Delete Certificate	88
Figure 6.13 Reports on Verified Certificates.....	89
Figure 6.14 Reports on Reported Counterfeit Certificates	90

Figure 6.15 UI Aesthetic Feedback 95
Figure 6.16 User Friendliness Feedback..... 96
Figure 6.17 Test Results on Functionality of the Mobile Application 97



ABBREVIATIONS

RFID - Radio Frequency Identification

2D - Two dimensional

QR - Quick Response

SHA - Secure Hash Algorithm

WES - World Education Services

USA - United States of America

US - United States

CUE - Commission for University Education

SDM - Software Development Methodology

RAD - Rapid Application Development

CMS - Content Management System\

DSDM- Dynamic Systems Development Method

UML - Unified Modelling Language

SDK - Software Development Kit

JSON- JavaScript Object Notation

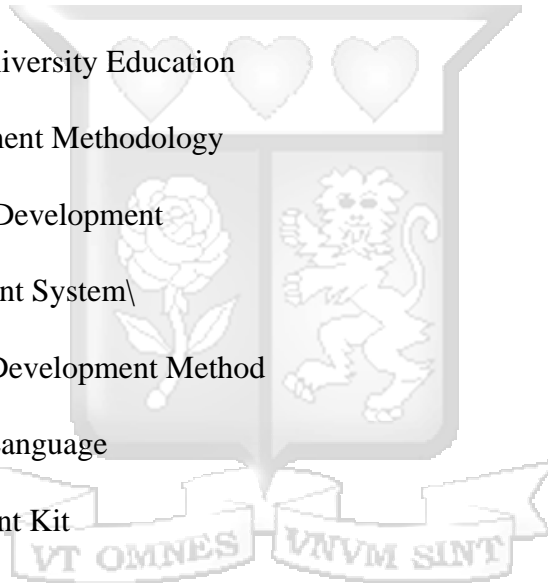
ADT - Android Development Tools

PHP - Hypertext Pre-processor

HTTP - The Hypertext Transfer Protocol

ERD – Entity Relationship Diagram

SSD – System Sequence Diagram



CHAPTER 1: INTRODUCTION

1.1 Background

Every company need to hire trained and academically qualified staff in order to provide quality service delivery (Allen, 2012). Levels of Academic qualifications in Kenya include PhD, Master degree, Bachelor Degree, Higher Diploma, Diploma, Certificate, Kenya Certificate of Secondary Education and Kenya Certificate of Primary Education (Nuffic, 2015). Currently there is tremendous increase in the production of fake academic certificates in Kenya and all over the world, and companies are incurring financial and productivity losses as a result of hiring unqualified employees (Glasner, 2015).

Forgery is making of a false document with intent to defraud or deceive (Government of Kenya, 2010). Forgery of academic certificates leads to hiring of unqualified employees. Over 50% of employers in each of the ten biggest world economies have been victims of bad hires which always lead to massive financial loss and low productivity in addition to information theft, and infrastructure damage (Glasner, 2015).

It is necessary for employers to verify academic certificates for prospective employees, however, the current systems for verifying academic certificates are time consuming and expensive, resulting to low number of certificates being verified. Therefore there is need for a fast and reliable system to ease the verification of academic certificates.

1.2 Problem Statement

Generation of fake academic certificates has become a problem in all over the world and in Kenya. Companies and organisations are incurring serious financial and productivity problems as a result of hiring unqualified employees (Quest Staffing Solutions, 2014).

Verification of academic certificates for prospective employees has become a huge problem for companies and organisations (Gupta, 2013). This problem is facilitated by the lack of an effective and uniform process for prospective employers to verify the legitimacy and authenticity of academic certificates. Because of this, many employers usually fail to verify the credentials of their prospective employees (Garwe, 2015). This presents a pressing need for universities to adopt an automated

system for easy verification of their academic certificates. Therefore there is an opportunity to come up with a mobile application to solve this problem.

1.3 Research Objectives

- I. To identify the challenges facing verification of academic certificates.
- II. To analyse the current systems used for verification of academic certificates.
- III. To design, develop and test a mobile application for verification of academic certificates.
- IV. To validate that the mobile application for verification of academic certificates solves the challenges faced using the current techniques for verification of academic certificates.

1.4 Research Questions

- I. What are the challenges facing verification of academic certificates?
- II. What are the current systems used for verification of academic certificates?
- III. How can a mobile application for verification of academic certificates be designed, developed, and tested?
- IV. Does the mobile application solve the challenges faced using the current techniques for verification of academic certificates?

1.5 Research Justification

In order to reduce the current losses and threat that forgery of academic certificates possess to companies, academic institutions, legitimate graduates and the society, there is need to verify academic certificates presented by job candidates. Providing an efficient and uniform process for prospective employers to verify academic certificates will ensure that all employees in an organisation are qualified and competent to carry their roles. This will prevent financial and productivity losses that are incurred as a result of hiring unqualified employees.

Using a mobile application to verify academic certificates will be fast, effective, efficient and affordable. This is because of the high adoption of mobile phone technology and the easy accessibility of mobile phones in Kenya. This study aims to build a mobile-based solution that takes advantage of the increasing use of mobile phones to ease the task of verification of academic certificates in Kenya.

1.6 Scope and Limitations

The application will be implemented for Android operating system and will only be used to verify degree certificates for universities in Kenya. The solution will be customized for Kenyan companies.



CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

This section discusses forgery of academic certificates, which includes the major reasons why people forge academic certificates, types of forged academic certificates, and some of the negative impacts of forgery of academic certificates. It then discusses the existing techniques for verification of academic certificates and the challenges faced in verification of academic certificates using the current techniques. Finally it discusses the adoption of mobile phone technology in Kenya.

2.2 Forgery of Academic Certificates

The 21st century has experienced a lot of cases of forgery of academic certificates (Victor & David, 2014). Glasner (2015) supports this by noting that the increase in the production of fake academic certificates has been tremendous all over the world. According to Grolleau, Lakhali, and Mzoughi (2008), the United States alone was reported to have over two million fake academic certificates. Herly (2005) adds that between 25 and 35 percent of candidates in Australia have either falsified or exaggerated their academic credentials to obtain employment.

Similar trends of forgery of academic certificates have been noted in Kenya. Garwe (2015) observes that more than two hundred fake degrees submitted by prospective lecturers and professors from Kenya were discovered by The University of Dodoma in Tanzania. In 2012, the minister for Public Service issued a warning that civil servants who used forged academic certificates to acquire government jobs would be interdicted. This followed with an audit of academic certificates for over 230,000 civil servants in the country (Daily Nation, 2012). It was also discovered that Job applicants in Kenya engage in several cases of impersonations and forgery of academic certificates (Mathew, 2014).

There are several reasons that lead to forgery of academic certificates. The major reasons include the desire to obtain employment and lack of a uniform process and means to verify the authenticity of academic and professional qualifications by prospective employers (Garwe, 2015). Glasner (2015) supports this by noting that job candidates forge academic certificates in order to get an edge in the current competitive job market. Gware (2015) adds that the forgery is motivated by unemployment since the high unemployment rate in most countries is making employers to consider only candidates with high academic qualifications.

There are several negative consequences that results from forgery of academic certificates. According to Quest Staffing Solutions (2014), forgery of academic certificates leads to serious financial and productivity problems. In support of this, Glasner (2015) notes that companies in the United States lose up to US\$50,000 and also experience loss of productivity for a single employee with a forged academic certificate. In addition, forgery of academic certificates devalues the institution where the qualification is purported to be obtained and also ruins the reputation of the legitimate students of that particular institution (Garwe, 2015). Lastly, Gollin, Lawrence, and Contreras (2014) observe that forgery of academic certificates poses a big threat to the public safety through recruitment of unskilled people.

Production and Circulation of fake academic certificates therefore poses a big problem to the society and to the economy of a country and also to the integrity of both the academic institutions and their legitimate certificate holders. This therefore presents a serious need for verification of academic certificates for prospective employees.

2.3 Types of Forged Academic Certificates

Garwe (2015) defines an authentic, genuine or valid academic qualification as a qualification that is legally awarded by an academic institution that is legally authorised to award such qualification. Grolleau, Lakhali, and Mzoughi (2008) defines fake degrees as counterfeit degrees bearing the names and signs of real and fully accredited universities or degrees from bogus or unaccredited universities, sold outright and that can require some academic work, but significantly less than comparable to legitimate accredited programs.

There are five major types of forged academic certificates as defined by Garwe (2015) and Grolleau et al. (2008)

i. Degree or Diploma Mills

Thus refers to schools or universities that sells or awards diplomas requiring less than the minimum level of standard academic work. They are normally unaccredited or accreditation bodies. They generate and sell fake academic qualifications to individuals who have not undergone the required studies.

ii. Counterfeit degrees

Refers to fake academic documents designed to deceive as have been issued from a valid academic institution. They are degrees that are meant to give the impression of academic achievement, but in reality represent little or no study.

iii. Modified Documents

This refers to valid academic documents which have been altered by performing omissions and additions on the legitimate documents. Changes may include name of candidate, enrolment and graduation dates, grades, course content and date of birth.

iv. Produced in-house

Refers to fake academic documents manufactured by employees of the academic institution. These documents can either be modified or fabricated but appear on authentic paper complete with institutional seals, stamps and appropriate signatures. The Grades in such documents are usually inflated, credits falsified and degrees awarded for incomplete programs.

v. Translations

Refers to academic documents inaccurately translated with the aim of misleading and falsifying them. This is done by altering grades and course titles to match those in the receiving country.

2.4 Existing Techniques for Verification of Academic Certificates

2.4.1 Radio Frequency Identification (RFID)

The RFID technology is a means of gathering data about a certain item without the need of touching or seeing the data carrier, through the use of inductive coupling or electromagnetic waves. The data carrier is a microchip attached to an antenna (together called transponder or tag), the latter enabling the chip to transmit information to a reader (or transceiver) within a given range, which can forward the information to a host computer (Ilie-zudor, Kemeny, Egri, & Monostori, 2006).

RFID systems consist of small transponders/tags (attached to physical objects) and readers/transceivers interacting with objects/certificates and database systems to provide an information or operational function. When wirelessly interrogated by RFID transceivers/ readers, tags respond with identifying information that is associated with arbitrary data records, providing automatic identification system

similar to optical bar codes (Weis, 2007). RFID represents an improvement over bar codes in terms of non-optical proximity communication, information density, and two-way communication ability (Roberts, 2006).

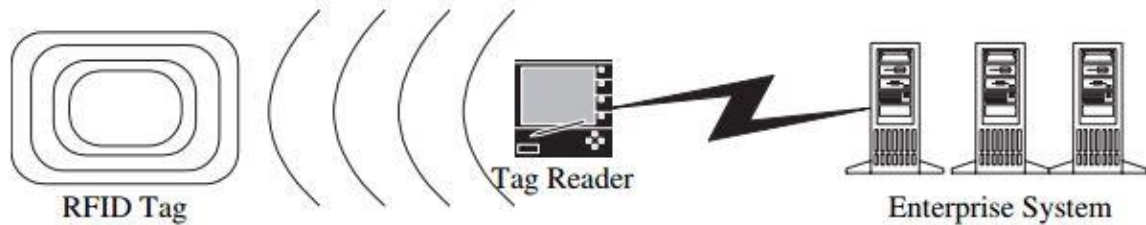


Figure 2.1 Radio Frequency Identification (RFID) Adapted From Roberts (2006)

The origins of RFID technology dates back to 19th century when great scientific advances in electromagnetism that laid the foundation for modern radio communications were made. These advances include discovery of electronic inductance by Michael Faraday, formulation of equations describing electromagnetism by James Clerk Maxwell, and the experiments by Heinrich Rudolf Hertz's validating Faraday and Maxwell's predictions. Their discoveries laid the foundation for modern radio communications (Weis, 2007).

RFID was used during World War II to identify 'friendly' aircraft and has been used into other application areas which include toll payment, supply chain management, cashless payment, ticketing, brand authentication, security access, patron identification and amusement parks, tracking animals, tagging new born babies with their mothers, controlling access, managing inventory and certificates and many more (TaTa Consultancy Services, 2009).

RFID has also been used in verification of academic certificates, in a project known as "Smart DEGREE". Smart DEGREE uses an embedded passive 13.56 MHz RFID tag. Each tag has 4-8 kilobytes of memory and is encoded with the certificate holder's name, date of graduation, type of degree and entire transcript, photograph and the biometrics (fingerprints) of the holder. All these information is digitally signed by the university authorities. The fingerprint authentication is combined with the digital encryption to authenticate the information in the degree certificate. Using RFID reader one can easily access the information from the RFID Tag to verify the authenticity of the certificate (TaTa Consultancy Services, 2009).

2.4.2 2D Barcodes

2D barcodes or matrix codes are symbologies that are capable of storing more data than 1D barcodes. The need for storing more data in barcodes led to the development of 2D barcodes as an improvement of 1D barcodes. 2D barcodes can store large amount of data in a small area to support information distribution and detection without accessing a database. Two dimensional (2D) barcodes was invented at the end of 1980s, and are of two types. The first type is stacked 2D barcodes, for example Code 49 and PDF417. The second type is Matrix 2D barcodes, for example Data Matrix and QR Code (Gao, Prakash, & Jagatesan, 2007).



Figure 2.2 Types of 2D Barcodes Adapted From GAO Et Al. (2007)

Gao et al. (2007) notes that 2D barcodes has been used in for many applications which include:

- i. *Wireless advertising and marketing*

2D barcode is one of best cost-effective advertising and marketing tool for advertisers and manufactures. A customer can easily input a 2D barcode on a product advertisement by use of a mobile camera phone, to find more product information from the barcode. When the customer likes the product, a trading transaction can be done with the backbone M-commerce application system.

- ii. *Wireless trading (pre-sale, sale-and-buy, post-sale)*

Using 2D Barcodes on products and goods, mobile customers can find more detailed product information. Using mobile camera phones, customers can easily scan a 2D barcode of a product to find more detailed information about each product, which

include producers, harvest date, shipping date, and agricultural chemicals in each product.

iii. Product information tracking and checking for mobile users.

Examples include an application that can be used to trace the fishery products using QR codes, CyberCodes used for indoor navigation or indoor guidance, for instance, CyberCode tags are printed on the items inside a museum. Visitors can then retrieve the relating information by scanning the CyberCode tags on the items.

iv. Mobile security

An example is the system called Seeing-Is-Believing. The system uses 2D barcodes and camera-phones to implement a visual channel for authentication and demonstrative identification of devices.

2D barcodes have also been used in verification of academic certificates and academic transcripts as explained below:

a) Stacked 2D barcodes

The information on the academic certificate/transcript is presented as a 2D barcode and printed on the bottom or top side on the academic certificate. A centralized document authentication system is then created to store information of certificates. This centralized authentication system serves users through an internet network. When an academic certificate need to be verified, the 2D barcode is read by either barcode scanner or smart phone with a camera and then the data is transmitted over the secure network to get a response from the centralized authentication system. The returned data is then manually compared with the certificate being verified to determine the authenticity of the certificate (Hewlett-Packard, 2006).

b) QR Code

The Quick Response (QR) Code is a 2D barcode which consists of a black square pattern on white background and it contains information in the vertical direction as well as the horizontal direction. QR code was developed as an improvement to the 1D barcode because it can contain more information (Singhal & Pavithr, 2015).



Figure 2.3 A Sample QR Code Adapted From Narayanan (2012)

QR code is used in verification of academic certificates. Below is a procedure for generation of degree certificates having QR codes as outlined by Singhal and Pavithr (2015).

- A message M is composed using the details such as name, enrolment number and of the student.
- A hash value of the message M is then obtained using SHA-256.
- The university private key is then used to sign the obtained hash value of the message M to create a digital signature of the message M.
- Message M along with digital signature are combined together and fed into QR code generator. The system also makes an entry of message M into the university database.
- The QR code generator generates a QR code which stores the message M and the digital signature.
- The QR code is then printed on the certificate.

In order To verify the authenticity of the academic certificate, Singhal and Pavithr (2015) outlines the following steps;

- The QR Code is scanned and then decrypting of the signature from the university's public key is done in order to generate the hash value (M2).
- A new hash value (M1) is then generated using the message M and compared with the decrypted signature's message digest (M2).
- If both the values are identical then the certificate is verified as authentic.
- However, if the hash values are different, then the certificate is verified as fake, forged or tampered with.

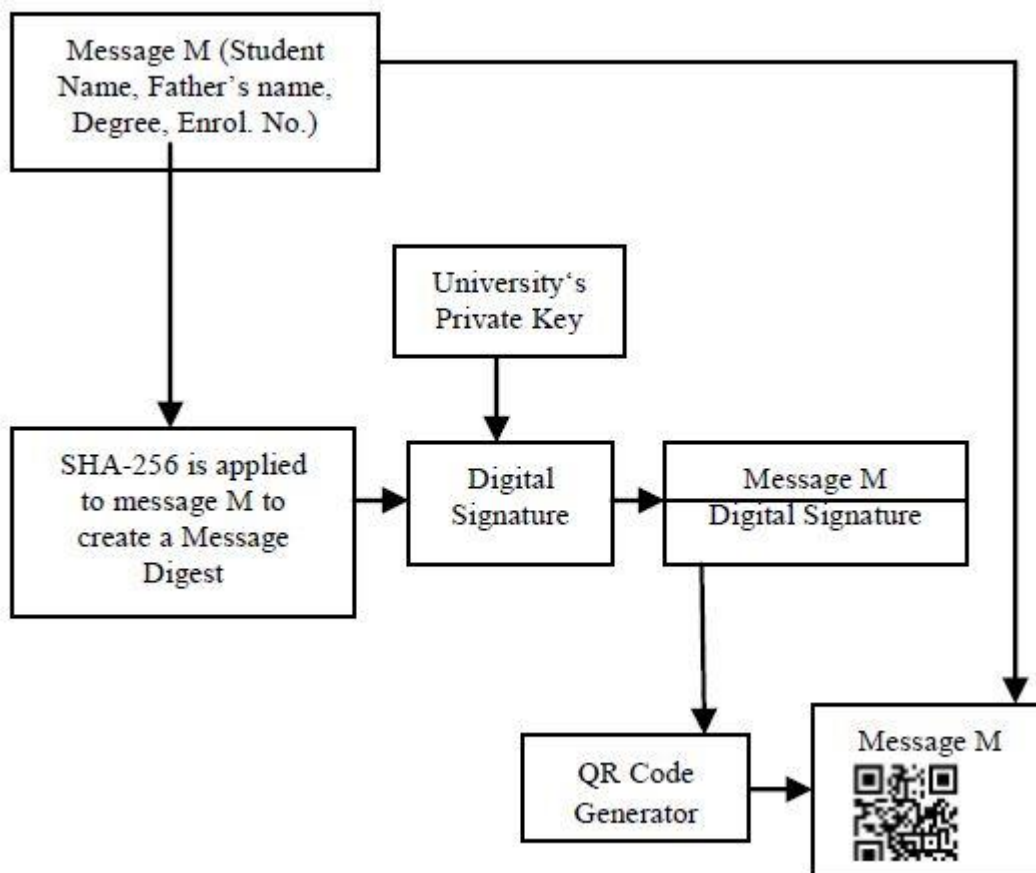


Figure 2.4 Development of a Degree Certificate Adapted From Singhal and Pavithr (2015)

2.4.3 Online Verification

A number of universities provide online web portals to assist employers, staff of other higher learning institutions or members of the public to verify claims to academic qualifications conferred by those universities (National University of Singapore, 2016). This makes the verification process fast and easy as it eliminates the time consuming manual verification. It also reduces the cost of verification considerably compared to the cost incurred using the manual process (The Hindu, 2013)

To verify an academic certificate using the web portal, one has to complete an online verification request by providing Student ID or Number (if known), Degree/s to be confirmed, Date of degree conferment and the Details of enquirer among others depending with the university where the verification is being done. Using this information, A search into the university database is made, if there is a marching record in the database, the certificate is verified as legitimate, while if there is no march, the certificate is verified as fake (National University of Singapore, 2016).

Certificates Reference System

Please key in the certificate number to confirm the details with our database.

This Verification is for Certificates issued from June 2005 to date. For previous certificates contact Examination Department

Certificate No.

Or

Admission Number

For further enquiries contact the "Head of Examinations, KIM" or the nearest KIM branch.

[Back to KIM](#) | [Feedback](#)

Figure 2.5 Certificate Reference System Adapted From Kenya Institute of Management (2016)

2.4.4 Manual Verification of Academic Certificates

2.4.4.1 Verification by Academic Institutions

An academic certification is an official document provided by the University Registrar verifying dates of attendance, award of degree, and/or student status (full-time or part-time) by semester (Columbia University, 2016).

For such academic certificates to be verified, Employers, agencies or persons seeking for verification of the documents must submit a written request for verification of the certificate to the registrar of the university that issued the certificate. This request is sent together with a copy of the certificate to be verified and the university verification fee where this applies (Embassy of India, 2016).

These documents can be sent by fax, email, post or using courier services. The Verification requests are addressed to the title of the officer who issued and signed the document. Once the request is received, the university registrar checks their records to verify the legitimacy of the certificate and the results is communicated back to the requester (Kenyatta University, n.d).

2.4.4.2 Third Party Verification

This refers to use of companies or organisations that offer services for verification of academic certificates. Some of these organisations acts as agents of participating academic institutions on whose behalf data is captured and disclosed to third parties, in compliance with statutory guidelines (Qualifications Verification Services, 2016).

World Education Services (WES) is an organisation that verifies international academic credentials in USA. This is done by requesting institutions abroad to send transcripts directly to US institutions. The mode of delivery may be by mail or by electronic means that is approved. An official transcript must bear the signatures and seal of the institution that issued it. It is upon the WES to determine whether it should be accepted as official. In detecting fraudulent credentials, the WES scrutinizes each document for inconsistencies and Credentials are accepted only if they are issued by authorized educational institutions (World Education Service, 2008).

In Kenya, the Commission for University Education (CUE) is tasked with recognition and equation of degrees, post graduate diplomas and post graduate certificates awarded by foreign universities and institutions in accordance with Section 5. (1)(g) Of the Universities Act No. 42 of 2012, and the universities regulations, standards and guidelines set by the Kenya, Commission for University Education (Commission For University Education, 2012).

2.5 Advantages and Disadvantages of Techniques for Verification of Academic Certificates

2.5.1 RFID

The following are some of the advantages RFID (Kaur, Sandhu, Mohan, & Sandhu, 2011)

- Tag detection not requiring human intervention reduces employment costs and eliminates human errors from data collection
- As no line-of-sight is required, tag placement is less constrained
- RFID tags have a longer read range than barcodes
- Tags can have read/write memory capability, while barcodes do not
- An RFID tag can store large amounts of data additionally to a unique identifier

- Unique item identification is easier to implement with RFID than with barcodes
- Its ability to identify items individually rather than generically.
- Tags are less sensitive to adverse conditions (dust, chemicals, physical damage etc.)
- Many tags can be read simultaneously
- RFID tags can be combined with sensors,
- Automatic reading at several places reduces time lags and inaccuracies in an inventory
- Tags can locally store additional information; such distributed data storage may increase fault tolerance of the entire system
- Reduces inventory control and provisioning costs
- Reduces warranty claim processing costs.

The following are some of the disadvantages of RFID (Kaur et al., 2011).

- Standardisation- the sparse standards leave much freedom in the choice of communication protocols and the format and amount of information stored in the tag.
- RFID tags are expensive
- Collision- Attempting to read several tags at a time may result in signal collision and ultimately to data loss.
- Frequency The optimal choice of frequency depends on several factors, such as Transmission mode, Behaviour of tagged goods and environment and International standards in frequency allocation.
- Faulty manufacture of tags - Manufacturing of tags is not yet 100% failure-free today
- Faulty or deficient detection of tags -Tags may be damaged during usage.
- Adverse conditions of the environment and improper placement may corrupt reading.
- Registration of data from tags which pass within range of an RFID reader accidentally.
- Reader malfunction cannot be predicted or completely avoided, making alternative fall back measures (such as barcodes) necessary for the case of reader failure.

2.5.2 2D Barcodes

According to (Adaptalift, 2012), the following are the advantages of barcodes

- Much smaller and lighter than RFID tags and therefore easier to use.
- Less expensive than RFID tags
- Barcodes work with the same accuracy on various materials in which they are placed.
- Barcodes are a universal technology in that they are the norm for retail products; stores that own a barcode reader can process barcodes from anywhere in the world.
- Barcode accuracy is the same or even better than RFID tags.
- Barcode s are found on almost every item and there are no privacy issues involved with its use

According to (Adaptalift, 2012), the following are the disadvantages of 2D barcodes

- They are very labour intensive; as they must be scanned individually.
- Barcodes have less security than RFID; as they can be more easily reproduced or forged.
- Barcodes are more easily damaged; as the line of sight is needed to scan, the printed bar code has to be exposed on the outside of the product.
- If a barcode is ripped or damaged there is no way to scan the product.

2.5.3 Manual Verification

According to Kenyatta University (n.d), the following are the challenges faced using the current methods for verification of academic certificates in Kenya.

- Verification is a lengthy, costly, and labour intensive process
- Some organisations and institutions choose to respond to document verification request only if they have authorisation from the certificate holder
- Institutions are asking for a verification fee payment often to be made to a financial institution outside Kenya in local currencies (i.e. Indian rupees, Chinese Yuan etc.).This slow down the document verification process, resulting in unnecessary delays.
- Transcripts, presumably received directly from the issuing institution, fail to meet all the criteria of an official l document

- Documents received provide information that is not consistent with other information already on record i.e. disparities

2.6 Gaps and Limitations

Review of existing techniques for verification of academic certificates has shown that the approaches that are currently used for verification of academic certificates include use of RFID, 2D barcodes (Stacked 2D barcodes and QR code), online verification and the manual process.

The manual process for verification of academic certificates is done by the academic institutions that issued the certificates and qualifications verification companies. This method is time consuming, tiresome and expensive (The Hindu, 2013).

Use of RFID is very expensive and therefore not affordable since the RFID tags are expensive compared to barcodes, it also requires separate reader for reading the tags and a sophisticated software which is difficult to implement, and finally it is difficult to implement RFID due to lack of regulatory standards (Kaur et al., 2011).

Barcodes have less security than RFID and can be more easily reproduced or forged. They are also more easily damaged; as the line of sight is needed to scan, the printed bar code has to be exposed on the outside of the product and again If a barcode is ripped or damaged there is no way to scan the product (Adaptalift, 2012).

The online verification (web portal) bridges the gaps and limitations in RFID, 2D barcodes and the manual process. This is because it is fast, affordable and cannot be forged. However, at present, there is no unified system for online verification for academic certificates for all the universities in Kenya. This research will therefore improve on the online verification and QR-Code verification by implementing a mobile application for verification of the legitimacy of academic certificates. Using a mobile application will maximise on the advantages of online and 2D verification and also bridge their gaps and limitations by providing a unified system for verification of academic certificates for all universities in Kenya and providing a verification technique that cannot be forged.

2.7 Conclusions

The current methods for verification of academic certificates are slow, unreliable and expensive. The proposal to come up with a mobile application for verification of academic certificates is more justified given the costly and unreliable alternatives that RFID, 2D barcodes and the manual techniques provide. A mobile application for

verification of academic certificates combines the benefits of other techniques which include affordability; efficiency and security. In addition, it provides a unified system for verification of academic certificates for all universities in Kenya.



CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

This chapter discusses the methodology used in carrying out the research in line with the research questions. The methodology aimed at answering the following research questions:

- i. What are the challenges facing verification of academic certificates?
- ii. What are the current systems used for verification of academic certificates?
- iii. How can a mobile application for verification of academic certificates be designed, developed, and tested?
- iv. Does the mobile application solve the challenges faced using the current techniques for verification of academic certificates?

3.2 Agile Development Methodology

Agile methods are a subset of iterative and evolutionary methods and are based on iterative enhancement and opportunistic development processes. Each iteration is a self-contained, mini-project with activities that span requirements analysis, design, implementation, and test and each of the iterations leads to an iteration that integrates all software across the team and is a growing and evolving subset of the final system. The purpose of having short iterations is so that feedback from iterations N and earlier, and any other new information, can lead to refinement and requirements adaptation for iteration N + 1 (Boehm, 2007).

