INTERNATIONAL JOURNAL OF
INNOVATIVE RESEARCH AND KNOWLEDGE
ISSN-2213-1356 www.ijirk.com

A Prototype for Authentication of Secondary School Certificates: A Case of Kenya Certificate of Secondary Education

Kaibiru Mutua Raphael
Strathmore University, Kenya.

Dr. Bernard Shibwabo
Strathmore University, Kenya.

Abstract

The demand for educated labor force has increased in developing countries like Kenya. Owing to this fact, more often Universities and training colleges in Kenya enroll students who want to further their education. Meeting the minimum entry requirements is key for one to get admitted into an institution of higher learning. However, the use of illegitimate secondary school certificates to join Universities in Kenya has been reported in political and business sectors. Perpetrators of this academic crime have succeeded to an extent of enjoying benefits of higher education, despite there being measures to authenticate secondary school certificates. The aim of this study was to develop a prototype that can be used by institutions of higher learning to authenticate secondary school certificates using QR-Code and digital signatures. Agile software development methodology was adopted to develop the prototype which included; requirements gathering, architecture and design, development and testing. This study targeted the Kenya National Examination Council, research department for data collection. Ten respondents were purposively selected in this department. Questionnaire was used as the main data collection tool for both qualitative and quantitative data. The findings indicated that 87% of respondents said that the current security features on the certificates were not sufficient to prevent document fraud. In addition, 98% said that a computer based system would help in detecting illegitimate certificates. During prototype testing 78% agreed that a computer system was leveraging on the existing methods of authentication. The study recommended the adoption of a computer system by the Kenya National Examination Council to help

Universities and Colleges verify and authenticate secondary school certificates before enrollment of new students.

Keywords: *Certificate, Authentication, QR-Code, QR-Code Scanner and Digital Signature*

Introduction

Very often universities and colleges in Kenya 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, the Kenya Certificate of Secondary School Education (KCSE) 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.

Success of using illegitimate academic 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).

Despite the rigorous exercise of authenticating academic certificate, cases of using fake KCSE documents have 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.

Research Problem

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 academic 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 QR-Code and 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.

Purpose of the Study

The main objective of the study was to develop a prototype using QR-Code and Digital signatures to authenticate secondary school certificates during enrollment of new students in Universities and colleges in Kenya.

Study 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 is useful to academicians and future researchers by contributing to the existing body of knowledge.

Literature Review

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 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.

Types of Fraudulent Documents

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.

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.

Security Features on KCSE Certificates in Kenya

Paper based security has been in use for a very long time. In the case of secondary school certificates in Kenya the following security features are used.

1. Watermark

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 Kenya National Examination Council (KNEC) on KCSE certificates, it is indicated that these certificates are made of special paper which are watermarked with KNECs logo.

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 to secure Secondary school certificates in Kenya.

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 this important document.

4. Printed Security Patterns

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 method 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.

Technologies for Protecting Documents

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. Figure 1, shows the process of signing and verification of a digital signature.

