



Strathmore
UNIVERSITY

Strathmore University
SU+ @ Strathmore
University Library

Electronic Theses and Dissertations

2017

A Prototype for authentication of secondary school certificates: case of the Kenya Certificate of Secondary Examination certificates

Raphael Mutua Kaibiru
Faculty of Information Technology (FIT)
Strathmore University

Follow this and additional works at <https://su-plus.strathmore.edu/handle/11071/5637>

Recommended Citation

Kaibiru, R. M. (2017). *A Prototype for authentication of secondary school certificates: case of the Kenya Certificate of Secondary Examination certificates* (Thesis). Strathmore University.

Retrieved from <http://su-plus.strathmore.edu/handle/11071/5637>

**A Prototype for Authentication of Secondary School Certificates: Case of the Kenya
Certificate of Secondary Examination Certificates**

KAIBIRU MUTUA RAPHAEL

Masters of Science in Information Technology

2017

**A Prototype for Authentication of Secondary School Certificates: Case of The Kenya
Certificate of Secondary Examination Certificates**

KAIBIRU MUTUA RAPHAEL

088995

**Submitted in partial fulfilment of the requirements for the Degree of Masters of Science in
Information Technology at Strathmore University**

Faculty of Information Technology

Strathmore University

Nairobi, Kenya

June, 2017

The thesis is available for Library use on the understanding that it is copyright material and that no quotation from the thesis may be published without proper acknowledgement.

Declaration

I declare that this work has not been previously submitted and approved for the award of a degree by Strathmore or any other University. The thesis contains no material previously published or written by another person except where due reference is made.

© No part of this thesis may be reproduced without the permission of the author and Strathmore University.

Kaibiru Mutua Raphael

.....

09/06/2017

Approval

The thesis of Kaibiru Mutua Raphael was reviewed and approved by the following:

Dr. Bernard Shibwabo

Academic Director, Faculty of Information Technology

Strathmore University

Dr. Joseph Orero

Dean, faculty of Information Technology

Strathmore University

Prof Ruth Kiraka

Dean, School of Graduate Studies

Strathmore University

Abstract

More often Universities and training institution in Kenya enroll students who want to further their education. Due to increased demand for educated labor force, the number of individuals reported to have used illegitimate KCSE certificates to join these Universities has increased. Perpetrators of this crime have succeeded despite the fact that there are measures to verify and authenticate KCSE certificates.

The study examined common forms of document fraud as well as current features used to secure paper documents. Therefore, the aim of this research was to develop a prototype based on digital signature and QR-code technique which would assist institutions in verification of certificates.

Agile software development methodology was adopted in developing the prototype. This involved requirements gathering, architecture and design, development and testing. This research was conducted in Nairobi County, targeting a population of thirty seven accredited Universities. In the study both public and private universities were considered in order to eliminate any form of biasness.

Data collection tools such as questionnaires were used to gather both qualitative and quantitative data. This data was analyzed qualitatively and quantitatively and presented in pie charts and bar graphs and frequency tables with the aid of statistical tool SPSS. More than 87% of respondents said that the current features were not sufficient in preventing document fraud. In addition, 98% confirmed that a computer based system would greatly contribute towards detecting fake certificates. Consequently, after the prototype was developed and tested 78% of the respondents agreed that a digital system was leveraging on the current security measures and authentication processes.

Keywords: Authentication, Digital signature, Certificate, Public Key Cryptography, QR code

Table of Contents

Declaration and Approval.....	ii
Abstract.....	iii
Table of Contents	iv
List of Figures.....	viii
List of Tables	ix
List of Abbreviations/Acronyms.....	x
Acknowledgement	xi
Dedication	xii
Chapter 1 : Introduction	1
1.1 Background	1
1.2 Problem Statement	2
1.3 General Objective.....	3
1.3.1 Specific Objectives	3
1.4 Research Question.....	3
1.5 Justification	4
1.6 Scope and Limitation	4
Chapter 2 : Literature Review	5
2.1 Introduction	5
2.2 Illegitimate Academic Certificates.....	5
2.3 Types of Fraudulent Documents	6
2.4 Security Features on KCSE Certificates	7
2.4.1 Watermark	7
2.4.2 Holograms.....	8
2.4.3 Ink Based Security	8
2.4.4 Printed Security Patterns.....	8
2.5 Electronic Technologies for Document Protection	9

2.5.1 Digital Signatures.....	9
2.5.2 Quick Response Code (QR-code).....	10
2.6 Algorithms used in QR Codes.....	13
2.6.1 QR Code Recognition Algorithm Based on Image Processing.....	13
2.6.2 Automatic Recognition Algorithm of QR Code Based on Embedded Systems.....	16
2.6.3 Barcode Reader Algorithm using the Camera Device in Mobile Phones	18
2.7 Limitations of QR Codes.....	20
2.8 Existing Systems used to Authenticate Certificates	20
2.8.1 Protecting Documents using Authenticated 2D Barcode	20
2.8.2 Elliptic Curve Based Method of Controlling Fake Paper Certificates	22
2.8.3 Web-Based Certificate Authentication System.....	23
2.9 Proposed Prototype	25
2.10 Conceptual Framework	26
2.10.1 Signing Process.....	26
2.10.2 Verification Process	26
Chapter 3 : Research Methodology.....	28
3.1 Introduction	28
3.2 Research Design.....	28
3.3 Target Population	28
3.3.1 Sampling Design and Sample Size	29
3.4 Data Collection Techniques	29
3.5 Processing and Data Analysis	30
3.6 Validity and Reliability.....	30
3.7 Software Development Methodology	31
3.7.1 System Analysis.....	32
3.7.2 System Design	33
3.7.3 System Implementation.....	33
3.7.4. System Testing.....	33
Chapter 4 : System Design and Architecture.....	34

4.1 Introduction	34
4.2 Questionnaire Results.....	34
4.2.1 Number of Years worked in Research Department.....	34
4.2.2 Document Fraud Awareness	35
4.2.3 Negative Effects of Illegitimate Academic Document.....	36
4.2.4 Method used to Falsify KCSE Certificates	37
4.2.5 Security Features on a Genuine KCSE Certificate.....	38
4.2.6 Request for Authentication of KCSE Certificates.....	39
4.2.7 Challenges Faced by Institutions when Authenticating Certificates	40
4.2.8 Importance of a Digital Authentication System	41
4.2.9 System Requirements.....	42
4.3 Requirements Analysis.....	43
4.3.1 Functional Requirements	43
4.3.2 Non-functional Requirements	44
4.4 Proposed Prototype Architecture	44
4.5 System Use Cases.....	45
4.6 Use Case Scenarios	46
4.6.1 Use Case Scenario 1.....	46
4.6.2 Use Case Scenario 2.....	47
4.6.3 Use Case Scenario 3.....	47
4.6.4 Use Case Scenario 4.....	48
4.7. System Sequence Diagram.....	49
4.8 Systems Domain Model	50
4.9 Entity Relationship Diagram.....	50
Chapter 5 : Implementation and Testing	52
5.1 Introduction	52
5.2 Development Technologies.....	52
5.3 System Implementation.....	53
5.3.1 Create and Print Certificate.....	53
5.3.2 User Registration	55

5.3.3 User Approval Form	56
5.3.4 Log-In Form.....	56
5.3.5 Validation Key	57
5.3.6 Validated Certificate	58
5.4 Prototype Testing	59
Chapter 6 : Discussion	62
6.1 Introduction	62
6.2 Types of Fraud Associated with Academic Documents	62
6.3 Security Features used to Authenticate Paper Documents	63
6.4 Existing Systems used to Authenticate Academic Certificates.....	63
6.5 Certificate Authentication Prototype.....	64
6.6 Authentication Prototype Testing.....	64
6.7 Merits of Authentication Prototype.....	65
6.8 Demerits of Authentication Prototype.....	65
Chapter 7 : Conclusion, Recommendation and Future Work	66
7.1 Conclusion.....	66
7.2 Recommendation.....	66
7.3 Further Research	66
References	68
Appendix	71
Appendix A: Introductory Letter.....	71
Appendix B: Questionnaire.....	72
Appendix C: Questionnaire Response Tables.....	77
Appendix D: Sample Code used to Generate QR Code.....	84
Appendix E: Sample Code for Generating Validation Code	86
Appendix F: Turnitin Report.....	87

List of Figures

Figure 2.1: Digital Signature Process -----	10
Figure 2.2: Example of a QR-code -----	11
Figure 2.3: Image Processing Algorithm -----	14
Figure 2.4: Sample Service of AuthPaper -----	21
Figure 2.5: Creation of Signature -----	22
Figure 2.6: Verification of Signature -----	23
Figure 2.7: E-Verification Conceptual Model-----	24
Figure 2.8: Automatic Web System -----	24
Figure 2.9: Digital Authentication System -----	25
Figure 2.10: Proposed Model for Certificate Authentication -----	27
Figure 3.1: Agile Software Development Process -----	31
Figure 4.1: Number of Years Worked in Research Department-----	34
Figure 4.2: Those Aware of Illegitimate KCSE Certificates -----	35
Figure 4.3: Use of Fake Certificate -----	36
Figure 4.4: Effects of Illegitimate Academic Documents -----	37
Figure 4.5: Methods of Falsifying KCSE Certificates -----	38
Figure 4.6: Sufficiency of Security Features -----	39
Figure 4.7: Ever Received Request to Authenticate Document -----	40
Figure 4.8: Challenges of Authenticating KCSE Certificates-----	41
Figure 4.9: Importance of a Digital Authentication System -----	42
Figure 4.10: System User Requirements-----	43
Figure 4.11: System Architecture -----	45
Figure 4.12: System Use Case Diagram -----	46
Figure 4.13: System Sequence Diagram -----	49
Figure 4.14: System Domain Model-----	50
Figure 4.15: Entity Relationship Diagram -----	51
Figure 5.1: Certificate Created by the system Administrator -----	54
Figure 5.2: User Registration Form-----	55
Figure 5.3: User Approval Form -----	56
Figure 5.4: Log in Form -----	56
Figure 5.5: Validation Code -----	57
Figure 5.6: QR code Validation Form-----	58
Figure 5.7: Authenticated Certificate-----	58
Figure 5.8: Prototype Testing Result -----	60

List of Tables

Table C 2: Years worked in Research department-----	77
Table C 3: Heard of Illegitimate Certificates-----	77
Table C 4: Heard of People using Fake Certificates -----	77
Table C 5: Reputation Damage-----	77
Table C 6: Lack of Credibility-----	78
Table C 7: Poor Quality -----	78
Table C 8: Other Effects-----	78
Table C 9: Double use of Certificates -----	78
Table C 10: Altered Documents-----	78
Table C 11: Fabricated Document -----	78
Table C 12: Omission of Data-----	79
Table C 13: Quality of Paper -----	79
Table C 14: Hologram -----	79
Table C 15: Patterns Printed on Paper-----	79
Table C 16: Watermark-----	79
Table C 17: Security Thread-----	80
Table C 18: Other -----	80
Table C 19: Sufficiency of these Features -----	80
Table C 20: Duration to get Feedback from KNEC -----	80
Table C 21: Tedious-----	80
Table C 22: Time Consuming -----	80
Table C 23: Difficult to tell a genuine and a fake Certificate-----	81
Table C 24: Difficult Authenticating Documents from other Countries -----	81
Table C 25: Others -----	81
Table C 26: Stable Employment -----	81
Table C 27: Higher Chances of Employment -----	81
Table C 28: Higher Income -----	81
Table C 29: General Development of the Society -----	82
Table C 30: Others -----	82
Table C 31: Authentication -----	82
Table C 32: Data Integrity -----	82
Table C 33: Privacy -----	83
Table C 34: Non-repudiation -----	83
Table C 35: System User Requirements Frequencies-----	83

List of Abbreviations/Acronyms

BOT- Bank of Tanzania

CUE- Commission of University Education

DSA- Digital Signature Algorithm

ECDSA- Elliptic Curve Digital Signature Algorithm

KCSE- Kenya Certificate of Secondary School Education

KNEC- Kenya National Examinations Council

RSA- Rivest Shamir Adelman

SDLC- Software Development Life Cycle

SHA-2 Secure Hashing Algorithm-2

SSL- Secure Socket Layer

UNMC- Uganda Nursing and Medical Council

Acknowledgement

My heartfelt gratitude goes to my parents Mr. and Mrs. Kaibiru for their unrelenting support and encouragement in my studies. Special thanks goes to my sister Angeline for funding my studies and for being my role model in academic. I would also like to recognize all my family members Alvin, Lucy, Sylvia and Rose for their continued regular checks on my progress with thesis research. To my grandmother, I owe her warm regards for her great love for education, which has been a guiding light in my studies. Sincere acknowledgements goes to my most special friend Suzzie for her constant reminder that I should not give up and remain focused on the prize.

I will be indebted if I do not express my sincere appreciation to my classmates Fiona, Doreen, Waweru, Baru and Kumbu for their intelligent insights from inception to completion of this research. Finally, I would like to acknowledge my supervisor Dr. Shibwabo for his guidance and mentorship in research.

Dedication

I dedicate this thesis to my family for supporting me during masters and when writing this thesis.

I also dedicate it to my supervisor Dr. Bernard Shibwabo and Strathmore community.

Chapter 1 : Introduction

1.1 Background

Very often universities in the country advertise for enrollments of new students. In every call-up of students to join a course or program, mostly dubbed as ‘intake’ every institution sets some minimum qualifications that must be taken into considerations. Key to these are minimum education requirements. The same institutions need to verify all certificates presented but also fall prey to falsified and illegal academic certificates (Muthoni, 2015).

In Kenya, Kenya Certificate of Secondary School Certificate is one key document that makes one an ideal candidate to join institution of higher learning. In addition, the candidate must have attained the set minimum qualification. According to Gudo and Olel (2011), some scrupulous entrepreneurs have turned the desire to have minimum qualifications to enroll into a university or college into a money minting business in which they manufacture KCSE certificate. This is a challenge that universities have to accept to face and overcome.

As far as authentication of KCSE certificate is concerned, this exercise ensures that there is fairness and objectivity in enrolling students by ensuring that meritocracy and quality is not ignored. Universities must exercise extra care during student admission process to identify those students with genuine certificates before they are admitted for courses commensurate with their grades (Gudo & Olel, 2011). Students who join institutions of higher learning with credible and genuine KCSE certificates tend to replicate the same results even in universities. According to Wambua (2003) as cited by Gudo and Olel (2011), found that KCSE grade contributed more significantly in predicting university performance in comparison to other predictors.

Institutions, particularly in Kenya, are faced with the challenge of authenticating genuine KCSE certificates especially when they are admitting new students or recruits. This challenge has been exemplified by increased cases of illegitimate KCSE certificates being used in various circumstances. Universities, employers and colleges have fallen victim of this crime, whereby, students and employees alike have been caught having used fake or illegitimate KCSE

certificates to join these institutions (Komu, 2015; Mwaura, 2010; Ombati, 2011; Pesa Times, 2015).

Success of using fake KCSE certificates has been favored by numerous challenges facing the verification process. Lengthy, tedious, labor intensive and manual process are some of the key impediments to ensuring institutions have taken in qualified students (Gudo & Olel, 2011; Kamanda, 2015; Muthoni, 2015; Waithaka, 2013).

Demand for quality education in Kenyan institutions have intensified efforts to weed out fake certificates from the academic system. With regard to this, authentication of KCSE certificates during enrollment of new students has been taken serious by both private and public institutions as opined by Gudo and Olel (2011). From their study it was identified that 66.7% private and 65.8% of public universities authenticated certificates for their new students. Consequently, 79% private universities and 55% public universities confirmed that they had not enrolled students with fake certificates.

Despite the rigorous exercise of authenticating academic certificate, cases of using fake KCSE documents has continued to be reported in the print media and other news sources (Komu, 2015; Ombati, 2011; Pesa Times, 2015). Owners of these documents have managed to compete “fairly” with those that have genuine certificates and gaining upper hand illegally. Therefore, due to challenges facing authentication of KCSE certificate among other academic documents, there is need to conduct a research on how QR-code and cryptographic technology such as digital signature techniques can be applied to curb the ever growing problem in the academic sector in Kenya.

1.2 Problem Statement

In every call-up of students to join institutions of higher learning, minimum requirements are set to determine the qualification of applicants. Key to ensuring these requirements are met is verification of certificates, however, these institutions fall prey to fake certificates (Muthoni, 2015). A number of individuals have managed to use illegitimate secondary school certificates to gain admission into institutions of higher learning as well as training institutions (UNMC, 2014).

Success of using fake academic documents to get enrolled into these institutions is a proof that methods being used to ascertain the authenticity of these documents are not sufficiently effective (Komu, 2015; Mwaura, 2010; Ombati, 2011). This malpractice has the potential of hurting the reputation and credibility of learning institutions, while employers who hire individuals with fraudulent credentials run the risk of humiliation, wounded business reputation and profit losses (CAPSLE, 2009; Garwe, 2015).

There is need to develop a prototype that uses digital signature techniques to authenticate and verify legitimacy of Secondary School Certificates. This will ensure that learning and training institutions as well as employers enroll and employ individuals with genuine and legitimate secondary school credentials.

1.3 General Objective

The main purpose of this study is to develop a prototype to authenticate secondary school certificates in using QR-code and digital signature techniques.

1.3.1 Specific Objectives

- i. To investigate forms of fraud and security features commonly associated with academic documents.
- ii. To analyze existing systems used to authenticate academic certificates.
- iii. To develop an authentication prototype for secondary school certificate
- iv. To test the functionality of certificate authentication prototype.

1.4 Research Question

- i. What are the common forms of fraud and security features associated with academic certificates?
- ii. What are the existing systems used in authentication of certificates?
- iii. How can certificate authentication prototype be developed?
- iv. How can the functionality of the prototype be tested?

1.5 Justification

Authentication of academic certificates has grown to be an important exercise in many institutions and organizations(Li, Hu, & Lau, 2015; Muthoni, 2015; Warasart & Kuacharaone, 2012). The system, therefore, will be of benefit to universities, training institutions, employers and any other interested parties that require valid and authentic academic documents. This research will be useful to academicians and future researchers by contributing to the existing body of literature.

1.6 Scope and Limitation

Both primary and secondary school certificates are key when joining university or training institution in Kenya. However, this research focused on authentication of the Kenya Certificate of Secondary Schools certificates because it is the key document used to determine qualification for one to enroll into institutions of higher learning. The study was limited to Kenya National Examination Council for data collection.

Chapter 2 : Literature Review

2.1 Introduction

Use of illegitimate academic certificates is a problem spanning across countries in the world. Eckstein (2003) opines that academic fraud is on the rise in both developed and developing countries in the world. As discussed in the previous chapter, effects of using illegitimate academic credentials range from legal implications, loss of employment, loss of credibility and reputation to lack of trust from the public in general. Academic fraud is a costly threat to the society, to their efficient operation and to public trust in reliability and security of their institutions (CAPSLE, 2009; Eckstein, 2003; Garwe, 2015).

This section will review existing literature in relation to illegitimate academic certificates, forms of document fraud, methods used to authenticate documents, technologies that are used to authenticate documents, existing systems in relation to document authentication and proposed approach of the system.

2.2 Illegitimate Academic Certificates

According to Adan (2002), illegitimate academic certificate includes both international academic credentials altered in a variety of ways, from a simplistic whiteout to a sophisticated creation produced in-house by college personnel in some countries, to identical reproductions of legitimate international diplomas and transcripts. Illegitimate document therefore can be said to be one that lacks integrity. The question that boggles the mind is why do people engage in illegitimate academic certificate business?

Plethora of scholars have tried to answer this question with regard to benefits attached to education, especially success in higher levels of education. Individuals who are academically successful and with high levels of education are more likely to be employed, have stable employment, have more employment chances compared to those that are less educated and earn higher salaries and they enjoy better health care services (Pargaru, Gherghina, & Duca, 2009; Regier, 2015).

The emergent of public with desires to gain quick access to post-secondary education or tertiary education and in search of better professional opportunities and higher pay are increasingly

contributing to the traffic of illegitimate documentation and products acquired through the carefully marketed campaigns of the “Diploma Mill” industry (Adan, 2002). Consequently, Eckstein (2003) argues that, credentials such as records of accomplishment, diplomas and certificates are relied upon as significant evidence of achievement, and thus have great value for the possessors as well as employers and admissions officers in higher education. As the pressure for achievement, selection and qualifications grow and examinations increases in importance, academic misconduct has become a matter of extreme concern.

From these three opinion, it is clear that individuals engage in academic fraud for reasons related to benefits attached to academic success especially in higher level of education. The problem surrounding certificate forgery cannot be discussed in entirety without looking at the main facilitating mechanism. Computer-based technology has been blamed for the increase of illegitimate academic certificates.

Openings for fraud are currently being enhanced by economically accessible technology that includes laser printers, easy-to-program type fonts and designs, color photocopying, scanning devices, and easy access to academic information via internet which, in some cases, may include the signature of institutional officials, ready for scanning, copying and reproduction (Adan, 2002; Garwe, 2015). Both benefits of education and technology compounded have been the main reason why people acquire illegitimate academic credentials.

2.3 Types of Fraudulent Documents

Document fraud is of different types. According to ACEI (2013); Adan (2002); Byram (2011), there are five types of document fraud associated with academic credentials. These types include; Altered Documents- which refers to any official, legitimate legal documents that have been altered through omissions, additions, or changes. This alterations may include, but are not limited to, changes in the date of birth, dates of attendance, initial enrollment and graduation dates, grades, curricular content among others. Fabricated Documents- are documents created to represent a legitimate or fictitious institution and or program.

Another form of fraudulent document is manufactured in-house. These are documents produced by institutional representative. These include both altered and fabricated documents in the national language or the language of the receiving country and designed “specifically for foreign

consumption.” In many cases, grades are inflated; contact hours or credits are doubled, and professional titles or degrees are awarded for programs that represent only completion of a partial or intermediate qualification. Diploma Mills- produce bogus products (transcripts/diplomas) that although not defined as a fabrication, the study or qualification they claim to represent is illegitimate. Interpretative Translations- are inaccurate translations of documents which are interpretative in nature and systematically misleading. Samples include the well-known (and often unintentional) literal translation of the Latin American high school diploma of *bachiller* into bachelor’s), the conversion of grades into the US grade scale, A-F, and the translation of course titles to comparable subjects in the receiving country to enhance the possibility of transfer credit.