Principles of agile development is Active user involvement is imperative, this relates to the users giving inputs with regards to the developments made on the application at a certain stage. The team must be empowered to make decisions; it should be easy to make decision and hence changes easily made to the product without having to follow long procedures (VIJAYASARATHY & TURK, 2008)

Agile Methodology suited this research appropriately because the following reasons as outlined by (Petersen & Wohlin , 2009).

- The methodology helps teams stay competitive and throughout long projects
- Changes can be made to the applications and not have such a long impact.
- The methodology encourages participation from clients and hence user acceptance is almost guaranteed.
- Unlike the Waterfall and other old Methodologies where the requirements are to be stated at the beginning of development, then the development divided

into phases and assigned to various developers who would discuss after completion of those phases. Agile helps to remove this by making communication easy among the teams and changes that should be made are easy.

Agile development methodology has got five main phases which include Planning Phase, Requirement Analysis Phase, Design Phase, Building Phase and lastly Testing Phase (VIJAYASARATHY & TURK, 2008)

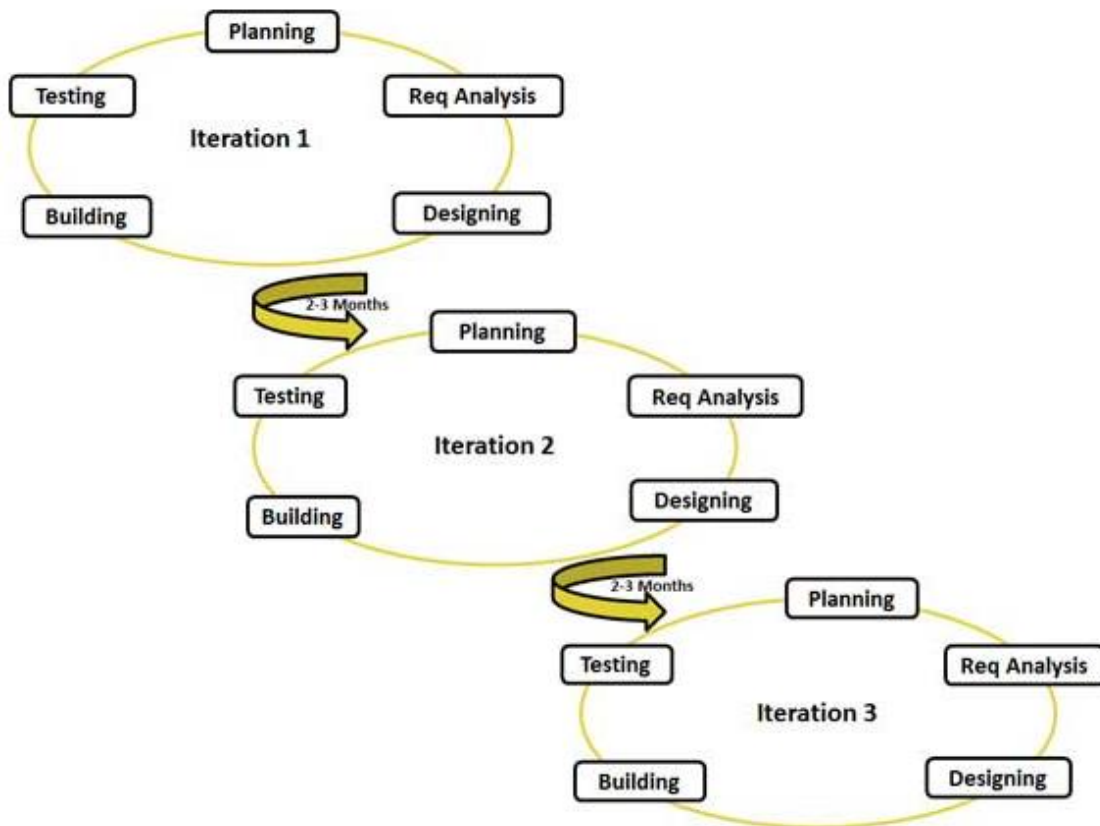


Figure 3.1 Agile Software Development Methodology Adapted From Agile Methodology (2016)

3.2.1 Planning Phase

This is the initial phase of the methodology and its main function is to facilitate in planning of how the entire process will be undertaken (Highsmith, 2011). Planning helped to identify the resources that were needed to build the system.

3.2.2 Requirement Analysis Phase

This is the second phase which involves analysing the requirements of the system or what the system is expected to do. Analysis helped to reveal important information like what environment was needed to develop and test the application, what

parameters that needed to be in place for the successful development and what exactly does the client want.

Information on verification of academic certificates was collected from respondents who included employees from universities, employer companies, recruitment agencies and qualifications verification companies that are located in Nairobi. The information was collected through the use of online questionnaires and document review. These methods were chosen because of their high chance in providing accurate information, which would be helpful in understanding the scenario on the ground, as well as provide information which would be useful in coming up with requirements of the application.

Online Questionnaires in appendix C was also administered to respondents who included academic registrars of universities, human resource managers of employers companies and employees of both recruitment agencies and qualifications verification companies. This helped the researcher to identify the various challenges faced in verification of academic certificates and the current techniques used for verification of academic certificates.

The researcher also reviewed both secondary and primary sources of information which included journals, books, academic articles and previously done research on verification of academic certificates, which helped to identify the current techniques used for verification of academic certificates which are documented in the reviewed documents.

Questionnaire in Appendix D was also sent out to end users of the application to test for user satisfaction and finally, the questionnaire in Appendix E was sent to the end users of the application to validate if the developed mobile application solves the challenges faced using the current techniques for verification of academic certificates.

3.2.2.1 Location of Study

The location of study for the research was universities, employer companies, recruitment agencies and qualifications verification companies that are located in Nairobi. Nairobi was chosen because it is the capital city of Kenya and most of headquarter offices for employer companies, recruitment agencies and qualifications verification companies are located in it and also most recruitment for all employees are carried out in the headquarter offices. In addition, most of the main campuses of top universities in Kenya are located within Nairobi and its neighbouring towns. Therefore, Nairobi was the most convenient place to carry out the research.

3.2.2.2 Sampling Strategies

In this study, stratified random sampling was used to come up with the sample population. In this technique the target population is divided into groups based on relevant characteristics, then participants selected from these groups. This is the appropriate sampling strategy because it ensures people from specific subgroups (in this case departments) are adequately represented within the sample space. Moreover, it ensures that all aspects of the research are adequately covered.

3.2.2.3 Target Population

The target population is the group of elements to which the researcher wants to make inference (Fricker, 2013). The target population was split into two groups, first group was before the application was developed to determine the right features and development environment of the application, then second group was after the development of the application to verify the application functions as required.

The first group was split into four categories; universities, employer companies, qualifications verification companies, and recruiting agencies in the entire country. The universities were targeted because they have the certificates to be verified and they also carry out verification of their certificates to employers, the employer companies were targeted because they verify academic certificates of their prospective employees. Recruitment agencies and qualifications verification companies were targeted because they carry out verification of academic certificates for employer companies during recruitment of new employees. The target population comprised of 20 academic registrars in universities, 10 human resource managers from employer companies and organisations, 10 employees from recruitment agencies and 10 employees from qualifications verification companies. This was resulted to a target of 50 respondents in total. This formed a representative sample for the entire country and was used to give requirement specification of the system and appropriate feedback on the prototype.

3.2.2.4 Sample Size

A total of 20 respondents were involved in this study. These respondents were selected using Stratified random sampling strategy. They included employees of universities, employer companies, recruitment agencies and qualifications verification companies that are located in Nairobi. This was the appropriate sample size because the respondents were directly involved in the certificate verification process.

3. 2.2.5 Data Analysis and Functional Model

Google Forms were used to collect and analyse data from pre-formulated questionnaires after which qualitative data was represented as graphs and charts to provide clear interpretation of the findings.

Object oriented analysis was employed to ensure all user requirements were modelled and analysed comprehensively. Objects were also developed and their relationship identified. Functionality of the system were modelled with the use of use case diagrams and use case descriptions. The flow of the system was be modelled using the system sequence diagram. For the database the entity relationship diagram with the tables, their attributes and their relationship were shown.

3.2.3 Designing Phase

After the requirements had been analysed, then design of the system was done. System analysis and design methods were applied to guide the researcher to understand what was needed and to analyse data flow systematically, process data, store data and to output information in context of the study (Kendall & Kendall, 2013).

Google Forms, online data analysis tools was used to collect and analyse data from pre-formulated questionnaires. Qualitative data was represented as graphs and charts to provide clear interpretation of the findings.

Object oriented analysis was employed to ensure all user requirements were modelled and analysed comprehensively. Objects were developed and their relationship identified.

Unified Modelling Language (UML) was used as the modelling language to model analysis and design diagrams and to offer clarifications on user requirements.

Use case diagram and its corresponding use case descriptions was used to model system functionality. The system functionality was identified and partitioned using the use cases and this enabled the researcher to separate the system into actors and use

cases. The use cases were represented as a text that describes the action the user is effecting on the system.

System sequence diagram showing information passing between the main entities of the system was used to model the system flow. It showed how objects interact with each other and in an orderly way. This enabled the researcher to display how the system works from one point to another.

Entity relationship diagram showing the tables, their attributes and their relationships was used to model the database. This enabled the researcher to create different objects that actually have relationships in real life. The table structure was modelled using the database schema showing the fields, data type and its description.

3.2.4 Building Phase

This is actual implementation phase of the designs that were done on the previous phase. The database was created with the guidance from Entity Relation Diagram bringing out all the tables and their relationships, the design mock-ups were transformed to actual system windows and the functionality of the system was added.

a) Prototype Development

This involved coming up a mobile and web application. Both the mobile and web application were connected to the central database. The application development environments that were employed include:

i. Mobile Application

The mobile application was developed for the Android operation system. Java programming language was used for the development of the mobile client application. JavaScript Object Notation (JSON) was used as the web service, which provided an interface between the mobile application and the database. The application was compiled and tested using the android Software Development Kit (SDK) emulator and an android device. Android was chosen as the client application because of the flexible SDK, availability of Android Development Tools (ADT) and availability of abundant support from online developer communities.

ii. Web Application

The web application was built using Laravel 5.1 content management systems (CMS) written in Hypertext Preprocessor version 5 (PHP 5). Reasons for choosing Laravel 5.1: it is open source, it provides security and user management as part of the CMS, it offers good performance, easy to scale and customize and available online community support.

iii. Database

MySQL database management system was used to store application data for both mobile and web application. The website was hosted on an online Apache Hypertext Transfer Protocol (HTTP) server. Reasons for choosing MySQL database include: it is open source; it provides full compatibility with the Laravel 5.1 framework.

3.2.5 Prototype Evaluation and Testing

After building each build or a module, testing was done on it. This was aimed at ensuring that it achieved its objective or what it was meant to do. All types of testing were done on the module of build or the system (Agile Methodology, 2016).

a) Testing of the Prototype

To test the prototype functionalities and its user acceptance, various types of test were subjected on it, these are:

i. Usability Testing-

This was done to determine the usability of the application that was developed. This helped to check whether the application would be easy to use or what pitfalls would the users come through. To achieve this, 15 respondents were sampled to test the application and they gave their response on the same. The 15 respondents were sampled from the 20 respondents who participated in the survey. The sampling strategy that was used to come up with the 15 respondents was stratified random sampling. The sampling was done by giving the prototype to the end users and observing whether they would easily use it or whether it would be difficult for them. Also, the backend was subjected to this test where the administrator was given the same to see whether he would easily use it.

ii. Compatibility Testing

Both the mobile and web applications were tested with different Android operating system (versions) and different web browsers respectively. This test was for compatibility.

iii. **Load Testing**

This was done to check the amount of time the application takes to process a request. This was tested by querying genuine academic certificate details and observing how long it took to return the results back.

iv. **Integration Testing**

This was conducted on the system because various features were developed as modules and therefore it was necessary to know whether when the modules would operate as desired when joined together. This was done by combining all modules of the prototype and testing if they worked together well without any issue.

v. **Validation**

To validate if the developed mobile application solves the challenges faced using the current techniques for verification of academic certificates, a total of 10 respondents were selected from the sample population of 20 respondents who participated in the survey for collecting user requirements and also participated in the usability testing of the mobile application. An Online questionnaire were designed (as shown in Appendix E) and sent to all the respondents to collect data from them.

Stratified random sampling was used to come up with the 10 respondents,. It comprised of 2 academic registrars in universities, 4 human resource managers from companies and organisations, 2 employees of recruitment agencies and 2 employees of qualifications verification companies. The user's response is discussed in chapter 6.

3.3 Conclusions

This chapter has described the methods and processes that were used to collect data and the methodologies that were used to answer the research questions. It also helped to decide on the logistics with regards to the population to collect data from and to check if the data collected was sufficient to make conclusions with regards to the current systems that exist, and whether a mobile application would be a solution to the challenges being faced.

CHAPTER 4: REQUIREMENT ANALYSIS

4.1 Introduction

This chapter discusses requirement analysis. The researcher discusses the results of the findings of the research carried. This involves the Analysis of the results obtained from the online questionnaires. The analysis was done using Google forms analysis tools. The responses from the users were represented using graphs and Charts in order to offer clear visualisations of the responses and to enhance deeper understanding of the results. The results obtained were used to answer some of the research questions in section 1.3. The responses were also used to come up with the system design for the application. The questionnaires are attached in Appendix C.

The sample size was 20 respondents from different organisations. The number of respondents who participated in the survey is 20 while the number of respondents who completed the survey was 18 hence the response rate was 90.0%.

Response Rate=Number of respondents who completed the survey/The total sample size

$$\text{ResponseRate}=18/20*100=90.0\%$$

4.2 Functional Requirements

Functional requirements define the capabilities and functions that the implemented application and its components must perform successfully.

i. Create account

All users must create an account, set username and password in order to access the system

ii. Login

All users must login into their accounts using their username and password for them to access the system.

iii. Verify certificates

All users should be able to request verification of a certificate and receive feedback

iv. Logout

All users should be able to logout of their accounts.

v. View verification reports

Users of academic institutions and administrators should be able update the details of all the academic certificates added into the system

vi. Add users

Administrators should be able to add new users into the system

vii. Update users

Administrators should be able to update the user's accounts

viii. Delete users

Administrators should be able to delete users.

4.3 Non Functional Requirements

These requirements that do not affect the way the application works or its core business, the application can still work without it but, are part of the system. They include:

- i. Security – The system should allow access to only authorized users.
- ii. Usability – The system should have an interface that is easy to use.
- iii. Reliability and availability - The system should be reliable and always available to perform user tasks.
- iv. Scalability – it should be easy to add additional functionalities into the system.
- v. Performance – The system should have an acceptable response time while performing its functions.
- vi. Integrity – the system ensure that data stored is not altered or corrupted.
- vii. Search – a user should be able to search a particular university in the system.

4.4 Type of Organisations

The Respondents indicated the category of the organisations they worked for. The respondent's organisations were categorised as employers, academic institutions of higher learning, recruitment agencies and qualifications verification companies. This was done in order to ensure that all the organisations that the research was conducted were directly or indirectly involved in recruitment of new employees and verification of academic certificates. Among the respondents, 40% were registrars of academic affairs in universities, 20% were employers, and 20% were recruitment agencies staff, and the other 20% were staff from qualifications verification companies in Kenya. Figure 4.1 shows a summary of the respondents' distribution in their respective types of companies and organisations.



Figure 4.1 Respondents Distribution in Different Types of Companies and Organisations

4.5 Departments

The respondents indicated their departments in the organisations. They also indicated if their verification of academic certificates was carried in their departments. This was to ensure the respondents were taken from departments that carried out verification of academic certificates. 40% of the respondents worked in the human resource departments, another 40% worked in the office of the registrar academic affairs while the other 20% worked in the examination department in academic institutions of higher learning. This is because majority of academic institutions does verification of their academic certificates in the office of the registrar of academic affairs, however, in few institutions, this is done in the examination office while all the employers that participated does verification of academic certificates in the human resource departments. Figure 4.2 shows a summary of the respondents' distribution in their respective departments.

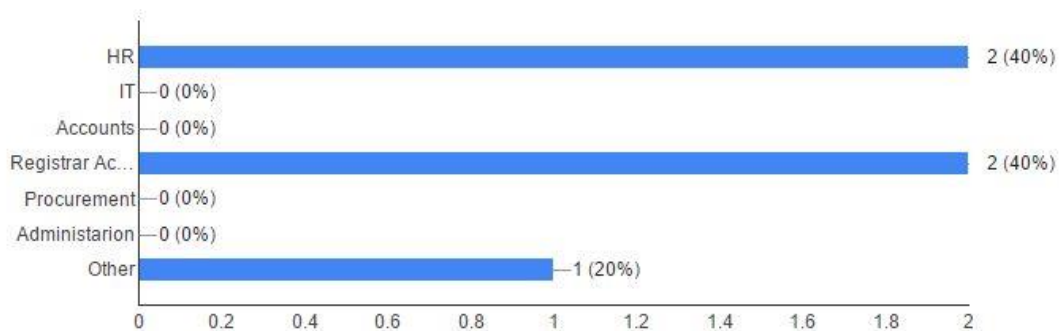


Figure 4.2 Respondents' Distribution in Company Departments

4.5 Roles in the Department

The researcher assumed that accurate information could only be obtained from respondents who are directly involved in the process of verification of academic certificates and therefore respondents were asked to indicate whether part of their roles in the departments included carrying out verification of the academic certificates. This was used to ensure that the respondents were actively involved in process of verification of academic certificates. 80% of the respondents indicated that their roles in the department included verification of academic certificates, with a majority of them working as verification officers. The other 20% of the respondents indicated that at the time the survey was being conducted, their roles did not directly include verification of academic certificates, but previously verification of academic certificates was part of their roles, before they took up other roles in the departments. Figure 4.3 shows a summary of the respondents' roles on verification of academic certificates in their respective departments

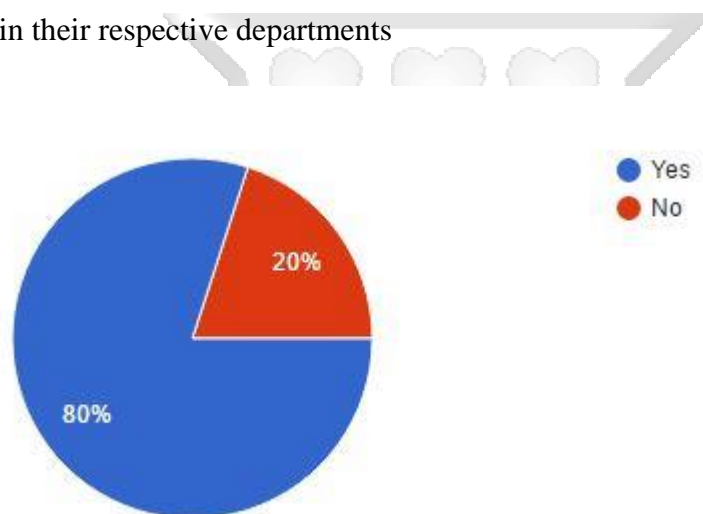


Figure 4.3 Respondents' Roles on Verification of Academic Certificates in Their Respective Departments

4.6 Number of Years Performing the Roles

Respondents were also asked to indicate the number of years they have performed the roles for verification of academic certificates in their organisation. This was used to gauge the quality of responses. As the ones who worked in the roles for longer period understands the academic certificate verification process and the challenges facing the verification process. 40% of the respondents had performed the roles of verification of academic certificates for over five years, 20% for between three to five years while the remaining 40% had performed the task for a period one year and below. Figure 4.4 shows a summary of these results.

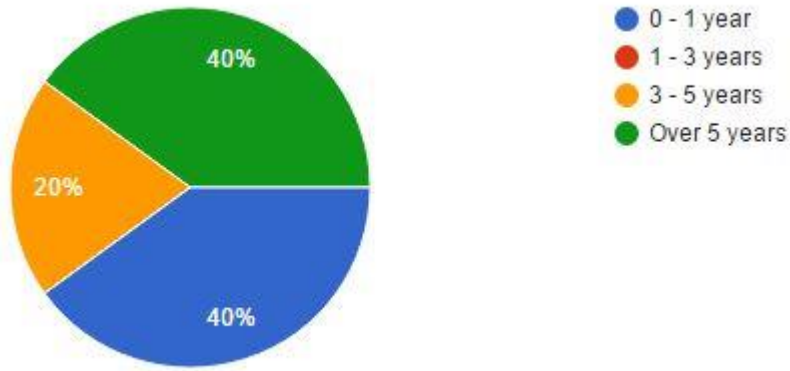


Figure 4.4 Number of Years Respondents Has Performed the Task of Verification of Academic Certificates

4.7 Techniques for Verification of Academic Certificates

The respondents were asked to indicate the technique they use in verification of academic certificates. This helped to know the most common techniques that are used in the verification of academic certificates in Kenya. 80% of the respondents indicated that they use the manual process to verify academic certificates while the remaining 20% of the respondents indicated that they use other techniques which included writing of emails and making phone calls. Figure 4.5 shows the various techniques used for verification of academic certificates.

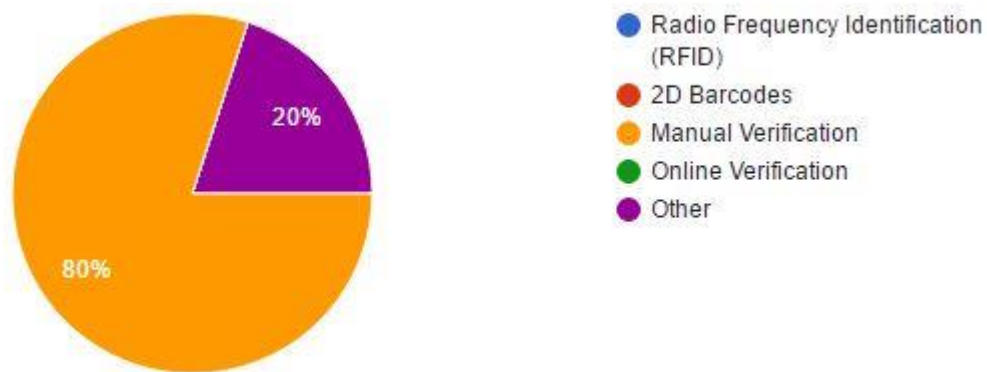


Figure 4.5 Techniques Used For Verification of Academic Certificates in Kenya

4.8 Academic Certificate Verification Process

The respondents were asked to describe the process for verification of academic certificates. The manual process for verification of academic certificate requires an employer or any organisation that seeks to verify an academic certificate to write and

official letter to the university that issued the certificate, requesting for verification of the certificate. This letter is sent to the university together with the copy or copies of the certificates to be verified. The letter is addressed to the registrar of academic affairs. When the request is received in the registrar's of academics office, the staffs in charge of verification of certificates manually check the copies of the certificate to be verified with the records of graduated students and the details of their certificates. If the certificate is genuine, the copies of the certificate are stamped and signed registrar. The copies are then sent back to the employer together with a letter detailing the results of the verification.

Other processes involved calling the universities and giving them the details of the certificates to be verified to ask them to confirm if they are genuine or not, while others involve writing emails to the respective universities. The registrar then verifies the certificates and reply by calling or writing emails to the employers respectively.

4.9 Parameters Used for Verification of Academic Certificates

Respondents were asked to indicate the parameters that they used to determine whether a certificate is genuine or not. University name, university logo, university seal, candidate's name, candidate's Identification Number, candidate's Registration Number, Course Studied, Grade Attained, Date of Graduation and Issuer's Signature. Figure 4.6 shows the various parameters used to determine the genuineness of an academic certificate.

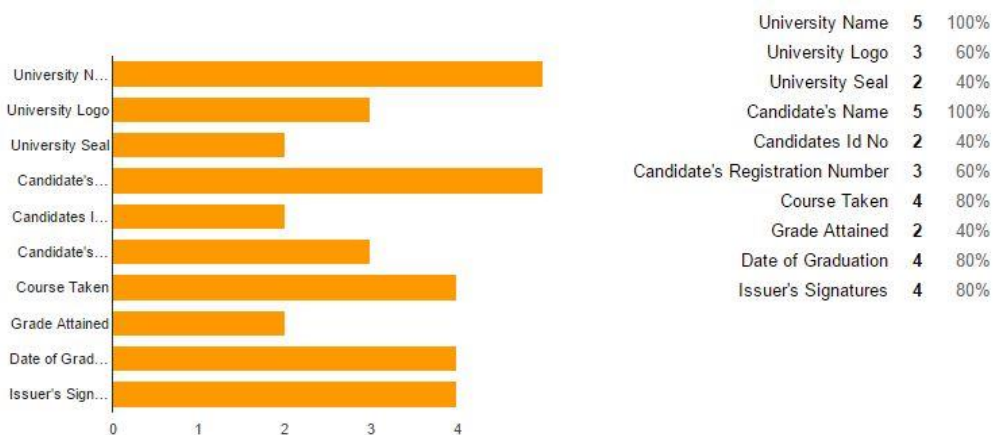


Figure 4.6 Parameters Used for Verification of Academic Certificates

4.10 Time Taken for Verification of Academic Certificate

Respondents were asked to indicate the time it takes them to verify the academic certificates. It takes a minimum of two days and a maximum of two weeks to verify

academic certificates and get the verification results from back from the university to the employer.

4.11 Cost Incurred in Verification of Academic Certificates

The respondents were asked to indicate the cost that is incurred for verification of academic certificates. The universities do not charge fees to verify academic certificates for employers. The employers incur between one thousand and two thousand Kenya shillings for each certificate verified. These costs are paid to qualifications verification companies that do the certificate verification on their behalf. In addition, the costs are incurred on courier services or on transport during travelling to the various universities to verify academic certificates.

4.12 Cases of Academic Certificate Forgery

The respondents were to indicate whether they have ever had cases of forged academic certificates as they carry out verification. All the respondents indicated that they have had cases where job candidates are present forged academic certificates. However, the respondents indicated that such cases are rare and were estimates to one out of every ten certificates.

4.13 Challenges Experienced in Verification of Academic Certificates

The respondents were asked to describe some of the challenges that they face in the process of verification of academic certificates using the current methods.

All the employers indicated that the using the current process takes a long time. They indicated that it takes even weeks to receive the verification results and sometimes they receive the results as late as when they are already done with the recruitment process. They also cited that it is very expensive to verify academic certificates and they spend between one thousand and two thousand Kenya shillings depending with the location of the university where they need to verify the academic certificates. In addition, a number of respondents added that sometimes the universities do not respond to their verification requests by not answering their emails, or do not call them back or send back the verification results to them.

The universities indicated that the process is tiresome and time consuming to them, more so when a large number of certificates need to be verified. This is because the verification process involves manually searching for records of a particular certificate among all the records of all the certificates that have been issued by the university.

4.14 Mobile Phone Ownership

Because the proposed solution is a mobile application, the respondents who are the potential users of the application, were asked to indicate whether they owned a mobile phone. All the respondents owned a smart phone. Figure 4.7 shows the respondents that owned a smart phone.



Figure 4.7 Respondent's Smart Phone Ownership

4.15 Mobile Device Operating System

The Respondents indicated the operating system on their mobile phones, which helped to determine the operating system the proposed solution should be based on. 80% of the respondents were using android phones while the remaining 20% were having windows phone. Figure 4.8 shows the respondents' smart phone's operating system.

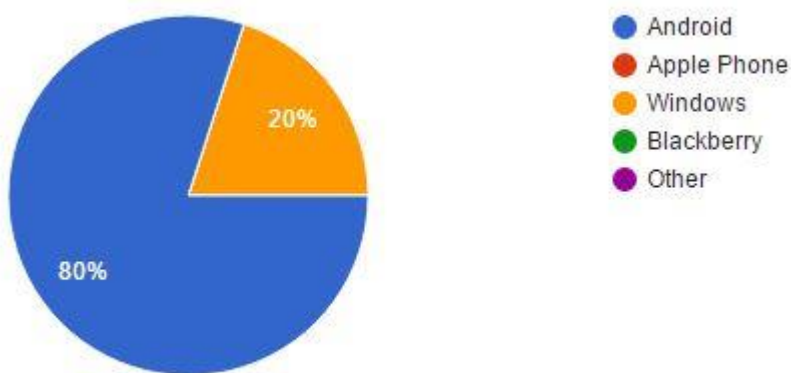


Figure 4.8 Respondents' Smart Phone's Operating System.