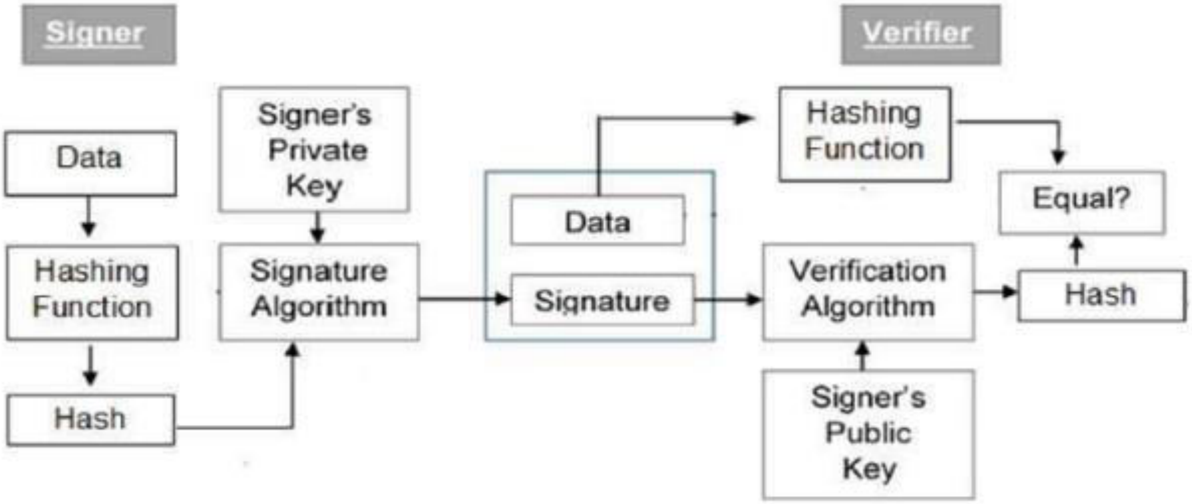


Figure 1: Digital Signature Process (Adopted from Li et al (2015))

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.

Quick Response Code (QR-Code)

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 that enables scanning the QR-Code by use of scanning tools. Figure 2 shows an example of a QR-code.

Figure 2: Example of QR-Code (Adopted from Lau et al., (2015))

Existing Document Authentication Systems

Web-based Certificate Authentication Systems

The problem of illegitimate academic documents has attracted attention from other scholars, who developed web based solutions to the problem. Three scholars developed web-based prototypes to facilitate verification and authentication of academic credentials (Kamanda, 2015; Muthoni, 2015; Nwokeafor & Abraham, 2015). In their work, Muthoni (2015) and Nwokeafor 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; Nwokeafor and Abraham, 2015). Figures 3 and Figure 4 presents prototypes by Muthoni (2015) and Nwokeafor and Abraham (2015) respectively.

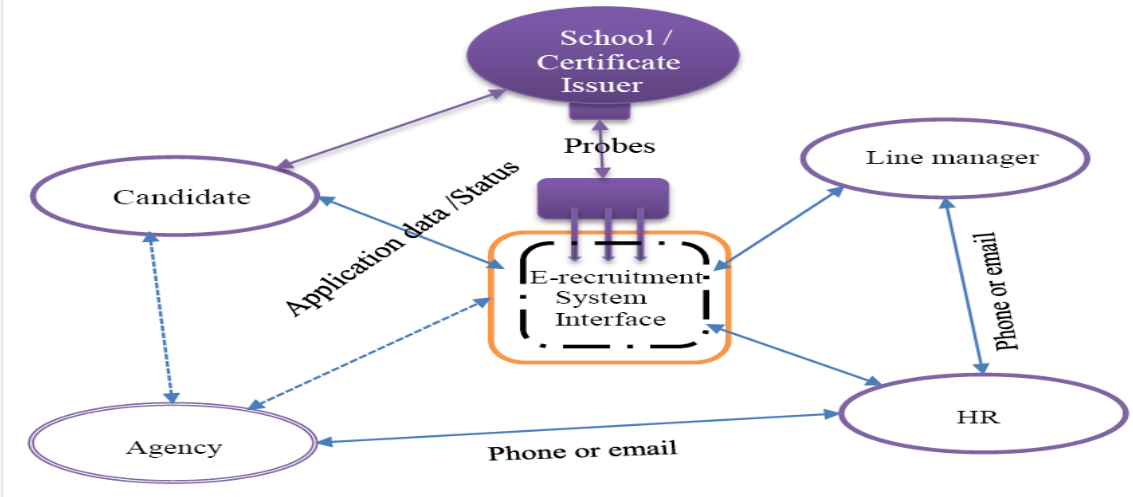


Figure 3: E-Verification Conceptual Model (Adopted from Muthoni, 2015)