2.4 Security Features on KCSE Certificates

Paper based security has been in existence for ages in many countries. Crucial documents such as money (notes), title deeds, wills, passports and visa, academic credentials and other legal documents have been provided with special features which help to determine their originality as well as authenticity. Despite there being these features, human has managed to reproduce identical documents using technology. The following section explains some of the security features used to protect the integrity of paper documents such as academic certificates.

2.4.1 Watermark

Academic documents, bank notes and other government documents often use special papers for security purposes. Most secure documents use watermark as a component of paper security that acts as a highly effective security device. A watermark is an image that is implanted into the substrate during the paper creation process(Nakamura, 2010). Watermarking is one technique that has become synonymous with security because of its long and reliable use. According to instructions given by the KNEC on KCSE certificates, it is indicated that these certificates are made of special paper which are watermarked with KNECs logo.

Technological advancement has been a major contributor to production of documents which mimic the original and legitimate document. Therefore, this method of security has been used by criminals to reproduce documents similar to original and genuine ones. Hence, proliferation of

counterfeit documents ranging from fake money, illegitimate academic certificates and other important legal documents.

2.4.2 Holograms

According to Jeong (n.d), a hologram is a recording in a two-or three dimensional medium of the interference pattern formed when a point source of light of fixed wavelength encounters light of the same fixed wavelength arriving from an object. He adds that, when the hologram is lit up by the reference beam alone, the diffraction pattern recreates the wave fronts of light from the original object. Thus the viewer sees an image indistinguishable from the original object.

Validity of a document is determined if the hologram is available on a particular secured document. From the inspection done on secondary school certificates in Kenya, there is a directive on the document, from the issuing body stating that the certificate is invalid if the hologram is missing. This is a clear indication that hologram is another technique employed by KNEC to secure certificates.

2.4.3 Ink Based Security

Document security has been implemented through the use of special ink. There are types of ink which respond to change in temperature, for example thermochromics reversibly changes color with temperature variation(Nathe, 2012). In security applications these inks can be inspected in fist line by warming to body temperature, at which they become transparent and the color temporarily disappears. Other types of ink such as fugitive ink disappears once bleaches or organic solvents are applied. The disappearance of the background printing exposes the attempt to alter variable information(Nathe, 2012). Special ink security has been used in the KCSE certificates to render legitimacy to the important document.

2.4.4 Printed Security Patterns

Patterns have been in use for a very long time with the purpose of document security. A common pattern used to secure documents is guilloches. This is geometric fine-line pattern formed from two or more interlaced bands with openings containing round devices or a pattern made by interlacing curved lines (Nathe, 2012). Guilloches is extensively used in the security printing industry to denote sophisticated ornamental borders and emblems consisting of fine curved lines.

Another pattern used is see-through register. This methods allows printing of related image, letters or words in seamless front-to-back register on both sides of the document. If held against the light, the register of front and back image is revealed (Nathe, 2012).

Both guilloches and see-through register have been used to secure KCSE certificates. To verify authenticity of the document, KNEC advices one to hold the certificate up to the light and ensure that the word *mtihani* and the genuine security thread are available. Security threads are also found in many bank notes of different countries, for example, all Kenyan shillings notes have a security thread.

2.5 Electronic Technologies for Document Protection

2.5.1 Digital Signatures

A digital signature is an electronic stamp similar to a handwritten signature that a sender places on document he or she wishes to send. In more technical terms, Rouse (2014) defines digital signature as a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.

Digital signature is built on public key encryption. This is to mean that, a digitally signed document or message has both private and public keys used together with hashing function. Digital signature takes the following steps.

- i. Apply hashing function to the message or document you wish to send. This can be done through hashing algorithm. Once this is done the output is a message digest.
- ii. The second step is to encrypt the message digest with sender's private key in order to get a digital signature.
- iii. Append the digital signature on the message or document then send.
- iv. On receiving the message, the receiver will decrypt the digital signature using public key in order to get message digest. The receiver can also create message digest directly from information given by the sender.

- v. The receiver compares the two message digests. If they are similar, it means that the message is original as sent by the sender. However, if they are not similar, it means that, the message is not authentic.

Digital signatures combined with QR codes can be used to provide security to both electronic and paper documents. This will be discussed more on existing systems in the literature review.

Figure 2.1 shows the process of signing and verification of digital signatures in a document.

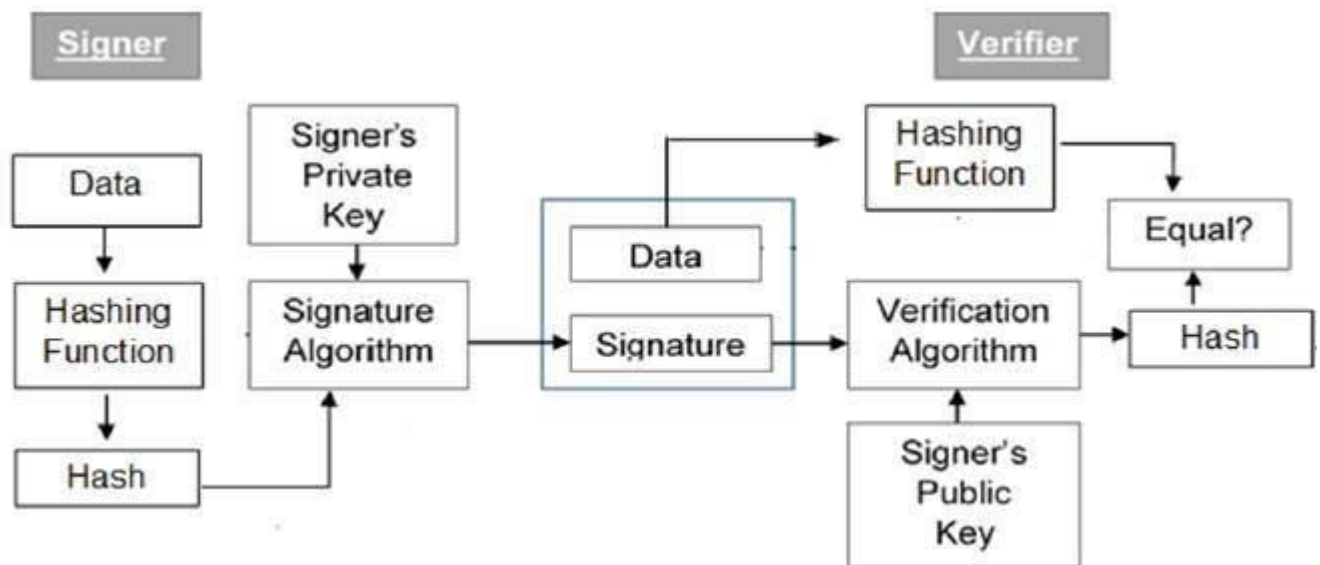


Figure 2.1: Digital Signature Process (Adopted from Li et al (2015)).

2.5.2 Quick Response Code (QR-code)

According to Peng et al (n. d), Quick response codes are 2-dimensional barcodes that visually codes bits of data represented as black square dots placed on a white square grid. QR code was designed to leverage on the weaknesses of the 1 Dimension Barcode (1D-barcode) because it would carry or store more information. At the beginning QR-code was used in Japan in automotive industry but later it started gaining popularity outside automotive industry. Increase in the use of QR code has been facilitated by advancement in technology especially the smartphone technology. This is because through a smartphone one can scan and read the content of a QR code. Figure 2.2 shows an example of a QR code.

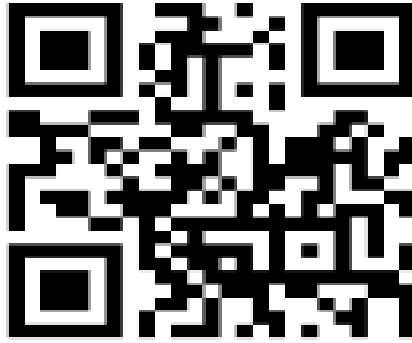


Figure 2.2: Example of a QR-code (Adopted from Lau et al., (2015)).

2.5.2.1 Characteristics of QR Code

QR codes when compared to its predecessor bar code has various characteristics that make it stand out. According to Mehta (2015), these characteristics include:

High Capacity Encoding Data

While conventional bar codes are capable of storing a maximum of approximately 20 digits, QR Code is capable of handling several dozen to several hundred times more information. QR Code is capable of handling all types of data, such as numeric and alphabetic characters, Kanji, Kana, Hiragana, symbols, binary, and control codes. Up to 7,089 characters can be encoded in one symbol.

Small Printout Size

Since QR Code carries information both horizontally and vertically, QR Code is capable of encoding the same amount of data in approximately one-tenth the space of a traditional barcode. For a smaller printout size, Micro QR Code is available.

Dirt and Damage Resistance

QR Code has error correction capability. Data can be restored even if the symbol is partially dirty or damaged. A maximum 30% of code-word can be restored. A code-word is a unit that constructs the data area. In the case of QR Code, one code-word is equal to 8 bits. Data restoration may not be fully performed depending on the amount of dirt or damage.

Readable from any Direction

QR Code is capable of 360 degree (Omni-directional), high speed reading. QR Code accomplishes this task through position detection patterns located at the three corners of the symbol. These position detection patterns guarantee stable high-speed reading, circumventing the negative effects of background interference.

2.5.2.2 Advantages and Disadvantages of QR Codes

According to Sungupta (2013), QR codes have both advantages and disadvantages when used in the day today transactions.

Advantages of QR Code

- i. Versatility- QR codes can be used for anything and everything. This is to mean that they can be appended on any product may it be a software or a hardware.
- ii. Can be embedded on different forms of media.
- iii. It does not require understanding of writing a QR code. This is because there are free open source applications to assist in generating a QR ode.
- iv. Data restoration- when compared to barcode, QR codes are able to be scanned even if there is a damage on them. At least 30% of words can be scanned when a QR code is damaged hence restoration of data.
- v. Scan position and speed- Barcodes must be scanned in the correct position. But QR code can be scanned from any position. This is due to the three position detection patterns located in three corner of the QR code. The QR reader locates these three detection patterns and then determines how to correctly read the code. This feature speeds up the time needed to scan objects.

Disadvantages of QR Codes

- i. Lack of Awareness: One disadvantage of QR codes and perhaps the biggest problem is the lack of familiarity of the QR code among people.

- ii. Expensive Smartphone and apps required: User needs to have a smartphone in order to use one. Along with the smartphone they also need a QR code reader application. Not everyone in the world owns a smartphone so QR code may not be available to everyone.
- iii. QR code feature not provided by default on phones: QR code reader are not preinstalled on most phones. It is installed by user.

2.6 Algorithms used in QR Codes

QR technology has attracted insatiable interest from scholars to try and develop efficient algorithms to encode and decode QR code information. In this section, various algorithms will be discussed as explained by different scholars.

2.6.1 QR Code Recognition Algorithm Based on Image Processing

In practical applications, barcode reading technology will encounter the following difficulties. (i) Together with much of information that is nothing to do with the bar code, the bar code symbols are printed on the packaging of commodities resulting into a complex barcode image background. (ii) Changes in illumination, resulting in uneven image brightness, increase the difficulty of identification. (iii) Acquisition in different angles and distances, coupled with the geometric distortion and flat distortion caused by image capture device, the image of the QR codes will be rotated, zoomed and stretched (Gu & Zhang, 2011). To solve the problems above, Gu and Zhang (2011) proposed that a two-dimensional code image should have a series of image processing before adopting national standards for rapid response code decoding algorithm. Figure 2.3 shows the algorithm proposed by Gu and Zhang (2011).

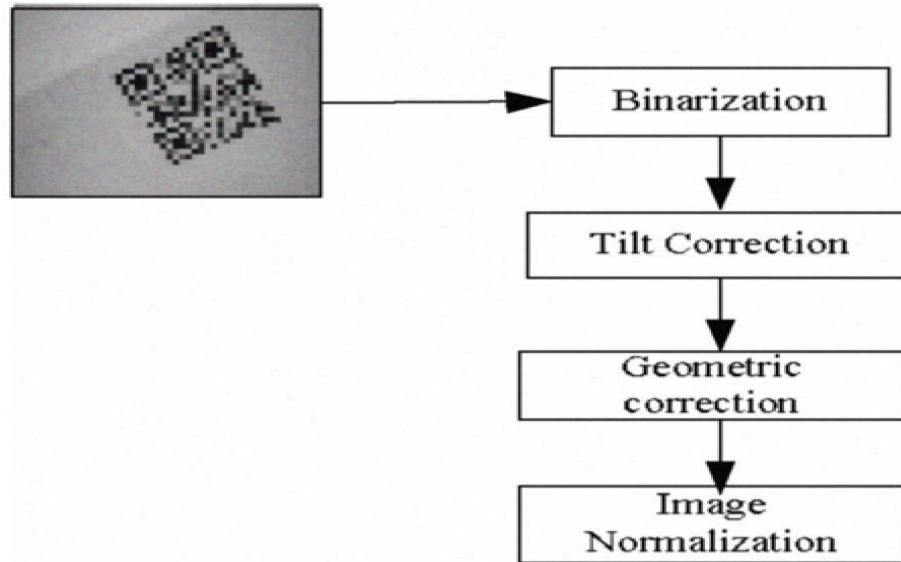


Figure 2.3: Image Processing Algorithm (Adopted from Gu & Zhang, 2011).

The following is a brief discussion of how the algorithm works:

Image Binarization

In this algorithm, image acquisition uses a general chat camera and apply camera control program for image acquisition under the intake image pattern. Images collected are converted to grayscale format by gray-scale processing. A good binarization method takes a very important role in the entire bar code identification system. This algorithm uses the global threshold method (OTSU method) in ordinary light condition while a local threshold method (adaptive threshold) is used in the uneven light condition.

Tilt Correction

When the image is being scanned, the position of QR code often occurs tilt and it needs rotating operation for correction. This algorithm proposes the following strategy for positioning and rotation. Firstly it needs to extract the QR code symbol, and then capture the image region to ensure that the center of the QR code is the center of the new image, this step eliminates the surrounding noise information. Then the rotation angle should be determined, and finally the rotation is carried on with bilinear interpolation (Gu & Zhang, 2011).

Image Geometric Correction

The image geometric distortion will emerge because of the shooting angle, image rotation and other issues. QR code geometric distortion will bring great recognition errors and reduce the

recognition rate. In general, the QR code image distortion is linear distortion. As a result, QR codes can be used to correct for the characteristics of being a square. Distortion correction algorithm is as follows.

- i. **Obtain images of the four vertices of QR codes.** Due to the rotation process the external noise information has been ruled out, so we can scan QR code image line by line, from the eight directions of the QR code region (up, down, left, right, upper left, lower left, upper right, lower right) in a straight line to scan the QR code until two or more intersection between the line and black block. After the scan at eight directions, we will get 16 points at least; the point appeared in both directions is the vertex. When these steps are completed, there are three or more vertices. Based on the distance between vertices and the center of position detection patterns, 3 shortest vertices can be obtained and there are the vertexes.
- ii. **Determine the fourth vertex.** In this algorithm according to the known relationship among the location of three vertexes, we can determine the orientation of the fourth vertex in the QR code (upper left, lower left, upper right, lower right). Then the location of the adjacent two lines to the resulting the fourth vertex can be known. Scanning along the center coordinates of position detection patterns until the intersection between black line and the QR code module. The slope of the two boundary lines can be calculated. Then the point at which these two straight lines intersect is the fourth vertex,

Image Normalization

The QR code image which is almost on regular can be obtained by geometric transformation. According to Gu and Zhang (2011), image normalization takes the following steps: Firstly, make sure the version number of the QR code based on the decoding algorithm given in the national standard and symbol structures of QR code itself. Secondly, divide equally the QR image into $n \times n$ small grids according the version number, re-sample the center of each grid as the sampling point and get the normalized QR code symbol. In this process, since the computer step length is integer, the cumulative error must produce more or less.

By using of averaging method, some modules that are supposed to be within the grid shift, leading to errors in QR codes dividing. Therefore, it is better to make a full-scale expansion to the image before grid-dividing based on the principle of image scaling so that it minimize the

error which is generated when cutting image. While the new gray values generated in amplifying procedure can be solved using bilinear interpolation. Thirdly, decode the standard QR code symbol according the National Standard Method of Quick Response Code after image re-sampling.

2.6.2 Automatic Recognition Algorithm of QR Code Based on Embedded Systems

The automatic recognition algorithm of Quick Response Code was developed by (Lui & Lui, 2006). They described an image processing system based on embedded system to be able to binarization, location, segment, and decoding the QR Code. This algorithm has four basic steps which include binarization, location, segmentation and decoding. These steps will be discussed briefly in the following section.

Binarization

Binarization of gray scale images is the first and important step to be carried out in pre-processing system. Selection of a proper binarization method is critical to the performance of barcode recognition system. In binarizing an image, a simple and popular method is threshold. There are two types of threshold methods: global and local threshold. By using a global threshold method, if an image has variable lighting conditions, the resulting binary image will be very bad. In this case, a local threshold method performs better.

This method including following steps. Firstly, calculate the histogram of gray image. In order to decreasing the effect of noise, filter the histogram, and analysis the feature of histogram peak. If the filtered histogram is bimodal distribution, the lowest of trough or the middle value of flat trough will be used as the global threshold. In common light conditions, this global threshold is used to binarizing image and its result is satisfied. If the histogram is single peak histogram, and single peak area in lower gray area, it means that barcode image is in weak illumination, otherwise the barcode image is in strong illumination, Lui and Lui (2006) adopted an iterative threshold method, which form the threshold with mean between old global threshold and center of dark area or light area. If histogram shows multi-peak distribution that means the image is in the case of uneven light conditions or complex background. The local threshold algorithm is used. The multi-level threshold method integrate global threshold and local threshold method, it

is meted the real-time binarization in common lighting condition, and also satisfied the binarization in special illumination condition.

Determine the Location and Orientation

The second step according to Lui and Lui (2006) is to locate the finder patterns is premise of getting version, orientation and distortion of QR Code. There are three identical position detection patterns located at three of the four corners of QR Code. Determine the orientation of symbol after getting the location of finder patterns. QR Code can be readable from any direction from 360 degree, so rotated symbol is oriented commonly by sine and cosine transformation. Rotate symbol first, then implement interpolation operation. The amount of calculation is great and is not accurately in this algorithm. A modular distance offset algorithm was used without rotating symbol. After Locate the orientation of symbol, the center of three finder patterns formed a triangle. By adopting the Law of cosines, the largest angle is obtained (Point0), and it is the upper left center point of finder pattern before rotated symbol. Take this point as coordinate origin, upper right (Point1) and down left (Point2) position detection pattern can be determined based on the distributing of the other points in this coordinate.

Locate the Central Coordinates of Alignment Patterns

In order to correct the contorted QR Code symbol, there are many alignment patterns in symbol. Increased the version of QR Code can result the number of alignment patterns added. Link the central point of the alignment patterns and three position detected patterns, the small sampling grid is formed. In small sampling grid, distortion is overcome. Therefore, locate the central coordinates of alignment pattern is critical for recognition barcode. This method scan the outline of the white square in alignment patterns starting from the pixel of the provisional central coordinate to find the actual central coordinates (Lui & Lui, 2006).

Decode

The decoding process is the last step of recognition barcode, and it just reverse of the encoding procedure (Lui & Lui, 2006). The test results of the algorithm showed that 99% of barcode were able to be recognized using automatic recognition algorithm on embedded systems.

2.6.3 Barcode Reader Algorithm using the Camera Device in Mobile Phones

In order to address the problem of alignment and reorganization of the image during decoding of the QR, Ohbuchi, Hanaizumi, and Ah Hock (2004) developed an algorithm to enable them solve the mentioned problem. The algorithm as opined by Ohbuchi, Hanizumi and Ah Hock (2004), has five steps; Pre-processing, Corner marks detection, Fourth corner estimation, Inverse perspective transformation and Scanning of code. The details of this algorithm are discussed in the following subsection

Pre-processing

As the pre-processing, three steps of image processing are applied: histogram calculation to define the threshold of black-white boundaries, resizing of original image to reduce the calculation costs in the next phase: recognizing QR-code area, and the filtering for the area dilatation (Ohbuchi et al., 2004).

In the histogram calculation, nine parts of 60x60 square areas nearby the image center are selected as sampling points to define the threshold value between the black and white luminance levels to convert the bi-level image. The pixel density is sorted for each selected area, and the threshold in this area is calculated as a center value of sorted density (the median luminance). After that, a threshold is defined as the minimum values from the threshold of all selected areas according to experimental results. After the definition of threshold, the resized image which is scaled down into half for x and y coordinate directions, is used for the original luminance component image to reduce the calculations.

Finally, the filtering, which works for filling the holes (area dilatation), is used to recognize the QR-code area. The minimum density among the original four pixels is assigned to one pixel, and in our implementation, this filtering is also combined with the resizing process.

Code area Detection

The filtered and resized image are used for the rough code area findings, and these processes are shown in the following list.

- i. Calculate the position of the gravity center (x_c, y_c).
- ii. Scan a line from outer to inner in eight directions until the line touches the area.
- iii. If there are two or more pixels on a line their edge points are obtained.
- iv. After eight direction scanning, we get 16 points at most.

- v. The nearest point to $(0,0)$ is one of the targets.
- vi. Define a vector P as $(x_0, y_0) - (x_c, y_c)$.
- vii. Calculate the inner product for finding other corner points.

After the above process, the positions of corners are refined in the original size of image as follows.

- i. Set a line from (x_0, y_0) to (x_c, y_c) .
- ii. Cross-point is in the outer edge of the mark.
- iii. Start recursive area growing from the cross-point.
- iv. Get gravity center of outer mark and this is in the inner mark.
- v. Restart recursive area growing from the gravity center.
- vi. Mark center is defined as the gravity center of inner mark.
- vii. Corner point is defined as the farthest point from the image center.

This process obtains the three corner points using finder patterns, but the fourth corner point has no found pattern, and also the case where there is no corner cell in the fourth corner exists. Because of these features of QR-code, they introduce the new corner detection algorithm for the fourth corner point reorganization.

- i. Set line from known corner points to roughly obtained point
- ii. Move the cross-point so that line segments are shown by touching the code area (line attachment method).

The calculated code size and recognized code feature by the above processes can be used for the verification of code specification about the code size (code size is always odd), equally both width and height, and position of alignment mark before the decoding.

Inverse Perspective Transformation

The input image has a deformed shape because of being captured from the embedded camera device and we use the inverse perspective transformation to normalize the code shape (Ohbuchi et al., 2004).