4.16 Use of Mobile Applications

Respondents were asked to indicate whether they use other mobile applications apart from calling and messaging applications and they were also to name three applications that they mostly used. 60% of the respondents indicated that they use other mobile applications in addition to calling and messaging. Some of applications that were named to be mostly used by respondents included email, Google search, WhatsApp, Skype and Face book. Figure 4.9 shows the respondents' use of other mobile applications.

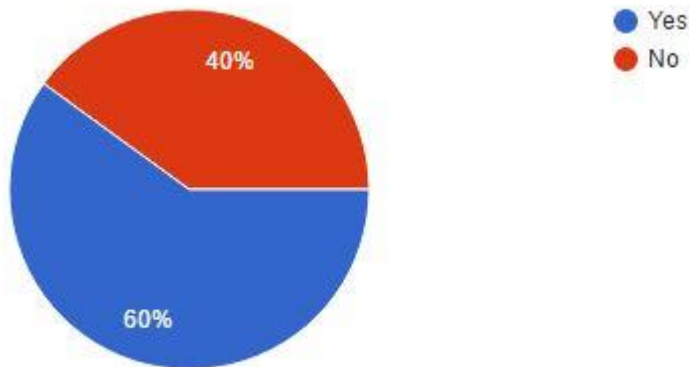


Figure 4.9 Respondents' Use of Other Mobile Applications

4.17 Suitability of a Mobile Application for Academic Certificate Verification

Respondents were asked to indicate whether they thought a mobile application would be suitable to be used to verify academic certificates and whether the use of a mobile application in the verification of academic certificates would solve some of the challenges faced while using the current processes for verification of academic certificates. 80% of the respondents indicated their confidence on the suitability to use a mobile application to address the challenges faced in the verification of academic certificates. Figure 4.10 shows the respondents' response on the suitability of a mobile application in verification of academic certificates.

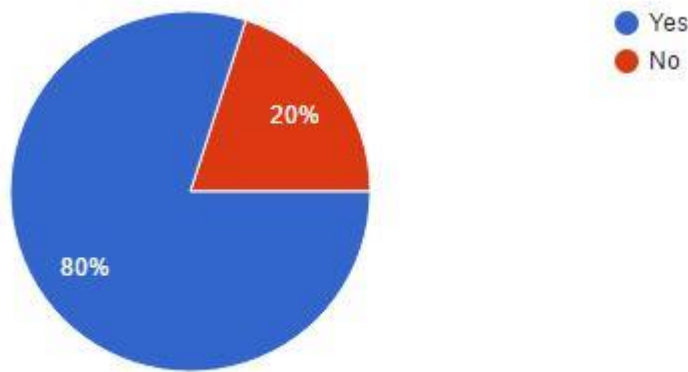


Figure 4.10 Suitability of the Mobile Application in Verification of Academic Certificates

4.18 Proposed Features for the Academic Certificate Verification System

The respondents who believed that a mobile application would be suitable to be used in verification of academic certificates proposed features of the application. These features were used to come up with the system requirements and functionality. Below is a summary of the proposed features.

- The application should have user management and information should be accessed based on user levels and roles.
- The application should offer a single platform for verification of all certificates for all universities and colleges in Kenya.
- The application should offer instant verification of academic certificates
- The application should enable users to report certificates verified as fake to the respective universities.

4.19 Conclusions

Based on the analysis of data provided by the respondents, the results were used to come up with the following conclusions:

- The application should offer comprehensive reports.
- Android is the preferred platform for development of the proposed solution.
- The common parameters used for verification of academic certificates include University name, candidate's name, candidate's Identification Number, candidate's Registration Number, Course Studied, Grade Attained and Date of Graduation

- The current system for verification of academic certificates experiences major challenges that need to be addressed.
- The proposed mobile application would be acceptable by majority of the users.



CHAPTER 5: DESIGNING

5.1 Introduction

This section of the dissertation provides a detailed explanation of the design and architecture of the proposed solution. Design diagrams showing the detailed design and architecture for both the Android mobile application and the website were drawn under the Unified Modelling Language (UML). The design diagrams include use case diagram with detailed follow-up use case descriptions, system sequence diagram, partial domain diagram, and entity relationship diagram.

5.2 Systems Architecture

The architecture adopted for the development of the application was the Client Server Architecture. Client server architecture is a model that acts as distributed application that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients.

The client side consisted of the Android mobile application. The mobile application contains a QR code reader and certificate verification application. Users interact with the application by selecting the UNIVERSITY that its academic certificate need to be verified from a list of Kenyan universities listed on the application. The user then captures the unique identifier of the certificate by scanning the QR code printed on the certificate. Through an INTERNET connection the application verifies with a central database if the certificate is genuine or counterfeit. In this scenario, all UNIVERSITIES maintains central database of certificates, and the application to this databases to verify if the certificate is legitimate. If the certificate exists, the user will clearly see the valid details of the certificate which includes full names of the certificate owner as they appear in the certificate, passport photo of the owner, ID Number, University attended, Course studied, grade attained, year and date of graduation. These details are compared with the details on the copy of the certificate being verified to determine if the certificate is genuine. If the certificate does not exist, the user will get a response “Counterfeit Certificate”. The user will also have an option to report the certificate by pressing a button that will appear at the bottom of the screen. On pressing the button, information on the date, organisation doing the verification and the details of the certificate will be sent to the respective university.

The application server verifies if the certificate queried is genuine. It also collects feedback on certificates verified and those reported as counterfeit. A system

administrator has access to the application server and can manipulate data for secondary reporting.

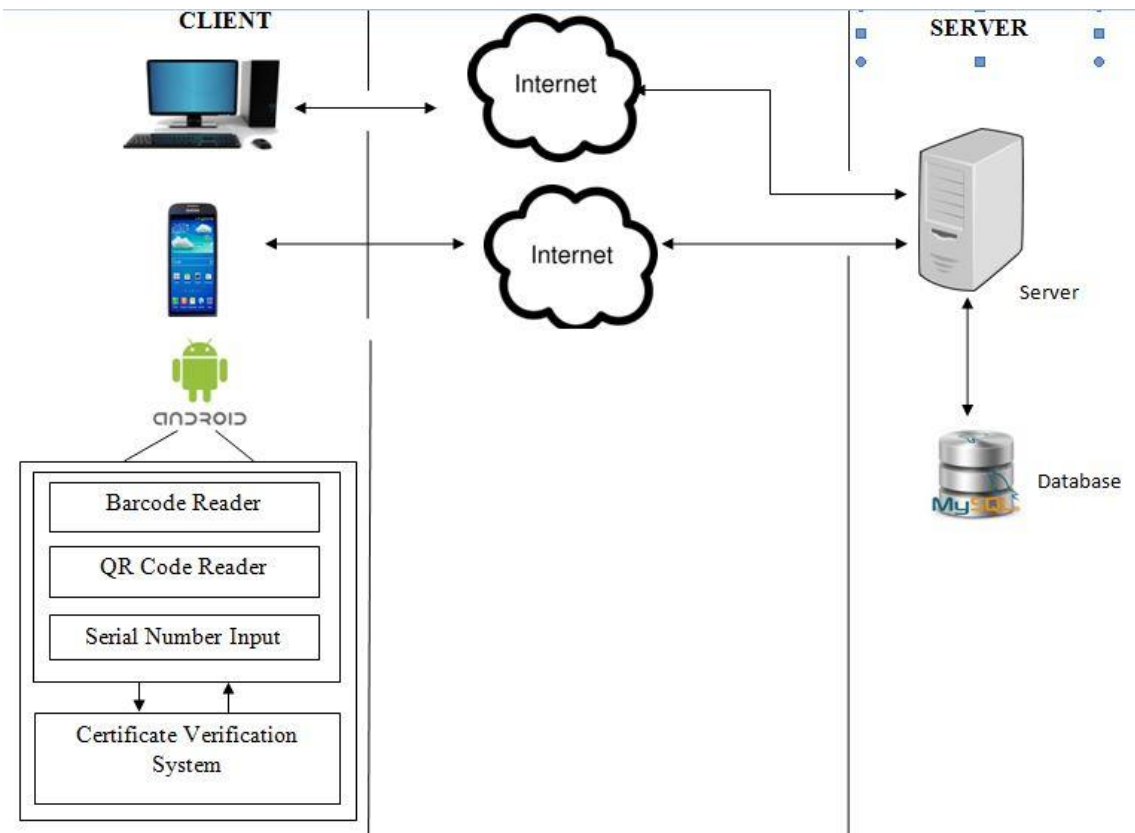


Figure 5.1 System Architecture for the Proposed Application

5.3 Systems Design

The system design that fulfils the functional requirements, non-functional requirements and the research objectives was developed. It presented the proposed solution in a logical manner using different Design diagrams and also gave insights to the actual implementation of both the mobile application and the web application. It consisted of the following components:

- Use Case Diagrams and Descriptions
- Sequence Diagrams
- Partial Domain Diagrams
- Context Diagram
- Entity Relationship Diagram
- Database Schema
- User Interface Flow Diagram

5.3.1 Use Case Diagram and Descriptions

Use Case diagram is a behavioural diagram that shows the functionalities of a system in terms of actors and their goals as represented by use cases and any dependencies on those use cases. The following are a list of actors who interact with the system:

Employer – these include any staff members in the organizations, recruitment agencies or the government public service that are responsible for verification of academic certificates for job candidates.

University Staff –these include any staff members in the registrar’s academics offices in universities that carries out verification of academic certificates and manage certificates.

System Administrator - these include developers of the system who are also responsible for the management and maintenance of the system

The following are the main processes in this application:

1. Create Account - Primary actors are the employers who want to verify academic certificates and University Staff who want their certificates to be verified.
2. Login and Logout - Primary actors are the employers who want to verify academic certificates and University Staff who want their certificates to be verified and the System Administrator who manages users.
3. Verify Certificates - Primary actors are the employers who want to verify academic certificates.
4. Report fake certificate - Primary actors are the employers who want to verify academic certificates and report cases of counterfeit academic certificates.
5. View verification reports - Primary actors are the Employers and University Staff who want to view certificates reported as counterfeit and other verification details.
6. Manage certificates - Primary actors are the University Staff who add, update and delete certificates details.
7. Manage users - Primary actors are the System Administrators who create, update and delete user’s accounts.

Use Case	Description
UC 1 - Create Account	Primary Actors; Employer, University Staff

	<p>Stakeholders: Employer, University</p> <p>Preconditions: Need for verification of certificates.</p> <p>Post condition: Activation request sent</p> <p>Success Scenarios: Account created and activated</p> <p>Frequency of occurrence Once</p>
<p>UC 2- Login</p>	<p>Primary Actors; System Administrator, Employer, University Staff</p> <p>Stakeholders:</p> <p>Preconditions: Need to verify certificates, view verification details or manage users</p> <p>Post condition: Verify certificates, view verification details or manage users</p> <p>Success Scenarios: User successfully logs in</p> <p>Frequency of occurrence Process occurs often</p>
<p>UC 3- Logout</p>	<p>Primary Actors; System Administrator, Employer, University Staff</p> <p>Stakeholders:</p> <p>Preconditions: User is logged into the system</p> <p>Post condition:</p>

	<p>Success Scenarios: User successfully logs out</p> <p>Frequency of occurrence Process occurs often</p>
<p>UC 5 - Verify Certificates</p>	<p>Primary Actors; Employer</p> <p>Stakeholders: Employer</p> <p>Preconditions: User is logged into the system Presence of copies of certificates to be verified</p> <p>Post condition: Enter serial number of the certificate, scan QR code or barcode of the certificate Verification results received</p> <p>Success Scenarios: Certificate verified as genuine or fake</p> <p>Frequency of occurrence Process occurs often</p>
<p>UC 4 -Report fake certificate</p>	<p>Primary Actors; Employer</p> <p>Stakeholders: Employer</p> <p>Preconditions: User is logged into the system Certificate verified as fake</p> <p>Post condition: Details of reported certificate sent to University Staff</p> <p>Success Scenarios: Details of reported certificate received by</p>

	<p>University Staff</p> <p>Frequency of occurrence</p> <p>Process occurs often</p>
UC 5 - View verification reports	<p>Primary Actors;</p> <p>Employer, University Staff</p> <p>Stakeholders:</p> <p>Employer, University</p> <p>Preconditions:</p> <p>User is logged into the system</p> <p>Certificate verification successful</p> <p>Post condition:</p> <p>Success Scenarios:</p> <p>Verification details available</p> <p>Frequency of occurrence</p> <p>Process occurs often</p>
UC 6 - Manage users	<p>Primary Actors;</p> <p>System Administrator</p> <p>Stakeholders:</p> <p>Preconditions:</p> <p>User is logged into the system</p> <p>User accounts successfully created and activated</p> <p>Post condition:</p> <p>Create, update or delete user account</p> <p>Success Scenarios:</p> <p>Accounts successfully created, updated or deleted.</p> <p>Frequency of occurrence</p> <p>Process occurs often</p>
UC 7 - Manage certificates	<p>Primary Actors;</p>

	<p>University Staff</p> <p>Stakeholders:</p> <p>University</p> <p>Preconditions:</p> <p>User is logged into the system</p> <p>User accounts successfully created and activated</p> <p>Post condition:</p> <p>Create, update or delete certificate details</p> <p>Success Scenarios:</p> <p>Certificates successfully added, updated or deleted.</p> <p>Frequency of occurrence</p> <p>Process occurs often</p>
--	---

Table 5.1 Use Case Descriptions

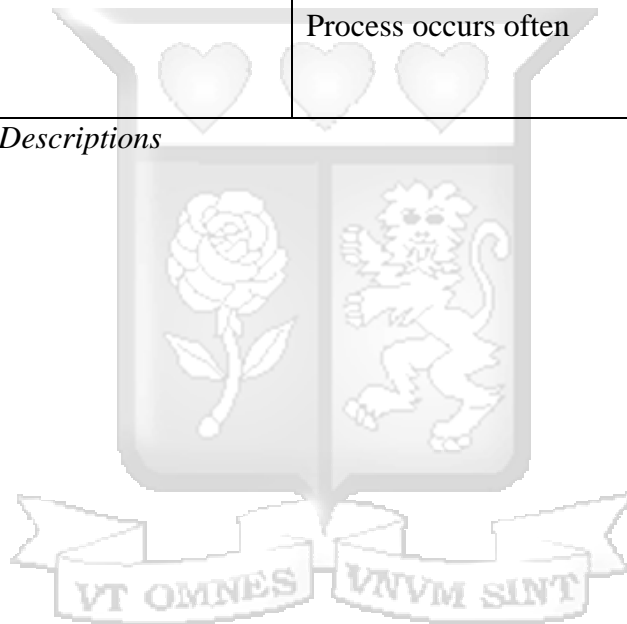




Figure 5.2 Use Case Diagram

5.3.2 System Sequence Diagram

The system sequence diagram shows how users interact and receive feedback and messages to and from the system. It also shows how other activities in the system communicate i.e. from the applications interface and the database where information is added and retrieved. The diagram also shows how users receive feedback messages from the system. This diagram (Figure 5.3) displays the sequential flow of information passing through the four main entities in the system.



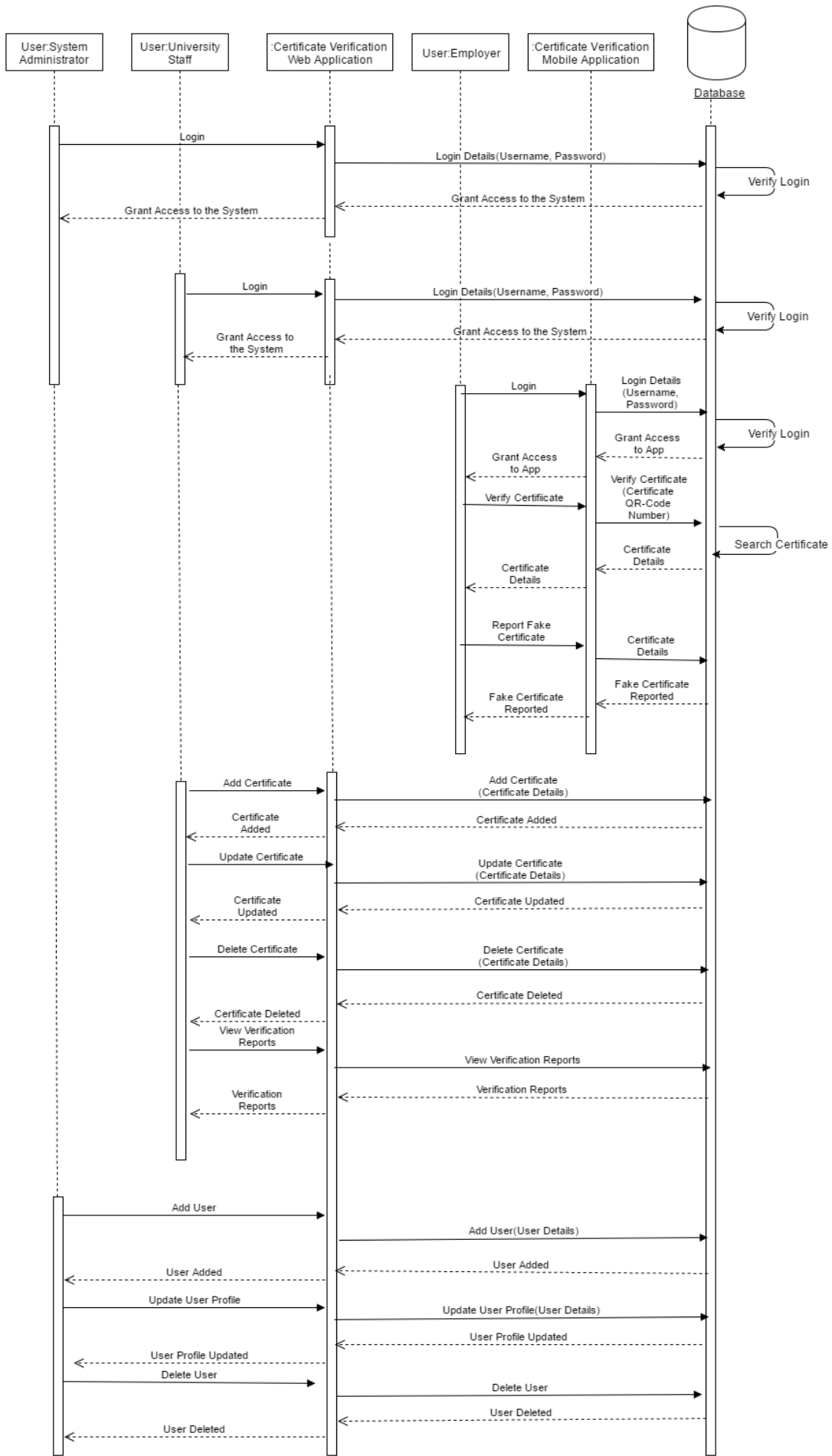


Figure 5.3 System Sequence Diagram

5.3.3 Partial Domain Diagram

Figure 5.4 shows the partial domain diagram identifying relationships between entities of the application. A domain model is a visual representation of conceptual classes or real-situation objects in a domain (Larman, 2002).

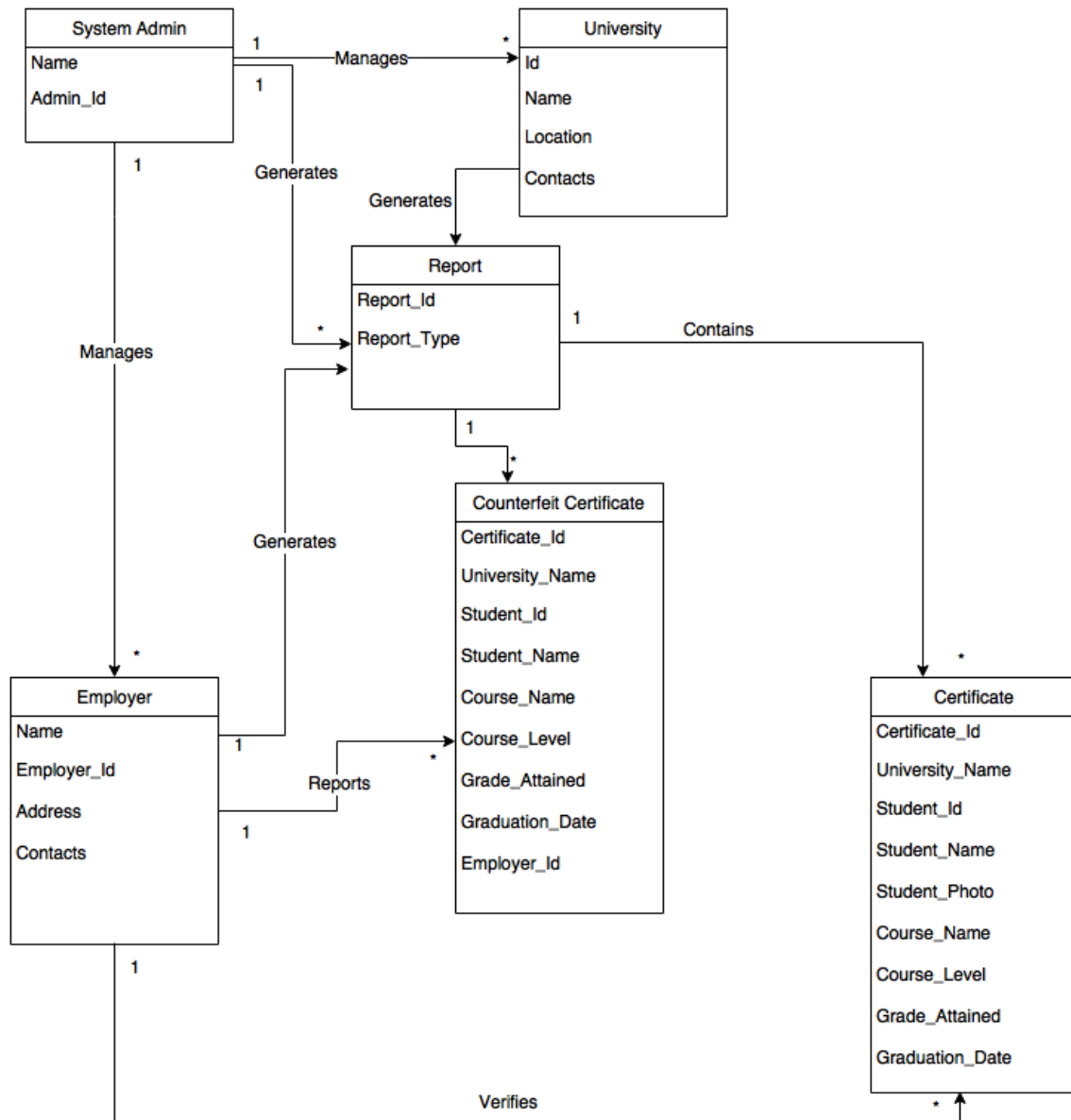


Figure 5.4 Partial Domain Diagram

5.3.4 Context Diagram

A Context Diagram is a component of Functional Modelling that stands out on its own as a valuable tool. This allows for the production of a high level model of an existing or planned system defining the boundary of the system of interest and interactions with critical elements in its surroundings (Burge, 2011). A context diagram was used to represent actors outside of the system that directly interacted with the mobile and web application. They consisted of entities and relationships.

Entities represented the main system while multiple external entities represented external actors.

Entities of the application included:

Employers: these represented primary entities of the application

University Staff: Manages application data

System Administrators: Manages users of the system.

Figure 5.5 shows relationships between entities representing flow of information through a context diagram.

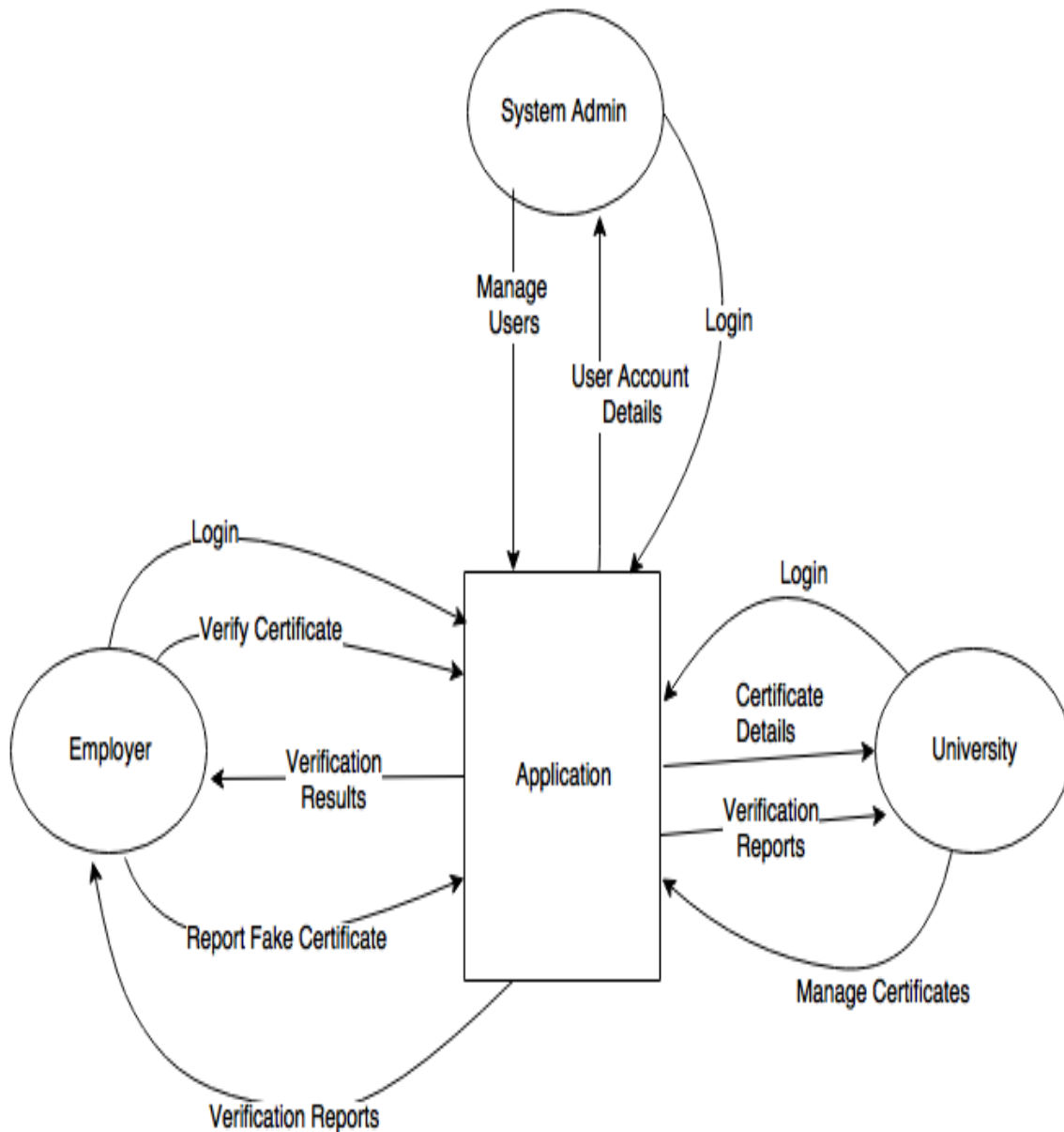
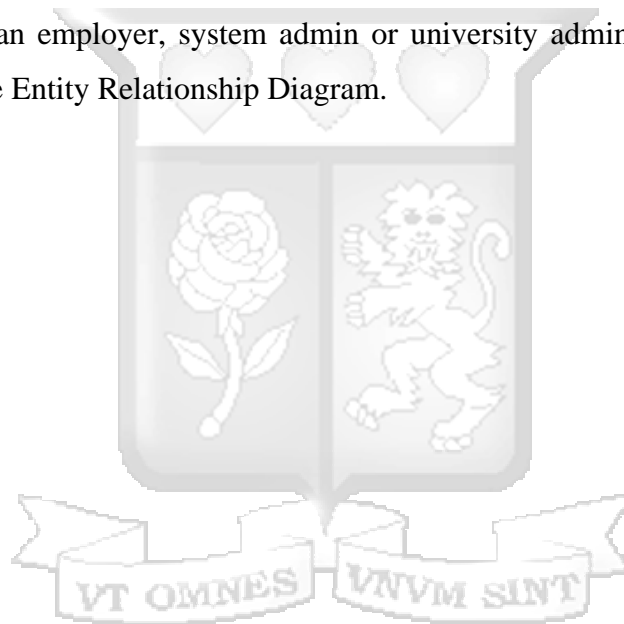


Figure 5.5 Context Diagram

5.3.5 Entity Relationship Diagram

The entity relationship diagram shows the conceptual view of the database by illustrating the tables and their relationship to each other. The following are the descriptions for the entity relationship diagram shown in figure 5.6 below.