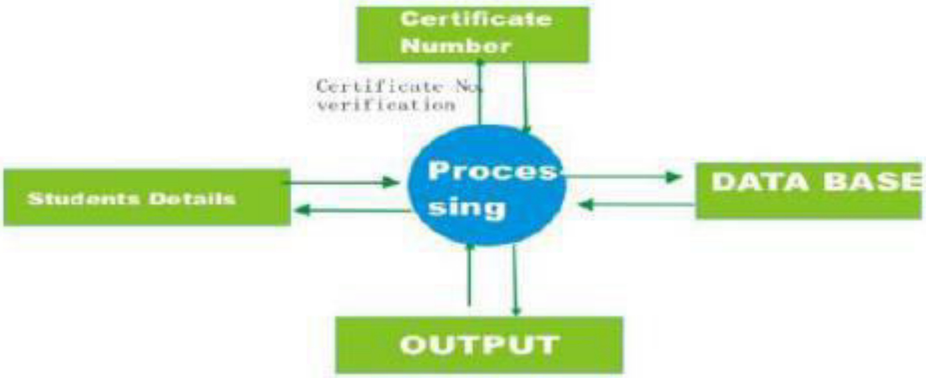


Figure 4: Automatic Verification Web System (Adopted from Nwokeafor & Abraham, 2015)

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. 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 5 presents conceptual framework used to develop the system by Kamanda (2015).

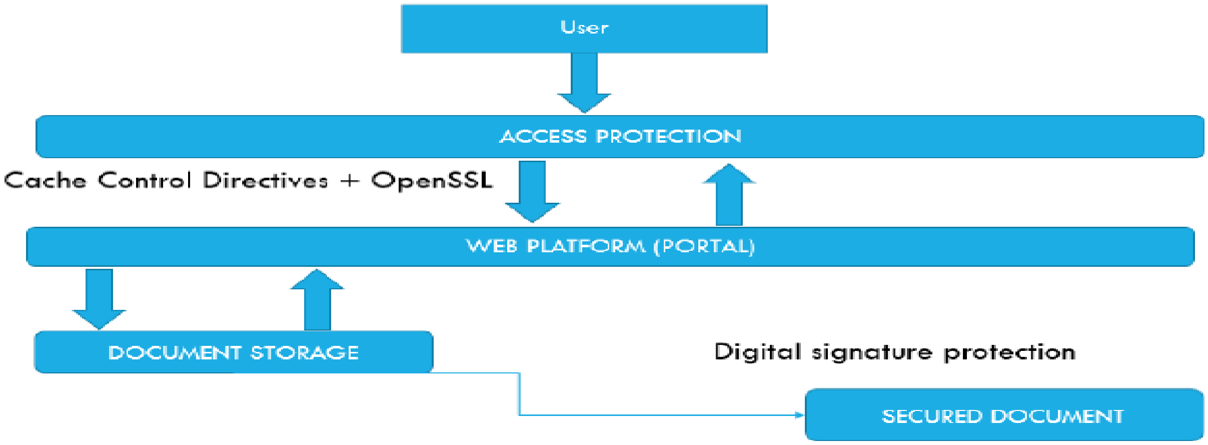


Figure 5: Digital Authentication System (Adopted from Kamanda, 2015)

Proposed Authentication System

The prototype will be web based while using digital signature and QR-code to secure the generated certificate. The prototype will also make use 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. Figure 6 shows the conceptual model for Authentication of Secondary Certificates.