Scanning of Code

The proposed algorithm was based on the four corners points, so each cell in the code symbol can be scanned directly by using the inverse perspective transformation. In this method, the calculation cost depends on the size of the code, not the size of image, and this is good for big

image size input. Finally, the scanned image is output as a normalized bi-level image to host application (Ohbuchi et al., 2004).

2.7 Limitations of QR Codes

When used on a paper document QR codes exhibit different challenges. Some of the challenges as documented by Li et al. (2015) include; decoding of the QR code and print out size. Decoding of high capacity QR codes is usually attributed to low resolution of camera images. Print out size affects clarity of the image due to printer resolution capability. To address this problems, Reed-Solomon code embedded in the Bacon QR Code Generator library was used in the proposed solution. Bacon QR Code Generator library is a free open source multi-format 1D/2D barcode image processing library implemented in PHP with ports to other programming languages. In reference to the Algorithms discussed, barcode reader Algorithm using Camera Device in Mobile Phone was used.

2.8 Existing Systems used to Authenticate Certificates

The problem of illegitimate academic credentials and other documents has triggered an insatiable urge from scholars and research to provide ideal solutions. A plethora of research work has been done specifically to find out how computer based methods can be used to ensure authenticity of academic documents. This section will look at various research work in relation to certificate authentication from different authors.

2.8.1 Protecting Documents using Authenticated 2D Barcode

(Li et al., 2015), Warasart and Kuacharaone (2012) and Murthy (2011), proposed a phone-based document authentication prototype using 2D barcode. 2D and digital signatures technologies were used to provide security required for the documents. The reason for use of barcode was that it can store very large data when compressed. The benefits of using phone based authentication prototype is that, the verification process does not involve any document databank or real-time access to honest party as well as the document issuer. The self-authenticating document is able to be redistributed with the barcode even through standard photocopier and printers.

To generate the digital signature Warasart and Kuacharaone (2012) used Secure Hashing Algorithm (SHA-256 and RSA Algorithm while, Li et al. (2015), used Eliptic Curve Digital

Signature Algorithm (ECDSA). According to Li et al. (2015), ECDSA provides the same level of security with Rivest Shamir Adelleman (RSA) Algorithm and Digital Signature Algorithm (DSA). He further points out that a 512 bit digital signature in ECDSA provides the equivalent strength of 3074-bit RSA signature. This is to mean that ECDSA will occupy less memory space while providing the same level of security as that of RSA.

Despite the success of the model, several challenges were encountered. Li et al. (2015), identified limitations which he categorized into two: one dealing with limit of print out size of QR-Code and challenge of decoding QR code. There was a problem due to printer resolution due to print out size. It was also identified that there was a limitation because of smartphone camera constraints. This problem was also aggravated by the fact that there was blurring due to shaking when taking the photo using a camera for decoding of data. On the decoding part it was identified that, even after capturing clear images there was a problem of decoding high capacity QR code using ZXing library. Following is Figure 2.3 showing the paper based authentication model.

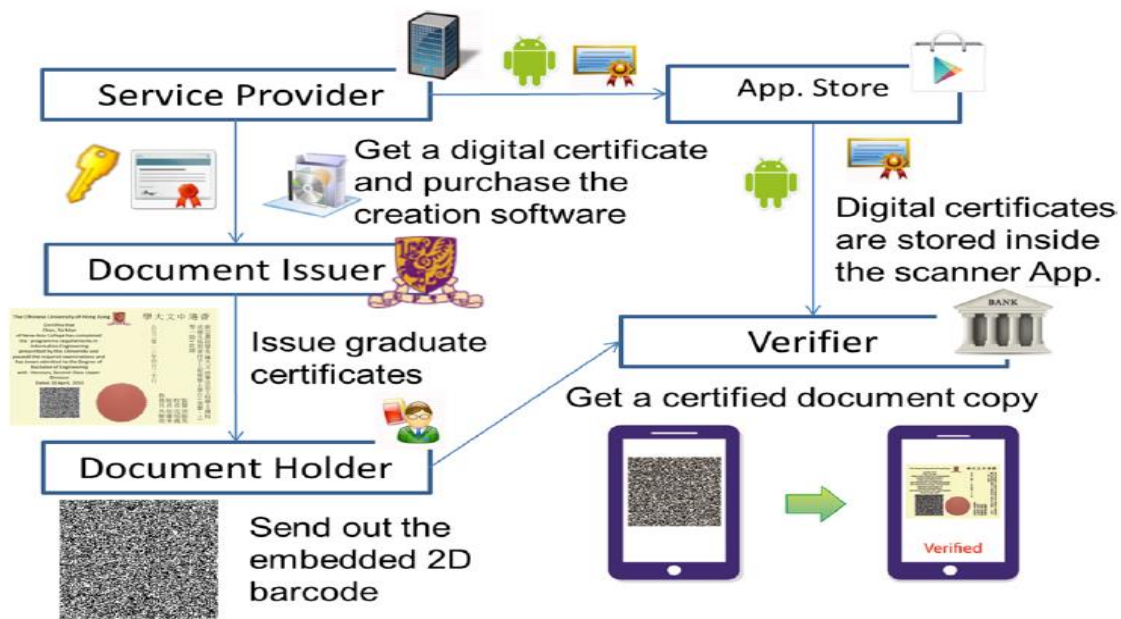


Figure 2.4: Sample Service of AuthPaper (Adopted from Li et al., (2015)).

2.8.2 Elliptic Curve Based Method of Controlling Fake Paper Certificates

Murthy et al., (2011) proposed a prototype to control fake certificates but with emphasis on Elliptic Curve Digital Signature Algorithm. This was motivated by the fact that ECDSA provides strong signatures that occupy minimal space on the certificate (Li et al., 2015; Murthy et al., 2011). RSA, DSA and Elliptic Curve Cryptography are popular asymmetric crypto algorithms used for digital signature to authenticate information (Li et al., 2015; Murthy et al., 2011). Just like Li et al. (2015), Murthy et al. (2011) concurs that, when compared to other hard cryptographic problems elliptic curve provides more cryptography strength.

It is also worth noting that this method made use of barcode technique to authenticate certificates. Therefore, going by the challenges faced by Li et al. (2015) when using barcode it can be assumed that the same problem will befall this method. Below are Figures 2.4 and Figure 2.5 showing creation and verification of digital signature.

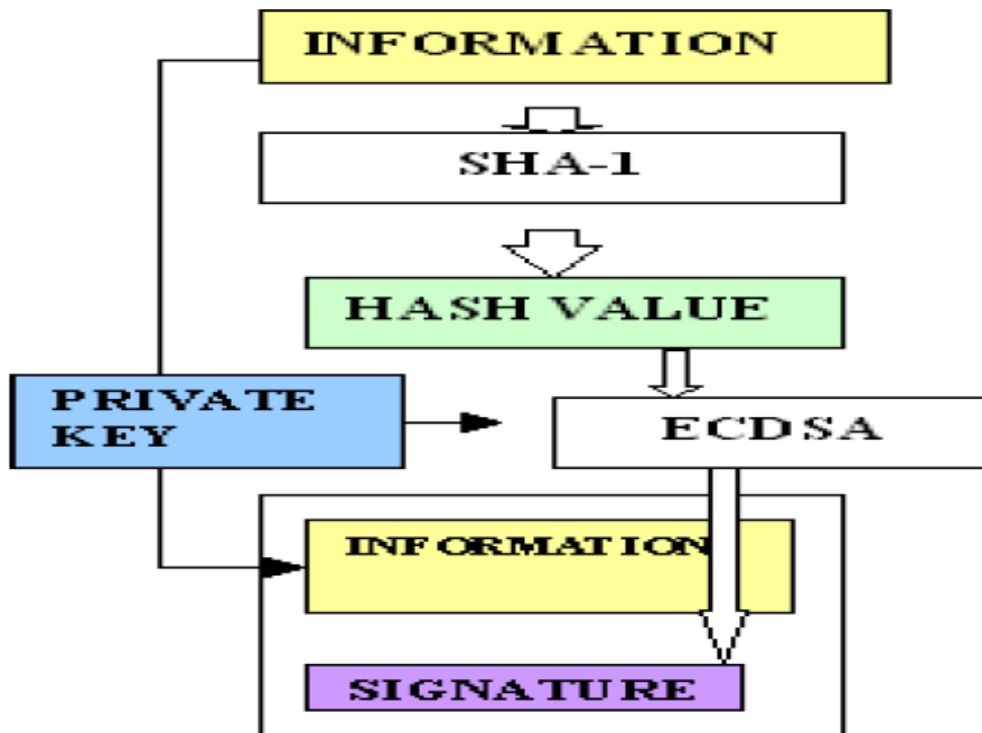


Figure 2.5: Creation of Signature (Adopted from Murthy et al., (2011)).

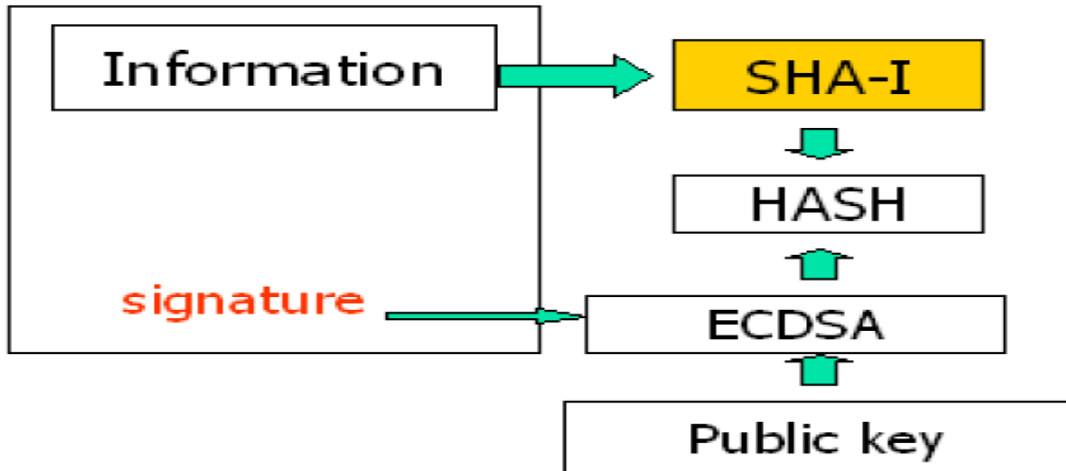


Figure 2.6: Verification of Signature (Adopted from Murthy et al., (2011)).

As noted earlier, Murthy et al., (2011) focused on Elliptic Curve Digital Signatures because of its benefits which include storage efficiency, stronger security, and minimum crypto analytic attacks when compared to other cryptographic methods such as RSA.

2.8.3 Web-Based Certificate Authentication System

Apart from phone based and 2D QR code verification systems, there is a web-based method of authenticating and verifying certificates developed by different scholars. Three scholars developed web-based prototypes to facilitate verification and authentication of academic credentials (Kamanda, 2015; Muthoni, 2015; Nwokefor & Abraham, 2015)

In their work, Muthoni (2015) and Nwokefor and Abraham (2015) focused on web based solutions without focusing on digital signatures. The verifier of document relied on the presence of hardcopy and the portal to determine whether the certificate at hand was from the alleged institution. The strength of using web-based method is pegged on the fact that; one is able to access the certificate portal from any place in the world without necessarily having to visit the institution for verification (Kamanda, 2015; Muthoni, 2015; Nwokefor and Abraham, 2015). Figures 2.6 and Figure 2.7 presents proposed prototypes by Muthoni (2015) and Nwokefor and Abraham (2015) respectively.

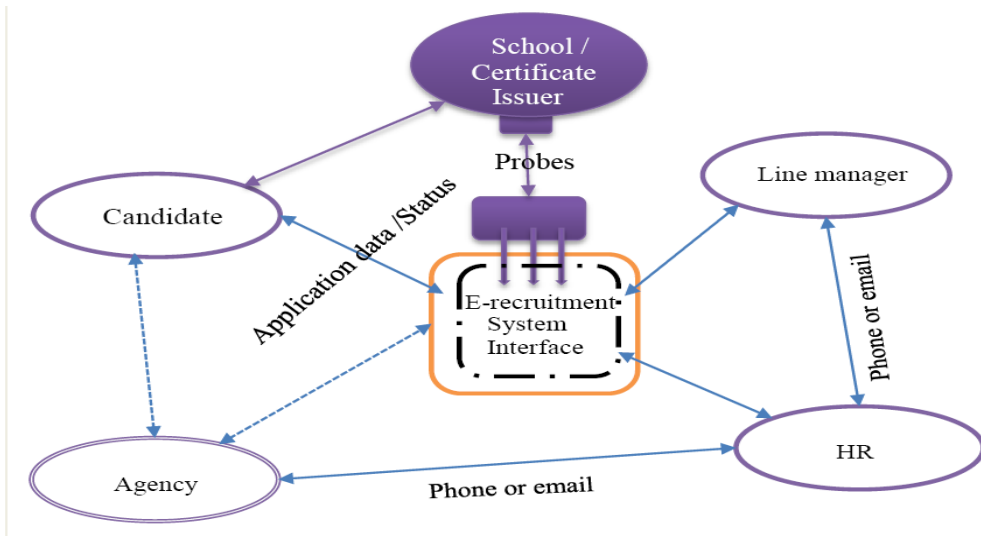


Figure 2.7: E-Verification Conceptual Model (Adopted from Muthoni, 2015)



Figure 2.8: Automatic Web System (Adopted from Nwokeafor & Abraham, 2015)

On the other hand different from Muthoni (2015) and Nwokeafor and Abraham (2015), Kamanda (2015) designed a web-based prototype which made use of digital signature to authenticate university certificates. A close investigation shows that Kamanda (2015), made use of Secure Socket Layer (SSL) together with digital signature to develop the prototype. The SSL is important when it comes to secure connection within the internet. To generate the digital signature, Kamanda (2015) made use of SHA-1 and RSA algorithm which, according to Murthy et al (2011), RSA provides weaker digital signatures compared to ECDSA. In addition the process of verifying was not efficient because the verifier had to rely on softcopy document from

the portal. This left room for illegitimate documents to be used because the system was not authenticating hardcopy certificate. Figure 2.7 presents conceptual framework used to develop the system by Kamanda (2015).

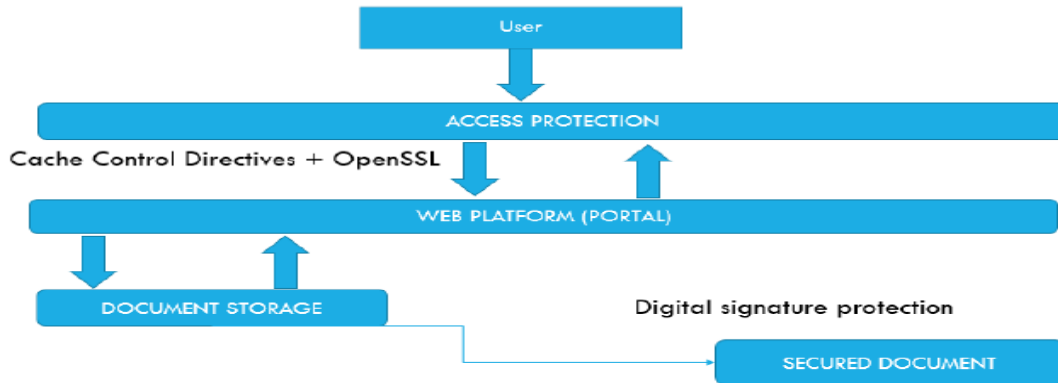


Figure 2.9: Digital Authentication System (Adopted from Kamanda, 2015)

2.9 Proposed Prototype

The proposed solution will make use of web portal and QR code. The prototype will also make use of SSL to ensure safe connection while on the internet. Certificate details will be hashed using Secure Hashing Algorithm (SHA) and later signed using private key of the issuer to generate a digital signature which will be converted into a QR code and appended on the certificate. The QR code will be printed on the certificate hence enabling reproduction of the same document through photocopy.

Since QR codes are prone to attacks, the proposed solution will make use of protected QR codes, which will be accessed by use of a password key generated by the certificate issuer. This will reduce the chances of people stealing the details of a certificate for the purpose of forgery or alteration. In order for one to verify the authenticity of the certificate, verifier will use free QR code scanner to scan the QR-code on the certificate and enter the passcode provided on the system portal. Later the certificate in question will open on the verification portal for further scrutiny. In addition, users of the system will be able to verify details of the certificate on the portal. In case the QR code is not authentic then the certificate will be rendered illegitimate.

2.10 Conceptual Framework

2.10.1 Signing Process

During signing of the document student's details, certificate serial number and grades will be hashed to get a message digest. These are the details which will be verified to confirm authenticity and integrity of the certificate. The message digest will then be encrypted using private key of the signer to generate a digital signature which will then be converted into a QR code and appended on the document for printing. The signing process will be done by the system administrator of the certificate issuing body.

2.10.2 Verification Process

The user of the system (institution) will log in into the system and scan the certificate presented to him or her by the student. Once the QR is scanned a password is generated, which will in turn be entered on the system to open the certificate being scrutinized. This process will involve decrypting of the digital signature and calculating the hash function. If the initial hash function is similar to the calculated, then the document is valid. Otherwise, it is invalid. Figure 2.9 shows a conceptual framework for the proposed prototype.

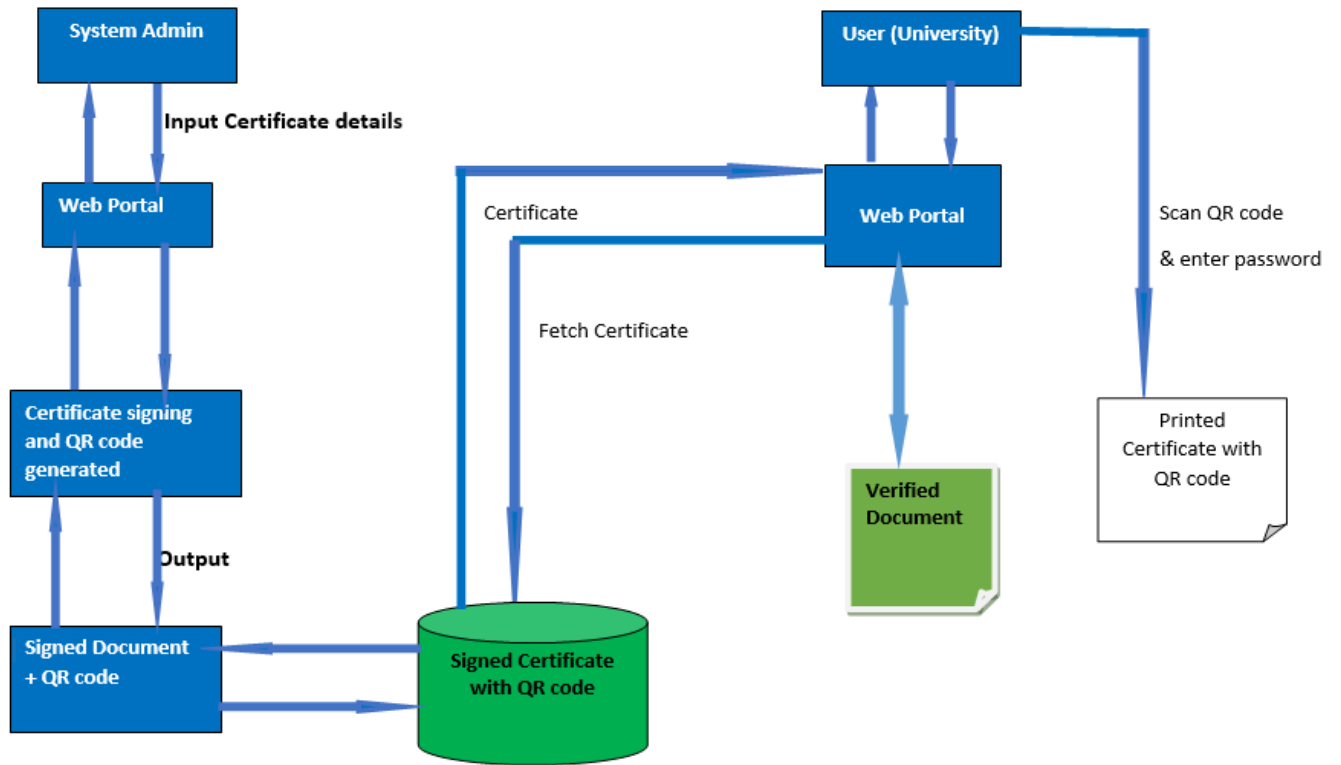


Figure 2.10: Proposed Model for Certificate Authentication

Chapter 3 : Research Methodology

3.1 Introduction

Research is a term that is liberally used to mean search for new information, knowledge or answers to questions. However, from a scholarly approach, Kothari (2004) defines research as the systematic method consisting of articulating the problem, formulating the hypothesis, collecting the facts or data, analyzing the facts and arriving at a conclusion either in form of a solution towards the concerned problem. For a researcher to accomplish this undertaking, he or she needs to follow a guided procedure. These procedures or steps refer to research methodology, which is a systematic way to solve a problem (Kothari, 2004).

This section will explain research design, target population and the sample size, data collection tools, data analysis tools system development methodology and system development tools.

3.2 Research Design

Research design comprises of three research approaches; qualitative, quantitative and Mixed method (Creswell, 2009). A qualitative research design is involved with phenomenon related with quality or kind. This approach does not allow analyzed data to be presented in numerical form. On the other hand quantitative research is involved with fact finding in which data can be analyzed and presented in numerical form. The Mixed method is a hybrid of both qualitative and quantitative method. That is, it exhibits characteristics of both qualitative and quantitative research (Creswell, 2009).

Mixed method approach formed the basis of this research because it has a benefit of allowing the researcher to collect data in both qualitative and quantitative methods. This method recognizes that each method (qualitative and quantitative) have limitations and therefore it neutralizes the bias of using a single approach.

3.3 Target Population

Population according to Kothari (2004) refers to all items in any field of inquiry. It is also referred to as a universe. The target population for this study was the KNEC a body which is mandated by the KNEC Act No. 29 of 2012 to confirm the authenticity of certificates and

diplomas issued by the council upon request by the government, learning institutions, public institutions, employers and any other interested parties among other services to ensure quality education for citizens (KNEC, 2015).

The KNEC has five administrative departments that work synergistically to ensure delivery of services required by the public. According to KNEC Charter (2015), these departments include test and development, reprographics and manuscript, finance, administration and human resource management, examinations administration and ICT/ research and data processing department.