A university has a mandatory one or many certificates and a certificate belongs to a mandatory one university. A report contains a mandatory one or many certificates and a certificate is contained in one or many reports. A user has mandatory one or many roles and a role belongs to one or many users. There are three types of users which include employers, system admin, and university admin. There are also three different types of roles i.e. employer role, system admin role, university admin role. A user will either be an employer, system admin or university admin. The Figure 5.6 below represents the Entity Relationship Diagram.



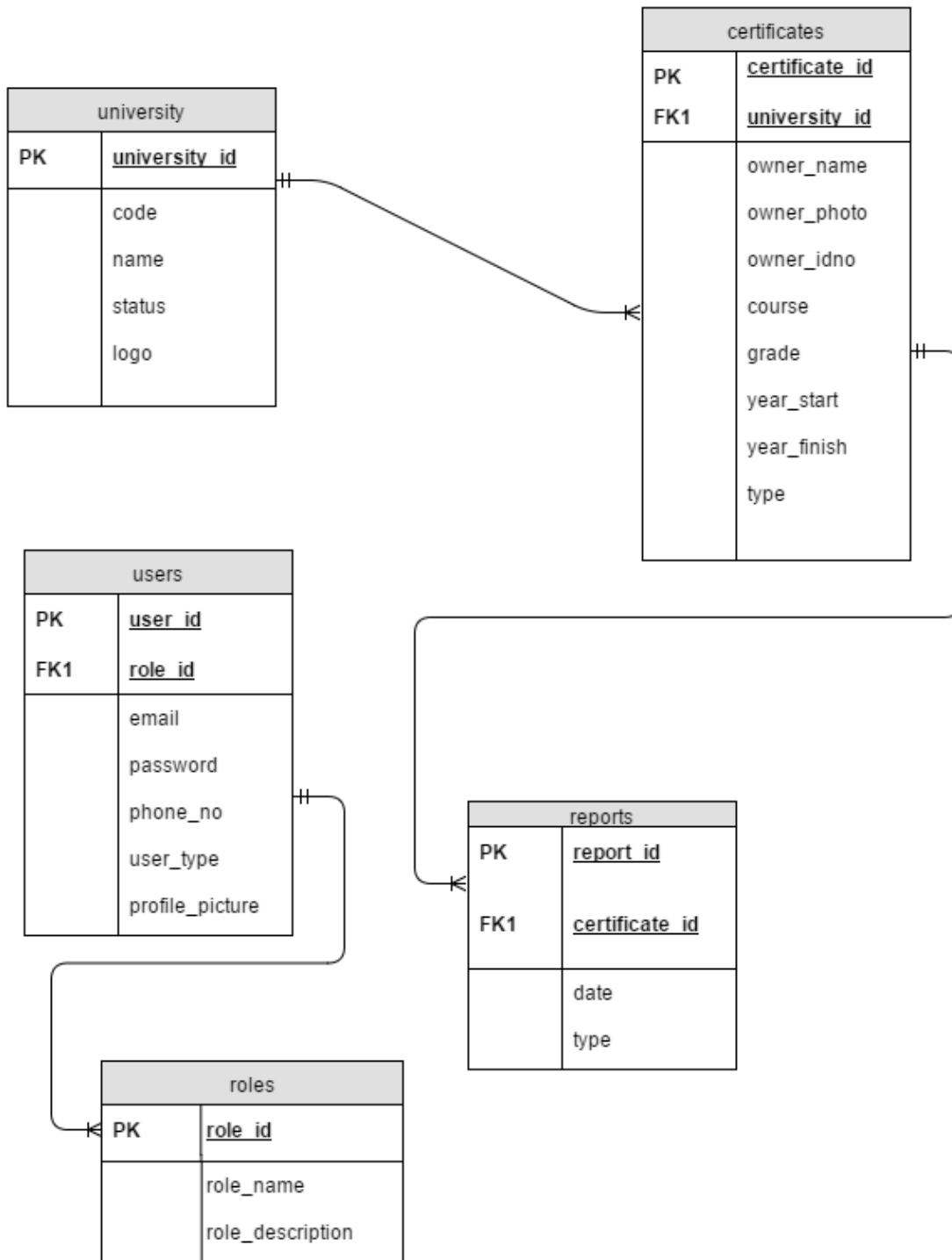


Figure 5.6 Entity Relationship Diagram

5.3.6 Database Schema

University Table

Column Name	Data type	Index
university_id	Varchar(30)	Primary key
Code	Varchar(30)	
Name	Varchar(50)	
Status	Varchar(30)	
Logo	Varchar(255)	

Table 5.2 University Table

Certificate Table

Column Name	Data type	index
certificate_id	Varchar(30)	Primary key
university_id	Varchar(30)	Foreign key
owner_name	Varchar(50)	
owner_photo	Varchar(255)	
owner_idno	Varchar(30)	
course	Varchar(50)	
grade	Varchar(30)	
score	Int(30)	
year_tart	Varchar(30)	
fear_finish	Varchar(30)	
Type	Varchar(30)	

Table 5.3 Certificates Table

Users Table

Column Name	Data type	index
user_id	Varchar(30)	Primary key
role_id	Varchar(30)	Foreign key
email	Varchar(30)	
password	Varchar(30)	
phone_no	Varchar(30)	
user_type	Varchar(30)	
profile_picture	Varchar(255)	

Table 5.4 Users Table

Roles Table

Column Name	Data type	index
role_id	Varchar(30)	Primary key
role_name	Varchar(30)	
role_description	Varchar(30)	

Table 5.5 Roles Table

Reports Table

Column Name	Data type	index
report_id	Varchar(30)	Primary key
certificate_id	Varchar(30)	Foreign key
Date	Varchar(30)	
Type	Varchar(30)	

Table 5.6 Reports Table

5.3.7 User Interface Flow Diagram

This section deals with the flow of screen presentations when the user interacts with the application. When the application is first run a splash screen appears followed by the login page. On successful login, the home screen displays a list of Kenyan universities. The user selects the university that its certificate needs to be verified and QR code scanner appears allowing the user to scan the QR-Code of the certificate. Once this is done successfully, the results of the verification are displayed to the user to compare with information contained on the certificate being verified or a message is displayed to the user that the details of the certificate being verified are not found. In this case, the user can report such a certificate to the respective university.

5.3.6.1 Mobile Application Wireframes

The figures below shows the wireframe designs of the Screens for the mobile application.