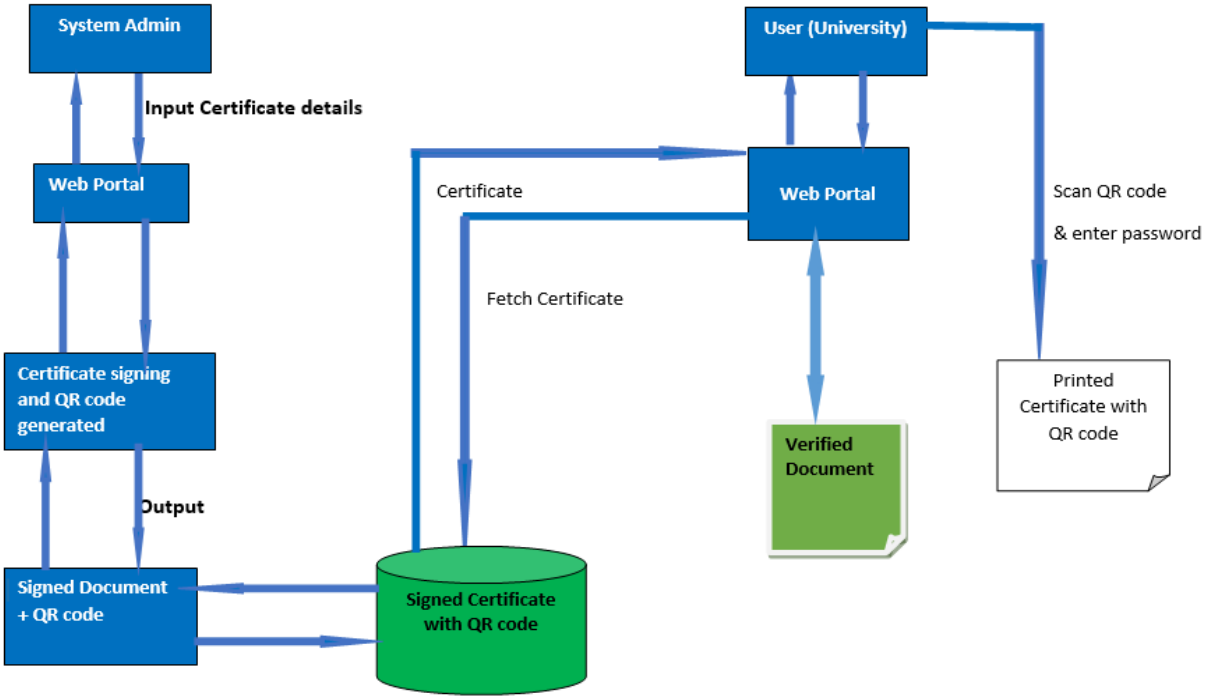

System Admin
Input Certificate details
Web Portal
Certificate signing and QR code generated
Output
Signed Document + QR code
Signed Certificate with QR code
Certificate
Fetch Certificate
User (University)
Web Portal
Verified Document
Scan QR code
& enter password
Printed Certificate with QR code

Figure 6: Proposed Authentication Prototype

Software Development Methodology

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 allow release schedule and user feedback opportunities this allows faster and more controlled improvements (CPrime, 2014).

System Requirements

The research sought to identify security requirements as needed by the users. These requirements included authentication, data integrity, privacy and non-repudiation. In response, 52% said authentication was very important, 48% said data integrity was important, 54% of respondents said privacy was very important and 40% said non-repudiation was important. This shows that most respondents wanted a system that can meet these securities. Users were also catered for by establishing user centered requirements as far as the prototype was concerned. Respondents said that ease of use, reliability and security which got 78%, 74% and 72% respectively was important in system. Other factors considered important by respondents are record keeping 58%, simple interface 54%, functionality 50% and cost 40%. The researcher worked hard to develop a prototype meeting these requirements.

Requirements Analysis

System analysis was classified into two categories; functional requirements and non-function requirements. **Functional requirements** are functions, processes and capabilities which a system has to perform if it is implemented. In this particular prototype functional requirements included management of the system by an administrator, verification and authentication of certificates-the user of the system would be able to register and later be able to verify the authenticity of the certificate by scanning the QR-Code. If the details on the certificate did not match with what was in the database, then the document was rendered invalid and illegitimate. **Non-functional requirements** are qualities that a system can do without but are required to make the system interactive, user friendly and easy to use. Security, ease of use, reliability, system availability were some of non-functional requirements implemented in this prototype.

Use Case Diagram

The proposed prototype had two actors; the system user (a university, college or business entity), and the system administrator. Figure 7 below shows a combined use case diagram for the proposed prototype.