3.3.1 Sampling Design and Sample Size

Sampling design refers to the process by which a small number of representation is determined from a population. Samples are ideal where the number of the population to be studied is large. Non random sampling method was used to come up with the sample size. Purposive sampling was used to target research department because according to the KNEC charter (2015), this department is the one that confirms authenticity of certificates issued by KNEC.

When used in quantitative research, purposive sampling uses predetermined number of people or department chosen by the researcher best positioned to provide the needed information (Kumar, 2011). Therefore, this study targeted research department to gather information on KCSE certificate falsification and security measures put to determine a genuine certificate. This department was best suited to provide relevant information as far as certificate authentication was concerned. Questionnaires were administered to ten employees in this department at least to get diverse opinion regarding use of fake certificates.

3.4 Data Collection Techniques

Data collection begins after the research problem and research design has been chalked out. Data can be of two types, primary data or secondary data. Primary data is the data that is being collected for the first time. On the other hand secondary data is data that has already been collected and recorded by another person. In primary data there are a number of methods used to collected data. For example, interviews, questionnaires, observation, schedules among others (Creswell, 2009; Kothari, 2004).

In this research questionnaires and document review were the main tools for collecting data. Document review was applied to investigate what the Kenya National Examination Council says about authentic certificates. This data was important in determining current security features on secondary school certificates. The data was also important in determining the efficiency of these security features in protecting document fraud. Since the main aim of this research was to develop a prototype to authenticate KCSE certificates, this data will be important in identifying functional requirements as well as the missing gaps in order to develop the proposed model, thus leveraging on existing security features.

3.5 Processing and Data Analysis

According to Kothari (2004), data processing implies editing, coding, classification, and tabulation of collected data so that they are amenable to analysis. He further explains that analysis refers to the computation of certain measures along with searching for patterns of relationship that exists among data-groups. Descriptive analysis was done using percentages and presented in pie charts, bar graphs and frequency tables for easy interpretation. In this research, data was processed and analyzed by use of Statistical Package for Social Science (SPSS) tool.

3.6 Validity and Reliability

Validity is the extent to which tests or tools are able to truthfully and accurately measure what we actually wish to measure (Kothari, 2004; Golafshani, 2003). Content validity was carried out to determine the soundness of the questionnaire in line with research objectives and research questions. Without validity it would be difficult to ascertain whether a tool is able to do its work efficiently. Pilot study testing the validity of data collection tools was conducted by sending sample questionnaires to the respondents in the target department before actual data collection.

Reliability refers to consistency of results over a specified time to determine precision and accuracy of data collection tool (Golafshani, 2003). To test reliability an exercise is repeated over a duration of time and if there is consistency in results then the tool and data is reliable. In this research questionnaires were re-issued a second time to find out whether the respondents will give similar feedback compared to the first instant data collection activity. This helped to determine the reliability of data collection tool and the research in general.

3.7 Software Development Methodology

Methodology is a formalized approach to implementing System Development Life Cycle (SDLC) (Dennis, Wixom, & Tegarden, 2012). Agile system development methodology was used to develop the system. This is because this method allows for faster iteration and more frequent release with subsequent user feedback. Agile processes allows release schedule and user feedback opportunities this allows faster and more controlled improvements (CPrime, 2014). This approach has four main steps which include, planning, analysis, design and implementation.

Figure 3.1 shows steps that were followed in the developing the proposed prototype.

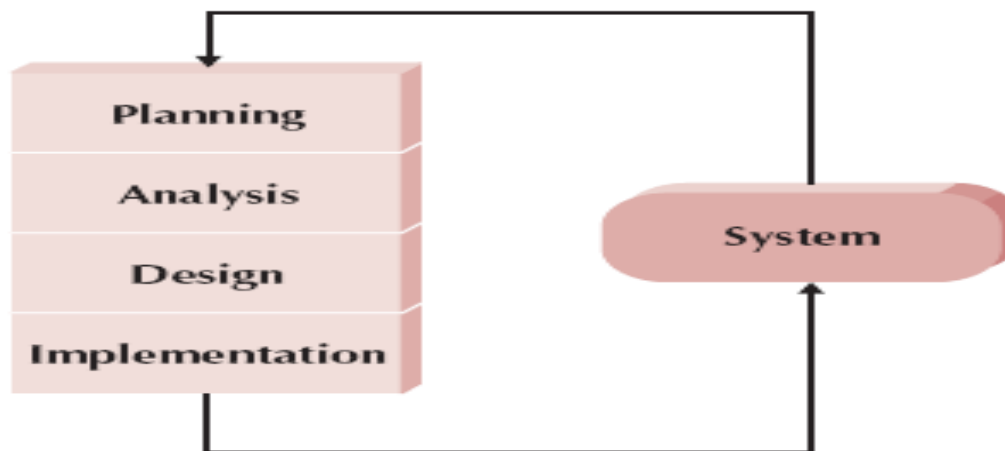


Figure 3.1: Agile Software Development Process (Adopted from Dennis et al., 2012).

Planning phase helps one to understand why an information system should be built. At this stage the problem requiring information system was identified. In this case, the problem at hand is the use of illegitimate secondary school certificates to enroll into universities and training institutions. This problem is aggravated by the fact that measures available for authentication of these documents are not effective.

The second step was system analysis, which seeks to answer the question who will use the system? What the system will do? Where the system will be used? And when the system will be used? In analysis phase, system development team investigates current systems, identifies areas to improve and develops a concept for the new system (Dennis et al., 2012).

System users were determined and in this case the users of the proposed system are universities, training institutions, employers and any other party wishing to verify the authenticity of applicants' certificate. The system will be used to authenticate the legitimacy and integrity of the details as provided by the issuing body. Also during analysis phase current systems were identified and determine the drawbacks so that the proposed system can be used to improve on them. This activity was carried out during system requirements gathering.

The third phase which is design stage explains how the system will operate, in terms of hardware, software and network infrastructure; the user interface, forms and reports and the specific programs, databases and files that will be needed. The last step is the system implementation, which entails translating the design phase into an actual system through coding, testing and maintenance of the system. The end result of this process was a working prototype (Dennis et al., 2012).

3.7.1 System Analysis

System analysis involves determining the users of the system, system requirements, how the users will interact with the system and what they can do with the system. This research used Object-oriented Analysis (OOA), which combines both process and data into single entities called objects.

In analysis stage, Use-case models were used to determine system users and what these users can do with the system. Use-case diagrams are used in the initial stage of system development to enable system developers get perfect understanding of functional requirements of the system without worrying how the system will be developed. Use-cases diagrams comprise of actors and use cases. An actor is an external entity that interacts with the system while a use case describes how the user interacts with the system to perform some activity, such as placing an order, making a reservation, or searching for information. The propose system had two main actors; system administrator and the user or verifier. Use cases are used to identify and to communicate the requirements for the system to the programmers who must write the system (Dennis et al., 2012).

3.7.2 System Design

The purpose of design is to decide how to build the system. It involves translating the requirements gathered in system analysis into a blueprint that can be used by programmers to come up with the system (Dennis et al., 2012). This research applied Object-oriented Design (OOD) technique to design the system. A major advantage of OOD is that, system analysts can save time and avoid errors by using modular objects and programmers can translate the designs into code, working with reusable program modules that have been tested and verified (Shelly & Rosenblatt, 2012). Class diagrams, Entity Relationship Diagrams (ERDs) and sequence diagrams were used in this research to show the relationship between objects, people and events.

3.7.3 System Implementation

System implementation involves translating design into program code. At this stage system developers begin programming the system as per the user requirements and system design. This involves using various tools such as database tools and programming language. In this research PHP and HTML languages was used to develop the web application while MySQL was used to develop the database. OpenSSL was also used to provide a secure connection between the client and the server during system use. Free QR-code scanner was installed in the smartphone to enable verification of certificate. These resources are preferred because they are open source.

3.7.4. System Testing

Once the system is developed it was tested to find out whether it meets users requirements. There are various types of system testing which include, unit testing, integration testing, system testing and acceptance testing.

During system testing unit testing, system testing and acceptance testing was conducted. Unit testing was carried out to ascertain that independent module or component was working properly. System testing was carried out to determine that all classes were working together without errors. Acceptance testing was carried out primarily by the user with support of system developer. The goal of this testing was to confirm that the system is complete, meets business requirements and that it was acceptable to the user.

Chapter 4 : System Design and Architecture

4.1 Introduction

The main aim of this study was to come up with an efficient and effective prototype to authenticate KCSE certificates. With regard to this, therefore, this chapter is based on analysis of collected data which informs the system design and architecture.

4.2 Questionnaire Results

4.2.1 Number of Years worked in Research Department

Question 2 of the questionnaire sought to find out the duration the respondent has been working in the research department office. This was to determine the level of awareness of certificate fraud. Figure 4.1 shows the number of years respondents said they have been working in the department. Most respondents 27% said they have been in this department for 16-20 years. This number was followed by those who said 11-15 years, 6-10 years and 1-5 years with 24%, 20% and 16% respectively. The least reported was those with less than a year and over 20 years with both having 6%. Longer number of years meant that the respondent had vast experience in dealing with authentication of students documents upon request.

Number of Years worked in Research Office

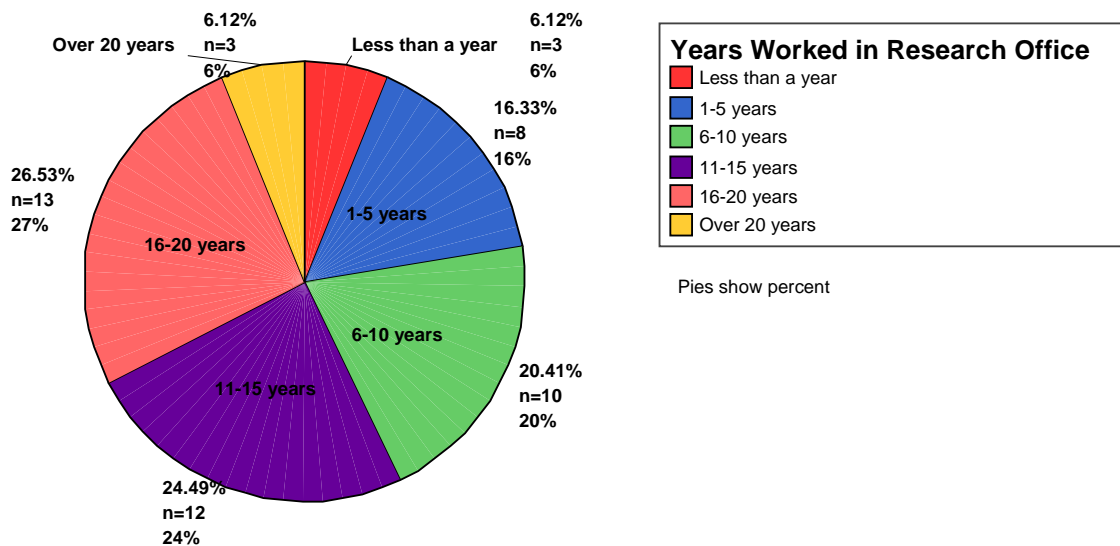


Figure 4.1: Number of Years Worked in Research Department

4.2.2 Document Fraud Awareness

Section B of the questionnaire was focusing on whether respondents were aware or knew about fraud in relation to KCSE certificate. Question 3 wanted to know whether respondents had heard about illegitimate academic documents. *Table C 3* in the appendix show the frequency distribution of responses. 88% of the respondents who said they were aware. This is to mean that, illegitimate certificate is not a new term to the respondents. Figure 4.2 shows an illustration of these statistics.

Those Aware of Illegitimate KCSE Certificate

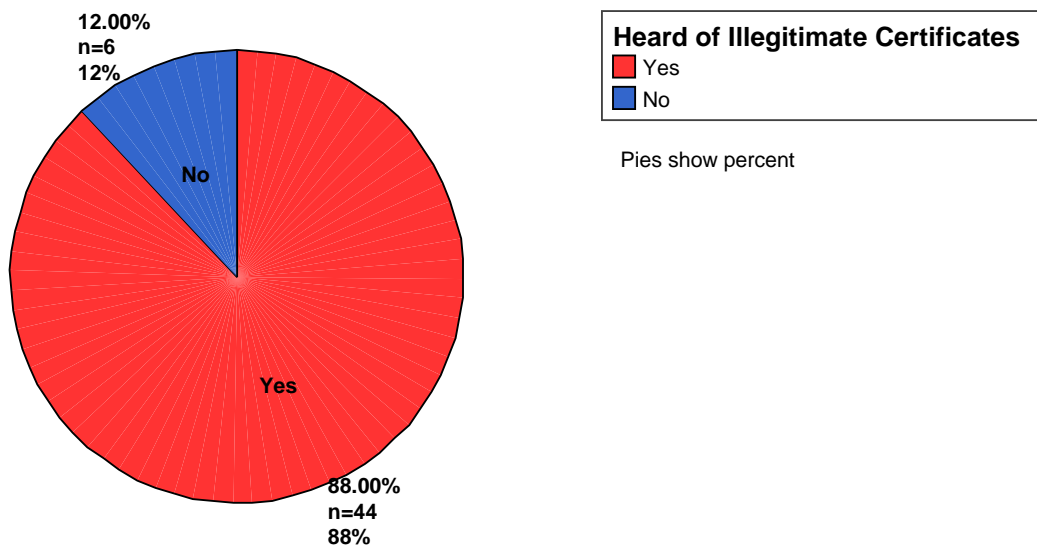


Figure 4.2: Those Aware of Illegitimate KCSE Certificates

Question 4 sought to determine whether there were cases of people using falsified KCSE certificates to join institutions of higher learning or gain employment. In Figure 4.3, 92% of the respondents said that they have heard cases of people who have used illegitimate certificate to enroll into universities and training institution. This statistics can be interpreted to mean that this malpractice is often carried out by individuals who want to further their studies in training and higher learning institutions.

Those Heard of People using Fake Certificates

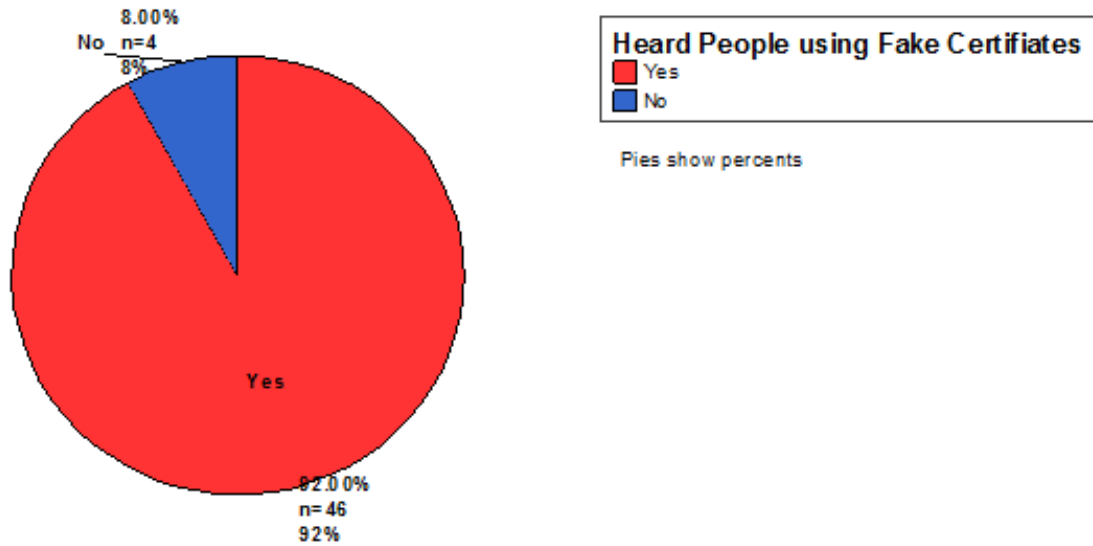


Figure 4.3: Use of Fake Certificate

4.2.3 Negative Effects of Illegitimate Academic Document

When asked about negative effects of using fraudulent academic documents, 82% said that it contributes to poor quality of education, 68% said it damages the reputation of an institution while 48% said it contributes to lack of credibility from the public. Frequency tables containing these findings can be found in Appendix C. Figure 4.4 illustrates these statistics. These findings echoes CAPSLE (2009) and Garwe (2015).

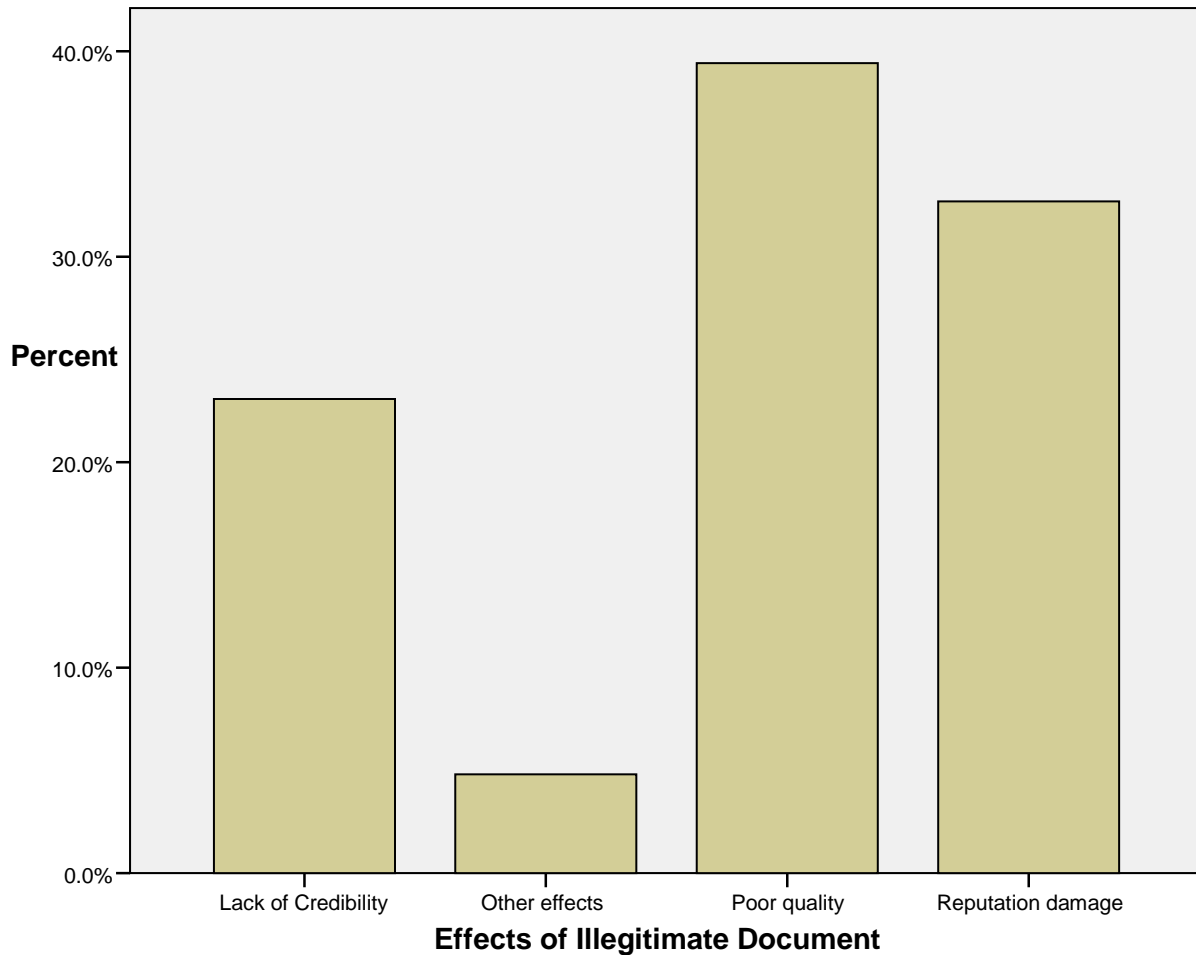


Figure 4.4: Effects of Illegitimate Academic Documents

4.2.4 Method used to Falsify KCSE Certificates

Question 6 sought to determine common types of document fraud used by fraudsters. This was in line with the first objective of this research. Understanding of these types was key to developing a prototype addressing these forms of document fraud. Some of the types included double use of certificate (one certificate being used by two people), altered document (some information changed in the original document), fabricated document (document created to look like an original document) and omission of data (removing some data from the document). From tables C 9, C 10, C 11 and C 12 in Appendix C, 38% of respondents said double use of certificate was common, 68% said altered document was common, 84% said fabricated document was common and 34% said omission of data was common respectively. Figure 4.5 below shows this data.