Figure 5.7 Register Wireframe

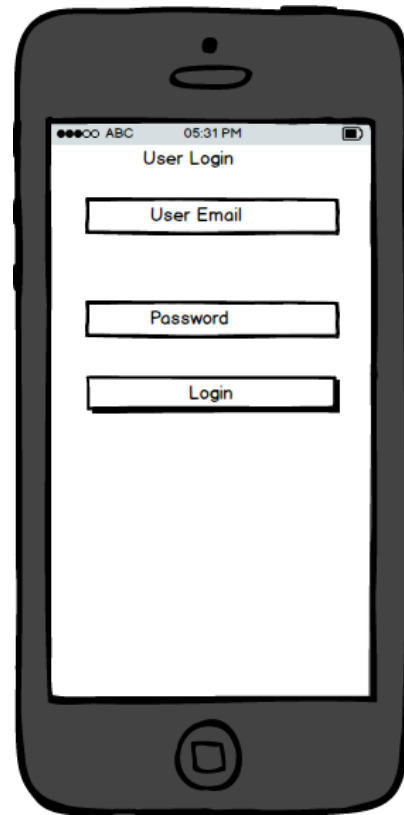


Figure 5.8 Login Wireframe

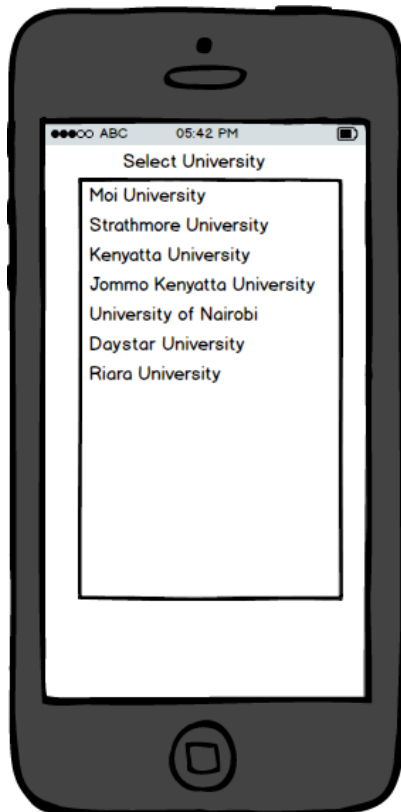


Figure 5.9 Main Page Wireframe



Figure 5.10 Scan QR Code Wireframe

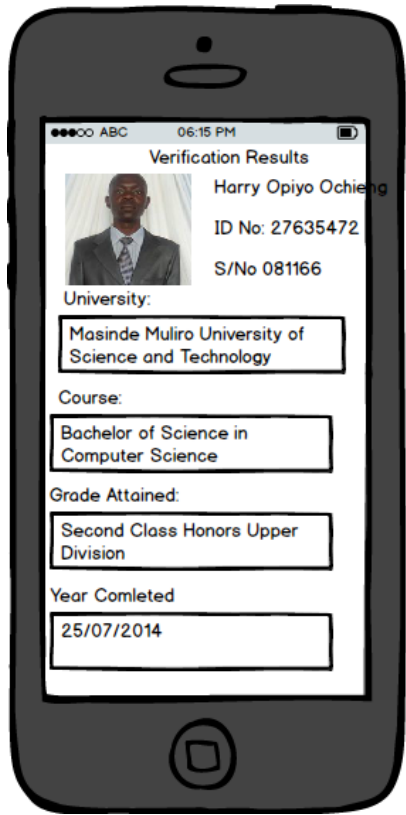


Figure 5.11 Genuine Certificate Verification Results Wireframe



Figure 5.12 Counterfeit Certificate Verification Results Wireframe



Figure 5.13 Reporting Counterfeit Certificate Wireframe



5.3.6.2 Web Application Wireframes



Figure 5.14 Web Login Wireframe

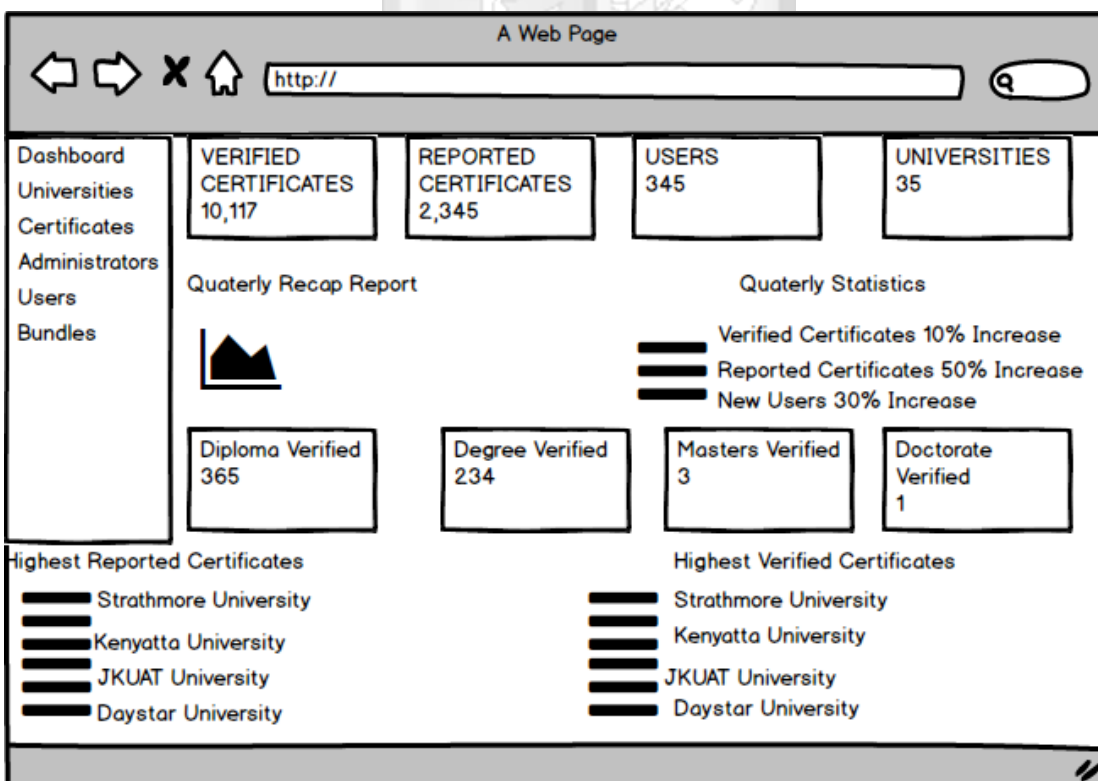


Figure 5.15 Dashboard Wireframe

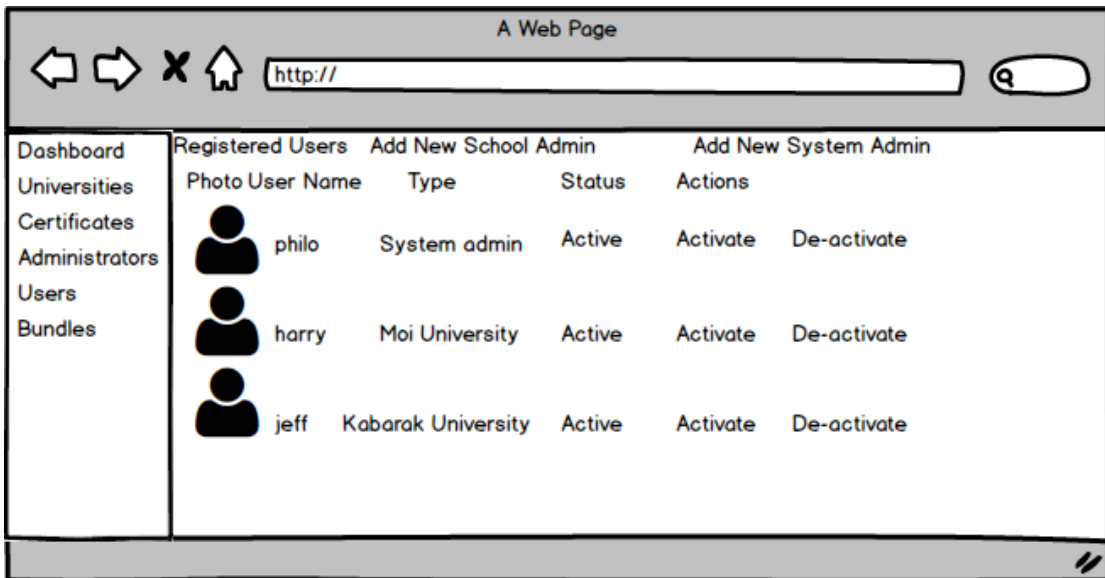


Figure 5.16 User Management Wireframe

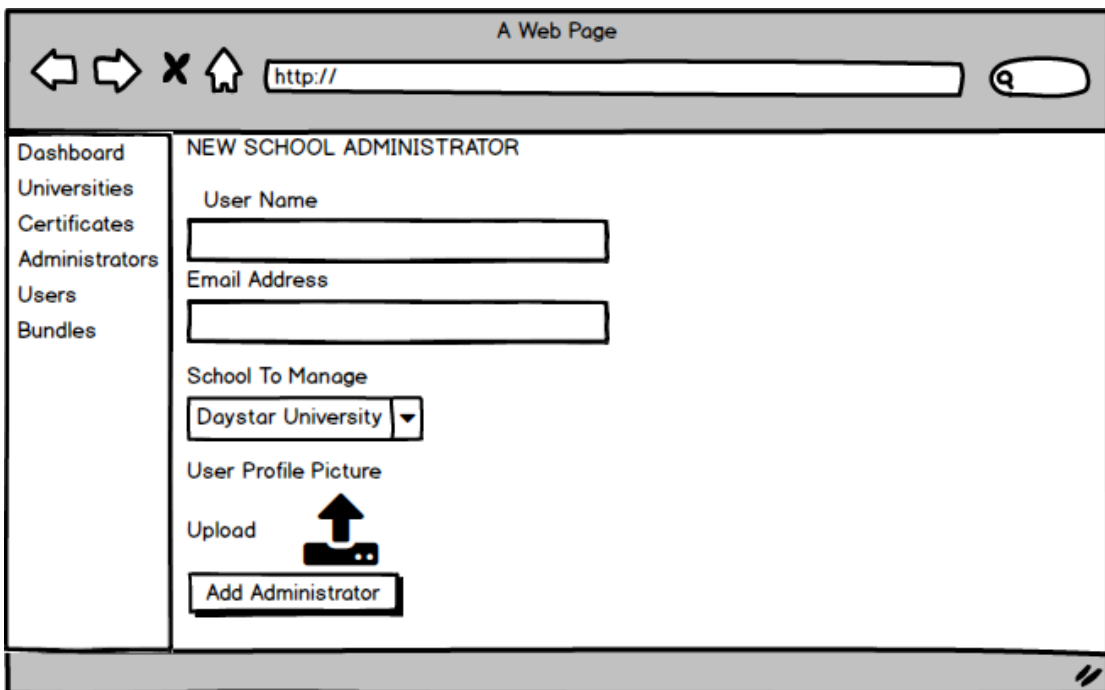


Figure 5.17 Add School Administrator Wireframe

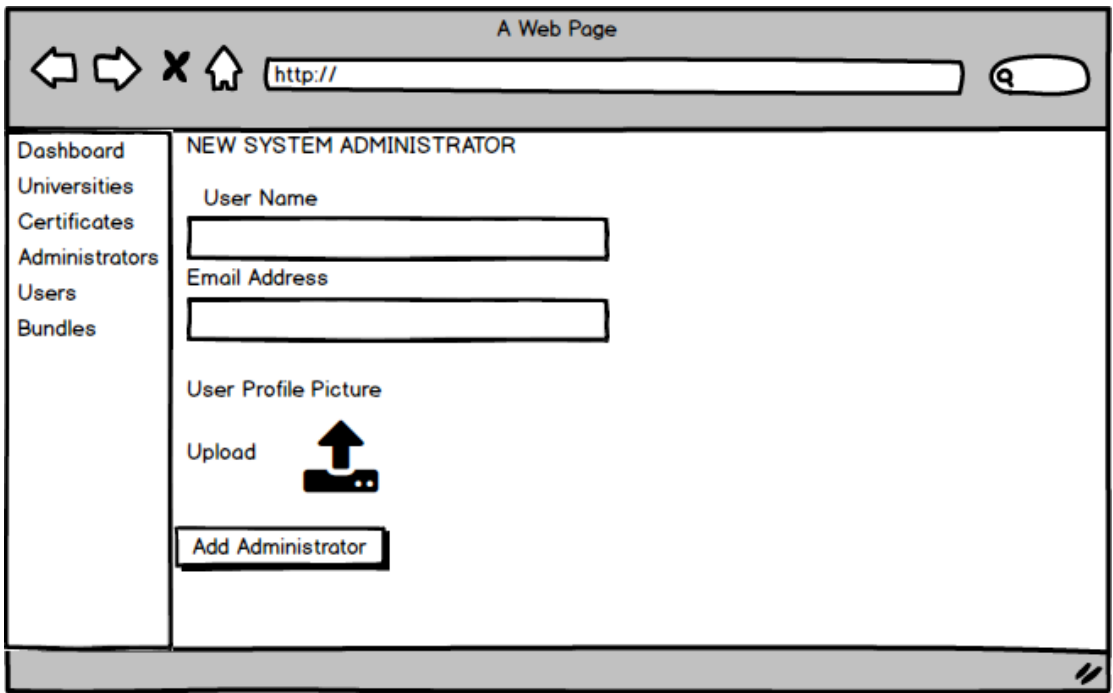


Figure 5.18 Add System Administrator Wireframe

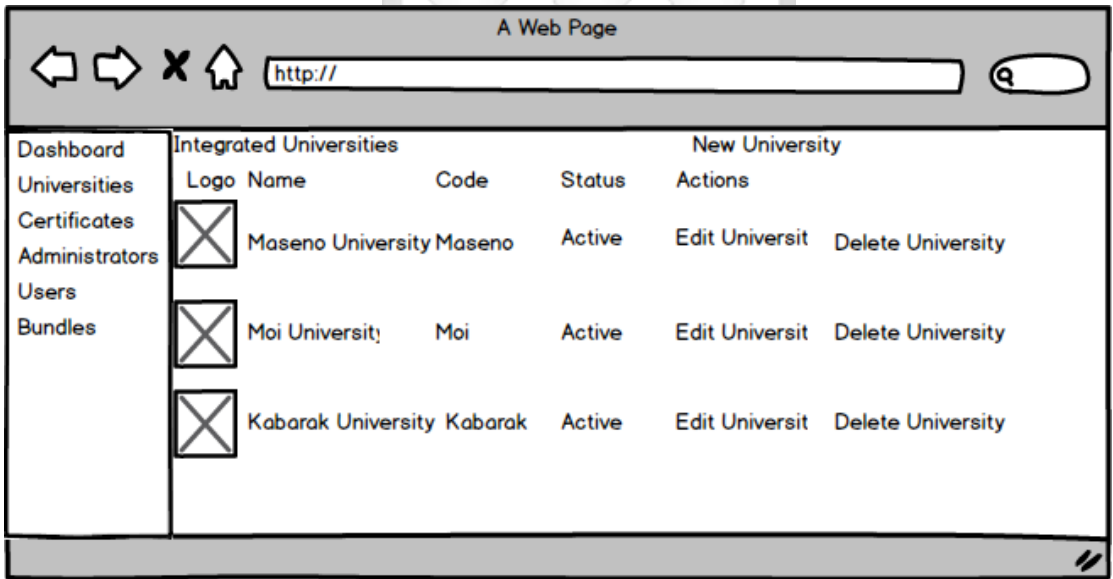


Figure 5.19 University Management Wireframe

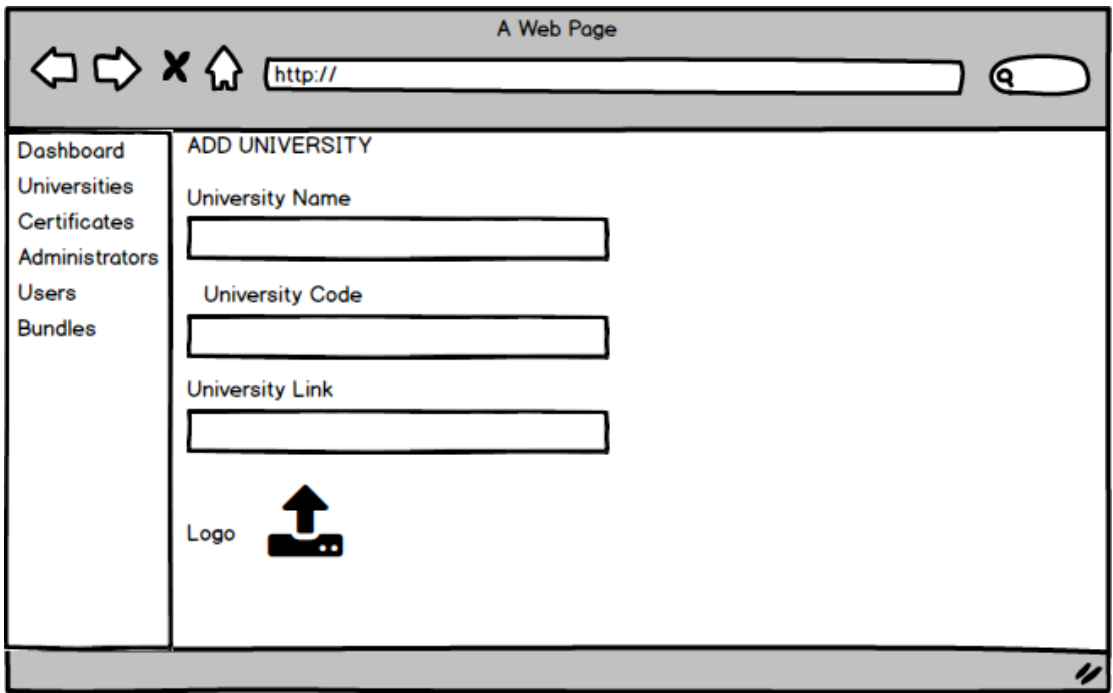


Figure 5.20 Add University Wireframe

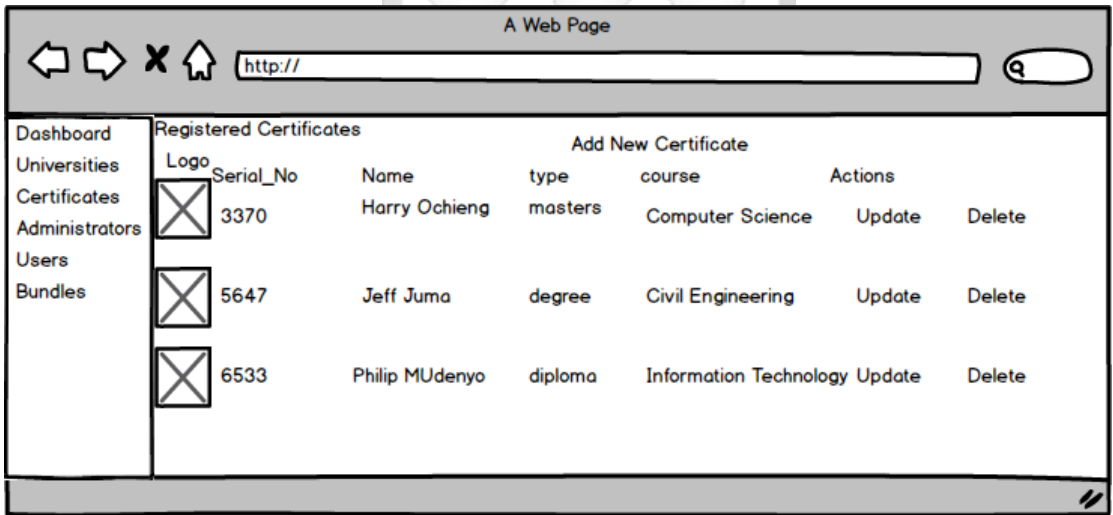


Figure 5.21 Certificate Management Wireframe

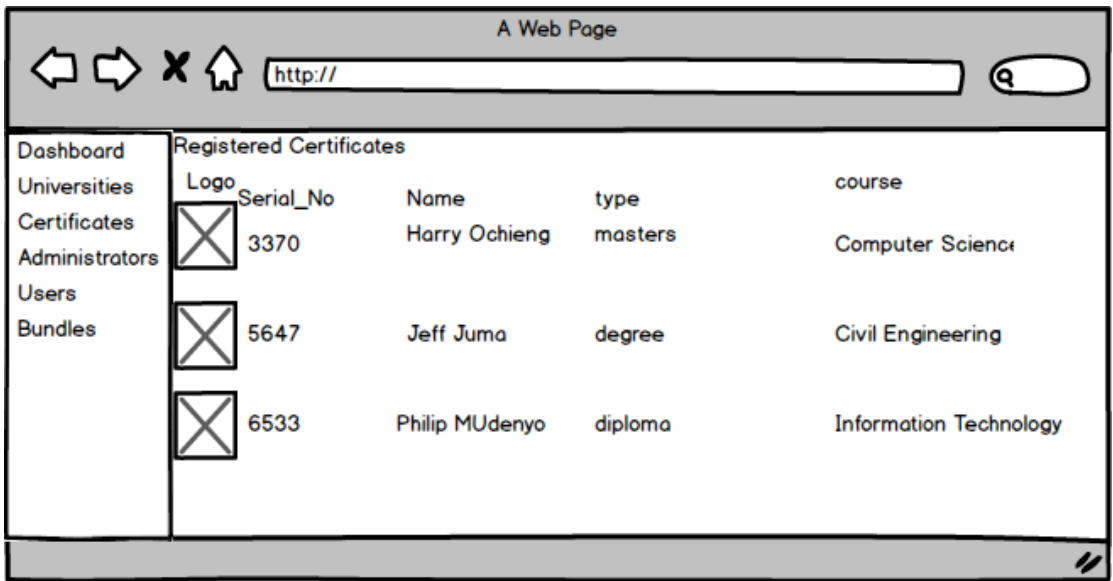


Figure 5.22 Registered Certificates Wireframe

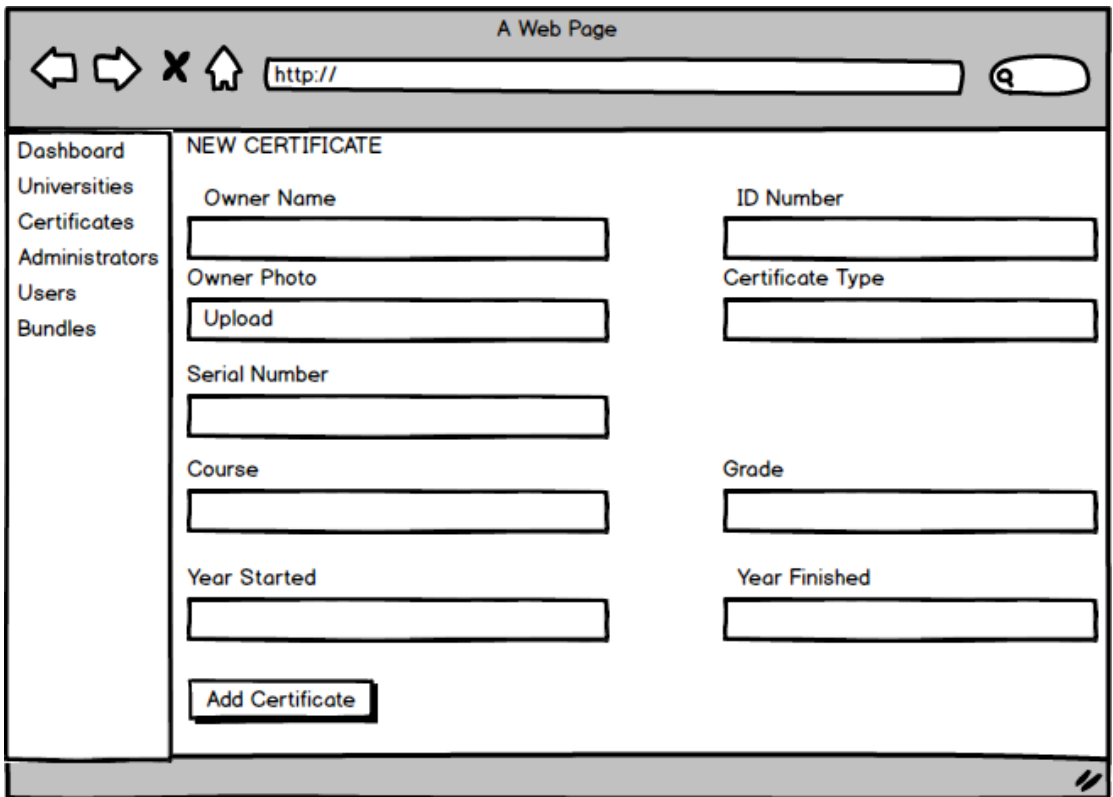


Figure 5.23 Add New Certificate Wireframe

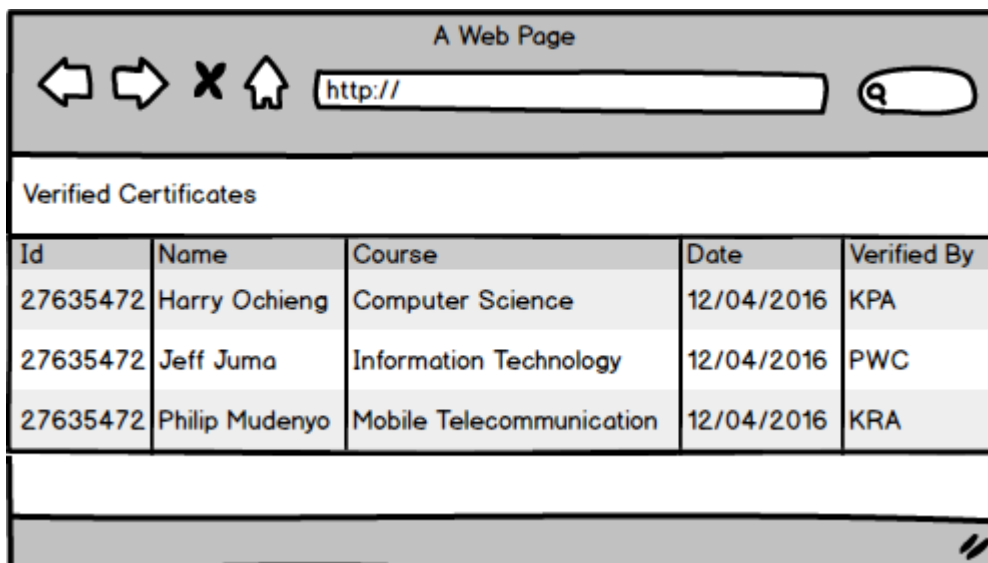


Figure 5.24 Verified Certificates Wireframe

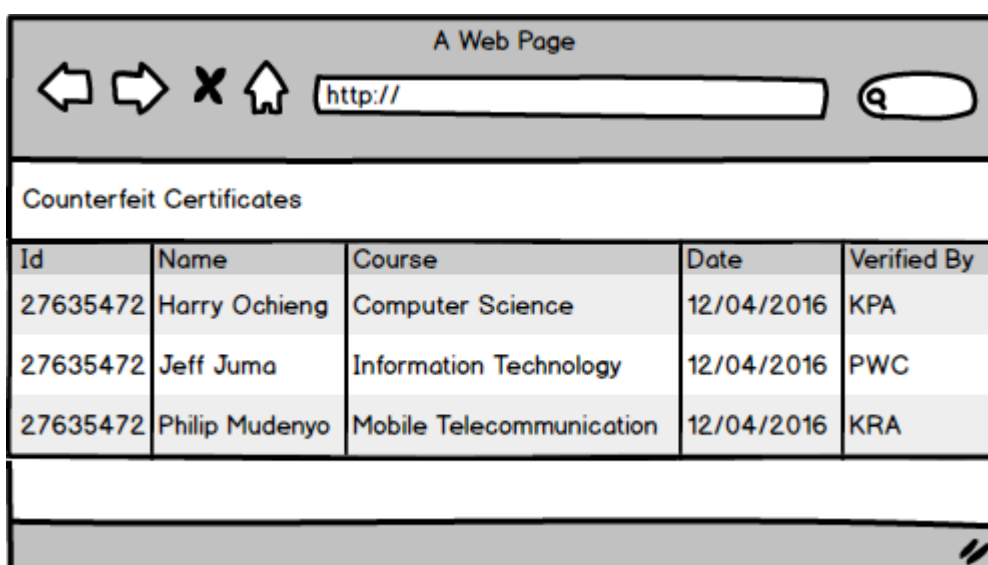


Figure 5.25 Counterfeit Certificate Wireframe

5.4 Conclusions

System analysis and design helped in understanding system requirements. UML notation was used to construct diagrams that aided in understanding the system. These diagrams include; the use case diagram used to show the system requirements, sequence diagram used to illustrate the system process, partial domain diagram used to identify relationships between entities, context diagram used to represent actors outside of the system that directly interacted with the system, level 0 data flow diagram used to show the interaction between external entities and processes of the system and the ERD used to show the database design.

The proposed architecture is a client server architecture where the mobile and web applications are in the client side while the server and database in the sever side.

CHAPTER 6: PROTOTYPE BUILDING, EVALUATION AND TESTING

6.1 Introduction

This chapter explains how implementation and testing of the proposed applications was carried out. The major functionalities of the applications were implemented and tests carried on them. The system functional requirements were incorporated in the prototype functionalities and the system design strictly adhered to the design presented in the system design.

6.2 Implementation Environment

6.2.1 Mobile Application

The Operating System for the mobile application implementation was Android. The source code was written in Java, utilizing android classes. The application was compiled and tested using the android Software Development Kit (SDK) emulator and an android device. The application is optimized for android version 4.4.2 compatible with android devices on minimum version 2.0 and maximum version 4.4.4. JSON was used as the web service that provides the interface between the android application and the database. Reasons for choosing android as the client application include: flexible SDK, availability of Android Development Tools (ADT) and availability of abundant support from online developer communities.

6.2.2 Web Application

The web application was developed using Laravel 5.1 framework based on Hypertext Pre-processor (PHP). The website was hosted on an online Apache HTTP server. Reasons for using PHP were; it is an Open Source platform, it is platform independent; it supports all major web servers and databases; it has multiple layers of security to prevent threats and malicious attacks.

6.2.3 Database

The database was developed using the MySQL database. Reasons for using MySQL were; it is an open source platform; it is fully compatible with PHP and other platforms; it is secure in that all passwords are encrypted before storage restricting unauthorized access to the database.

6.3 Implementation Details

6.3.1 QR-Code Generation

A unique QR code is generated for each and every certificate and printed on the certificates. The QR code is used as a unique identifier of the specific certificate. The procedure that is used for generation of the QR code includes:

- A unique QR code number is generated using a QR code generator application.
- The QR code number is entered into the UNIVERSITY database as a unique identifier of details of a particular academic certificate.
- The QR code number is then converted into a QR code image using the QR code generator.
- The QR code image is then printed on the academic certificate.

6.3.2 The Mobile Application

The prototype is designed to run on an Android Operating System device compatible with android devices with minimum version 2.0 and maximum version 4.4.4. The device running the application rely on an active INTERNET connection and a working camera. Full functionality of the application requires interaction with a QR-Code reader and an application that manages data manipulation and interaction with a backend server.

During verification, QR-Code image is captured by the mobile phone camera by scanning. A QR-Code reader application analyses and regenerates the QR code number. The QR code number is used to identify whether the certificate exists in the database or not and to view information about the certificate. The information captured includes the university name, names of certificate holder, national Identification number and passport photo size of certificate owner, degree name, date of graduation, and grade attained.

System Components

The main system components of the application are:

Application Create Account and Login

To gain access to the application, users have to login using a username and password. In order to get login credentials a user has to create an account which has to be validated and activated by a system administrator. Creation and activation of accounts

is done using the web application. For each login, the username and password are validated to ensure security and prevent unauthorized access. Figure 6.2 shows the login screen for the mobile application.

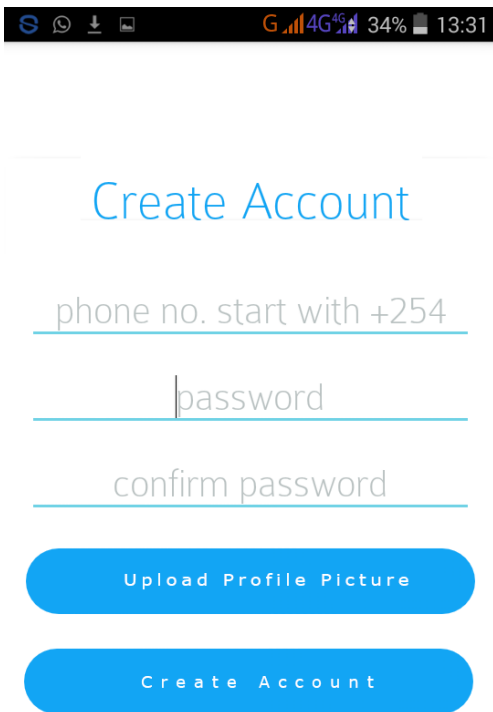


Figure 6.1 Create Account

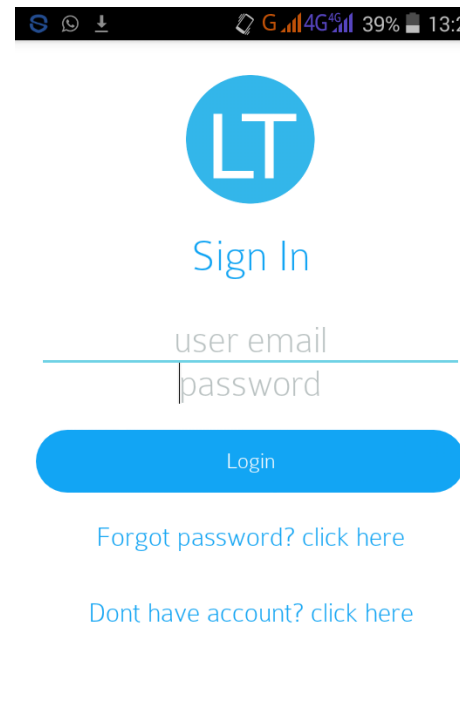


Figure 6.2 Application Login

Main Page

This screen as shown in Figure 6.3 shows the main page which provides a list of universities that their certificates can be verified using the application. The user selects the university that its certificate needs to be verified.

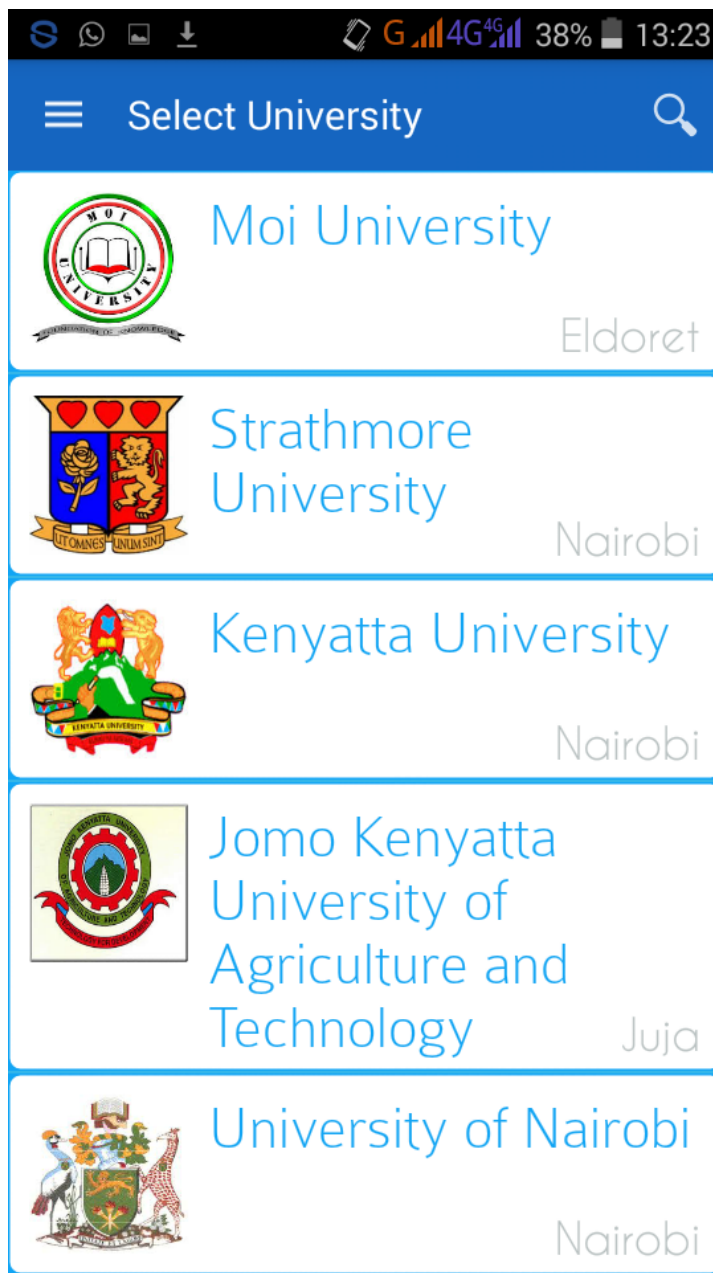


Figure 6.3 List of Universities

Scan QR-Code

This system component as shown in Figure 6.4, allows users to scan a QR -Code tagged on a certificate. The QR -Code scanner application analyses the QR-Code and regenerates a unique QR-Code number of the certificate being verified. The QR-Code number is used to query the database and return certificate information, which is displayed, to the user.

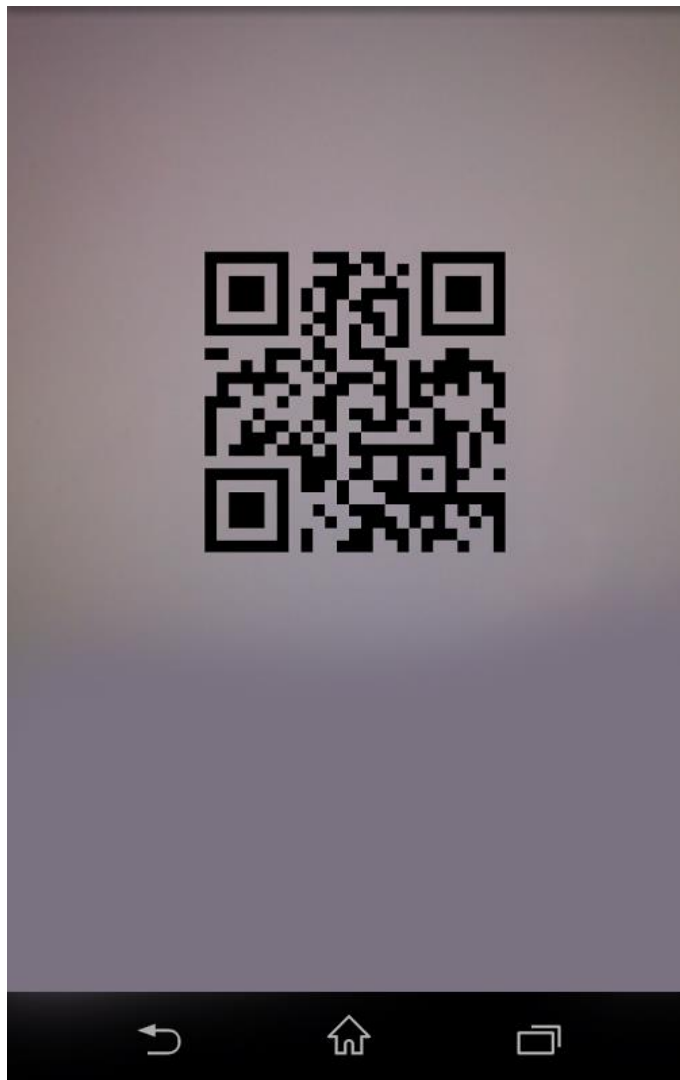


Figure 6.4 QR-Code Scanning

Verification Results

Figure 6.5 shows a screenshot of the feedback acquired upon verification of a genuine certificate. Details of the certificate are shown which include the university name, names of the owner, national Identification number and passport photo size of certificate owner, degree name, date of graduation, and grade attained. The user then compares the details displayed with the details on the copy of certificate that is being verified and the national identity card of the certificate holder to ascertain whether the certificate is accepted as genuine or reported as counterfeit.

Figure 6.6 shows a screenshot of the feedback acquired upon verification of a counterfeit certificate. Details of the certificate are not found and therefore is not displayed the user. Instead the user gets a message stating that “CERTIFICATE

DETAILS NOT FOUND”. A user has the option of reporting a counterfeit certificate as shown in Figure 6.6 below.

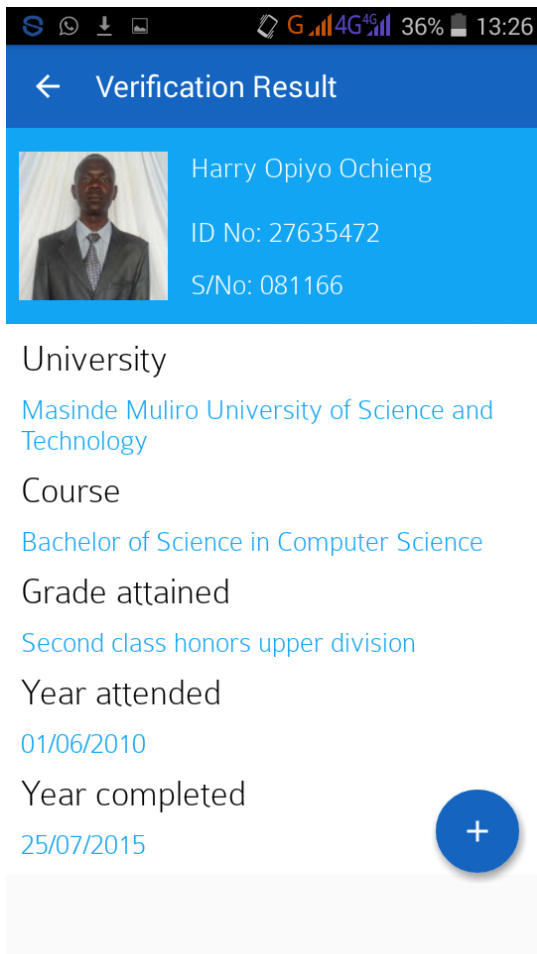


Figure 6.5 Verification Results for Genuine Certificate



Figure 6.6 Verification Results for Counterfeit Certificate

Reporting a Counterfeit Certificate

This system component as shown in Figure 6.7, allows users to report a certificate verified as counterfeit, to the university the certificate is purported to be obtained. It allows the user to send the details of the counterfeit certificate which allows the university administration to follow up and take legal action against the person who forged the certificate. These details include names and the national identification number of the certificate forger, the unique identifier of the certificate, course name, date of graduation and grade attained as contained on the forged certificate.

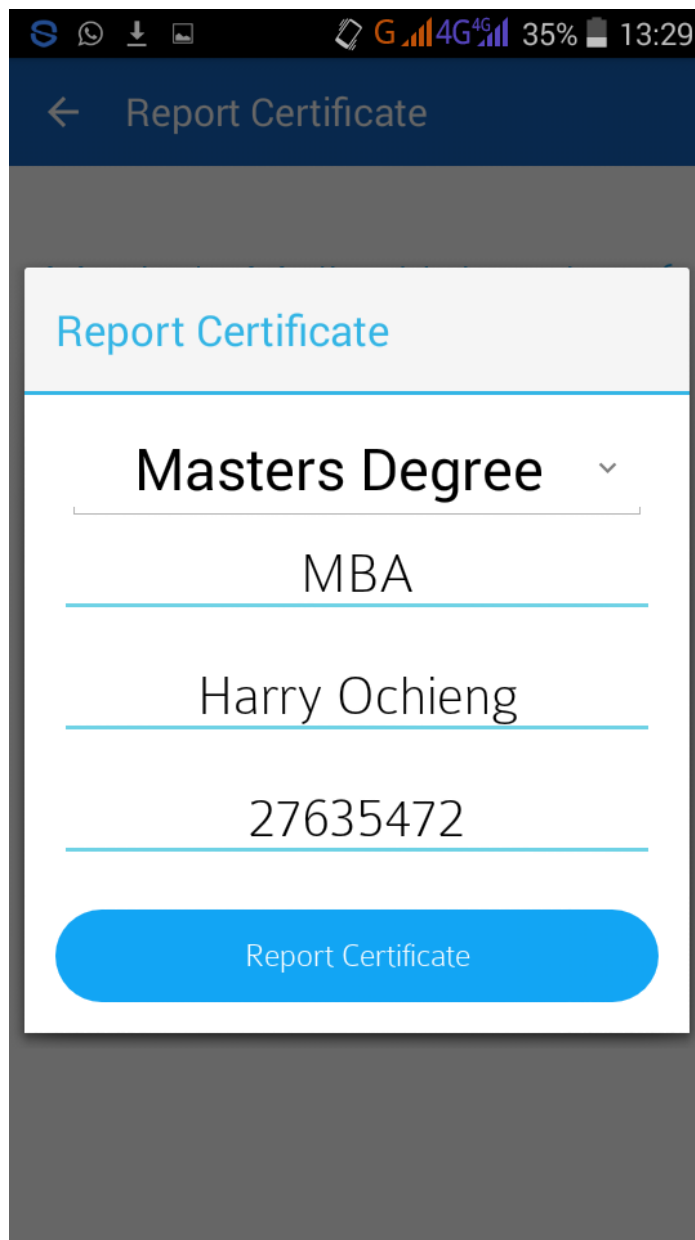


Figure 6.7 Report a Counterfeit Certificate

6.3.3 The Web Application

The web application's main function was to retrieve and receive information sent by the developed mobile application to the database. This application resides in the HTTP web server and is directly linked to the certificate management database. The web application was designed for use by administration to manage users, generate and view reports. It was also designed for use by the university staff to manage certificates, generate and view reports. The reports generated included: a report to view the number of registered users using the application; Number and details of certificates verified by each registered user; Total number of certificates verified by all registered users and the number and details of certificates reported as counterfeit.

System Components

The main system components of the certificate management web application are:

Login

To gain access to the web application users have to login using a username and password. The username and password are authenticated and verified then access is granted or denied. This prevents against unauthorized access. Figure 6.8 shows the screen shot for logging in the web application.

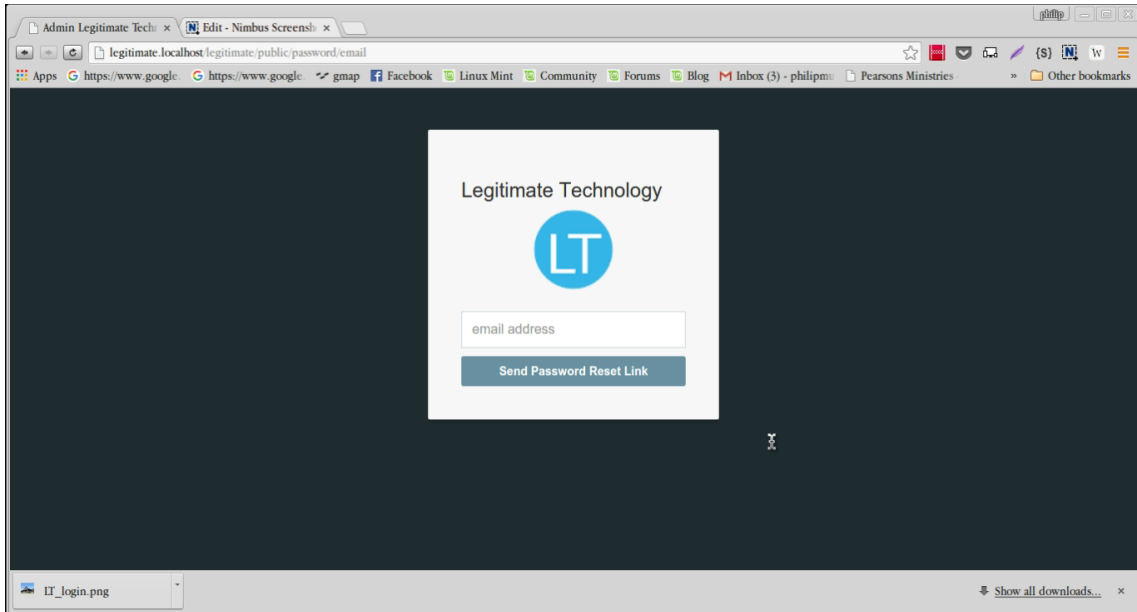


Figure 6.8 Web Application User Login

Dashboard

This gives a summary of all the components of the web application

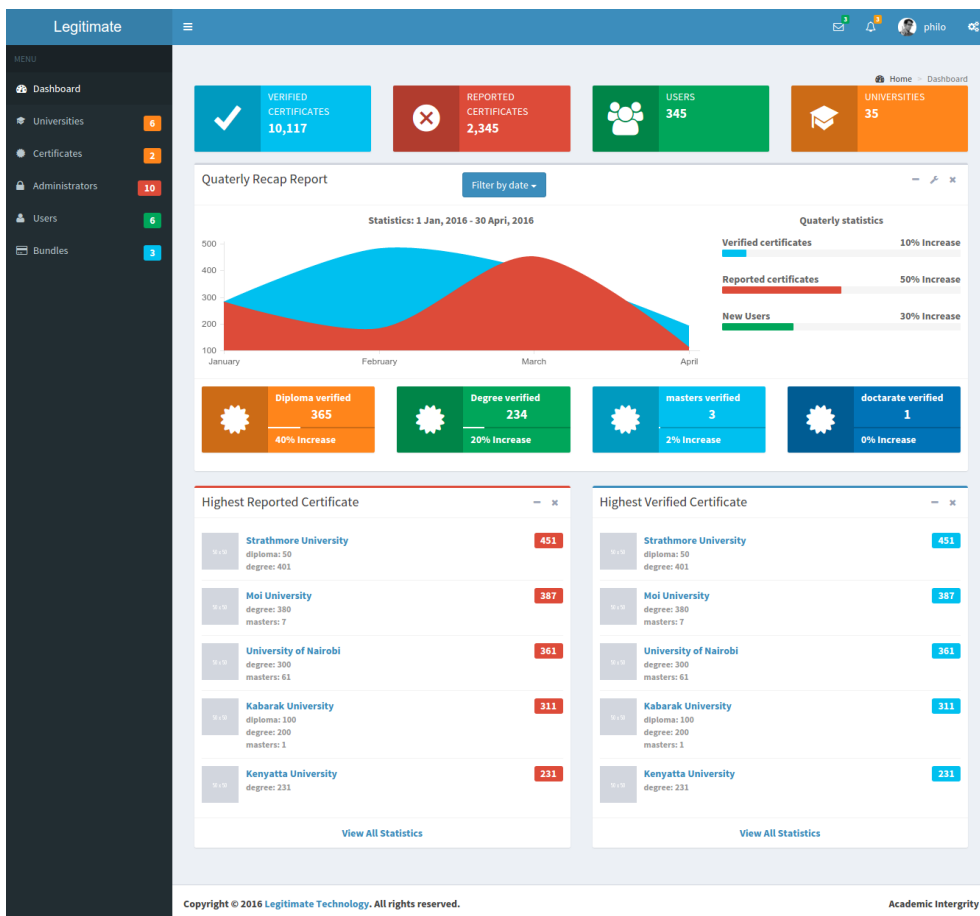


Figure 6.9 Web Application Dashboard

User Management

This component offers user management for the users for both the mobile and the web application. It allows an Administrator to View registered user's verification activities, to edit user profiles as activate and deactivate a user, and to manage user levels. A screenshot of the User Management Interface is below.