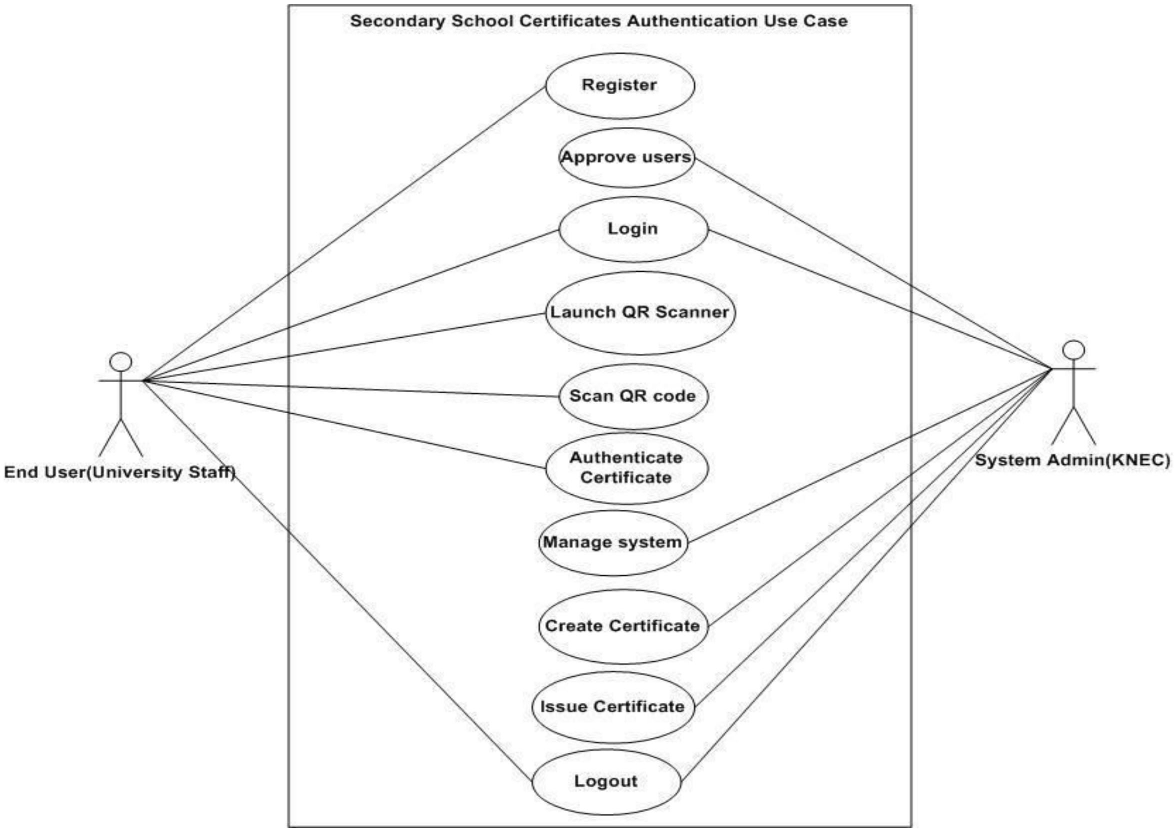


Figure 7: Use Case Diagram

Use Case Scenario

Following is use case scenario narrative for the authenticating the certificate when a candidate presents it to the university during admission.

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.

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 8 shows the ERD of the proposed prototype.