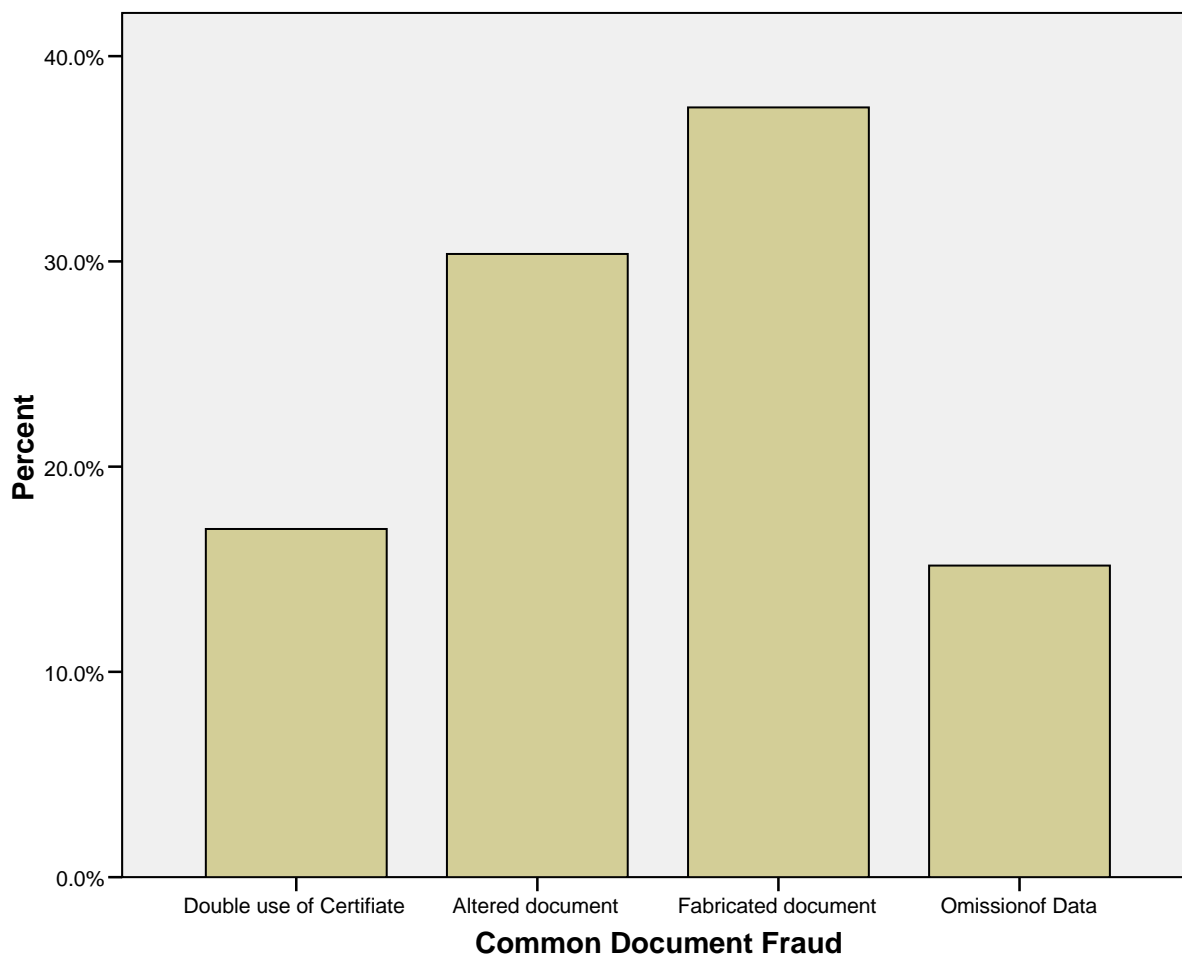


Figure 4.5: Methods of Falsifying KCSE Certificates

4.2.5 Security Features on a Genuine KCSE Certificate

The study also sought to know what features research officers looked at to when determining authenticity of certificates. Some of the features were gotten from the KCSE certificate according to the guidelines of the Kenya National Examinations Council. It was also determined that, when either of the feature was missing then the certificate was invalid.

These features are used to provide security to many legal document in many countries. Therefore, regarding this question, respondents were allowed to choose more than one features which they considered key when determining legitimacy of certificate document. In response 68% said they look at the quality of paper, 52% said they looked at holograms, 36% look at

patterns printed on paper, 48% look at watermark and 66% look at security thread. These findings are captured in table C 13, C 14, C 15, C 16 and C 17 respectively.

Respondents were also asked whether these features were sufficient in preventing document fraud. In response, 12% said these features were sufficient in preventing document fraud while 87.5% said the features were not sufficient in preventing document fraud. 4% did not answer this question. 84% of not preventing document fraud means that, a document can be created to look like a genuine document and in this case an academic certificate.

Sufficiency of Security Features

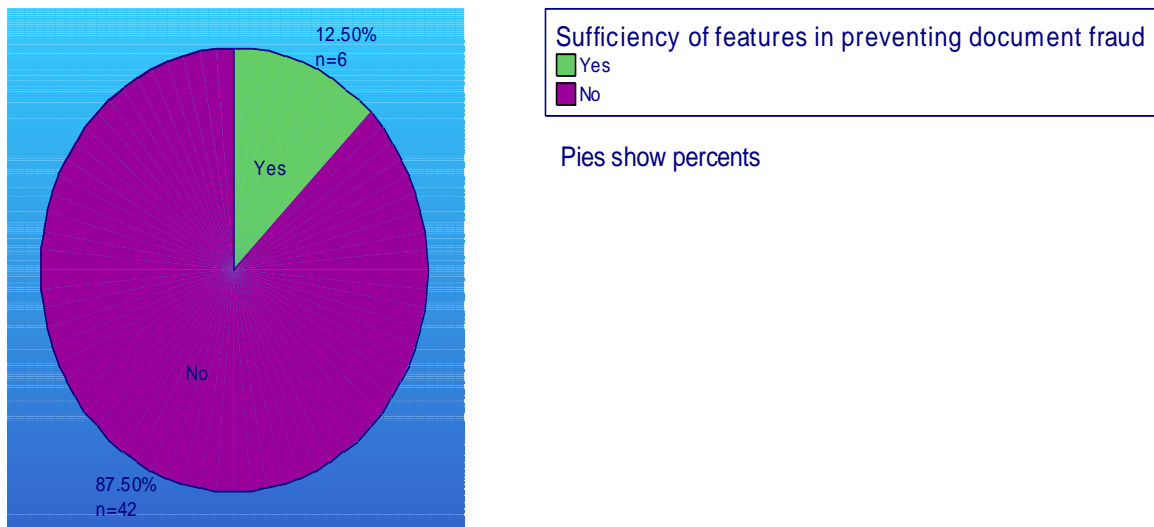


Figure 4.6: Sufficiency of Security Features

4.2.6 Request for Authentication of KCSE Certificates

The study sought to know whether the department received requests from institutions to authenticate KCSE or any other certificate. According to Figure 4.7, 26% said they have received request for authentication of certificates. This means that a majority of institutions trust the documents brought to them are genuine and this leaves room for fake certificate to be used in the market.

When a request is made the department take ten working days to give feedback to the institution or a person who made the request KNEC Charter (2015). Long waiting period means that there is

need for an online system that can be used by institutions such as universities, colleges and employers to get real-time feedback on authenticity and integrity of the certificate in question.

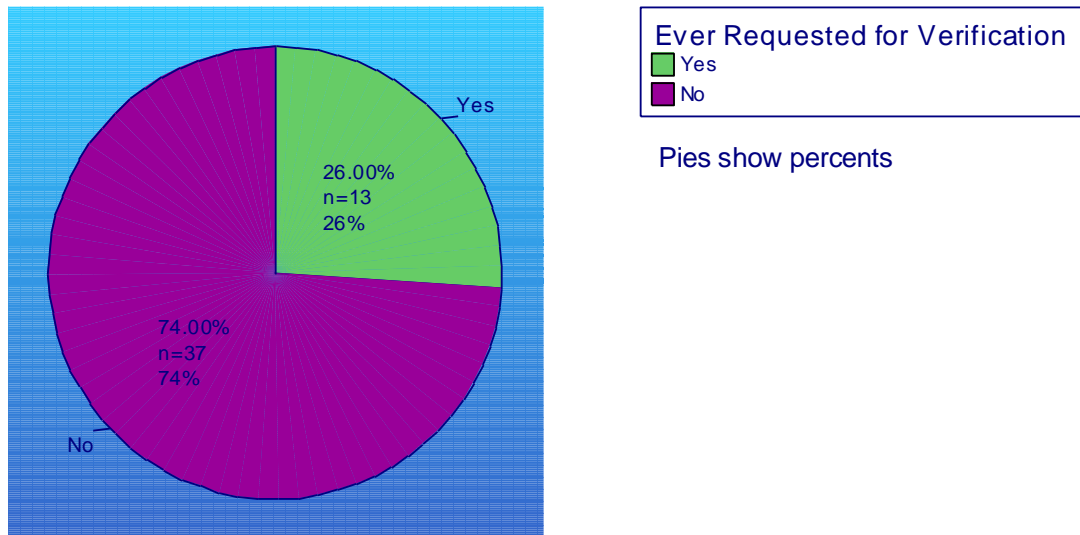


Figure 4.7: Ever Received Request to Authenticate Document

4.2.7 Challenges Faced by Institutions when Authenticating Certificates

Question 9 aimed at determining whether respondents faced any challenge when verifying authenticity of certificates. Due to increased cases of using fake KCSE certificates, it was ideal to find out some of the challenges faced by institutions when verifying academic certificates.

Respondents said that they faced challenges when verifying the authenticity of certificates. From frequency tables, 60% said that it was tedious, 60% said it was time consuming, 82% confirmed that it was difficult to tell a genuine and fake certificate, 76% said it was difficult to authenticate certificates from other countries and 100% had no other challenge regarding challenges. The proposed system will, therefore, assist users in distinguishing between a genuine and fake certificate. Figure 4.8 bellow shows a bar graph of challenges faced by institutions when verifying certificates.

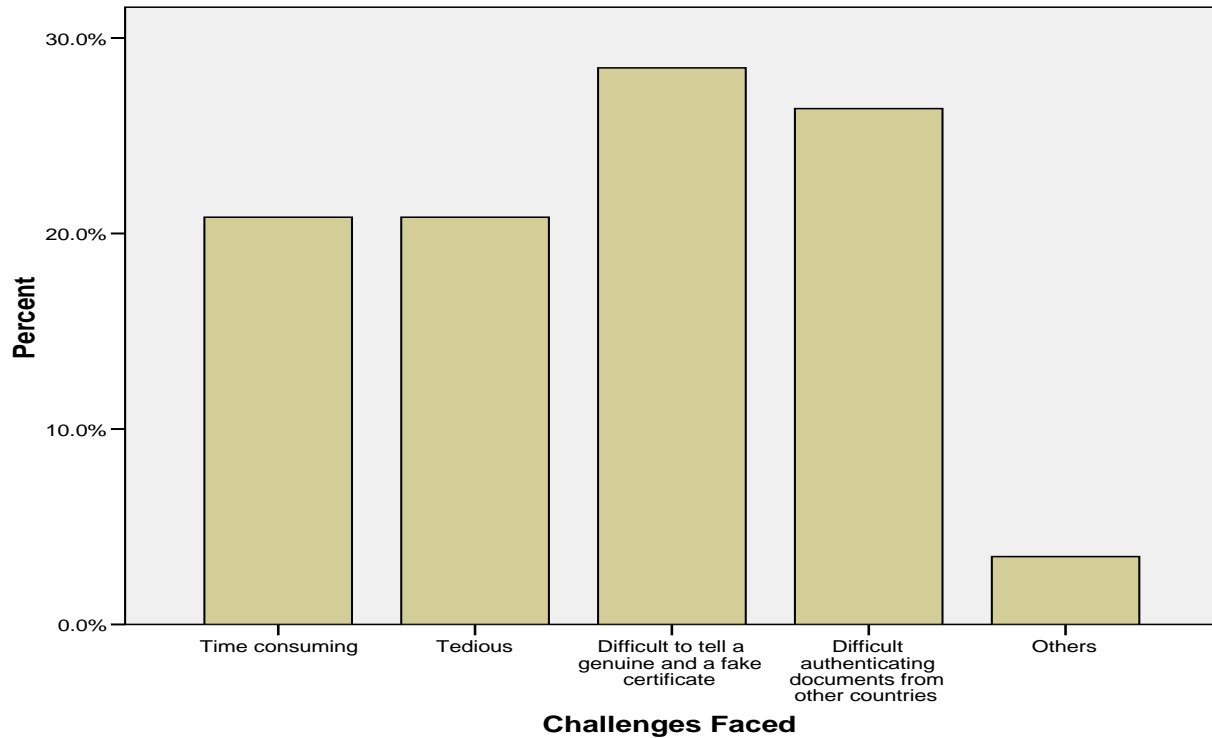


Figure 4.8: Challenges of Authenticating KCSE Certificates

4.2.8 Importance of a Digital Authentication System

This section of the questionnaire involved getting information about system requirements. Question 12 of this section was asking respondents whether they would consider adopting authentication system in their institution to enable consumers of KCSE certificates to authenticate this document. Figure 4.9 shows response regarding this question 2% of the respondents said that the proposed system would not be of important to them, 43% said the system would probably be of important and 55% said the system will definitely be of importance. This findings supports the fact that 87% of respondents said current features in certificates are not sufficient in preventing academic document fraud. Therefore, development of a computer based system would be helpful to leverage on the available features.

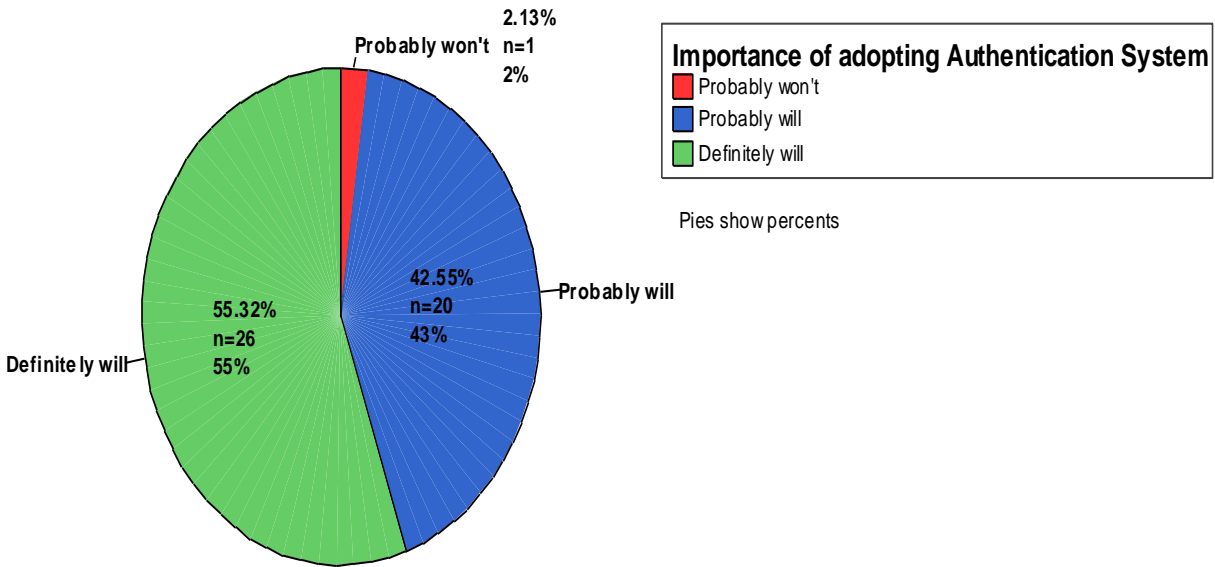


Figure 4.9: Importance of a Digital Authentication System

4.2.9 System Requirements

On question regarding requirements of a security system, respondents were required to indicate factors that were important to them. These requirements included authentication, data integrity, privacy and non-repudiation. In response, 52% said authentication is very important, 48% said data integrity is important, 54% of respondents said privacy is very important and 40% said non-repudiation is important. This shows that most respondents wanted a system that can meet these security goals.

The last question was meant to elicit response regarding user requirements of a good system. Ease of use, reliability and security got 78%, 74% and 72% respectively. Other factors considered important by respondents are record keeping 58%, simple interface 54%, functionality 50% and cost 40%. The researcher worked to develop a prototype meeting this requirements. Figure 4.10 shows bar graphs indicating response from the respondents.

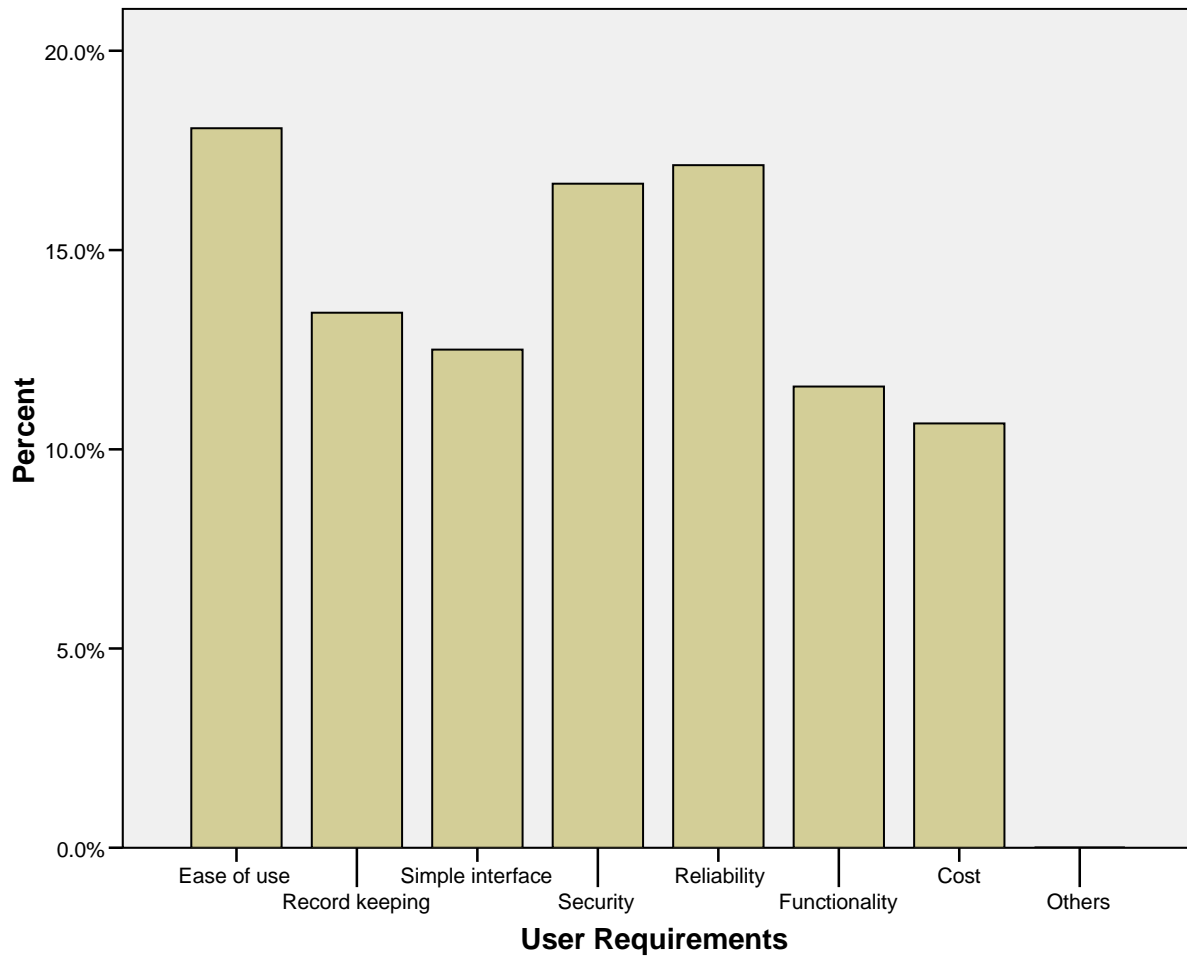


Figure 4.10: System User Requirements

4.3 Requirements Analysis

To explain the services and features that should be addressed by authentication prototype, system requirements were categorised into two-functional requirements analysis and non-functional requirements analysis. The former and the latter has been discussed in the following section.

4.3.1 Functional Requirements

Functional requirements are functions, processes and capabilities that the system has to perform and execute if it is implemented (Dennis et al., 2012; Mualuko, 2016). These functions are in relation to goals that the user wants fulfilled by the system. Functional requirements in this system include management of system (by KNECs system Administrator), Certificate

verification- the users of the system would be able to register login and verify certificates brought to them by scanning the QR code. The QR code contains unique features of the certificates that are encoded during generation of the certificate. In case the information in the certificate is not conforming to what is in the database, then the document is invalid and illegitimate.

4.3.2 Non-functional Requirements

According to Dennis et al (2012), non-functional requirements are behavioral properties that the system must have such as performance and usability. In addition, non-functional requirements are qualities that a system can do without but are desired to make the system interactive, user friendly, and easy to use (Mualuko, 2016).

Authentication system has the following characteristics in relation to non-functional requirements: security (SSL enabled web connection, username and passwords for both administrator and user, administrator has to validate users who register to use the system), ease of use (simple interface), system availability (no or little downtime), and reliability (giving correct results).

4.4 Proposed Prototype Architecture

The prototype will be a web based solution consisting of frontend and backend. The system administrator will be responsible for all backend operations such as managing users, adding subjects, students, schools, certificates and uploading certificate. The signed certificate together with the QR code will be stored in the database for future reference by user. To access the backend, users will have to login via web portal which is security enabled through the use of SSL. This ensures security to user details such as passwords and usernames as well as the security of the certificate being authenticated. Figure 4.11 shows the architecture that the system will use.

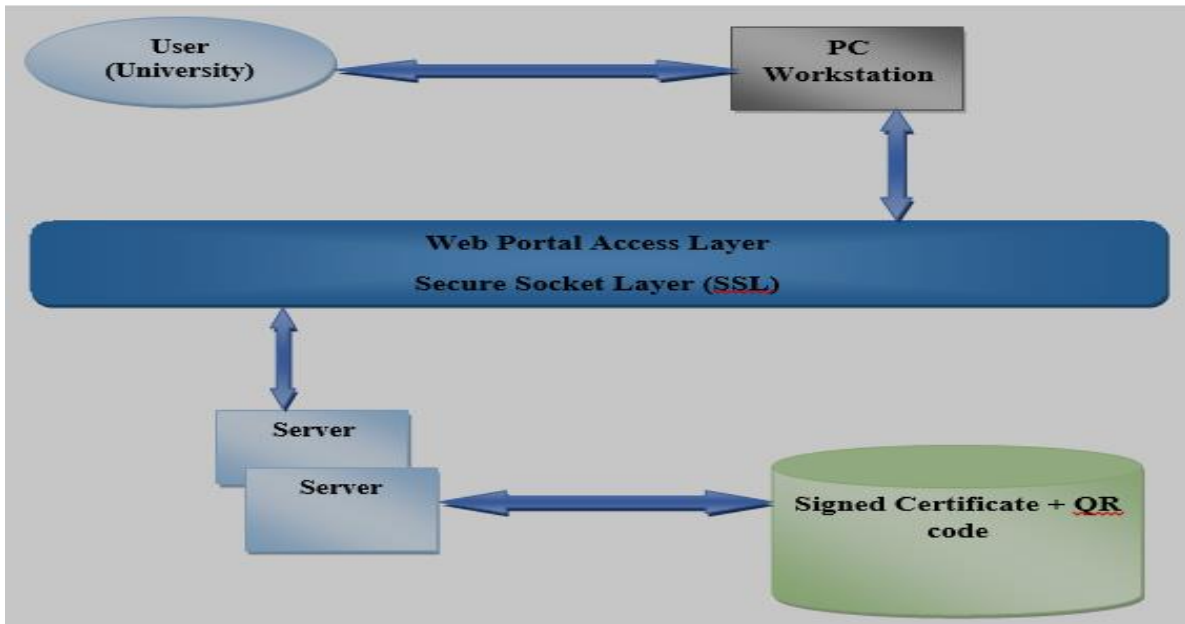


Figure 4.11: System Architecture

4.5 System Use Cases

Figure 4.12 above shows a combined use case diagram of the proposed system. There are two primary actors-the system user (university, employer or any other entity) and the system administrator from the KNEC.