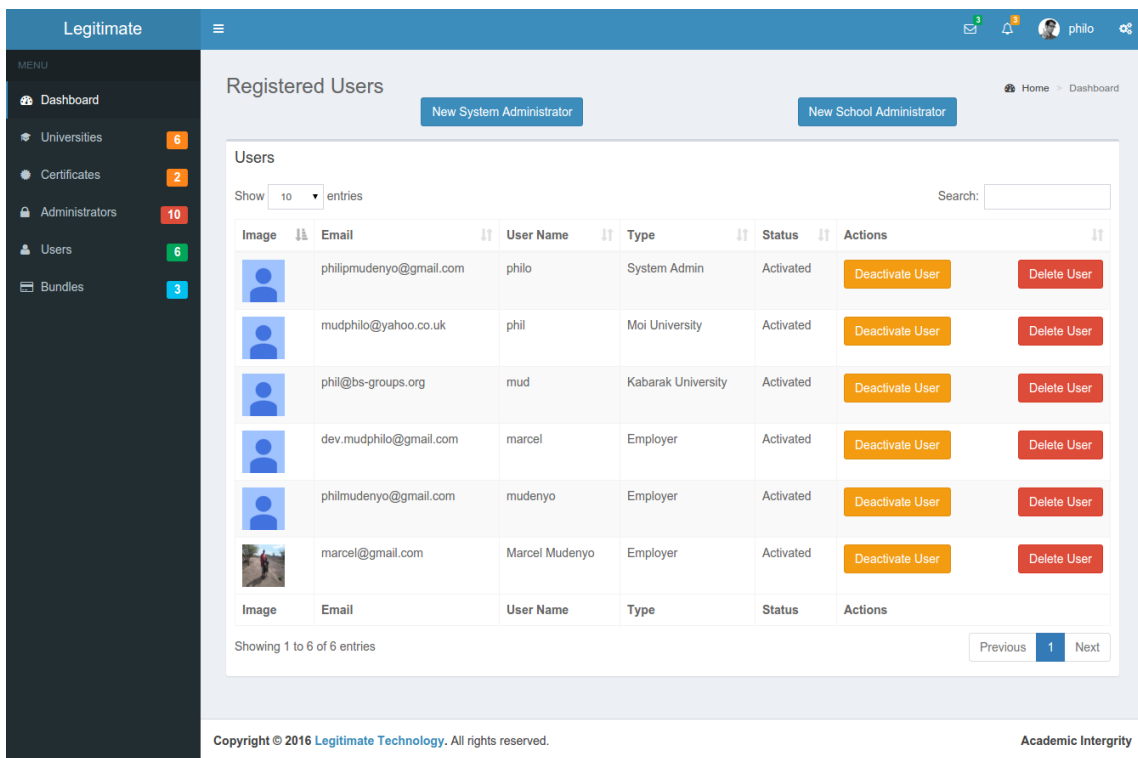


Figure 6.10 User Management

Add New University Administrator

This component is used by the system administrator to register a new university user into the system.

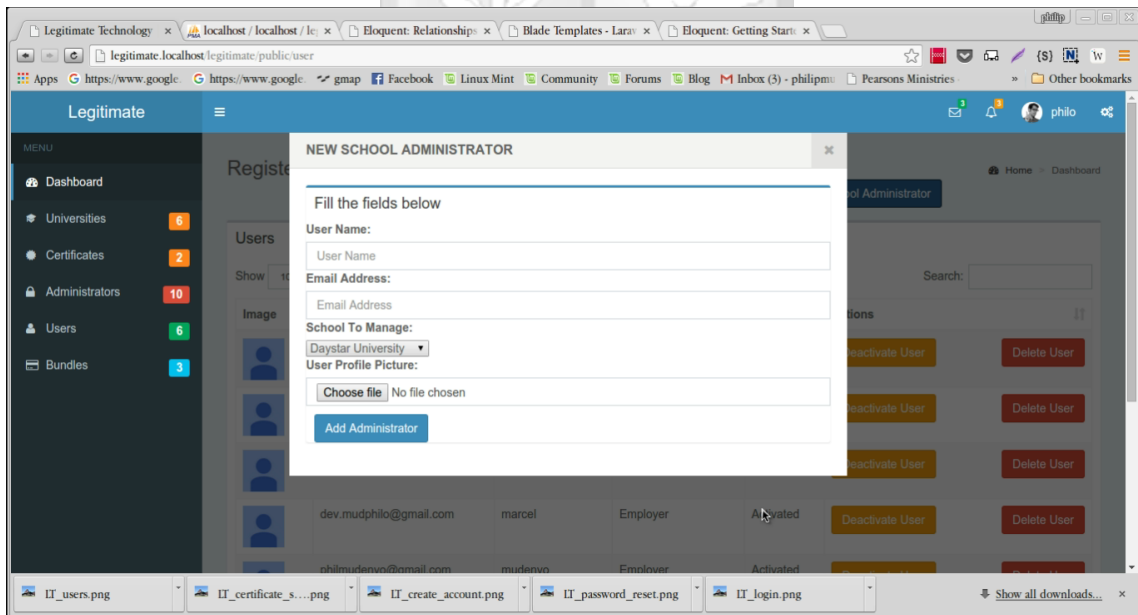
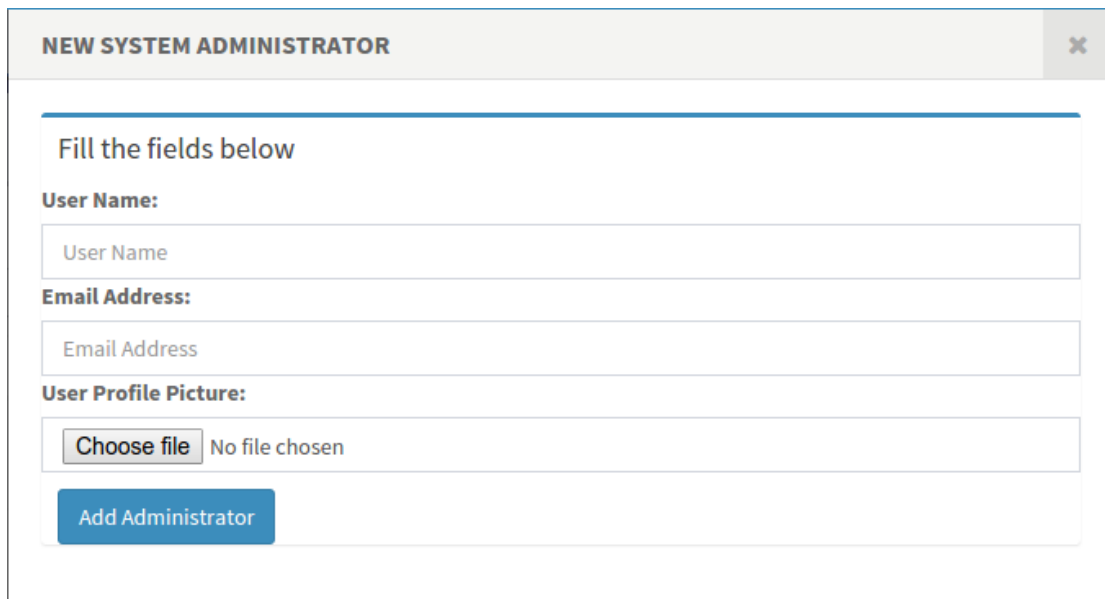


Figure 6.11 Adding a New User

Add New System Administrator

This component is used by the system administrator to register other system administrators into the system



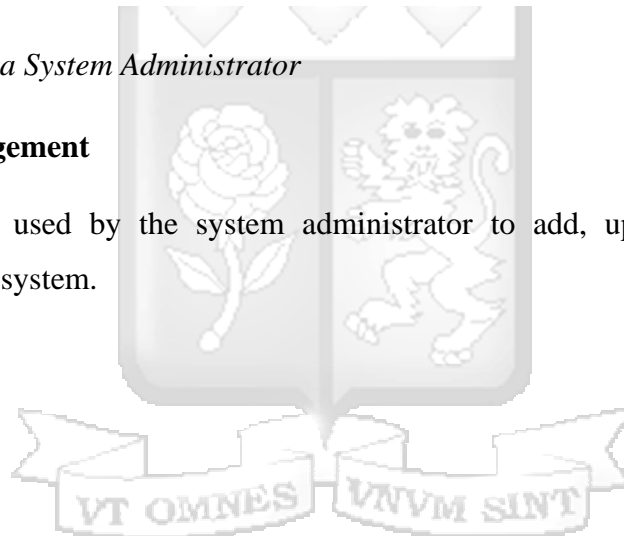
The screenshot shows a web form titled "NEW SYSTEM ADMINISTRATOR" with a close button (X) in the top right corner. The form contains the following fields and elements:

- A header section with the text "Fill the fields below".
- A "User Name:" label followed by a text input field containing the placeholder text "User Name".
- An "Email Address:" label followed by a text input field containing the placeholder text "Email Address".
- A "User Profile Picture:" label followed by a file selection area containing a "Choose file" button and the text "No file chosen".
- A blue "Add Administrator" button at the bottom of the form.

Figure 6.12 Adding a System Administrator







Universities Management

This component is used by the system administrator to add, update and delete universities into the system.



Dashboard New University Home > Dashboard

Integrated Universities Search:

Logo	Code	Name	Status	Task
	maseno	Masenos University	Active	Edit University Delete University
	moi	Moi University	Active	Edit University Delete University
	kabarak	Kabarak University	Active	Edit University Delete University
	uon	Universit of Nairobi	Active	Edit University Delete University
	kenyatta	Kenyatta University	Active	Edit University Delete University
	daystar	Daystar University	Active	Edit University Delete University
Logo	Code	Name	Status	Task

Showing 1 to 6 of 6 entries Previous 1 Next

[Print Table](#) [Download Table as PDF](#)

Figure 6.13 User Management

Add University

This component is used by the system administrator to add a university into the system.

NEW UNIVERSITY ✕

Fill the fields below

University Name:

University Code:

University Logo:

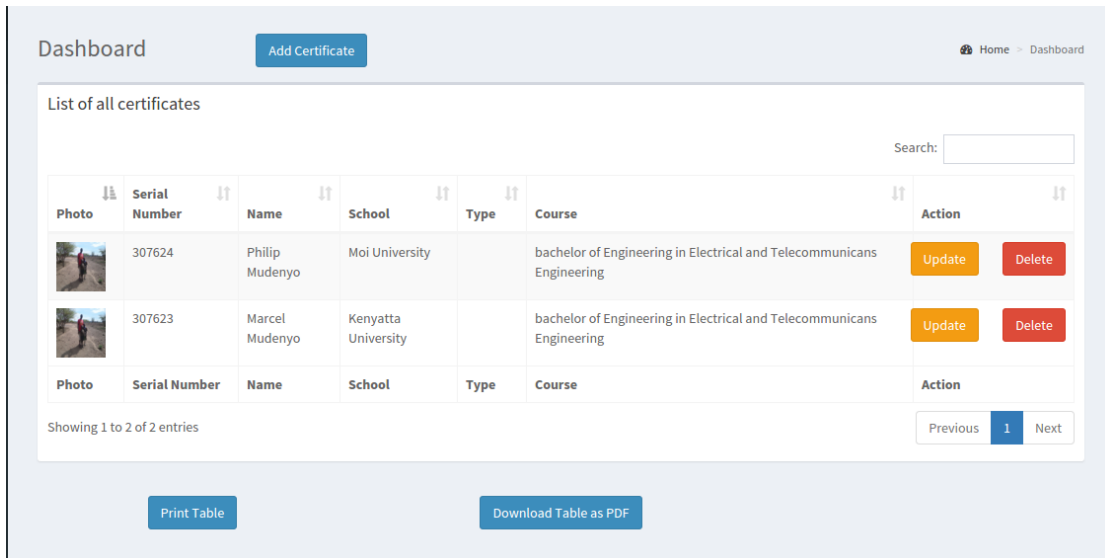
[Choose file](#) No file chosen

[Add University](#)

Figure 6.14 Add University

Certificates Management

The component also allow the university users to manage certificates by adding, updating and deleting details of certificates and to view verification reports which includes viewing number and details of verified certificates and reported fake certificates.



The screenshot shows a dashboard titled "Dashboard" with a navigation menu including "Home" and "Dashboard". A button labeled "Add Certificate" is visible. Below the dashboard header is a section titled "List of all certificates" with a search input field. The main content is a table with columns: Photo, Serial Number, Name, School, Type, Course, and Action. The table contains two entries:

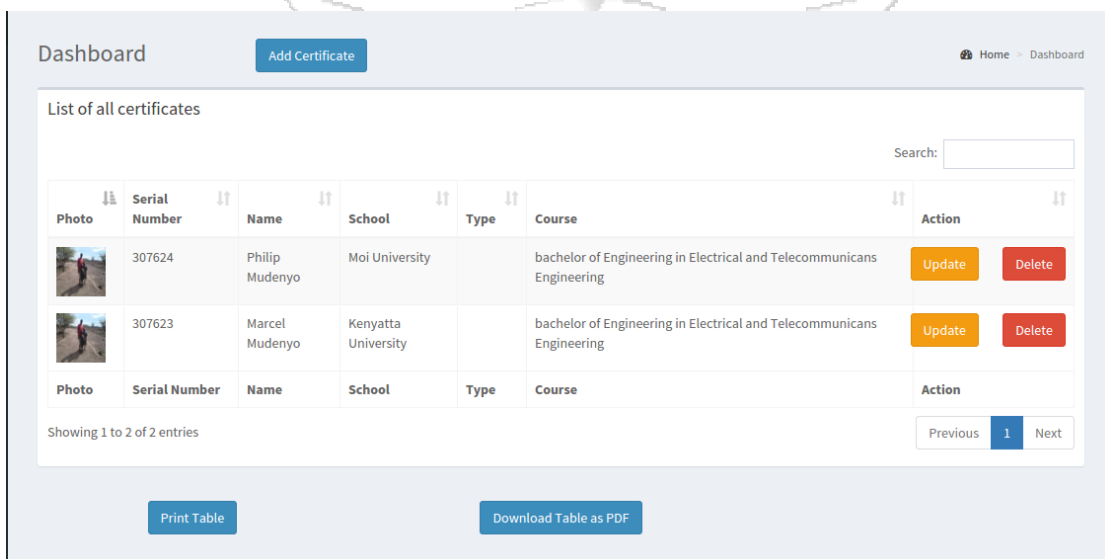
Photo	Serial Number	Name	School	Type	Course	Action
	307624	Philip Mudeny	Moi University		bachelor of Engineering in Electrical and Telecommunicans Engineering	Update Delete
	307623	Marcel Mudeny	Kenyatta University		bachelor of Engineering in Electrical and Telecommunicans Engineering	Update Delete

Below the table, it says "Showing 1 to 2 of 2 entries" and includes pagination controls for "Previous", "1", and "Next". At the bottom of the dashboard, there are buttons for "Print Table" and "Download Table as PDF".

Figure 6.15 Certificates Management

Registered Certificates

This component gives a list of all certificates registered into the system



The screenshot shows a dashboard titled "Dashboard" with a navigation menu including "Home" and "Dashboard". A button labeled "Add Certificate" is visible. Below the dashboard header is a section titled "List of all certificates" with a search input field. The main content is a table with columns: Photo, Serial Number, Name, School, Type, Course, and Action. The table contains two entries:

Photo	Serial Number	Name	School	Type	Course	Action
	307624	Philip Mudeny	Moi University		bachelor of Engineering in Electrical and Telecommunicans Engineering	Update Delete
	307623	Marcel Mudeny	Kenyatta University		bachelor of Engineering in Electrical and Telecommunicans Engineering	Update Delete

Below the table, it says "Showing 1 to 2 of 2 entries" and includes pagination controls for "Previous", "1", and "Next". At the bottom of the dashboard, there are buttons for "Print Table" and "Download Table as PDF".

Figure 6.16 Registered Certificates

Add Certificate

This system component allows the university staff to add details of a certificate into the certificate database. Figure 6.17 shows the screen short for the component for addition of a certificate.

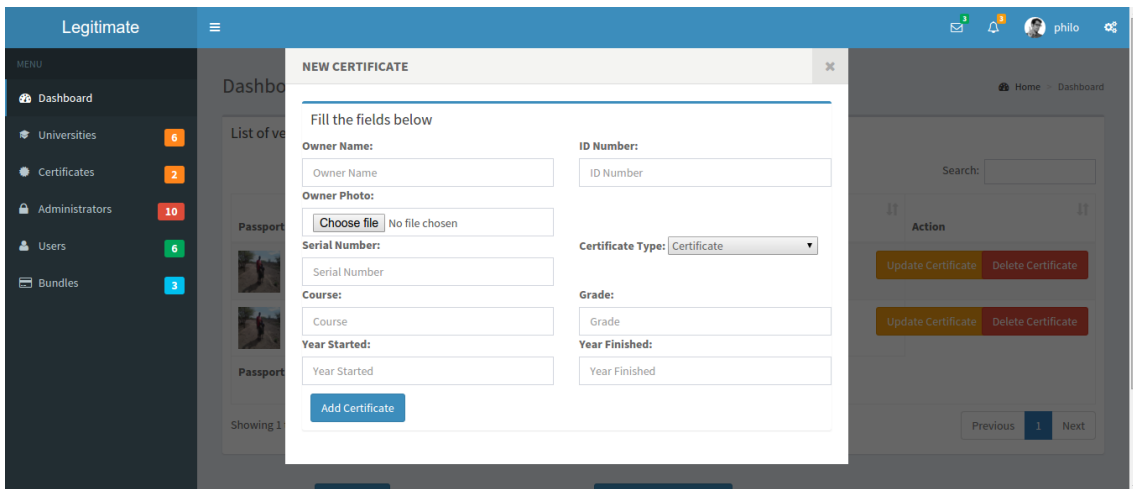


Figure 6.17 Add Certificate

Update Certificate

This system component allows the university staff to update details of a certificate. Figure 6.18 shows the screen short for the component for updating details of a certificate.

Delete Certificate

This system component allows the university staff to delete details of a certificate from the certificate database. Figure 6.18 shows the screen short for the component for addition of a certificate.

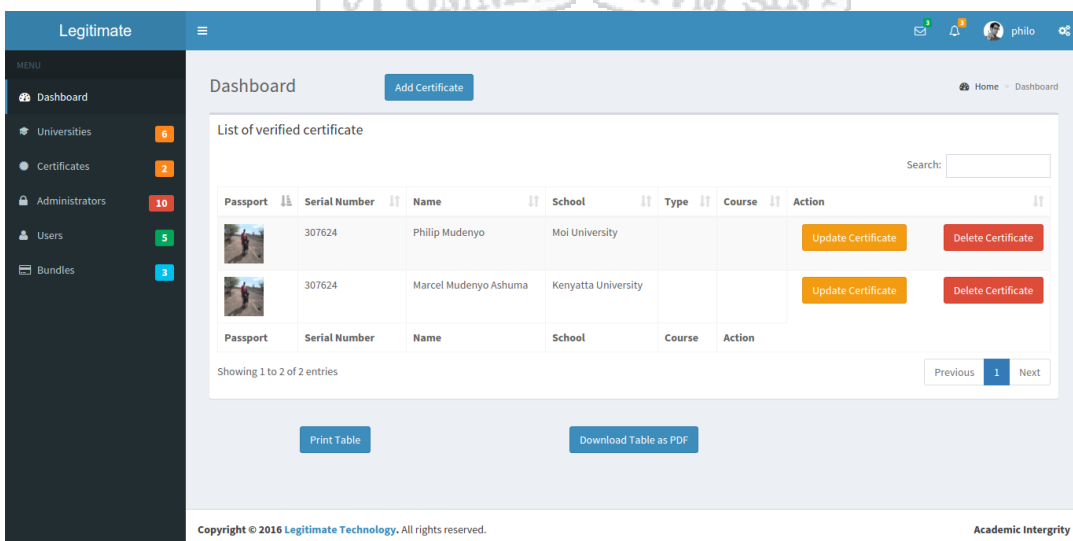
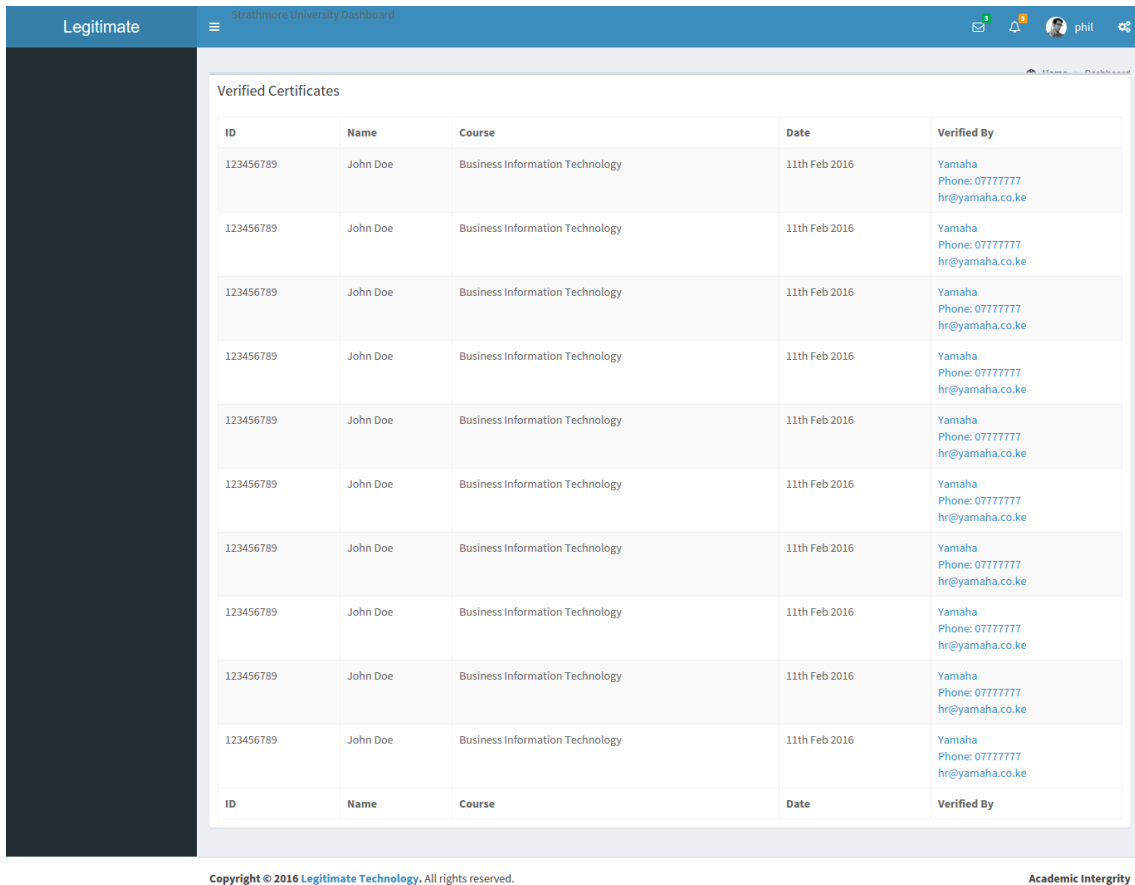


Figure 6.18 Update and Delete Certificate

Verification Details Reports

This system component generates a report for all the certificates verified and the users that verified the certificates, the time and dates of the verification.



Strathmore University Dashboard

Verified Certificates

ID	Name	Course	Date	Verified By
123456789	John Doe	Business Information Technology	11th Feb 2016	Yamaha Phone: 07777777 hr@yamaha.co.ke
123456789	John Doe	Business Information Technology	11th Feb 2016	Yamaha Phone: 07777777 hr@yamaha.co.ke
123456789	John Doe	Business Information Technology	11th Feb 2016	Yamaha Phone: 07777777 hr@yamaha.co.ke
123456789	John Doe	Business Information Technology	11th Feb 2016	Yamaha Phone: 07777777 hr@yamaha.co.ke
123456789	John Doe	Business Information Technology	11th Feb 2016	Yamaha Phone: 07777777 hr@yamaha.co.ke
123456789	John Doe	Business Information Technology	11th Feb 2016	Yamaha Phone: 07777777 hr@yamaha.co.ke
123456789	John Doe	Business Information Technology	11th Feb 2016	Yamaha Phone: 07777777 hr@yamaha.co.ke
123456789	John Doe	Business Information Technology	11th Feb 2016	Yamaha Phone: 07777777 hr@yamaha.co.ke
123456789	John Doe	Business Information Technology	11th Feb 2016	Yamaha Phone: 07777777 hr@yamaha.co.ke
123456789	John Doe	Business Information Technology	11th Feb 2016	Yamaha Phone: 07777777 hr@yamaha.co.ke
123456789	John Doe	Business Information Technology	11th Feb 2016	Yamaha Phone: 07777777 hr@yamaha.co.ke
123456789	John Doe	Business Information Technology	11th Feb 2016	Yamaha Phone: 07777777 hr@yamaha.co.ke

Copyright © 2016 Legitimate Technology. All rights reserved. Academic Integrity

Figure 6.19 Reports on Verified Certificates

Counterfeit Certificates Reports

This system component generates a report for all the certificates verified and reported as fake, the users that verified the certificates, the time and dates of the verification.

Utilized Use Case	Create Account
Results	Successful account creation and activation request sent to system administrator
Pass/Fail	Pass

Table 6.1 Creating User Account Test Case

Identifier	3
Test Case	Logging in or out of the system
Description	Users perform login with a username and password pair then logout.
Utilized Use Case	Login and Logout
Results	Successful login and access granted or Successful logout
Pass/Fail	Pass

Table 6.2 Logging In and Out Test Case

Identifier	4
Test Case	Verifying certificate
Description	Users verify certificate by scanning QR-Code/ barcode on the certificates or inputting the certificate serial number.
Utilized Use Case	Verify Certificate
Results	Certificate successfully verified as genuine or fake
Pass/Fail	Pass

Table 6.3 Verify Certificate Test Case

Identifier	5
Test Case	Reporting fake certificate
Description	Users report fake certificate by submitting the details of the certificate reported as fake.
Utilized Use Case	Report Fake Certificate

Results	Details of the fake certificate successfully submitted and received by the university that the fake certificate is purported to be obtained.
Pass/Fail	Pass

Table 6.4 Reporting Fake Certificate Test Case

Identifier	6
Test Case	Viewing verification reports
Description	Users query verification reports and the reports displayed to them
Utilized Use Case	View Verification Reports
Results	Verification reports successfully displayed to the user
Pass/Fail	Pass

Table 7 View Verification Reports Test Case

Identifier	7
Test Case	Manage certificates
Description	Users are able to add, update and delete certificates details
Utilized Use Case	Manage Certificates
Results	Certificate details successfully added, updated and deleted from the database
Pass/Fail	Pass

Table 6.6 Manage Certificates Test Case

Identifier	8
Test Case	Manage users
Description	Administrator is able to update user profile and user levels and also to activate and deactivate user accounts
Utilized Use Case	Manage Users
Results	User accounts updated, activated or deactivated successfully
Pass/Fail	Pass

Table 6.7 Manage Users Test Case

6.4.4 Compatibility Testing

Compatibility test was done to ensure that the mobile and web applications are compatible with the available platforms. The mobile application was tested against the available Android versions while the web application was tested against the available web browsers that are commonly used.