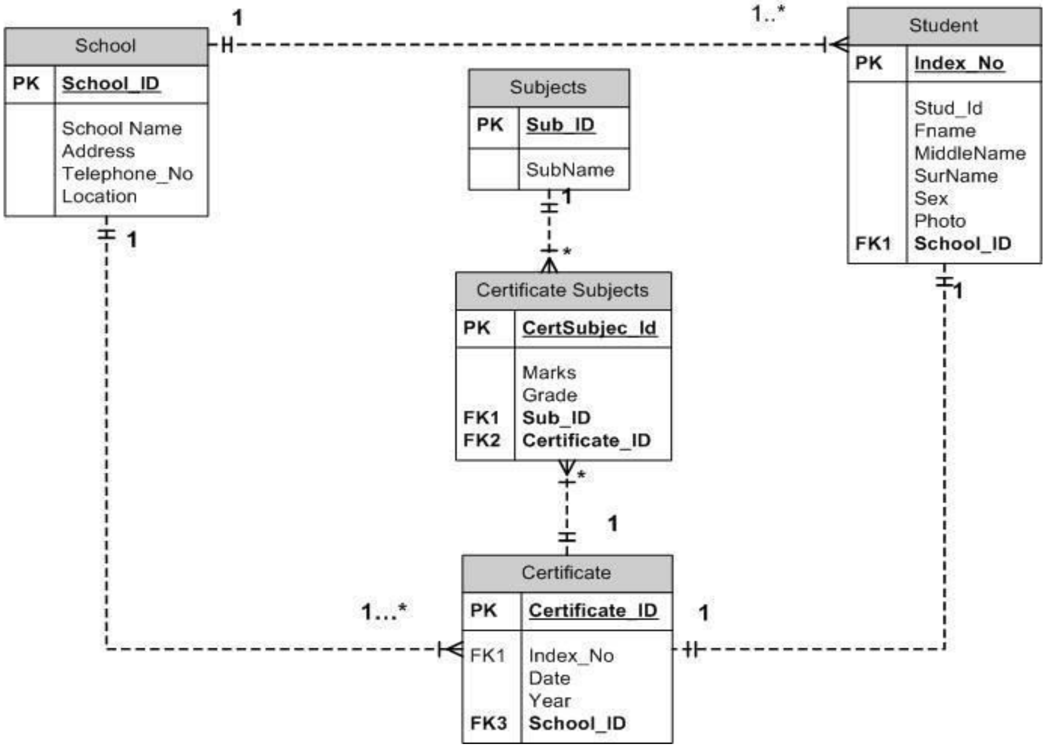


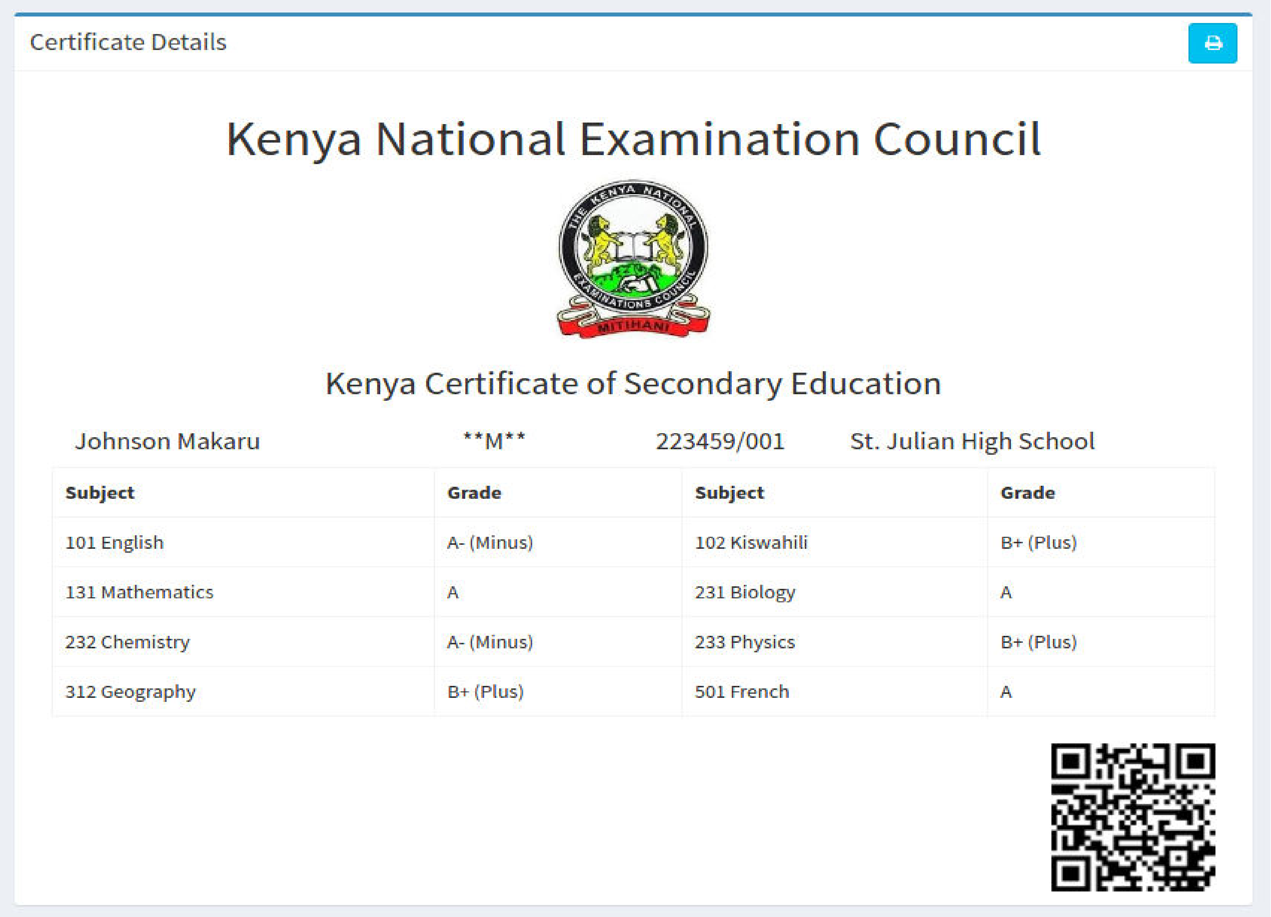
Figure 8: Entity Relationship Diagram

System Implementation

The prototype comprised 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 built on Laravel framework and 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 to scan the QR code, barcode reader algorithm using camera device in mobile phone was used. This algorithm is embedded within the Bacon QR code generator library.

Creation and Printing of Certificate

Upon completing school student's details which include names, subjects, grades, school, index number, and gender are used to create the certificate by the system administrator. During creation of the certificate these details are encoded into a QR-Code which is appended on the certificate for printing and later issued to the student. Figure 9 shows a sample certificate that was used to test the prototype.



Kenya National Examination Council