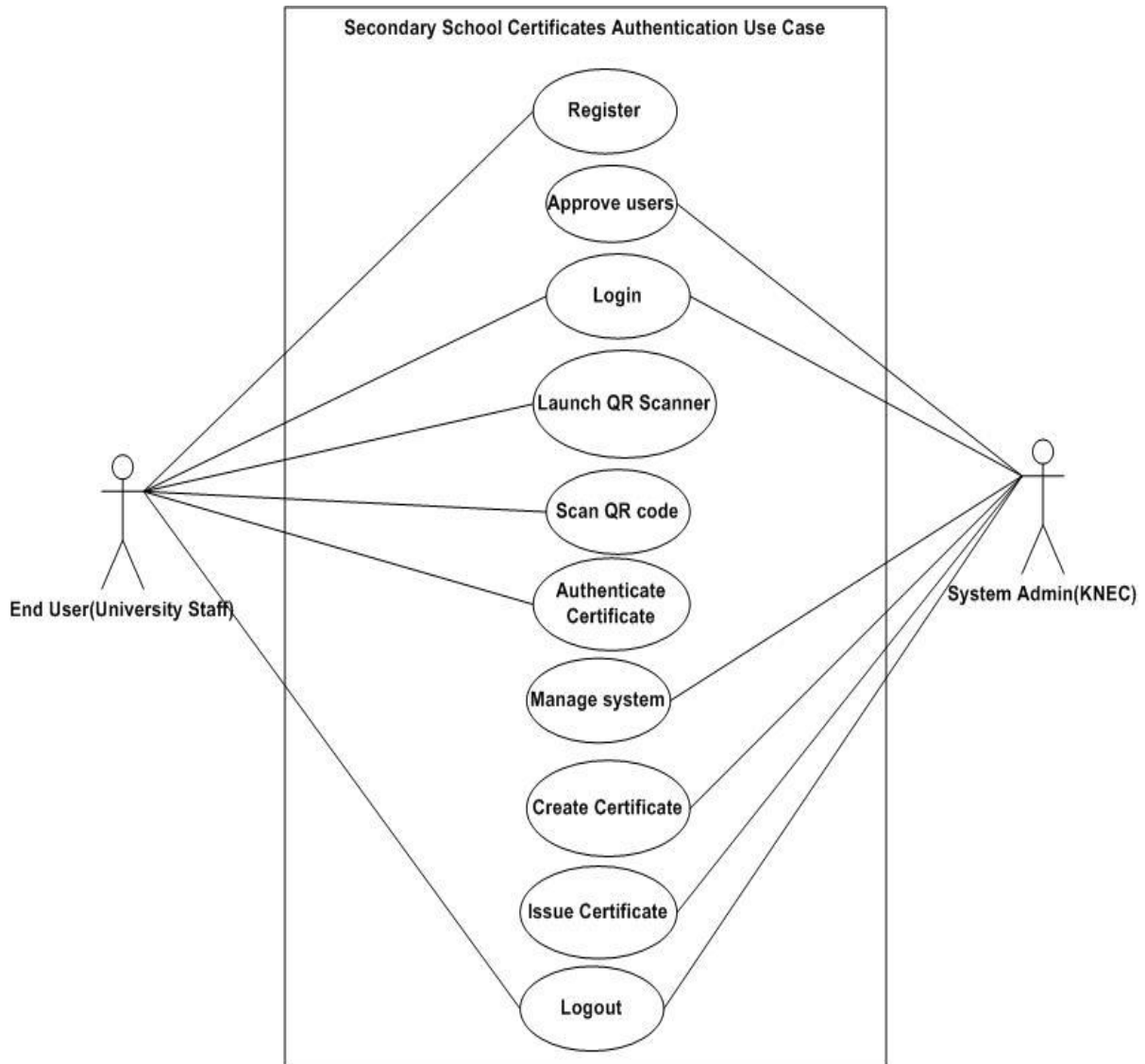


Figure 4.12: System Use Case Diagram

4.6 Use Case Scenarios

These are descriptions of different scenarios in the system. It seeks to explain the process undertaken by the actor in each use case. It also helps to know the outputs from the system with regard to the inputs given by the actor.

4.6.1 Use Case Scenario 1

Use Case Creating Certificate

Primary Actor: System Administrator

Preconditions: The system administrator is identified and authenticated on the system.

Success Guarantee (Post Condition): Student, school, subject and grades details are successfully saved on the system. These details are added to the certificate template and the QR code is generated and appended on the certificate for printing.

Main Success Scenario

- i. A soft copy certificate template is created.
- ii. Admin enters student details.
- iii. Admin enters school details.
- iv. Admin enters subject and grade details.
- v. Details in step 2, 3 and 4 are available for viewing and editing on the system.
- vi. Once these details are entered the QR code is generated automatically
- vii. A soft copy of certificate is created and printed.

4.6.2 Use Case Scenario 2

Use Case 2: Issuing Certificate

Primary Actor: System Administrator

Preconditions (Post Condition): Soft copy certificate is successfully created and printed.

Main Success Scenario

- i. Administrator prints the certificate for issuing.
- ii. The certificate is issued to the student.

4.6.3 Use Case Scenario 3

Use Case 3: Register

Primary Actor: User (University, Employer and or any other)

Preconditions: The system user is requested to register into the system.

Success Guarantee (Post Conditions): Login Successfully.

Main Success Scenario

- i. The user will enter registration information (Institution name, contact person name, email address, username and password)
- ii. User awaits approval from the system administrator.
- iii. If the user is a recognized institution the system admin approves the user otherwise, decline.
- iv. If approved, the system user gets a notification that he or she is able to log into the system.

4.6.4 Use Case Scenario 4

Use Case Authenticate Certificate

Primary Actor: User (University, Employer)

Preconditions: User is successfully signed in to the system.

Precondition: User successfully launches the QR code scanner on the phone

Success Guarantee (Post Condition): The user is able to scan the QR code

Main Success Scenario

- i. User will launch the QR scanner in the smartphone.
- ii. A QR code validation key is generated on the phone.
- iii. User enters the validation code on the system portal.
- iv. If the validation key is valid the certificate will open on the portal, otherwise, user gets a message of invalid certificate password.
- v. The system request for a new validation key from the user.
- vi. The user logs out from the system.

4.7. System Sequence Diagram

Figure 4.13 shows the sequence process of interaction between actors and the system. This interaction is in form of messages passed back and forth from the system and actors respectively.

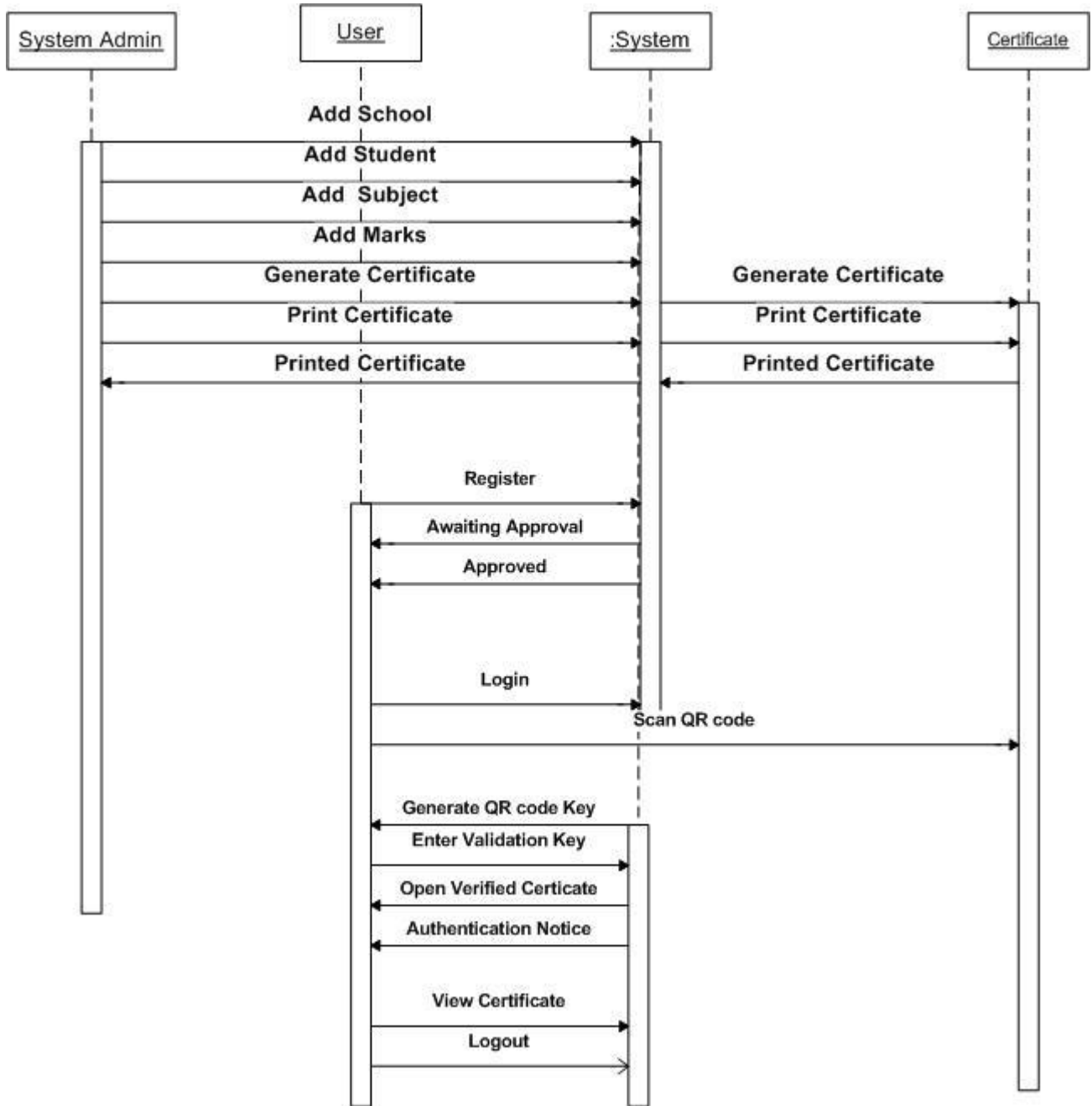


Figure 4.13: System Sequence Diagram

Figure 4.14 shows the partial domain model of the system. There is a relationship between one domain and the other. This has been showed by use of foreign keys. One student can take one or many subjects, while, one student can only be enrolled in one school at a time. Many subject can be found in one certificate, while one or many certificates belongs to one school.

4.8 System Domain Model

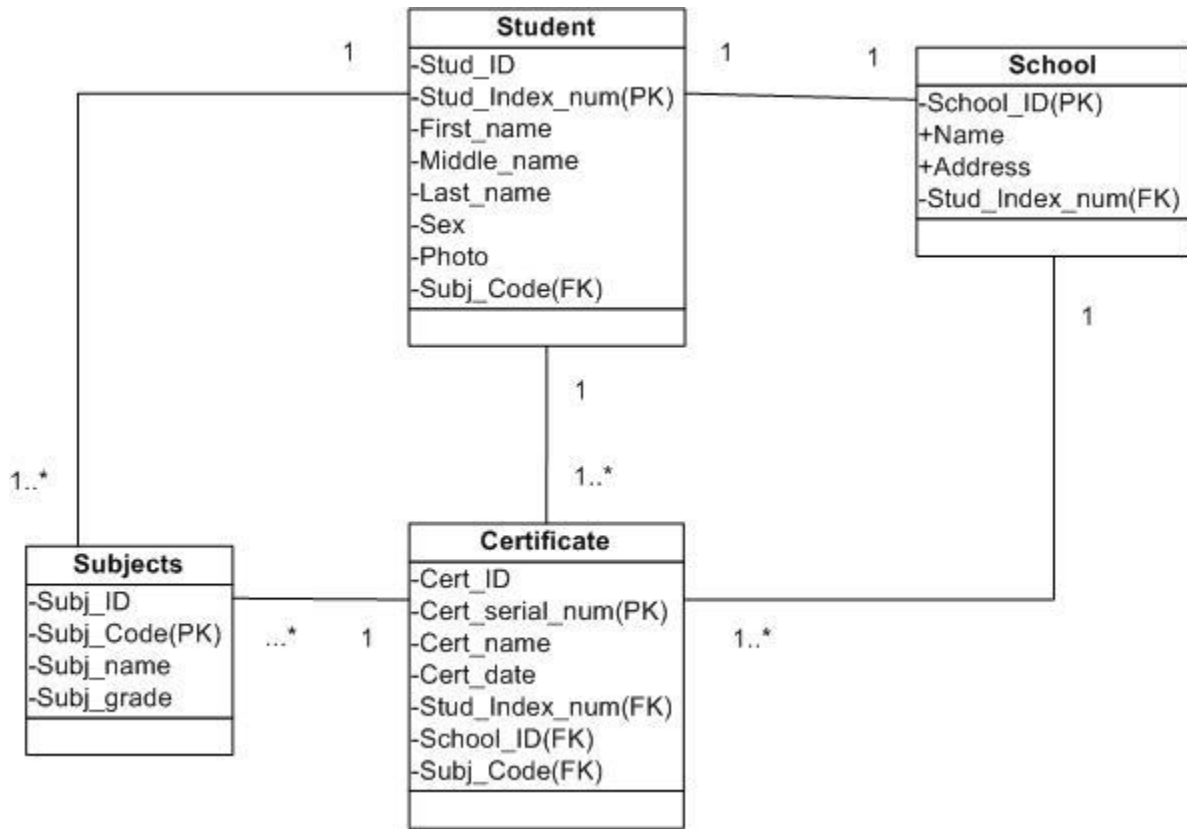


Figure 4.14: System Domain Model

4.9 Entity Relationship Diagram

One school has one or many students (one-to-many relationship), one student takes many subjects (one to many relationship), one certificate contains many subjects (one-to-many relationship), one certificate belongs to one students (one to one relationship) and one school has one or many certificates (one to many relationship). Figure 4.15 shows the ERD of the proposed prototype.

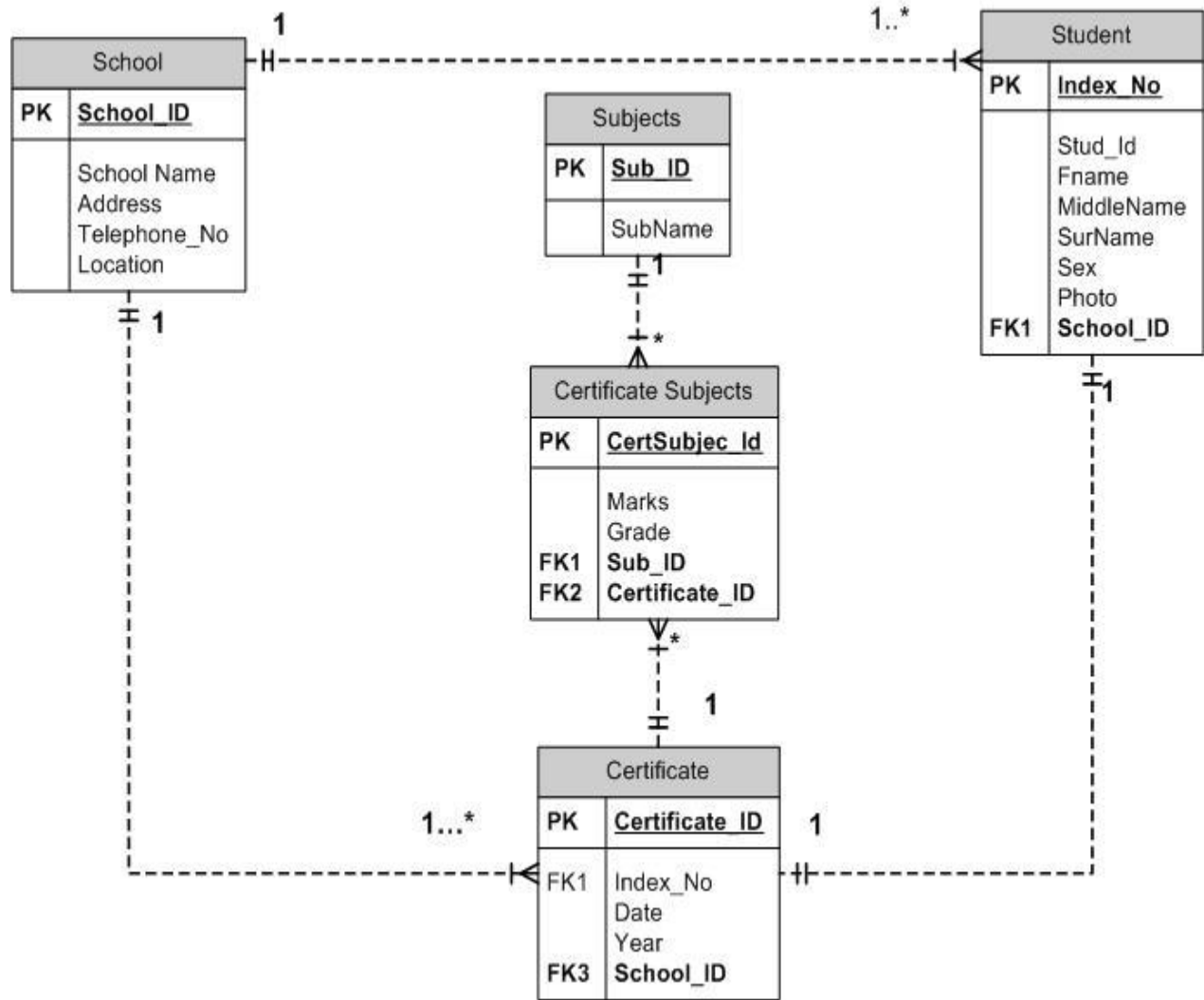


Figure 4.15: Entity Relationship Diagram

Chapter 5 : Implementation and Testing

5.1 Introduction

The proposed prototype was developed using various software tools. PHP scripting and HTML language was used for development of front end interface, while MySQL database management system was used. Since security was the main concern for this prototype, SSL was used to provide security on the portal. QR code was used to ensure hardcopy certificates were verified by scanning the QR code. A password key was generated to enable the user access the content of the QR code which is the certificate details.

5.2 Development Technologies

To develop authentication prototype several technologies were used. Following is explanation of these tools and technologies.

i. PHP

This is a common and powerful language for programming web based applications. This made it a perfect choice for me because it is used to create websites and related applications.

ii. OpenSSL

This is an open source tool for implementing transport Layer security. The main function of SSL was to provide secure connection of websites between a server and client.

iii. MySQL

This is a Database management tool which was used to create database for storage of data fed into the prototype. This was chosen because it is open source therefore no financial limitations.

iv. Apache Webserver

This is a standalone application that allows one to test a websites without having to host it in a commercial server.

v. Script Editor: Dreamweaver

This is the tool that was used to edit PHP and HTML code during the development of the prototype. The reason for using this tool is that it is easy to learn and use.

vi. Bacon QR Code Generator

This is a free tool used to generate QR codes. QR code was the preferred choice because it can store large amount of data in a small memory size. It contains an error correction library; Reed-Solomon code which helps solve the problem inherent in QR codes.

vii. QR code Scanner

This tool is a free mobile application which can be downloaded into a smartphone to enable users to scan and verify the authenticity of the certificate.

5.3 System Implementation

The prototype comprise of front-end and a back-end. The front end is a HTML form that allows the users to register, change password, enter verification code and authenticate document. The backend is PHP Laravel framework, Bacon QR code generator. To generate a QR code, student details, school, subject and grades must be entered. The certificate ID and other details are encoded into a QR code and a time stamp is generated to maintain the specific properties of each document. Since this prototype depended on smartphone camera phone to scan the QR code, barcode reader algorithm using camera device in mobile phone was used. This algorithm is embedded in the Bacon QR code generator library. Appendix D shows a sample code for generation of QR code.

5.3.1 Create and Print Certificate

Figure 5.1 shows the output of the certificate after student, subject, grade and school details have been entered by the system administrator. Once these details are captured they are converted into a QR code by Bacon QR Code generator. The certificate can be printed and issued to the student. Appendix D shows a sample code used to generate the QR code as explained above.



Kenya National Examination Council



Kenya Certificate of Secondary Education

Johnson Makaru

M

223459/001

St. Julian High School

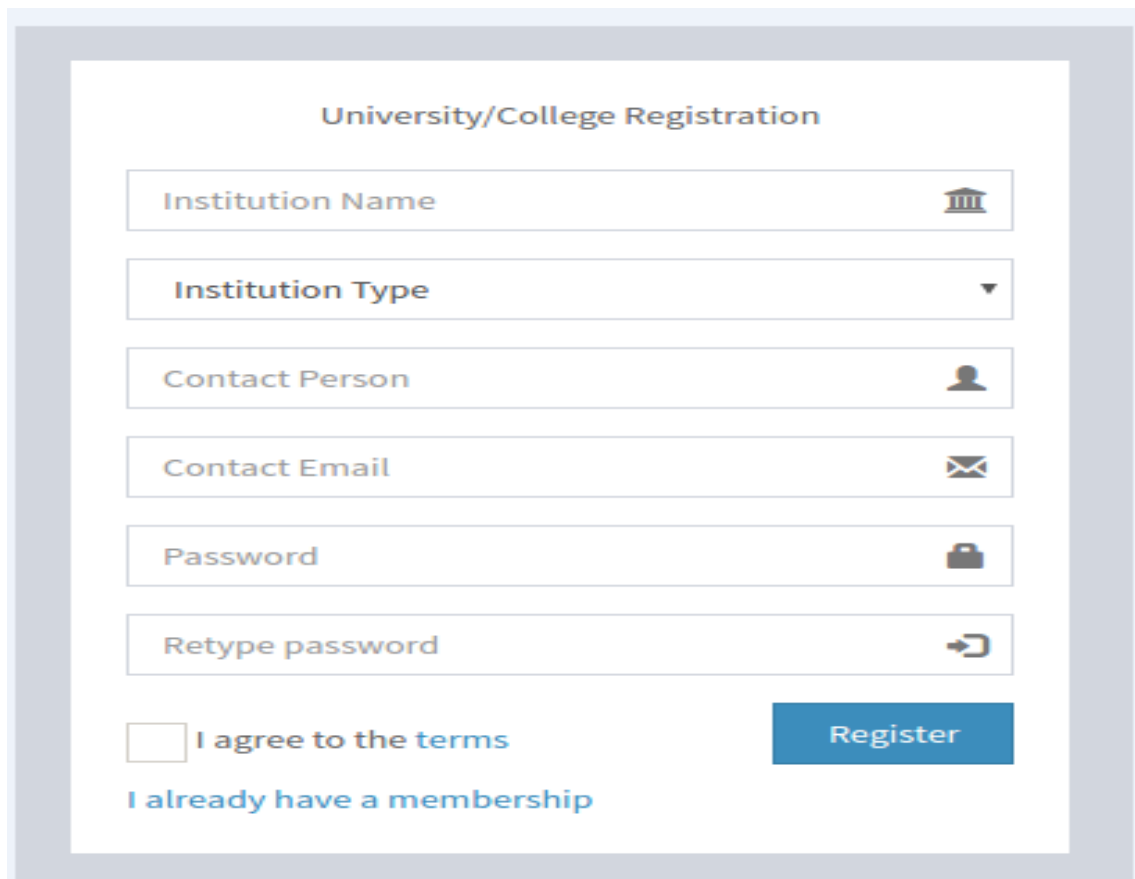
Subject	Grade	Subject	Grade
101 English	A- (Minus)	102 Kiswahili	B+ (Plus)
131 Mathematics	A	231 Biology	A
232 Chemistry	A- (Minus)	233 Physics	B+ (Plus)
312 Geography	B+ (Plus)	501 French	A



Figure 5.1: Certificate Created by the system Administrator

The form in Figure 5.2 allows user to register as an institution in order to be granted permission to access the system. This requirement is in line with the user requirement for authentication which was captured in the data analysis form the questionnaire. This will ensure that only authorized users are granted permission by the administrator to use this system. In case a user account exists, they will continue to sign in in order to use the system, otherwise register. Once a user registers, he or she will have to wait for approval from the system administrator.