Android Platform Compatibility Testing

Compatibility test conducted for each of the available Android platforms is shown in Table 6.8 below.

Android Platform	Compatible
Android 10 (2.3.3)	Yes
Android 11 (3.0)	Yes
Android 12 (3.1)	Yes
Android 13 (3.2)	Yes
Android 14 (3.3)	Yes
Android 15 (4.0.3)	Yes
Android 16 (4.1.2)	Yes
Android 17 (4.2)	Yes
Android 19 (4.4)	Yes

Table 8 Android Platform Compatibility Test

Web Browser Testing

Browser types	Compatibility
INTERNET Explorer (versions 4 and above)	Yes
Firefox (version 8.0 and above)	Yes

Chrome (All versions)	Yes
-----------------------	-----

Table 6.9 Web Browser Test

6.4.5 Load Testing

Load testing was done by running the mobile application on different devices such as smart phones and tablets with android operating system to check the performance of the application, response time, resource utilization rate and the application breaking point. This was used to determine how long the application take to respond, how long it takes to give back result and under what circumstances does the application fail. The figure below shows a loaded page of verification results for a genuine certificate.

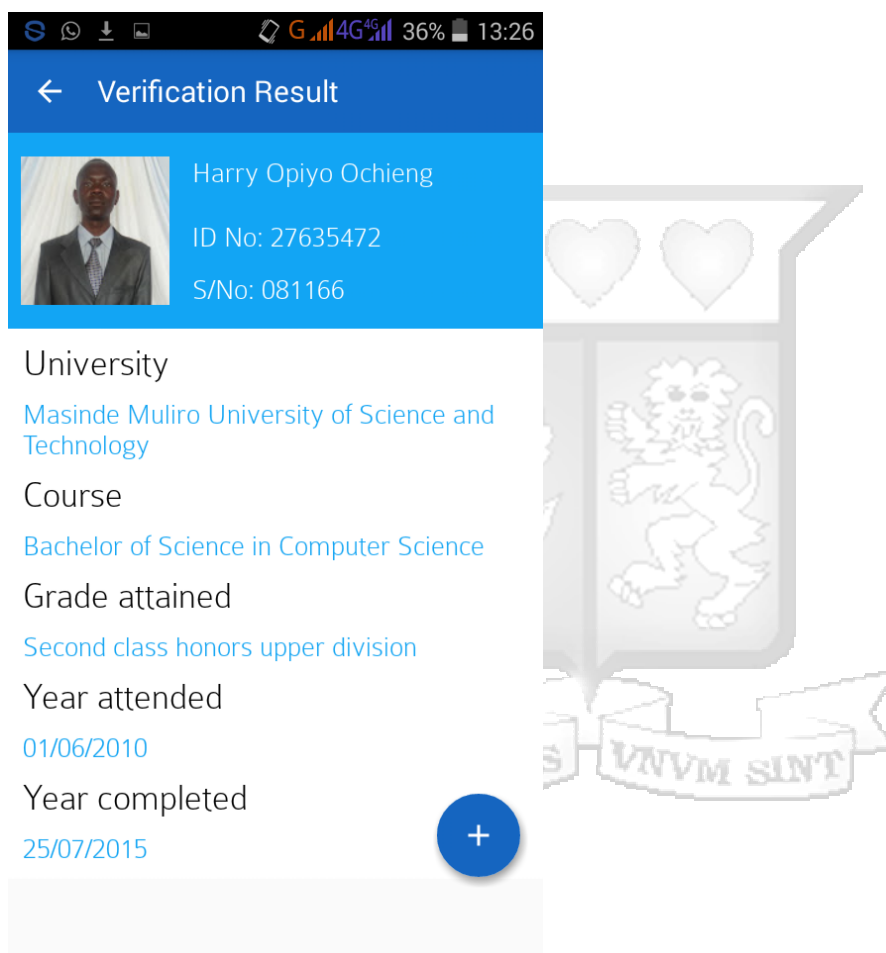


Figure 6.21 Verification Results for a Genuine Academic Certificate

6.4.6 Integration Testing

This was done by combining individual units of the application and then tested together. This type of testing was used to check how the entire application performed when all the units were integrated and working together.

6.5 User Testing

The end users of the application (target populations who are also) were directly involved in usability testing. A total of 18 respondents carried out the user testing and provided appropriate feedback which was used to refine the prototype until a satisfactory application was developed. 18 respondents participated in the user testing because they were the only ones who were available in the organizations while user testing was being carried out. User testing was done to achieve the following objectives:

- User friendliness
- Functionality
- Aesthetics
- Acceptance

Appendix D provides the user-testing questionnaire. Charts were used to represent user responses.

6.5.1 User Interface Aesthetics

The application appearance including the look and feel was tested by the end users. 77.3% of the respondents indicated that the application was attractive, 13.6% indicated that the application was fairly attractive while the remaining 9.1% of the respondents indicated that the application was not attractive at all. A summary of the results is shown in Figure 6.22

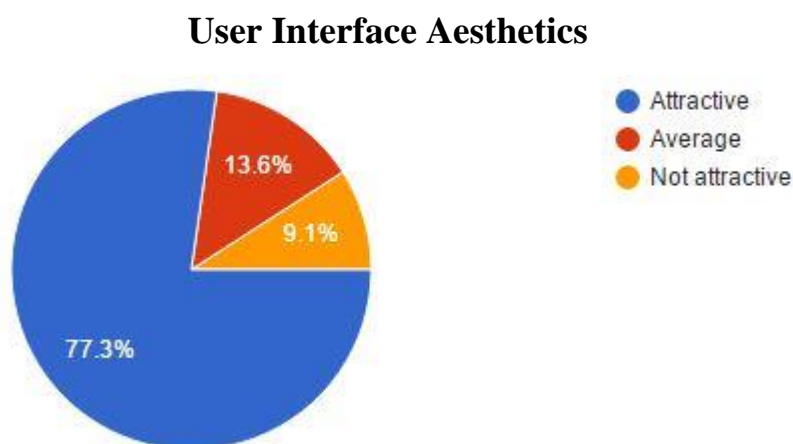


Figure 6.22 UI Aesthetic Feedback

6.5.2 User Friendliness

The ease of learning and using the application was tested by potential users. 68.2% of the potential users indicated that the application was easy to learn and use, they

managed to use the application without prior training. 22.7% indicated that the application was average meaning it was neither hard nor easy to learn or use, they needed the intervention of a trainer in some cases to confirm that what they were doing was right. The remaining 9.1% indicated that the application was difficult to use. Figure 6.23 shows a summary of the results.

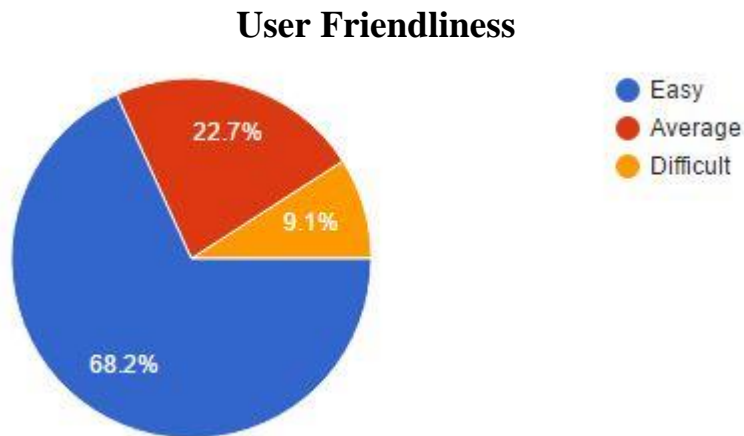


Figure 6.23 User Friendliness Feedback

6.5.3 Functionality

The end users of the application tested the system functionality against the user specifications. 76% of them indicated that the application's functionality was good meaning that the developer achieved most of the user functionality and requirements specification, 15.4 % indicated that the application's functionality was fair meaning that some of the user specifications were not entirely met, and the remaining 7.7% indicated that the application functionality did not meet the intended purpose of the application. This result was used to refine the prototype until an acceptable application was developed. A summary of the results is shown in Figure 6.24 below.

Functionality of the Application

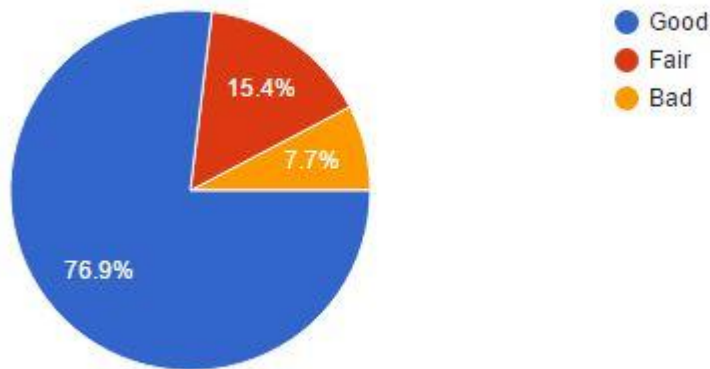


Figure 6.24 Test Results on Functionality of the Mobile Application

6.5.4 Acceptability

To measure if the application was great success user acceptance was tested. 78.6% of the potential users readily accepted the application for use in verification of academic certificates, 14.3% were undecided while the remaining 7.1% rejected the application. Since majority of the users readily accepted the application this test was a great success. Figure 6.25 provides a summary of these results.

Acceptability

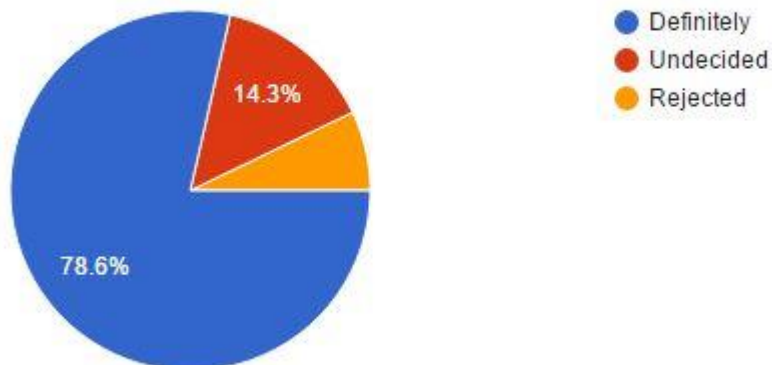


Figure 6.25 Acceptability Feedback

6.5.5 Validation

Validation was done in order to ascertain whether the implementation addressed the challenges that were raised as far as verification of academic certificates is concerned. An online questionnaire (In Appendix E) was designed and sent to end users to test

the applicability of the developed mobile application in verification of academic certificates in Kenya. 40% of the respondents were employers who do verification of academic certificates for their prospective employees, 20% were university academic registrars who verify certificates of their graduates to employers, and 20% were employees of recruitment agencies who also do verification of academic certificates for job candidates they recruit for companies and the other 20% were employees from qualifications verification companies that verify academic certificates of job candidates on behalf of employers. This is shown in Figure 6.26 below

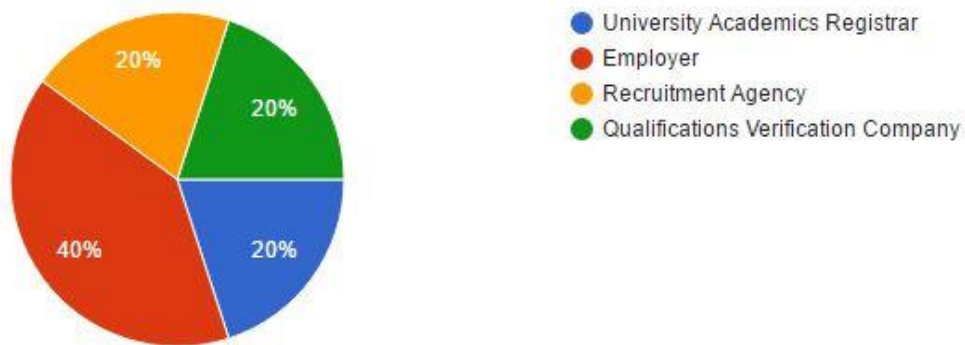


Figure 6.26 Applicability Test Respondents Categories

All the respondents who participated in the validation testing also participated in survey to collect user requirements and the usability test of the mobile application as shown in Figure 6.27 below. The respondents were asked to state whether they participated in the above mentioned survey and tests.



Figure 6.27 Respondents' Participation in User Requirements Survey and Usability Testing

The respondents were asked to indicate if the functionalities provided by the mobile application fully solves the problems posed by the current systems for verification of

academic certificates. 80% of the respondents indicated that the functionalities provided by the mobile application fully solves the problems that are currently posed by the current systems for verification of academic certificates while the other 20% stated that it partially solves the challenges. This is shown in Figure 6.28 below.

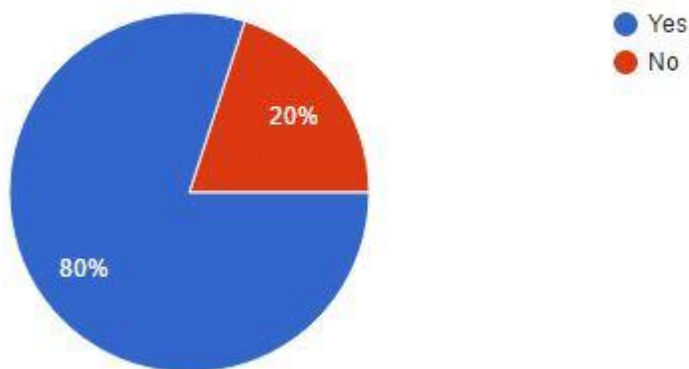


Figure 6.28 Respondents Take on Whether the Mobile Application Solves the Challenges Faced in Verification of Academic Certificates

The respondents who indicated that the functionalities provided by the mobile application fully solve the problems posed by the current systems for verification of academic certificates were further asked to state some of the key functionalities of the mobile application that provides solution to the current problems in verification of academic certificates. Some of the functionalities that the respondents stated as very key in the mobile application as far as verification of academic certificates is concerned included the functionality to display the details of a certificates including the Id number, names and photo of the holder of the certificate, the name of university attended, the course studied, grade attained and year of graduation. The other functionality that the respondents stated was the functionality to report to the universities certificates that purported to be issued by them but verified as fake. This was very important to the respondents as it involved submitting the details of the forged certificate and the details of the forger, as this would enable the universities to do follow up and persecute the forgers, which eventually would discourage forgeries of academic certificates. They also stated that the application provides instant verification results and therefore eliminates the time consuming process of manual verification of academic certificates. A number of university registrars also indicated that the instant provision of verification results eliminates the tedious and tiresome process of manual verification of academic certificates. In addition, the employers

indicated that the mobile application has also eliminated the high cost incurred in manual verification of academic certificates.

The respondents were also asked to indicate if they were satisfied with the solutions provided by the mobile application for solving problems in verification of academic certificates, and 60% of them expressed their satisfaction.

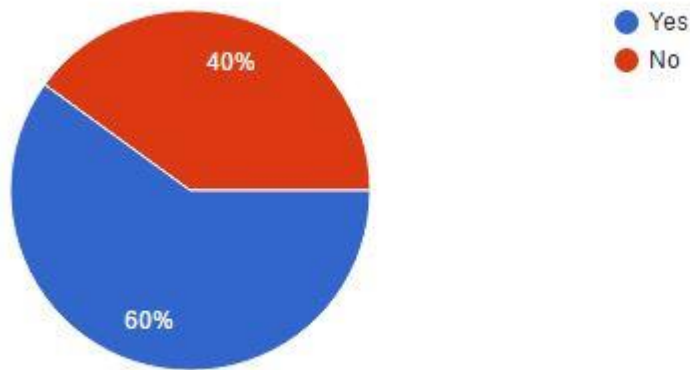


Figure 6.29 User Satisfaction on the Functionalities of the Mobile Application in Verification of Academic Certificates

Finally, the respondents were asked if they would recommend the mobile application to be adopted by all universities and employers in Kenya as an application solution to current challenges encountered in verification of academic certificates, and 80% of them indicated their confidence in the applicability of the mobile application in verification of academic certificates and recommended that the application should be adopted by all universities as a solution to solve the current problems faced by the current systems for verification of academic certificates.

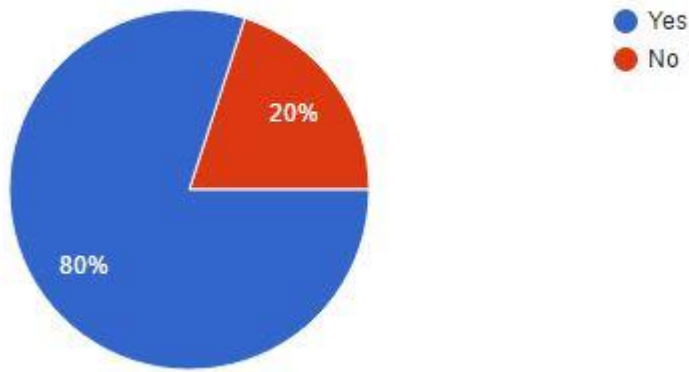
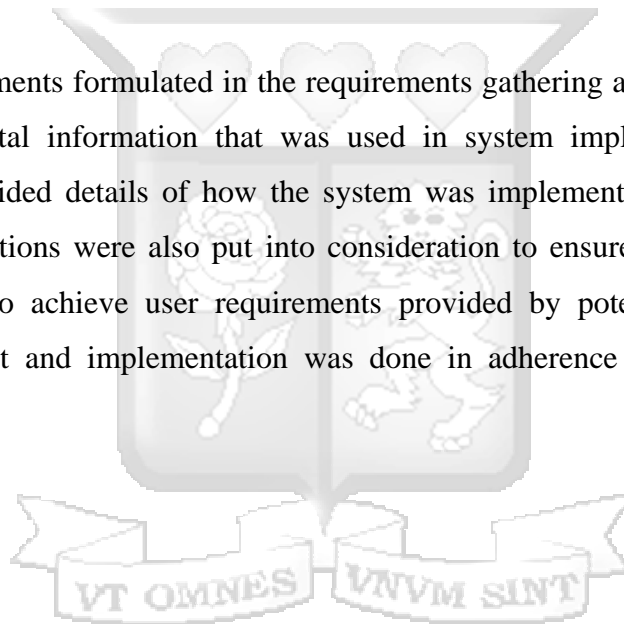


Figure 6.30 Respondents Recommendation on Adoption of the Mobile Application for Verification of Academic Certificates

6.6 Conclusions

The system requirements formulated in the requirements gathering and analysis stage provided fundamental information that was used in system implementation. The system design provided details of how the system was implemented. The research objectives and questions were also put into consideration to ensure that the system was implemented to achieve user requirements provided by potential users. The overall development and implementation was done in adherence to the proposed objectives.



CHAPTER 7: DISCUSSIONS

7.1 Introduction

The purpose of the research was to identify the challenges facing verification of academic certificates, to investigate the current techniques used for verification of academic certificates, to design, develop and test a mobile application for verification of academic certificates and to validate that the mobile application for verification of academic certificates solves the challenges faced using the current techniques for verification of academic certificates.

This was in order to identify and develop a suitable technique that will be adopted to address the current challenges faced in the verification of academic certificates. The research findings helped identify the appropriate technique which was adopted and a mobile and a web application that solves the current challenges were developed. By providing a mobile and web application for academic certificate verification, certificate verification was made easier, accurate and efficient.

The mobile application was developed for use by the employers who had access to a data enabled phone with a camera and running an android operating system. The web application was developed for management by system administrators and university users and could be accessed using a standalone computer, laptop or mobile device. This chapter describes research findings and achievements, how research objectives were obtained and it also provides a review of the application developed citing advantages and limitations of the developed application.

7.2 Findings and Achievements

A review of the literature indicated that the techniques used in verification of academic certificates include RFID, 2D Barcodes, online verification and manual verification. RFID application in certificate verification is expensive because the RFID chips and readers are expensive and experience many challenges due to lack of standards. 2D Barcodes have less security than RFID and can be more easily reproduced or forged. They are also more easily damaged. The manual process for verification of academic certificates is time consuming, tiresome and expensive.

The online verification is the most appropriate technique for verification of academic certificates since it is fast, affordable and cannot be forged. However, at present, there

is no unified system for online verification of academic certificates for all the universities in Kenya.

This research will therefore improve on the online techniques for verification by implementing a mobile application for verification of the legitimacy of academic certificates. Using a mobile application will maximise on the advantages of online verification and also bridge its gaps and limitations by providing a unified system for verification of academic certificates for all universities in Kenya.

The respondents were drawn from universities, recruitment agencies, employment companies and qualifications verification companies in Nairobi Kenya. 40% were staff in universities, 20% were from employment companies, 20% were from recruitment agencies and the other 20% were from qualifications verification companies. The respondents were also drawn from different departments in the organizations. 40% of the respondents were staff from the registrar of academic affairs while 20% were working in the examination departments in the universities and the other 40% were staff in the human resource departments in the employer companies, recruitment agencies and qualifications verification companies. All the departments that the respondents were drawn were involved in verification of academic certificates. 80% percent of the respondents were performing verification of academic certificates as their roles while the other 20% their previous roles included verification of academic certificates.

A total of 60% of respondents had had performed verification of academic certificates for over 3 years, indicating that the quality of respondents was good as most of them had participated in the process of verification of academic certificates.

All the respondents owned smart phones, of which, 80% had Android operating system and the other 20% had Windows phones. Since majority of the employees had smart phones with the Android operating system, Android was the preferred platform for the implementation of the proposed solution.

There was no automated system for verification of academic certificates as the system used was manual where the verification was done only by the universities that issued the certificates, by manually searching for the records of the academic certificates to be verified. Challenges faced in the current system includes: time wastage in the verification process, the process involves a lot of cost and the process is tiresome where many academic certificates need to be verified.

After providing a brief description of the mobile application, 80% of the respondents agreed that a mobile phone application would be viable solution for verification of academic certificates and would solve most of the challenges experienced in the verification process.

Based on the above-mentioned findings, an academic certificate verification application was designed and developed. It comprises of an Android mobile application and a web application. The Android mobile application is used mainly as the QR Code reader and capturing of academic certificate information while the web application is used for user management, data presentation and manipulation. Features of the application include verifying an academic certificate, generating verification reports and reporting academic certificates verified as counterfeit.

The application successfully passed the functional and user testing. In user testing a cumulative of 90.9% of the respondents stated that the application was attractive and fairly attractive, 68.2% of the respondents indicated that the application was easy to use, 76.9% of the respondents indicated that the applications' functionality was good and satisfactory, and the application was successfully accepted by 78.6% of the respondents.

7.3 Review of Research Objectives in Relation to the Mobile Application

This dissertation identifies the challenges faced in the verification of academic certificates, the academic certificate verification process and the techniques used for verification of academic certificates based on books, journals, websites and user feedback. A mobile and web application was designed and developed with a selected technique from the literature review and results from system analysis. The research objectives acted as a guideline to develop the mobile and web application.

The first objective was to identify the challenges faced in verification of academic certificates in Kenya. This objective was achieved through the use of an online questionnaire provided in Appendix C. Analysis of the responded feedback yield to the following challenges: time wastage, cumbersome, expensive, and failure by universities to respond to verification requests. The mobile and web application was developed to address the mentioned challenges.

The second objective was to investigate the current techniques used in verification of academic certificates. This information was useful as it enabled the researcher to gain an understanding of the techniques used and identify the strengths and weaknesses of each technique hence choosing the best technique to be adopted. This objective was

achieved by the review of literature based on the current techniques for verification of academic certificates used globally. Available techniques include: use of 2D Barcode, RFID, Online Verification and manual verification. Based on the information gathered and requirements provided by the respondents, online verification emerged to be the best technique for implementation of the academic certificate verification system.

The third objective was to design, develop and test a mobile-based solution for for verification of academic certificates. This objective was achieved through the design, implementation and testing of the mobile and web application. The mobile application was developed for the Android platform while the web application was developed using the Laravel 5.1 Framework. The following tests were carried out; integration testing, load testing, functional testing where the system functionality was tested, compatibility testing where the mobile application was tested against different Android versions and the web application was tested against different web browsers and finally user testing where the aesthetics, user friendliness, application functionality and user acceptance were tested.

The fourth objective was to validate that the mobile application for verification of academic certificates solves the challenges faced using the current techniques for verification of academic certificates. . This objective was achieved using an online questionnaire (In Appendix E). The respondents were asked to state weather the functionalities provided in the mobile applications were providing solutions to the challenges currently faced in verification of academic certificates, if they were satisfied with the mobile applications as solution in verification of academic certificates and if they would recommend the mobile application to be adopted for verification of academic certificates in Kenya. 80% of the respondents indicated that the features provided in the mobile application provides solutions to the challenges faced in verification of academic certificates, 60% indicated that they were satisfied with the solution provided with mobile application to be used as a solution to verification of academic certificates and 80% indicated that they would recommend the mobile application to be used for verification of academic certificates in Kenya.

7.4 Review of the Application in Relation to Current Methods Used for Verification of Academic Certificates

The proposed system is an Android application for verification of academic certificates. It uses a mobile phone inbuilt camera to capture a QR-Code printed on a

certificate, a QR-Code reader application analyses the QR-Code and returns a unique number stored in the QR-Code. This number is used as the unique identifier of the certificate. The unique certificate identifier is used in the certificate verification system (linked to QR-Code reader) for capture and retrieving of certificate information. Features of the application include: verify certificate, report fake certificate and generate verification reports.

The organisations in which the research was based on uses a manual verification technique for verification of academic certificates. This is clearly stated in the research findings where 80% of the respondents indicated that the certificate verification technique used is manual.

7.4.1 Advantages of the Application

Advantages of the application in relation to the current certificate verification techniques used in the organization include the following:

- i. It minimizes the time usage while tracking certificates.
- ii. It eliminates the budgets for verification.
- iii. It cannot be forged.
- iv. The application offers legitimacy
- v. The application offers real-time online access to information on certificates remotely and anywhere globally.
- vi. The application incorporates a web application that can be used for data manipulation and data representation

7.4.2 Limitations of the Application

The limitations of the application include the following:

- i. The mobile application can only be used by smart phone users with Android operating system.
- ii. The mobile application requires Internet connectivity for it to work.
- iii. The application does not cater for generation and printing of QR-Codes.
- iv. The application verification for only academic certificates.

CHAPTER 8: CONCLUSIONS, RECOMMENDATIONS AND FUTURE WORK

8.1 Conclusions

Information about verification of academic certificates and techniques used for verification of academic certificates was reviewed. From analysis carried out, the results pointed out that there are major problems in verification of academic certificates.

The result was the development of an academic certificate verification mobile and web application. The key features of the application include: verifying an academic certificates, reporting a fake certificate and generating reports. The application was aimed at: fast and easy retrieval of information on academic certificates, elimination of costs for verification of certificates, reporting fake certificates and generating verification reports. System testing was performed, look and feel, ease of use, system functionality and acceptance was done.

8.2 Recommendations

Verifying academic certificates for prospective job employees' is very important since it saves employers financial losses that results from employment of incompetent and unqualified employees. Therefore, my recommendations for the application to work better is, firstly, the universities should allow this application have access to their academic certificates details by registering their certificates to the central database, so that employers can have concrete details to validate an academic certificates before employing a job candidate. Secondly, before employing a graduate of any university, employers should verify the validity of their academic certificates. This is to be achieved by downloading the application on their phones and using it for verification of academic certificates.

8.3 Future Work

The weaknesses and limitations of the proposed solution in the research study have indicated the following areas as recommendations for further work.

- i. The application should add a model for QR-Code generation and printing.
- ii. The application should be developed for other mobile platforms to allow employers with phones other than Android to access the application's functionality.

- iii. The application can include other types of academic documents for example academic transcripts.