Kenya Certificate of Secondary Education

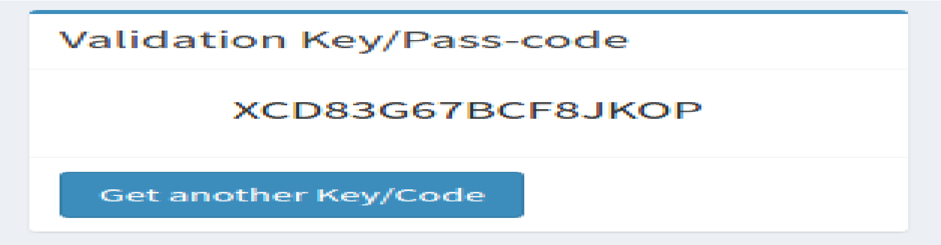
Johnson Makaru **M** 223459/001 St. Julian High School

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 9: Sample Certificate Created by System Administrator

Authentication of the Certificate

The printed certificate will be authenticated upon submission to the university during admission of the holder of this certificate. The system user having successfully registered into the system will login the system, scan the QR-code on the certificate, and enter the validation key generated on the phone for that particular certificate on the portal. If the generated code for that QR-code is valid then the certificate will open on the system with all details about the student appearing for verification, otherwise, the system will not recognize the QR-code validation key hence an invalid certificate. Figure 10 and figure 11 shows the validation Code and authenticated certificate for this process.