5.3.2 User Registration



The image shows a web form titled "University/College Registration". It contains several input fields, each with a corresponding icon: "Institution Name" with a building icon, "Institution Type" with a dropdown arrow, "Contact Person" with a person icon, "Contact Email" with an envelope icon, "Password" with a lock icon, and "Retype password" with a refresh icon. Below the fields is a checkbox labeled "I agree to the terms" and a blue "Register" button. At the bottom, there is a link that says "I already have a membership".

Figure 5.2: User Registration Form

5.3.3 User Approval Form

Figure 5.3 shows a list of registered users who are awaiting approval from the system administrator.

Institutions Pending Approvals					
#	Institution Name	Institution Type	Contact Person	Contact Email	Action
1.	Strathmore University	University	John Miturty	jmiturty@strathmore.edu	Reject Approve
2.	Michilly University	University	Jane Ochites	jochites@michilly.edu	Reject Approve
3.	Malgedra College	College	George Maguty	gmaguty@malgedra.edu	Reject Approve
4.	Bisfirty College	College	Cate Miguel	cmiguel@bisfirty.edu	Reject Approve

« 1 2 3 »

Figure 5.3: User Approval Form

5.3.4 Log-In Form

Once an institution is approved, users will be able to log into the system to start the process of certificate verification. Figure 5.4 shows a log in form.

Sign in

Remember Me Sign In

[I forgot my password](#)
[Register a new membership](#)

Figure 5.4: Log in Form

Verification process begins in the event when an applicant presents his or her documents for authentication before enrollment into the institution. A verifier scans the QR code on the certificate and a validation code is generated on the phone. Figure 5.5 shows generated code.

5.3.5 Validation Key

To generate the QR validation key certificate number and student index number and current time during generation of the certificate is used as the timestamp to generate password specifically for each certificate. In case the certificates details are updated or deleted a new validation key is generated. Appendix E shows sample code used to generate the validation key. Figure 5.5 shows a sample validation code.

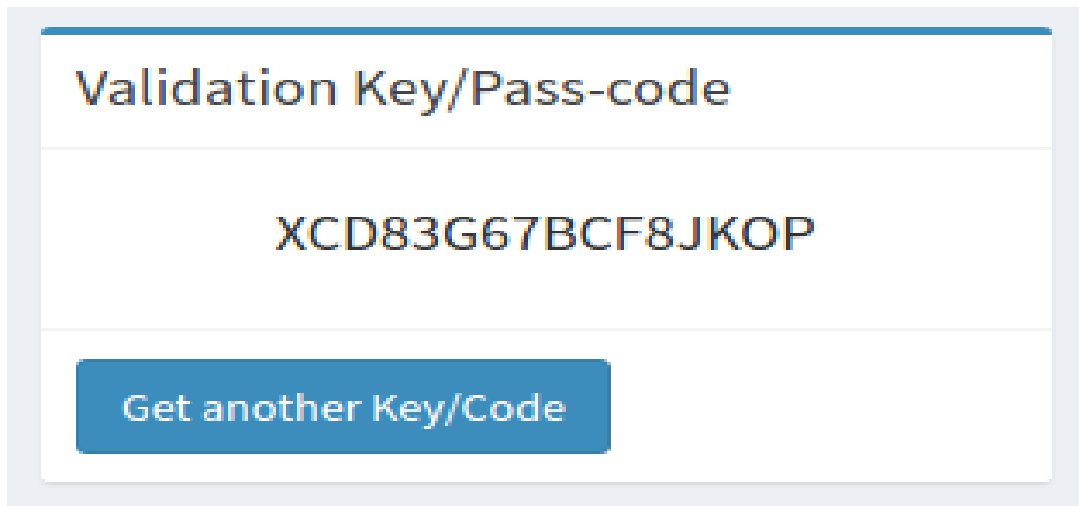
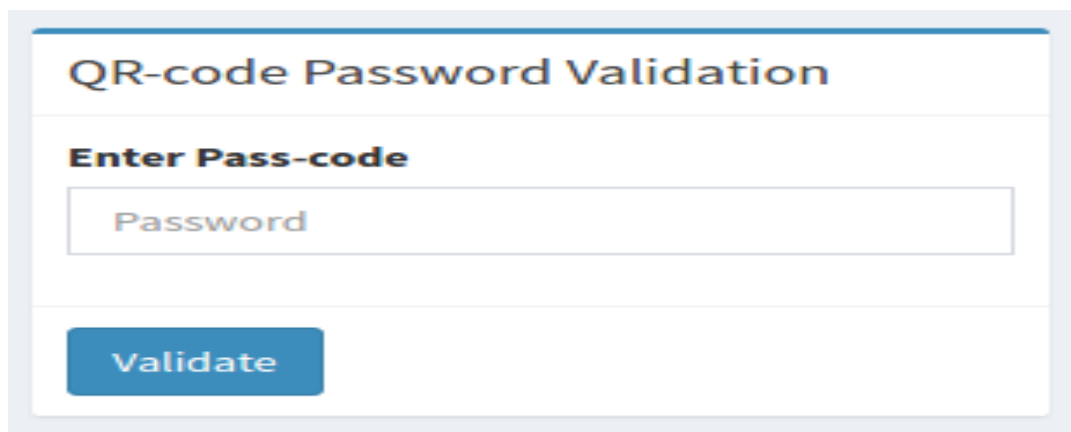


Figure 5.5: Validation Code

After generation of the above code, the user enters this password on the verification form on the system. Once the password is entered, the user will press verify button which will trigger authentication of certificate and it will open on the user's PC. Figure 5.6 shows QR code password validation form.

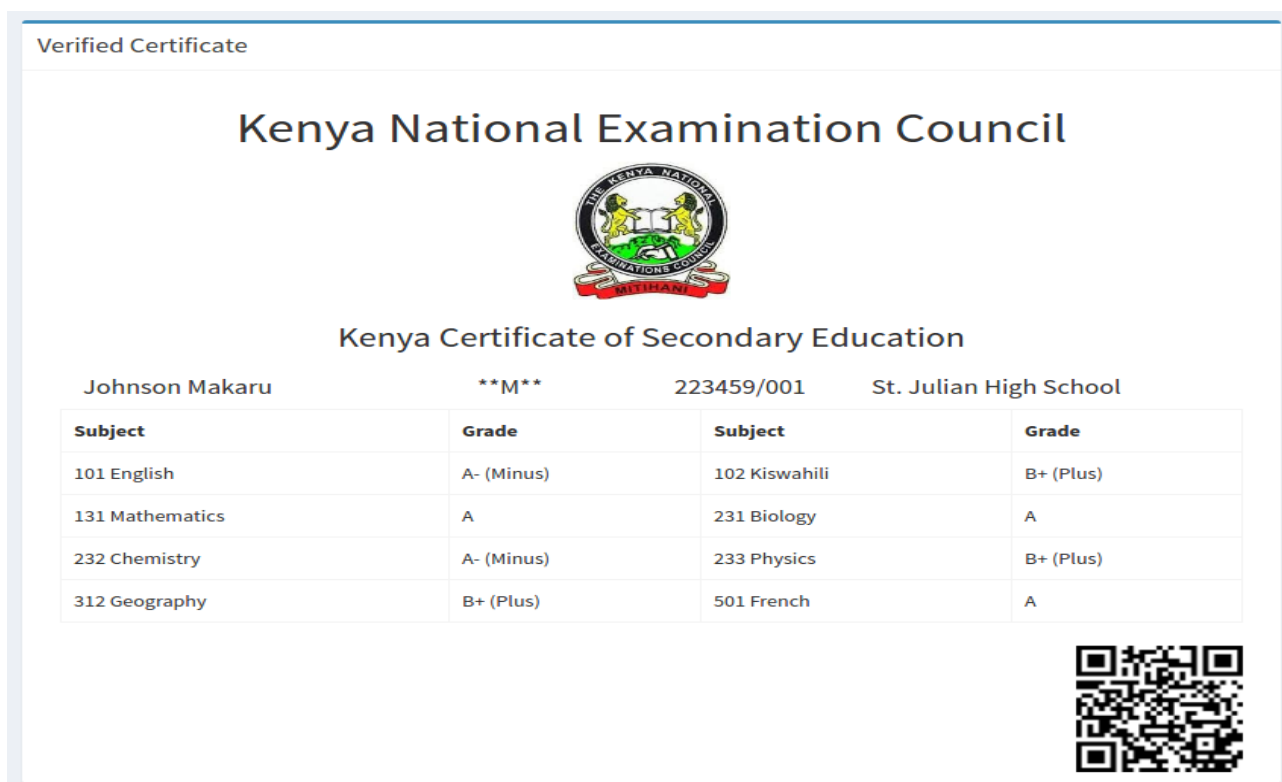


The image shows a web form titled "QR-code Password Validation". It has a header with the title, a section labeled "Enter Pass-code" containing a text input field with the placeholder text "Password", and a blue button labeled "Validate" at the bottom.

Figure 5.6: QR code Validation Form

5.3.6 Validated Certificate

Upon entering the generated password the certificate opens on the user’s PC interface. This will display the certificate details with a conformation message confirming the authenticity or otherwise of the document. Figure 5.7 shows the verified certificate that was scanned by the user.



The image shows a "Verified Certificate" from the Kenya National Examination Council. It features the council's logo and the title "Kenya Certificate of Secondary Education". The certificate details for Johnson Makaru are as follows:

Subject	Grade	Subject	Grade
101 English	A- (Minus)	102 Kiswahili	B+ (Plus)
131 Mathematics	A	231 Biology	A
232 Chemistry	A- (Minus)	233 Physics	B+ (Plus)
312 Geography	B+ (Plus)	501 French	A

Additional details include the name Johnson Makaru, the grade **M**, the ID number 223459/001, and the school St. Julian High School. A QR code is located in the bottom right corner of the certificate.

Figure 5.7: Authenticated Certificate

5.4 Prototype Testing

Prototype testing was carried out to determine whether both functional and non-functional requirements were met. Functional requirements includes ability to create and sign a certificate and generation of a QR code, registering into the system, signing in and verifying authenticity of the certificate. On the other hand, non-functional requirements includes usability, security, data storage, authentication etc.

Since this research applied agile software development methodology, agile testing was done to test for performance issues within the context of agile workflow. Testing prevents bad software from getting to the market, because testing is a quality assurance activity which ensures that only software that meet and are free from bugs get to the market. Figure 5.8 represents testing results as per the user requirements gathered during data collection.

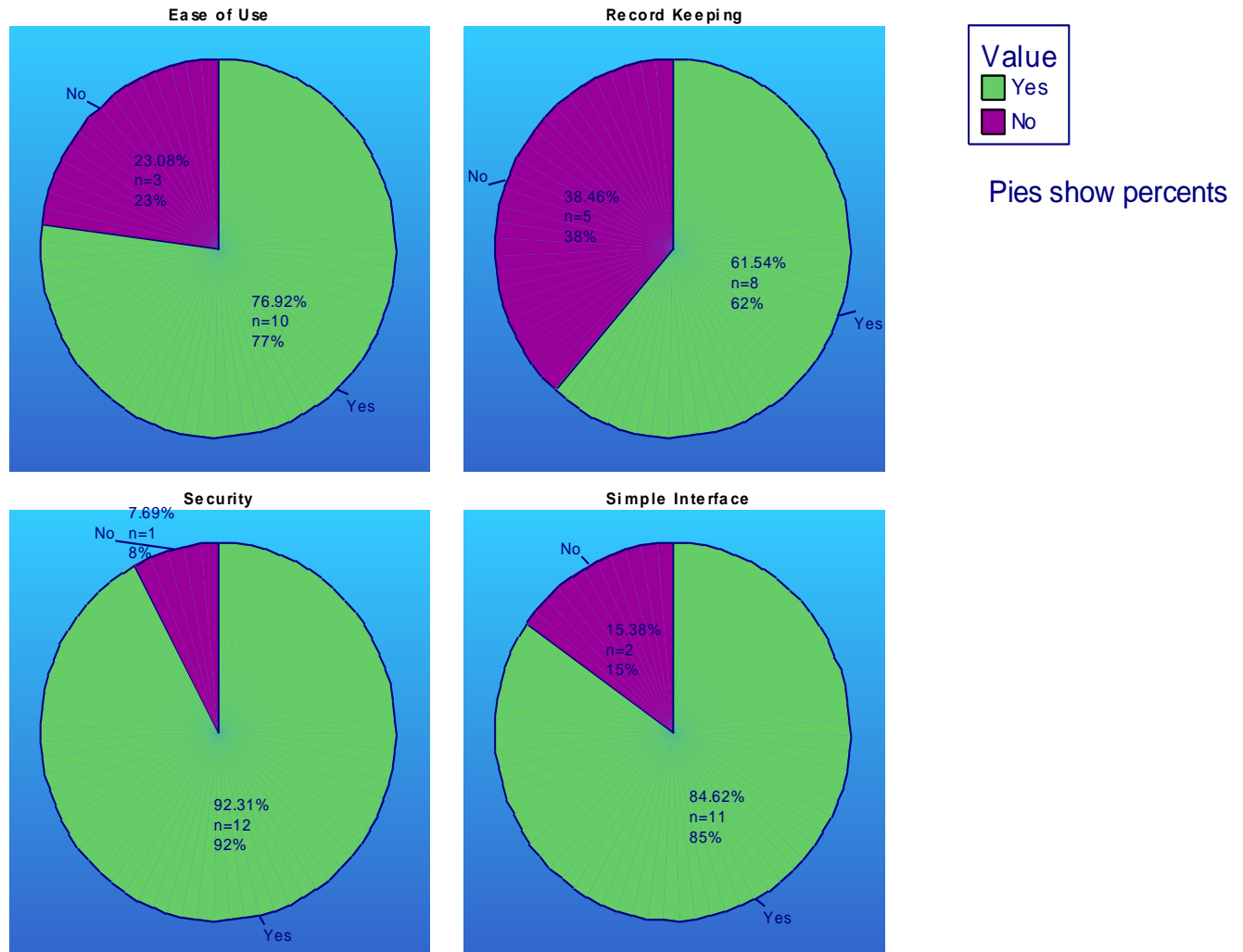


Figure 5.8: Prototype Testing Result

Out of the 13 people selected for testing the prototype, 77% found it easy to use while 23% said it was not easy to use. Going by the majority, from a researcher point of view, it can be concluded that the system was easy to use. This can be attributed to the simple interface as it can be seen in Figure 5.8, 85% of the respondents said the system had a simple interface, while 15% said it had no simple interface. The high number of those who said it had simple interface contributed to the opinion that it was easy to use.

Since security was the main focus in this research, security as a user requirement was also tested to determine whether the system was providing security in any way. With regard to this, approximately 93% said that the system provided security as it was stipulated in the user

requirements. This can be attributed to the high levels of security provided which include; waiting for approval from the system administrator before being allowed access into the system, login passwords, and encryption of the certificate information and use of protected QR code.

Record keeping as a user requirement was also tested and 62% said the system provided room for record keeping. This requirement is key because it enables users to retrieve document. This requirement was implemented by ensuring creation and storage of certificates in a database, where users of the system could retrieve certificate by entering the serial number.

Chapter 6 : Discussion

6.1 Introduction

The findings obtained in Chapter 4 formed the basis from which authentication system was developed. This chapter analyses the findings in relation to research objectives and literature review.

6.2 Types of Fraud Associated with Academic Documents

The study sought to find out the most common types of fraud regarding academic documents. This was in line with the first objective of this research. Findings from this question would determine what the system would do with regard to preventing document fraud. Some of the types examined included double use of certificate (one certificate being used by two people), altered document (some information changed in the original document), fabricated document (document created to look like an original document) and omission of data (removing some data from the document).

Study findings showed that fabricated document was the most form of document fraud with 84%, followed by altered document at 68%, while double use of certificate and omission of data having 38% and 34% respectively. These forms of document fraud were discussed in the literature review, where previous study indicates that these were the most commonly practiced forms of document fraud.

The developed authentication prototype addressed these issues by ensuring the use of student images on the document. This would help in comparing the image of the person with what is being shown on the system's portal. This is because success in changing another person's details on the paper document would not mean changing of these details in the system. Other forms of fraud were addressed by use of digital signatures which provide data integrity (that data on the certificate was not altered) since the document was created. The use of QR code ensured that the certificate came from authorized issuer which in this case is the Kenya National Examination Council.

6.3 Security Features used to Authenticate Paper Documents

The second objective sought to determine current features which provide security to paper documents. This was influenced by the fact that academic certificates are official and legal documents that require protection to maintain their authenticity. Therefore, regarding this question, respondents were allowed to choose more than one features which they considered key when determining legitimacy of certificate document.

Findings regarding this objective showed that 68% look at the quality of paper, 52% look at holograms, 36% look at patterns printed on paper, 48% look at watermark and 66% look at security thread. Owing to the fact that academic certificates are legal documents, these features are also used in other paper based document such as bank notes. This concurs with the literature review on paper based security whereby, most paper documents use these features to provide authenticity and integrity. A follow up question on whether these features were sufficient in preventing document fraud, showed that majority of the respondents were not convinced that they were completely efficient. This was represented by 84% who said the current features are not sufficient in preventing document fraud.

The mentioned features were derived from the KCSE document which indicates that some features were to be considered when determining the authenticity of this document. Despite there being these features, fraudsters have managed to use technology and reproduce documents which are similar to genuine ones. This inefficiency drove me to introduce the feature of QR code, digital signatures and online portal to leverage on the existing features.

6.4 Existing Systems used to Authenticate Academic Certificates

Review of existing system was a key contributor to development of authentication system. Security features discussed in 6.3 above formed part of the existing system which is used by institutions to verify authenticity of academic documents. Findings indicated that these system was not efficient in addressing the problem of document fraud. Other computer based systems which were reviewed had both advantages and disadvantages.

Following this, the developed system was an improvement of what already is in the literature. Therefore, web based combined with offline solution was applied in developing the proposed

prototype. This was made possible by enabling scanning of QR code on the printed document to authenticate the certificate as well as use of web portal to verify the details of document especially the student image.

6.5 Certificate Authentication Prototype

The main objective of this research was to develop a computer based prototype. The prototype would be used to authenticate secondary schools certificates for students who wished to join Universities in Kenya. Findings from the study showed that a majority of respondents (98%) were advocating for a system to aid in verification and authentication of academic certificates for new entrants. This decision was influenced by the fact that many institutions faced numerous challenges when authenticating documents and changes of allowing illegitimate certificates was high.

From frequency tables, 60% said that it was tedious, 60% said it was time consuming, 82% confirmed that it was difficult to tell a genuine and fake certificate, 76% said it was difficult to authenticate certificates from other countries and 100% had no other challenge. The developed prototype addressed this challenges by providing services on web platform for time saving, use of digital signatures and QR code to maintain originality and authenticity of the document.

In line with the literature review it was discovered that Elliptic Curve Digital Signature, cryptographic technologies, QR codes and web based solutions were efficient and effective in providing solutions to certificate fraud. This is because, when these features are combined together provide more security than when one technique. It is hard for one security measure to provide 100% security, therefore, integrated security is preferred.

6.6 Authentication Prototype Testing

The last objective was to test the developed prototype. System testing is key in software development cycle. Since the prototype adopted agile development methodology, testing was done at every stage of the system to ascertain the functionality of the prototype was guaranteed. In addition to this, users were given the prototype to use and feedback was sought. Findings regarding testing indicated that the requirements made by users were met. Ease of use, record keeping, security and simple interface were considered met in the developed prototype.

Security which was the main feature of the prototype was implemented at different levels; SSL was used to ensure safe connection between the server and client, registering of users was another security measure which ensured that only genuine and legitimate users accessed the system. Digital signatures were used to ensure that integrity, authenticity, non-repudiation of the document was maintained. While QR code was used to ensure that hardcopy certificate was authenticated. In addition, the QR was password protected to prevent people from accessing the details of the QR and reproduce a similar documents.

6.7 Merits of Authentication Prototype

The developed prototype provides efficient and effective way of authenticating certificates. This is attributed to the use of web portal and QR code which enables the user to authenticate both softcopy and hardcopy document. Use of ECDSA makes the prototype more secure and efficient on resources when compared to other algorithms used by authors such as Kamanda.

The prototype also uses free QR scanning application which can be installed in a smartphone, without incurring any cost. This advantage is supported by the fact that smartphones are common devices in the market and are easy to use.

6.8 Demerits of Authentication Prototype

This prototype cannot be used with non-smartphone device. This is because these devices do not support installation of applications hence no room for installation of QR code scanner.