REFERENCES

- Adams. (2014, December 12). *EMD Sorono launches Anti-counterfeit App*. Retrieved February 15, 2015, from Securing Industry: <http://www.securindustry.com/>
- Adaptalift. (2012). *RFID VS BARCODES: Advantages and disadvantages comparison*. Retrieved from Adaptalift: http://www.aalhyterforklifts.com.au/index.php/about/blog-post/rfid_vs_barcodes_advantages_and_disadvantages_comparison
- Allen, S. (2012). The benefits of employer investment in qualifications for the workforce. *Benefits of qualifications*.
- Andy. (2008, April 8). *Piracy, Bootlegging, and Counterfeiting*. Retrieved March 5, 2015, from Andy on the Road: <http://www.Andyontheroad.wordpress.com>
- Barry, F. (2014, December 16). *Anti-counterfeiting*. Retrieved February 20, 2015, from in-Pharma: <http://www.in-pharmatechnologist.com/>
- Bent, K. (2014, November 11). *Xerox Cracks Down On Counterfeit*. Retrieved March 19, 2015, from CRN: <http://www.crn.com/>
- Bently, John E. Wachovia Bank, Charlotte NC. (2004). Planning, Development and Support. *Concepts, Roles, and Terminology*, 12.
- Boehm, B. (2007). *A Survey of Agile Development Methodologies*.
- Columbia University. (2016). *Certifications*. Retrieved from Office of the University Registrar: <http://registrar.columbia.edu/content/certifications>
- Commission For University Education. (2012). *Recognition and Equation of Qualifications*. Retrieved from Commission For University Education.
- COMMUNICATIONS AUTHORITY OF KENYA. (2015). *FIRST QUARTER SECTOR STATISTICS REPORT FOR THE FINANCIAL YEAR 2015/2016*. Nairobi.
- Craddock, A., Roberts, B., Godwin, J., Todor, D., & Richards, K. (2014). *The DSDM Project Framework for Scrum*.
- Crawley, E. (2007, January 15). *System Architecture*. Retrieved March 11, 2015, from MITOpenCourses: <http://ocw.mit.edu/>
- Daily Nation. (2012). *Minister issues forged certificates warning to civil servants*. Retrieved from Daily Nation:

<http://www.nation.co.ke/News/politics/Minister+issues+forged+certificates+warning/-/1064/1489612/-/m7uquy/-/index.html>

Davies, R. (2004). *DSDM Explained*.

Embassy of India. (2016). *Verification of Genuineness of Certificates*. Retrieved from Embassy of India: <http://indembassyuae.org/verification-of-genuineness-of-certificates/>

Escobar, B. (2005). *WIPO/OECD EXPERT MEETING ON MEASUREMENT AND*. Santiago, Chile: Minister of the Economy and Energy- Chile.

Fighting Counterfeit Drugs With Mobile Technology. (2015, January 20). Retrieved February 25, 2015, from mPedigree: <http://mpedigree.net/>

Flora, H. K., & Chande, S. V. (2014). A Systematic Study on Agile Software Development Methodologies and Practices. *International Journal of Computer Science and Information Technologies*.

Fricker, R. (2013). *Target Populations, Sampling Frames, and Coverage Error*.

Gao, J. Z., Prakash, L., & Jagatesan, R. (2007). Understanding 2D-BarCode Technology and Applications in M-Commerce – Design and Implementation of A 2D Barcode Processing Solution. *Computer Society*.

Garwe, E. C. (2015). Qualification, Award and Recognition Fraud in Higher Education in Zimbabwe. *Macrothink Institute*.

Glasner, M. (2015, March). Keeping in check: Why Background Screening is Needed. *HR Strategy*.

Golafshani, N. (2003). *Understanding Reliability and Validity in Qualitative Research*.

Government of Kenya. (2010). *The Constitution of Kenya*. Nairobi: National Council for Law.

Grolleau, G., Lakhali, T., & Mzoughi, N. (2008). An Introduction to the Economics of Fake Degrees. *Journal of Economic Issues*.

Gupta, V. (2013). A NATIONAL ACADEMIC DEPOSITORY. Portugal.

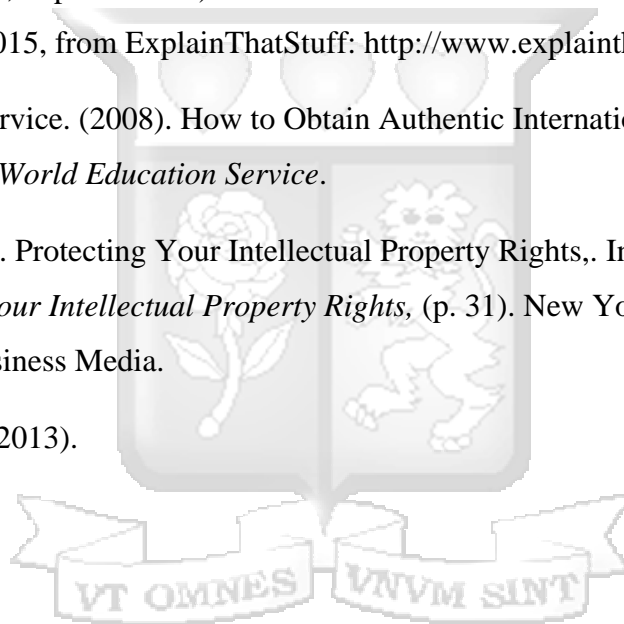
HandBook, W. I. (2008). *Intellectual Property HandBook*. Geneva: WIPO PUBLICATION.

- Hewlett-Packard. (2006). *Document Authentication System- Preventing and Detecting Fraud of Paper Documents*.
- IACC. (2005). *Negative Consequences of International Intellectual Property Theft*. Washington: IACC Publications.
- ICC. (2014, October 12). *Global Impact Study*. Retrieved January 29, 2015, from International Chamber of Commerce : <http://www.iccwbo.org/>
- Ilie-zudor, E., Kemeny, Z., Egri, P., & Monostori, L. (2006). THE RFID TECHNOLOGY AND ITS CURRENT APPLICATIONS. *Computer and Automation Research Institute, Hungarian Academy of Sciences*. Hungary.
- KACA. (2011, May 29). *IP Kenya*. Retrieved December 22, 2014, from Intellectual Property From a Kenyan Perspective: <https://ipkenya.wordpress.com>
- Kaur, M., Sandhu, M., Mohan, N., & Sandhu, S. P. (2011). RFID Technology Principles, Advantages, Limitations & Its Applications. *International Journal of Computer and Electrical Engineering*.
- Kendall, K. E. (2006). *System Analysis and Design*.
- Kenya University. (n.d). *Kenya's Academic Verification Process*.
- Khan, A. I., Qurashi, R. J., & Khan, U. A. (2011). A Comprehensive Study of Commonly Practiced Heavy & Light Weight Software Methodologies. *IJCSI International Journal of Computer Science*.
- Korte, T. (2013, July 19). *Using Data To Fight Counterfeit Goods*. Retrieved February 26, 2015, from The Innovation Files: <http://www.innovationfiles.org/>
- Krishna, S., Sreekanth, S., & Reddy, K. K. (2012). Explore 10 Different Types of Software Development Process Models. *International Journal of Computer Science and Information Technologies*.
- Kuacharoen, P., & Warasart, M. (2012). Paper-based Document Authentication using Digital Signature and QR Code. *International Conference on Computer Engineering and Technology*.
- Levin. (2009). A safe harbor for trademark. *Reevaluating secondary trademark liability after Tiffany v. eBay*, 24.

- Lorenzetti, L. (2013, July 10). *uFaker app turns consumers into detectives*. Retrieved february 26, 2015, from New York Business:
<http://www.crainsnewyork.com/news>
- Mahapatra, H. B., & Goswami, B. (2015). Selection of Software Development Methodology (SDM): A Comparative Approach. *International Journal of Advanced Research in Computer Science and Software Engineering*.
- Mainwaring, K. (2015, January 8). *Counterfeiting A Growing Problem*. Retrieved January 30, 2015, from Advanced Intellectual Property Protection:
<http://www.agmaglobal.org/>
- Mathew, K. (2014). *An Inquiry into Background Checks at Learning Institutions in Kenya*.
- Mellisa. (2012, October 24). *Sproxil uses Mobile Phone to Counter Counterfeit Drugs*. Retrieved December 19, 2014, from Socila Enterprice Buzz :
<http://SocialEnterpriseBuzz.html>
- Nalika, P. (2013, February 6). *East Africa Cables to fight counterfeits with Zinduka mobile app*. Retrieved February 25, 2015, from CIO:
<http://http://www.cio.co.ke/>
- Narayanan, S. (2012). QR Codes and Security Solutions. *International Journal of Computer Science and Telecommunications*.
- National University of Singapore. (2016, 02 16). *Degree Verification*. Retrieved 02 16, 2016, from National University of Singapore:
<http://www.nus.edu.sg/registrar/adminpolicy/degverify.html>
- Nuffic. (2015). The Kenyan education system described and compared with the Dutch system. *Education system*.
- Peter, N. (2013, February 6). *East Africa Cables to fight counterfeits with Zinduka mobile app*. Retrieved February 25, 2015, from CIO: <http://www.cio.co.ke/>
- Qualifications Verification Services. (2016). *Verify South African academic qualifications and student enrolments online*. Retrieved from Qualifications Verification Services:
<https://www.qvs.co.za/about.jsp?z=1&f=help&p1=about>

- Qualtrics. (2013). *Determining Sample Size: How to Ensure You Get the Correct Sample Size*. Retrieved from Qualtrics Website:
<http://www.qualtrics.com/blog/determining-sample-size/>
- Quest Staffing Solutions. (2014). *A REPORT ON THE CULTURE OF DISHONESTY -FRAUDULENT QUALIFICATION & FALSIFIED CURRICULUM VITAE*.
- Rastogi, V. (2015). Software Development Life Cycle Models Comparison, Comparison, Consequences. *International Journal of Computer Science and Information Technologies*.
- Roberts, M. C. (2006). Radio frequency identification(RFID). *computers & security*.
- Sangani. (2010). *Buyer beware:Engineering & Technology*. New York: IET.
- Schuchert-Guller. (2006). *Explaining Counterfeit Purchase*. Berlin: Academy of Marketing Science.
- Singhal, A., & Pavithr, S. R. (2015). Degree Certificate Authentication using QR Code and Smartphone. *International Journal of Computer Applications*.
- Sowder. (2013, June). *The Harmful Effects of Counterfeit Goods*. Retrieved February 4, 2015, from Athens State University: <http://www.athens.edu.co>
- TalTech. (2014, September 16). *How a Barcode Reader Works*. Retrieved March 12, 2015, from TalTech: <http://www.taltech.com/>
- TaTa Consultancy Services. (2009). *SmartDEGREE from TCS to combat Certificate Malpractices*.
- The Hindu. (2013, May 27). *Certificate verification goes online*. Retrieved February 16, 2016, from The Hindu: <http://www.thehindu.com/todays-paper/tp-features/tp-educationplus/certificate-verification-goes-online/article4754468.ece>
- Times Higher Education. (2002, February 15). *Kenya smashes fake degree scam*. Retrieved from The World University Rankings:
<https://www.timeshighereducation.com/news/kenya-smashes-fake-degree-scam/167201.article>
- Tudor, D. (2006). *PRINCE2 and DSDM: Why should I use both?*
- TutorialPoint. (2009). *Software Testing*. New York: Tutorial Point.

- Victor, E. C., & David, A. O. (2014). Character Proximity For RFID Smart Certificate System: A Revolutionary Security Measure To Curb Forgery Menace. *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*.
- Voigt, B. (2004). *Dynamic System Development Method*.
- walonick, D. S. (2011, November 20). *The Research Process*. Retrieved March 5, 2015, from Research Library: <http://www.statpac.org/>
- Weis, S. A. (2007). *Rfid (radio frequency identification): Principles and applications*.
- WIPO. (2008). *Intellectual Property HandbOOK*. Geneva: Wipo Publication.
- Woodford. (2014).
- WoodFord, C. (2014, September 14). *Barcodes and barcode scanners*. Retrieved March 10, 2015, from ExplainThatStuff: <http://www.explainthatstuff.com/>
- World Education Service. (2008). How to Obtain Authentic International Academic Credentials. *World Education Service*.
- Zimmerman. (2013). Protecting Your Intellectual Property Rights,. In Zimmerman, *Protecting Your Intellectual Property Rights*, (p. 31). New York: Springer Science+Business Media.
- Zimmerman, P. C. (2013).



APPENDICES

Appendix A: Authorization Letter to Carry out Research



Our Ref.: iLab/PP/16/83

08 March 2016.

TO WHOM IT MAY CONCERN

Dear Sir/Madam,

Re: Harry Ochieng - 84953

This is to certify that the above named is currently a student of Strathmore University undertaking Master of Science in Mobile Telecommunications and Innovation (MSc.MTI) in the Faculty of Information Technology.

The student is in his final (2nd year) of study and is seeking approval from you to collect data for his research project for *verification of academic certificates issued by universities and colleges in Kenya*.

The data is necessary for him to complete the Master's course.

Any assistance given to him will be highly appreciated.

Please contact us in case of any further clarifications.

Yours faithfully,

Dr. Everlyne Makhanu
Academic Director
emakhanu@strathmore.edu




Keri Road, Madaraka Estate
P.O. Box 59857 00200 City Square Nairobi Kenya
t: +254 (0) 703 034 000
f: +254-20: 600 7498

www.iLabAfrica.ac.ke www.strathmore.edu

Figure A1 Authorization Letter to Carry out Research

Appendix B: Certificate Verification Request Letter

 **Kenya Airports Authority**

Head Office, Airport North Road
P.O. Box 19001 - 00501 Nairobi, Kenya
Tel: +254 - 020 - 822111 / 6611000 / 6612000
Fax: +254 - 020 - 822078, 827304
Email: info@kenyaairports.co.ke
www.kenyaairports.co.ke

CAA/10/02 VOL. 7 (55)
THE REGISTRAR

STRATHMORE UNIVERSITY

NAIROBI
11.4.2015
Dear Sir/Madam

RE: VERIFICATION OF CERTIFICATES

Kenya Airports Authority would like to verify the Academic Certificates of its staff who have indicated that they studied in your Institution as shown below:

No.	Names	Degree Course	year	Registration number	I/D No.
1	Simon Peter	MBA	2012	MBA/0499/09	14546621

Please verify and revert to us as soon as possible.

Yours Faithfully,

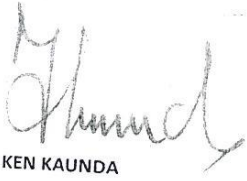

KEN KAUNDA
GENERAL MANAGER (HRD)

Figure B1 Certificate Verification Request Letter

Appendix C: Academic Certificate Verification Questionnaire

Academic Certificate Verification Questionnaire

University Survey

* Required

You are invited to participate in a research study investigating the implementation of a prototype for academic certificate verification using Mobile Application Technology.

The information collected through your participation will be purely used for academic purposes.

1. What is your name? (Optional)

2. Which category best describe your organisation? *

- University Academics Registrar
- Employer
- Recruitment Agency
- Qualifications Verification Company

3. Which department are you? *

- HR
- IT
- Administration
- Registrar Academics
- Other

If other, please specify

4. Does your department carry out verification of academic certificates? *

- Yes

No

5. Does your role in your department include verification of academic certificates? *

Yes

No

6. If yes, for how long have you performed this role? *

0 - 1 year

1 - 3 years

3 - 5 years

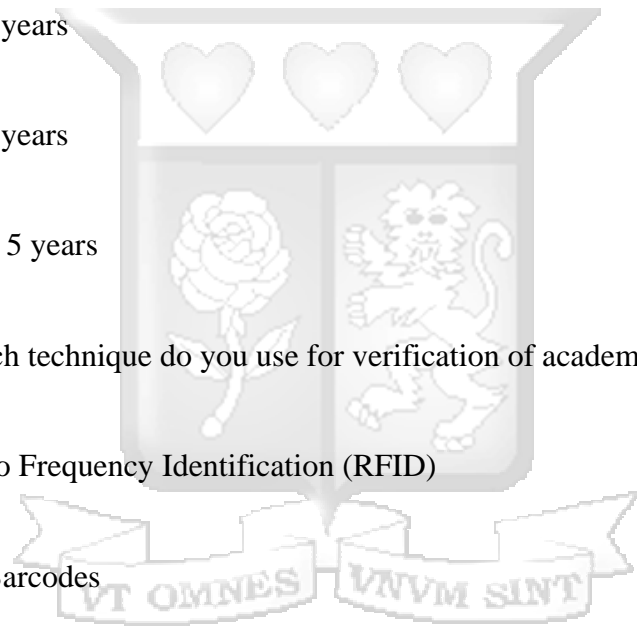
Over 5 years

7. Which technique do you use for verification of academic certificates?

Radio Frequency Identification (RFID)

2D Barcodes

Manual Verification



8. Describe the process for verification of academic certificate *

.....

.....

.....

.....

.....

9. What are the parameters you use to determine legitimacy of the certificate? *

Check all that apply.

University Name

University Logo

University Seal

Candidate's Name

Candidates Id No

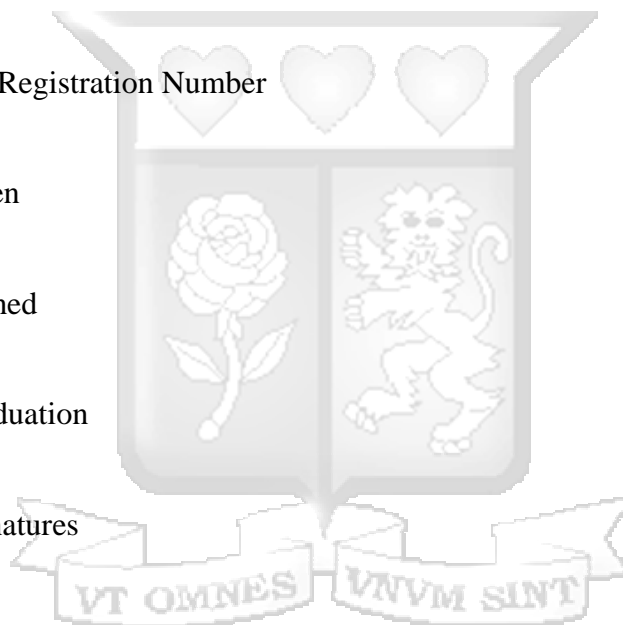
Candidate's Registration Number

Course Taken

Grade Attained

Date of Graduation

Issuer's Signatures



10. How long does it take (in terms of number of days) to verify an academic certificate using the current methods? *

11. How much do you charge/pay (in KES) for verification of academic certificate using the current methods? *

12. Have you ever had cases where job candidate forges your academic certificates? *

- Yes
- No

14. If yes, how often do you experience this?

.....

.....

.....

.....

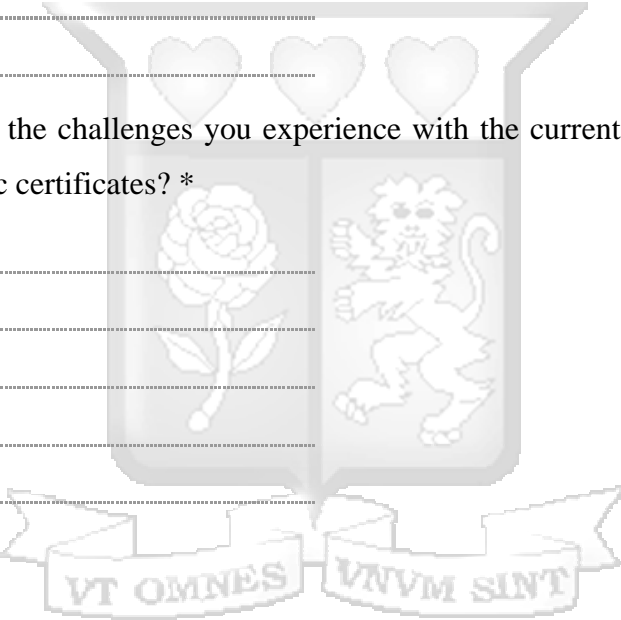
15. What are some of the challenges you experience with the current methods for verifying academic certificates? *

.....

.....

.....

.....



16. Do you own a smartphone? *

- Yes
- No

17. If yes, which operating system does your phone have? *

- Android
- IOS
- Windows
- Blackberry
- Other

If other, please specify

18. Do you use other mobile applications apart from calling and messaging? *

- Yes
- No

19. If yes, name 3 applications that you use mostly *

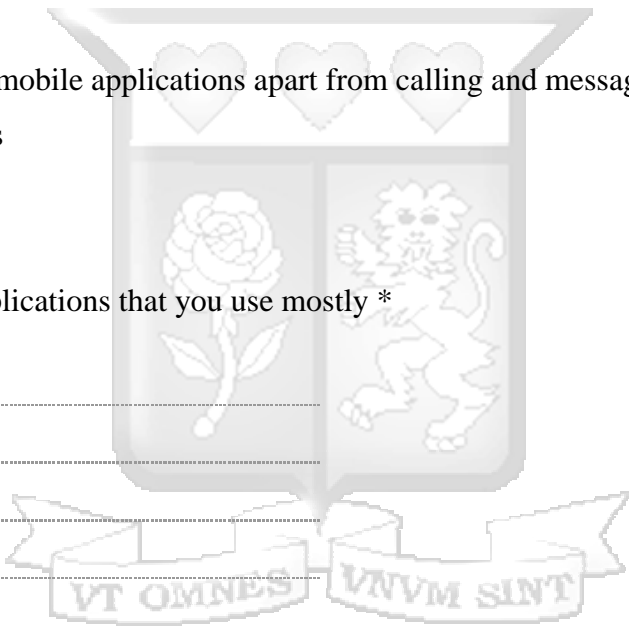
.....

.....

.....

.....

.....



20. Do you think a mobile application will solve the mentioned challenges? *

- Yes
- No

21. What features do you think application should have?

.....

.....

.....

.....

.....

Appendix D: User Testing Questionnaire

Certificate Verification System

User Testing Questionnaire

1. Did you manage to perform the following task? (Indicate Yes or No)

a) Create account

- Yes
- No

b) Activate and deactivate user accounts (only for system administrators)

- Yes
- No

c) Update users' profiles (only for system administrators)

- Yes
- No

d) Login and logout

- Yes
- No

e) Verify certificates

- Yes
- No

f) Report fake certificates

- Yes
- No

g) View verification reports

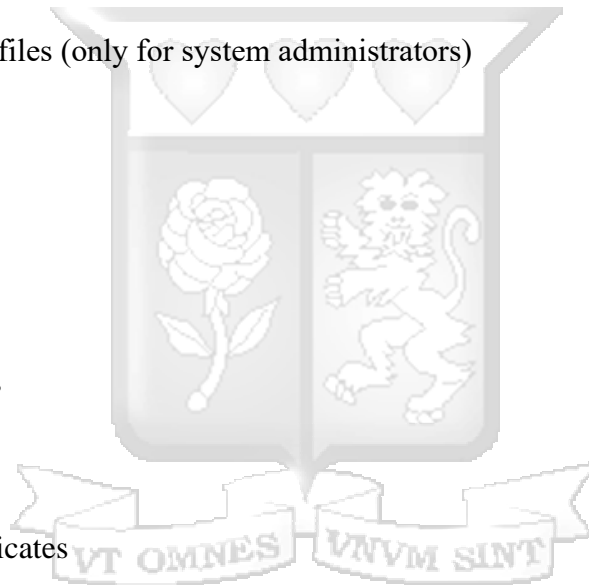
- Yes
- No

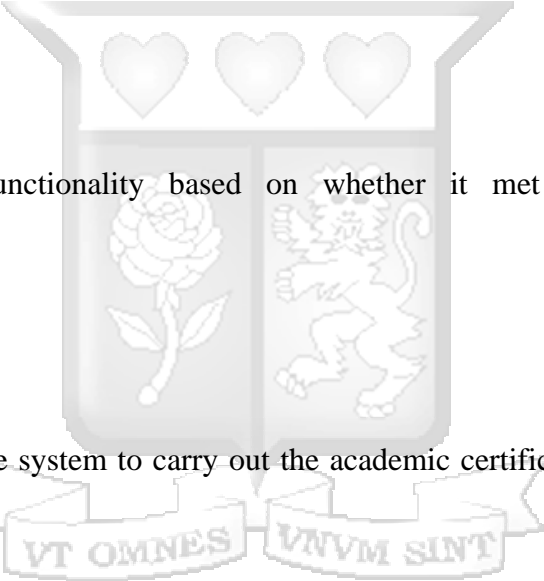
h) Add certificates (only for university staff)

- Yes
- No

i) Update certificates (only for university staff)

- Yes
- No



- j) Delete certificates (only for university staff)
- Yes
 - No
2. How did you find the user interface of the mobile and web application based on its look and feel?
- Attractive
 - Average
 - Not attractive
3. Rate the mobile and web application based on whether the application was easy to learn as a first time user and ease of using the application
- Easy
 - Average
 - Difficult
4. Rate the system functionality based on whether it met the user requirements (functionality)
- Good
 - Fair
 - Bad
5. Would you accept the system to carry out the academic certificate verification activities in this organization?
- Definitely
 - Undecided
 - Rejected
- 
- A large, faint watermark of a university crest is centered on the page. The crest features a shield divided into four quadrants: top-left with a rose, top-right with a lion, bottom-left with a heart, and bottom-right with a heart. Above the shield are three hearts. Below the shield is a banner with the Latin motto 'VT OMNES VNVM SINT'.

Appendix E: Academic Certificate Verification Validation Questionnaire

Mobile Application for Verification of Academic Certificates Applicability Test

1. Which category best describes you?
- University Academics Registrar
 - Employer
 - Recruitment Agency
 - Qualifications Verification Company

3. What is the name of your organisation? (Optional)

.....

4. Did you take part in the user testing of the mobile application for verification of academic certificates?

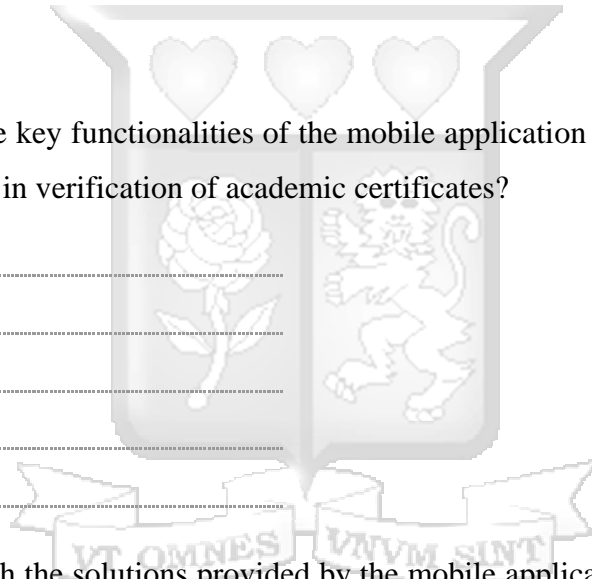
- Yes
- No

4. If Yes, Does the functionalities provided by the mobile application solve the problems posed by the current systems for verification of academic certificates?

- Yes
- No

5. What are some of the key functionalities of the mobile application that provides solution to the current problems in verification of academic certificates?

.....
.....
.....
.....



6. Are you satisfied with the solutions provided by the mobile application as far as verification of academic certificates is concerned?

- Yes
- No

7. Would you recommend that the mobile application to be adopted by all universities in Kenya as an application solution to current challenges encountered in verification of academic certificates?

- Yes
- No

Appendix F: Turnitin Report

Turnitin Document Viewer - Google Chrome
https://www.turnitin.com/dv?o=655265461&u=1050869653&s=&student_user=1&lang=en_us

Library Services Plagiarism Check... 2016 Plagiarism Check (UG) - DUE 31-D...

Originality GradeMark PeerMark

Harry Dissertation
BY HARRY OCHIENG

turnitin 30% SIMILAR -- OUT OF 0

A MOBILE BASED APPLICATION FOR VERIFICATION OF LEGITIMACY OF DEGREE CERTIFICATES IN KENYA

By

Harry Opiyo Ochieng
084953

A Dissertation submitted in partial fulfillment of the requirement for the award of a Master of Science Degree in Mobile Telecommunication and Innovation (MSc. MTI).

Faculty of Information Technology

No Service Currently Active

PAGE: 1 OF 127

6:31 PM 06-Apr-16

Figure C1 Turnitin Report