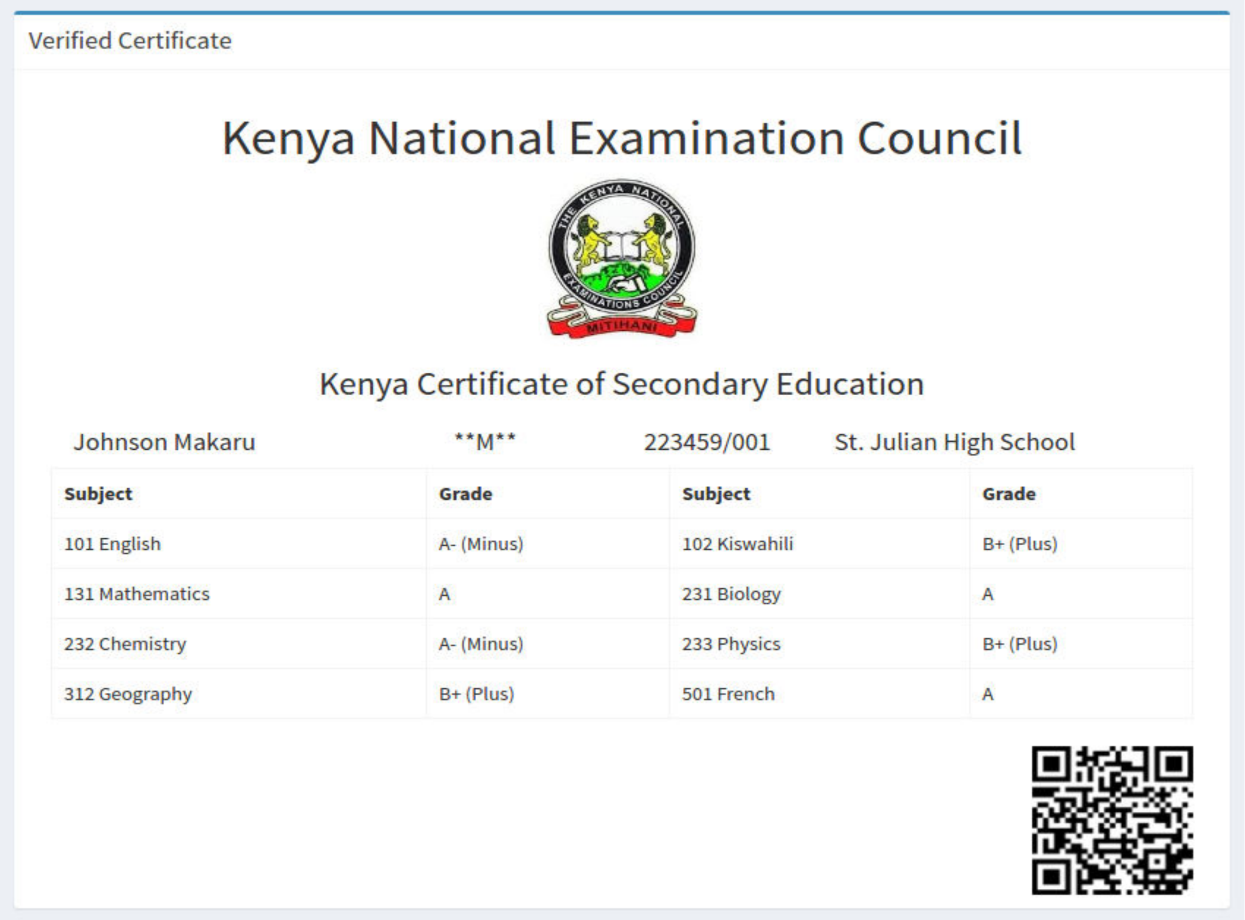


Validation Key/Pass-code

XCD83G67BCF8JKOP

Figure 10: QR-Code Validation Key

This code is the one used to validate the QR code on the scanned certificate. If the QR code was not generated from the genuine examination body then the certificate will not open on the portal.



Verified Certificate

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 11: Authenticated Certificate

The above figure shows a similar certificate that was created and issued to the student with the details as they had been printed without any alteration. This is to mean that the certificate was genuine and authentic, belonging to the authorized student.

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.

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 were not sufficient, the Universities and training colleges should adopt the proposed digital authentication system which would help institutions to prevent people from using fake KCSE certificate.

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.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.

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).

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.

Komu, N. (2015). Recruits charged for faking certificates. Daily Nation.

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.

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.

Nwokeafor, 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.

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.

Waithaka, S. (2013). Kenya’s Academic Verification Process. Kenyatta University.

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). Bankok Thailand.