Chapter 7 : Conclusion, Recommendation and Future Work

7.1 Conclusion

Problems and challenges associated with authentication of the Kenya Certificate of Secondary School Education (KCSE) certificates formed the basis for this research. The main aim of this research was to come up with solution to the problem by developing a prototype which can be used by institutions of higher learning, employers and other institutions to determine authenticity of certificate before admitting new students or employees.

The developed prototype provided an acceptable and relevant tool to enable institutions authenticate KCSE certificates. The tool would be more applicable in Universities and colleges to weed out applicants who present forged certificates. The tool can be accessed online as well as offline. This means that institutions and any other interested parties can access the system from anywhere. The system makes use of QR codes facilitated by QR scanning. It can be obtained for free from Google play store. The architecture as well as the test results indicate that the prototype is well secured since document security was the main focus among other requirements. OpenSSL, digital signatures, Passwords and registration were some of the security measures taken to ensure integrated security for both document and the prototype. The prototype is able to protect various forms of document fraud subjected to KCSE certificates in Kenya.

7.2 Recommendation

From the study, it is clear that the problem of enrollment fraud in our institutions is alive and kicking. Since study results indicated that current security feature on certificate are not sufficient, the Kenya National Examination Council should adopt digital authentication system that will help institutions to prevent people from using fake KCSE certificate. Going by the findings from the questionnaire, a digital system would greatly help in authenticating academic documents. The online platform would also be important in reducing the time to get response from KNEC from ten days to a few minutes.

7.3 Further Research

This particular research is not exhaustive of all solutions to the problem of enrollment fraud therefore, the following areas can be looked into by other researchers.

- i. To cater for those who do not have smartphones, a system can be developed to enable them use of USSD technology to authenticate secondary school certificates.
- ii. An intelligent system can be developed to identify salient features on KCSE certificates in order to determine its authenticity.

References

- ACEI. (2013). 5 Common Types of Non-Official and Illegitimate Academic Documents. Retrieved November 15, 2016, from <https://academicexchange.wordpress.com/>
- Adan, E. A. (2002). The Forensics of Academic Credential Fraud Analysis and Detection. NAFSA: Association of International educators. Retrieved from http://www.nafsa.org/uploadedFiles/NAFSA_Home/Resource_Library_Assets/Networks/ACE/forensics_of_academic.pdf
- Byram, S. (2011). Detecting Fraudulent Academic credentials. (pp. 1–10). Presented at the NAFSA REGION III CONFERENCE, Oklahoma City, OK.
- CAPSLE. (2009). “He’s got more degrees than a thermometer.” Degree Mills and Detecting Fraudulent Credentials. Ontario College of Teachers.
- Creswell, J. W. (2009). *Research Design: Qualitative, Quantitative and Mixed Method Approaches*. (3rd ed.). SAGE Publication.
- Dennis, A., Wixom, B., & Tegarden, D. (2012). *System Analysis and Design with UML version 2: An Object Oriented Approach* (4th ed.).
- Eckstein, M. A. (2003). Combating academic fraud towards a culture of integrity. International Institute for Educational Planning. Retrieved from <http://www.unesco.org/iiep>
- Garwe, E. C. (2015). Qualification, Award and Recognition Fraud in Higher Education in Zimbabwe. *Journal of Studies in Education*, 5(2).
- Gu, Y., & Zhang, W. (2011). QR Code Recognition Based on Image Processing. Presented at the International Conference on Information Technology and Technology, Nanjing, Jiangsu China: IEEE.
- Gudo, C., & Olel, M. (2011). Student’s Admission Policies for Quality Assurance: Towards Quality Education in Kenya Universities. *Internal Journal of Business and Social Science*, 2(8).
- Jeong, T. (n.d). Fundamentals of Photonics. Lake forest College.
- Kamanda, I. C. G. (2015). *Prototype for the Authentication of University Certificates: Case of Strathmore University*. Strathmore University.
- KNEC. (2015). KNEC Service Charter.
- Komu, N. (2015). Recruits charged for faking certificates. *Daily Nation*.
- Kothari, C. R. (2004). *Research Methodology: Methods and Techniques*. (Second Revised Edition). New Age International Publisher.
- Kumar, R. (2011). *RESEARCH METHODOLOGY: A Step by step guide for beginners*. (3rd ed.). SAGE Publication.
- Li, C. M., Hu, P., & Lau, W. C. (2015). AuthPaper: Protecting Paper-based Documents and Credentials using Authenticated 2D Barcodes. (pp. 7400–7406). Presented at the Communication and Information Systems Security Symposium, IEEE ICC.

- Lui, Y., & Lui, M. (2006). Automatic Recognition Algorithm of Quick Response Code Based on Embedded System. In *Sith International Conference on Intelligent Systems Design and Application*. IEEE.
- Mehta, A. (2015). QR Code Recognition from Image. *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(12).
- Mualuko, P. N. (2016). *Public Health Services Information Dissemination Platform: Case of Machakos County*. Strathmore University.
- Murthy, S., Murthy, R. M., & Sarma, C. A. (2011). Elliptic Curve based Signature Method to Control Fake Paper based Certificates. In *Proceedings of the World Congress on Engineering and Computer Science 2011* (Vol. Vol 1, pp. 1–3). San Fransisco, USA: WCECS.
- Muthoni, J. M. (2015). *E-Verification: A Case of Academic Testimonials*. University of Nairobi.
- Mwaura, P. (2010). Beware who you employ, some have fake university degrees. *Daily Nation*. Retrieved from <http://www.nation.co.ke/oped/Opinion/Beware-who-you-employ-some--have-fake-university-degrees--/440808-936750-8ysxkz/index.html>
- Nakamura, C. (2010). *The Security Printing Practices of Banknotes*. California Polytechnic State University, San Luis Obispo.
- Nathe, P. (2012). Analysis of Security Printing features accomplished by Sheetfed Lightographic Offset Process and Sheetfed Screen Printing Process., 3, 256–259.
- Nwokefor, N. K. C., & Abraham, I. (2015). Designing an Automatic Web-Based Certificate Verification System for Institutions (Case Study: Michael Okpara University of Agriculture, Omudike). *Journal of Multidisciplinary Engineering Science and Technology*, Vol 2(Issue 12), 3393–3399.
- Ohbuchi, E., Hanaizumi, H., & Ah Hock, L. (2004). Barcode Readers using the Camera Device in Mobile Phones. In *Proceedings of the 2004 International Conference on Cyberworlds (CW04)*. IEEE.
- Ombati, C. (2011). 27 Police recruits arrested over fake certificates. *Standard Digital*. Retrieved from <http://www.standardmedia.co.ke/article/2000041489/27-police-recruits-arrested-over-fake-certifica>
- Pargaru, I., Gherghina, R., & Duca, I. (2009). The Role of Education in the Knowledge-based Society During the Economic Crisis.
- Pesa Times. (2015). Eight BOT employees in trouble over fake form four certificates. *Pesa Times Website*. Retrieved from <http://pesatimes.co.tz/news/crime-and-court/seven-bot-in-trouble-over-fake-form-four-certificates/tanzania>
- Regier, J. (2015). Why is academic success important? SASKATCHEWAN SCHOOL BOARDS ASSOCIATION. Retrieved from <http://saskschoolboards.ca/wp-content/uploads/2015/08/2011SIAST.pdf>
- Rouse, M. (2014). Definition: Digital Signature. *TechTarget*. Retrieved from <http://searchsecurity.techtarget.com/definition/digital-signature>

- Shelly, G., & Rosenblatt, H. (2012). *System Analysis and Design*. (9th ed.). Course Technology. Cengage Learning.
- Waithaka, S. (2013). *Kenya's Academic Verification Process*. Kenyatta Univeristy.
- Warasart, M., & Kuacharaone, P. (2012). Paper-based Document Authentication using Digital Signature and QR Code. In *2012 4TH International Conference on Computer Engineering and Technology (ICCET 2012)*. Bangkok Thailand.

Appendix

Appendix A: Introductory Letter



Strathmore
UNIVERSITY

FACULTY OF INFORMATION TECHNOLOGY

Our Ref.: FIT/MSIT/RL/16/43

14th March, 2017

To whom it may Concern:

Re: Kaibiru Mutua Raphael - 088995

This is to confirm that the above named is a student at Strathmore University pursuing *Master of Science in Information Technology (MSc.IT)* since May 2015.

Raphael is a research scholar who is currently in his 2nd (final year) of study and is doing a research pertaining his masters which is entitled: **Prototype for Authentication of Secondary School Certificates: A case of Universities in Kenya.**

This research being a mandatory requirement towards successful completion of his studies, it would be great if you accord Raphael the necessary support that He may need from your organization to enable him complete this task.

Any assistance accorded him shall be highly appreciated.

In case you would wish to clarify any issues with us, please feel free to do so.

Yours faithfully,

A handwritten signature in black ink, appearing to be 'Brebner Momanyi'.

Brebner Momanyi (Mr.)
Administrator, Faculty of Information Technology
bmomanyi@strathmore.edu

Appendix B: Questionnaire

RESEARCH QUESTIONNAIRE

Prototype for Authentication of Secondary School Certificates: A Case of Universities in Kenya

Confidentiality/Non-disclosure Assurance

I Kaibiru Mutua Raphael am a student at Strathmore University (Student ID: 088995). I am currently conducting a research titled, “**A Prototype for the Authentication of Secondary School Certificates: Case of KCSE Certificates**”. The research aims at developing a prototype which can be used to authenticate Secondary School certificates during enrolment of new students.

The data or information collected in this research will be treated with paramount confidentiality and privacy and it will not be shared without your prior permission.

Research objectives

- i. To identify types of fraud commonly associated with academic documents.
- ii. To identify security features of paper document.
- iii. To review existing systems used to authenticate academic certificates.
- iv. To develop an authentication prototype for secondary school certificate using elliptic Curve Digital Signature Algorithm.
- v. To test the functionality of certificate authentication prototype.

Directions in responding to the questionnaire

Kindly check all boxes that apply in each question.

For questions indicated (**tick one**) please select only one choice. For questions indicated (**tick all that apply**) you may tick as many as you can.

Some questions are marked (**Optional**). This means you have the freedom to answer or not.

Correspondence/Inquiries

Mr. Kaibiru Mutua Raphael (rkaibiru90@gmail.com, rkaibiru@yahoo.com)

Phone No: +254 703 344 967

QUESTIONNAIRE

Section A: General Information

1. Please indicate the number of years you have worked in this department (*Tick only one*)
- Less than a year
 - 1-5 years
 - 6-10 years
 - 11-15 years
 - 16-20 years
 - Over 20 years

Section B: Document Fraud Awareness

2. Have you heard of illegitimate academic document/certificate?
- YES
 - NO

If **yes** tells us what it means to you (Optional)

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

3. Have you heard cases of people using fake certificates to join universities or training institutions?
- YES
 - NO

4. What effect would use of illegitimate academic document have to an institution? (*Tick all that apply*)

- Reputation damage
- Lack of credibility from the society
- Poor quality of education
- Others (**Please list them below**)

.....
.....

5. What type of academic document fraud is commonly applied by fraudsters? (**Tick all that apply**)

- Double use of Certificate (*Two people using one certificate to join university*)
- Altered document (*some information changed in the original document*)
- Fabricated document (*document created to look like an original document*)
- Omission of data (*removing some data from the document*)

6. What feature do you look at to authenticate KCSE certificates (**Tick all that apply**)

- Quality of paper
- Hologram
- Printed patterns on paper
- Watermark
- Security thread
- Other(**List them below**)

.....
.....
Would you say these features are sufficient in preventing document fraud?

- YES
- NO

7. Do you receive request to authenticate KCSE certificate

- YES
- NO

If **yes** how long did it take before you give feedback?

- Less than a week
- 1-2 weeks
- 3-4 weeks

8. What challenges do you face when verifying authenticity of certificates? (**Tick all that apply**)

- Tedious
- Time consuming
- Difficult to tell a genuine and fake certificate

- Difficult authenticating documents from other countries
- Others (**Please list them below**)

.....

.....

Section C: System Information

9. How much do you think adopting an authentication system would help your institution?

(Tick only one)

- Definitely won't (1)
- Probably won't (2)
- Probably will (3)
- Definitely will (4)

10. A security system should meet the following requirements. Kindly tick on each requirement to show how important it is to you.

	Not Important at all	Low important	Moderately important	Important	Very important
Authentication					
Data integrity					
Privacy					
Non-repudiation					

11. A good system must meet users' requirement. Below is a list of considerations when acquiring a good system. Tick on the requirements that you would consider when choosing an authenticating system. **(Tick all that apply)**

- Ease of use
- Record keeping
- Simple interface
- Security
- Reliability
- Functionality

Cost

Others (**Please list them below**)

.....

.....

.....

.....

.....

Thank you for your time and participation

Appendix C: Questionnaire Response Tables

Table C 1: Years worked in Research department

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than a year	3	6.0	6.1	6.1
	1-5 years	8	16.0	16.3	22.4
	6-10 years	10	20.0	20.4	42.9
	11-15 years	12	24.0	24.5	67.3
	16-20 years	13	26.0	26.5	93.9
	Over 20 years	3	6.0	6.1	100.0
	Total	49	98.0	100.0	
Missing	System	1	2.0		
Total		50	100.0		

Table C 2: Heard of Illegitimate Certificates

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	44	88.0	88.0	88.0
	No	6	12.0	12.0	100.0
	Total	50	100.0	100.0	

Table C 3: Heard of People using Fake Certificates

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	46	92.0	92.0	92.0
	No	4	8.0	8.0	100.0
	Total	50	100.0	100.0	

Effects of Illegitimate Academic Document to an Institution

Table C 4: Reputation Damage

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	34	68.0	100.0	100.0
Missing	System	16	32.0		
Total		50	100.0		

Table C 5: Lack of Credibility

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	24	48.0	100.0	100.0
Missing	System	26	52.0		
Total		50	100.0		

Table C 6: Poor Quality

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	41	82.0	100.0	100.0
Missing	System	9	18.0		
Total		50	100.0		

Table C 7: Other Effects

		Frequency	Percent
Missing	System	50	100.0

Q6. Types of Document Fraud Commonly used by Fraudsters

Table C 8: Double use of Certificates

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	19	38.0	100.0	100.0
Missing	System	31	62.0		
Total		50	100.0		

Table C 9: Altered Documents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	34	68.0	100.0	100.0
Missing	System	16	32.0		
Total		50	100.0		

Table C 10: Fabricated Document

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	42	84.0	100.0	100.0
Missing	System	8	16.0		
Total		50	100.0		

Table C 11: Omission of Data

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	17	34.0	100.0	100.0
Missing	System	33	66.0		
Total		50	100.0		

Security Features on Academic Certificates

Table C 12: Quality of Paper

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	34	68.0	100.0	100.0
Missing	System	16	32.0		
Total		50	100.0		

Table C 13: Hologram

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	26	52.0	100.0	100.0
Missing	System	24	48.0		
Total		50	100.0		

Table C 14: Patterns Printed on Paper

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	18	36.0	100.0	100.0
Missing	System	32	64.0		
Total		50	100.0		

Table C 15: Watermark

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	24	48.0	100.0	100.0
Missing	System	26	52.0		
Total		50	100.0		

Table C 16: Security Thread

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	33	66.0	100.0	100.0
Missing	System	17	34.0		
Total		50	100.0		

Table C 17: Other

		Frequency	Percent
Missing	System	50	100.0

Table C 18: Sufficiency of these Features

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	6	12.0	12.5	12.5
	No	42	84.0	87.5	100.0
	Total	48	96.0	100.0	
Missing	System	2	4.0		
Total		50	100.0		

Table C 19: Duration to get Feedback from KNEC

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than a week	1	2.0	6.7	6.7
	1-2 weeks	4	8.0	26.7	33.3
	3-4 weeks	10	20.0	66.7	100.0
	Total	15	30.0	100.0	
Missing	System	35	70.0		
Total		50	100.0		

Table C 20: Tedious

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	30	60.0	100.0	100.0
Missing	System	20	40.0		
Total		50	100.0		

Table C 21: Time Consuming

		Frequency	Percent	Valid Percent	Cumulative Percent

Valid	Yes	30	60.0	100.0	100.0
Missing	System	20	40.0		
Total		50	100.0		

Table C 22: Difficult to tell a genuine and a fake Certificate

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	41	82.0	100.0	100.0
Missing	System	9	18.0		
Total		50	100.0		

Table C 23: Difficult Authenticating Documents from other Countries

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	38	76.0	100.0	100.0
Missing	System	12	24.0		
Total		50	100.0		

Table C 24: Others

		Frequency	Percent
Missing	System	50	100.0

Benefits of Post-secondary Education

Table C 25: Stable Employment

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	17	34.0	100.0	100.0
Missing	System	33	66.0		
Total		50	100.0		

Table C 26: Higher Chances of Employment

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	39	78.0	100.0	100.0
Missing	System	11	22.0		
Total		50	100.0		

Table C 27: Higher Income

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	15	30.0	100.0	100.0
Missing	System	35	70.0		
Total		50	100.0		

Table C 28: General Development of the Society

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	27	54.0	100.0	100.0
Missing	System	23	46.0		
Total		50	100.0		

Table C 29: Others

		Frequency	Percent
Missing	System	50	100.0

Security System Requirements

Table C 30: Authentication

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Low important	2	4.0	4.1	4.1
	Moderately important	9	18.0	18.4	22.4
	Important	12	24.0	24.5	46.9
	Very important	26	52.0	53.1	100.0
Total		49	98.0	100.0	
Missing	System	1	2.0		
Total		50	100.0		

Table C 31: Data Integrity

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Moderately important	5	10.0	10.0	10.0
	Important	24	48.0	48.0	58.0
	Very important	21	42.0	42.0	100.0
Total		50	100.0	100.0	

Table C 32: Privacy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Moderately important	6	12.0	12.2	12.2
	Important	16	32.0	32.7	44.9
	Very important	27	54.0	55.1	100.0
	Total	49	98.0	100.0	
Missing	System	1	2.0		
Total		50	100.0		

Table C 33: Non-repudiation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not important at all	1	2.0	2.0	2.0
	Low important	4	8.0	8.0	10.0
	Moderately important	11	22.0	22.0	32.0
	Important	20	40.0	40.0	72.0
	Very important	14	28.0	28.0	100.0
	Total	50	100.0	100.0	

Table C 34: System User Requirements Frequencies

		Responses		Percent of Cases
		N	Percent	N
User Requirements(a)	Ease of use	39	18.1%	78.0%
	Record keeping	29	13.4%	58.0%
	Simple interface	27	12.5%	54.0%
	Security	36	16.7%	72.0%
	Reliability	37	17.1%	74.0%
	Functionality	25	11.6%	50.0%
	Cost	23	10.6%	46.0%
Total		216	100.0%	432.0%

a Dichotomy group tabulated at value 0.

Appendix D: Sample Code used to Generate QR Code

```
use BaconQrCode;
use BaconQrCode\Writer;
use BaconQrCode\Encoder\Encoder;
use BaconQrCode\Renderer\Color\Rgb;
use BaconQrCode\Renderer\Image\Eps;
use BaconQrCode\Renderer\Image\Png;
use BaconQrCode\Renderer\Image\Svg;
use BaconQrCode\Common\ErrorCorrectionLevel;
use BaconQrCode\Renderer\Image\RendererInterface;use RuntimeException;
use Illuminate\Contracts\Encryption\DecryptException;
use Illuminate\Contracts\Encryption\EncryptException;
use Illuminate\Contracts\Encryption\Encrypter as EncrypterContract;
    class Bacon Qr Code Generator implements QrCodeInterface
{
    protected $writer;
    protected $errorCorrection = ErrorCorrectionLevel::L;
    protected $encoding = Encoder::DEFAULT_BYTE_MODE_ECODING;
    protected $imageMerge = null;
    protected $imagePercentage = .2;
    public function __construct(Writer $writer = null, RendererInterface $format = null)
    {
        $format = $format ?: new Svg();
        $this->writer = $writer ?: new Writer($format);
        namespace Illuminate\Encryption;
        class Encrypter implements EncrypterContract
        {
            * The encryption key.
```

```

protected $key;
    * The algorithm used for encryption.
protected $cipher;
public function __construct($key, $cipher = 'AES-128-CBC')
{
    $key = (string) $key;
    if (static::supported($key, $cipher)) {
        $this->key = $key;
        $this->cipher = $cipher;
    } else {
        throw new RuntimeException('The only supported ciphers are AES-128-CBC and
AES-256-CBC with the correct key lengths. ');
    }
}
    * Determine if the given key and cipher combination is valid.
public static function supported($key, $cipher)
{
    $length = mb_strlen($key, '8bit');
    return ($cipher === 'AES-128-CBC' && $length === 16) ||
        ($cipher === 'AES-256-CBC' && $length === 32);
}
}

Generates a QRCode.
$text The text to be converted into a QRCode
$text= Certificate_Id, Student_Id, Subject_Id, School_Id,
{!! QrCode::size(120)->generate(url('/passcode').'/'. $student->certificate); !!}
return $qrCode;
    } else { file_put_contents($filename, $qrCode);
    }
}
    * Merges an image with the center of the QRCode.
Return this
}

```

Appendix E: Sample Code for Generating Validation Code

<?php

```
use Illuminate\Support\Facades\Schema;  
use Illuminate\Database\Schema\Blueprint;  
use Illuminate\Database\Migrations\Migration;
```

```
class PassCode extends Migration
```

```
{
```

```
public function up() {
```

```
Schema::create('pass_codes', function (Blueprint $table) {
```

```
    $table->engine = 'InnoDB';
```

```
    $table->charset = 'utf8';
```

```
    $table->collation = 'utf8_unicode_ci';
```

```
    $table->increments('id');
```

```
    $table->string('passcode');
```

```
    $table->uuid('certificate_id');
```

```
    $table->softDeletes();
```

```
    $table->timestamp('created_at')->default(DB::raw('CURRENT_TIMESTAMP'));
```

```
    $table->timestamp('updated_at')->nullable();
```

```
    $table->foreign('certificate_id')->references('certificate')->on('students')->  
onUpdate('cascade')->onDelete('cascade');
```

```
});
```

```
}
```

Appendix F: Turnitin Report

THESIS REPORT

ORIGINALITY REPORT

20%

SIMILARITY INDEX

13%

INTERNET SOURCES

3%

PUBLICATIONS

16%

STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

7%

★ Submitted to Strathmore University

Student Paper

EXCLUDE QUOTES OFF

EXCLUDE MATCHES OFF

EXCLUDE
BIBLIOGRAPHY OFF